Public Safety Answering Point (PSAP) Credentialing Agency (PCA) Certification Practice Statement

V1.1

2/22/2023

NG9-1-1 Interoperability Oversight Commission (NIOC)

https://ng911ioc.org

Document Revision History

This document was approved for publication on February 22, 2023 by the NG9-1-1 Interoperability Oversight Commission (NIOC). The following revisions have been made to the original document:

Revision	Date	Remarks
V1.0	2022-06-06	Initial version of the CPS; drafted from the Certificate Policy v1.0.1 and corresponds with initial v1.1 draft of the Certificate Policy, which was modified in parallel with the creation of this version of the CPS.
V1.1	2023-02-22	This update corresponds with additional edits made to the draft version of the v1.1 Certificate Policy before its publication. This published CPS fully corresponds with the published Certificate Policy v1.1. To reflect similar changes in the Certificate Policy v1.1, "Root CA" has been changed to "PCA" in the entire document except in a few limited circumstances.

TABLE OF CONTENTS

TABLE OF TABLES

TABLE OF FIGURES

Foreword

Background

Certification Authorities (CAs), and the infrastructure they support, form the basis for one of the primary mechanisms for providing assurance of identity. The widely placed trust in CAs is at the heart of security mechanisms used to protect sessions and transactions for Next Generation 9-1-1 (NG9-1-1). National Emergency Number Association's (NENA's) i3 and associated standards require Transport Layer Security (TLS) throughout the ecosystem to allow for secure communications and a single shared root of trust to assist with interoperability. TLS relies on CAs to identify Servers and Clients. The root of trust in the NG9-1-1 Public Key Infrastructure (PKI) is the Public Safety Answering Point (PSAP) Credentialing Agency (PCA).

The purpose of this document is to provide security requirements needed to support the secure issuance of Certificates[1] in NG9-1-1 by the PCA CAs in the NG9-1-1 PKI. In particular, this document has been developed to provide an appropriate level of assurance to support government emergency services including public safety, and applications, i.e., a high level of assurance as defined in the [Validation Policy (VP)]. The level of assurance refers to the strength of the Binding between the Public Key and the entity whose name is cited in the Certificate, the policies used to control the use of the corresponding Private Key, and the overall security provided by the PKI itself.

The PCA is a functional element in the NENA i3 Standard for Next Generation 9-1-1 core services[2] which establishes a root of trust for the NG9-1-1 ecosystem to facilitate interoperable security between disparate NG9-1-1 environments. The i3 standard includes not only a shared root of trust to build a PKI, but it also standardizes how identities are conveyed across NG9-1-1, and what roles those identities have in the NG9-1-1 ecosystem. In addition to participating within a PKI in a trusted environment, the standardization of conveying identities and roles provides for powerful abilities to manage permissions and other security configurations in NG9-1-1 that work across different NG9-1-1 environments and disparate public safety systems. The PCA as set forth in this document supports all of the functionality as required by the i3 standard to provide a PCA.

Certificate Policy

This baseline set of requirements has been written in the form of a "Certificate Policy." The International Telecommunication Union (ITU) Recommendation X.509, defines a

[1] **Capitalized words in this document are defined terms in the glossary - Appendix B – Glossary**

.

[2] See NENA STA-010.3-2020. Available at https://www.nena.org/page/Standards.

“Certificate Policy” as “a named set of rules that indicates the applicability of a Certificate to a particular community and/or class of application with common security requirements.” That is, a Certificate Policy (CP) defines the expectations and requirements of the PKI Participants (e.g., Subscribers, Relying Parties, etc.) that will trust the Certificates issued by its CAs. This document is also written to fulfill requirements set forth in i3, fulfilling the PSAP Credential Agency (PCA) functional element.

The governance structure that represents the PKI Participants is known as the Policy Authority (PA). The NG9-1-1 Interoperability Oversight Commission (NIOC) created by NENA is the PA for the PCA. The PA is responsible for identifying the appropriate set of requirements for a given community and oversees the CAs that issue Certificates for that community. This CP is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) Certificate Policy and Certification Practices Framework [RFC 3647]. The United States Government’s Federal PKI Common Policy (FPKI Common Policy) [FPKIPA] was used as a base document for this CP. The FPKI Common Policy is widely recognized for clearly articulating the requirements for Certificate issuance for the Certificates, which are primarily used by government entities to Authenticate to government systems.

1. Introduction

The traditional analog voice-centric 9-1-1 system is no longer able to support many of the common communication methods in use today. NENA and other standards bodies have developed a NG9-1-1 system that modernizes emergency calling systems by allowing multiple forms of multimedia communications, native location handling, and enhanced routing mechanisms. To enable secure communication between Relying Parties, a PSAP Credentialing Agency (PCA) PKI has been created. This CP sets the requirements for the use of PKI Certificates for NG9-1-1 and follows the technical requirements set forth in the NENA i3 Standard for NG9-1-1 [NENA i3].

1.1 Overview

A Certification Authority (CA) is a collection of hardware, software, personnel, and operating procedures that issue and manage Public Key Certificates, also known as digital Certificates. The Certificate binds the Certificate holder's (also known as the Subscriber) Public Key to a set of named Subject attributes identifying the Subscriber. This allows Relying Parties to Authenticate and trust signatures or assertions made by the Subject contained in the Certificate.

A fundamental element of modern secure communications is establishing trust in Public Keys via Public Key Certificates. This begins with a Relying Party obtaining an entity's Public Key Certificate that is issued by a trusted entity (e.g., a Trust Anchor) certifying that the Public Key belongs to that entity as the Subscriber of the Certificate. Entities that are not trusted directly MAY become trusted through successive validation of their Subscriber Certificate through a hierarchical chain of CA Certificates from the Subscriber's Certificate to a Trust Anchor (typically a Root CA (hereafter the PCA) Public Key). Trust Anchors are an authoritative entity for which trust is assumed and not derived and thus are explicitly trusted by Relying Parties. Relying Parties SHALL be responsible for securely obtaining Trust Anchors (e.g., the PCA Public Key) and for securely managing their Trust Anchor store (e.g., a database containing a set of CAs used as Trust Anchors). Relying Parties must configure Trust Anchors in their Trust Anchor stores with great caution and must give full consideration to the requirements of this CP and NENA i3.

A Certificate issued in accordance with this CP conveys within the NG9-1-1 community a level of digital identity proofing associated with the Subject of the Certificate and membership within the NG9-1-1 PKI. Certificates within the NG9-1-1 PKI communicate three important things within the NG9-1-1 ecosystem to allow for security and interoperability: an entity's agency, and entity's identity and the entity's role within NG9-1-1 (for example, as a first responder with a specific role, a calltaker or as a functional element within NG9-1-1 core services). These values are included in the Certificate Subject Alternative Name (SAN).[3]

[3] See NENA STA-010.3-2020 at Section 6: Security.

Other important documents supporting this CP in the PCA PKI include the CA Certification Practice Statement(s) (CPSs) and Subscriber agreements.

The PCA PKI shown in Figure 1 is comprised of a mandatory offline PCA at tier 1, an Intermediate CA (ICA) at tier 2, and End-Entity Certificates at the bottom tier. Branches of the PKI may include several more tiers per section 7.1.2.6 of this CP.

Note: Tier 2 can be expanded to add multiple optional ICA Tiers below it, by approval of the NIOC, to support current and future use cases for the PCA, as the need for digital Certificates evolves in the deployment of the PKI. Current use cases involve creating generic hosted ICAs so that any integrator can receive their device Certificates directly from the hosted ICA, or to create ICAs dedicated to a specific integrator to meet their Certificate issuance requirements. Tier 2 is also where ICA cross-certification can take place and also where resigning of third party ICAs with the PCA can occur, as long as the third party ICAs are compliant with this CP and its cross-certification requirements. For future use cases, the PKI could add ICAs for issuance of user agent Authentication Certificates. The PKI is designed to be flexible to meet the varying needs of the NG9-1-1 community.

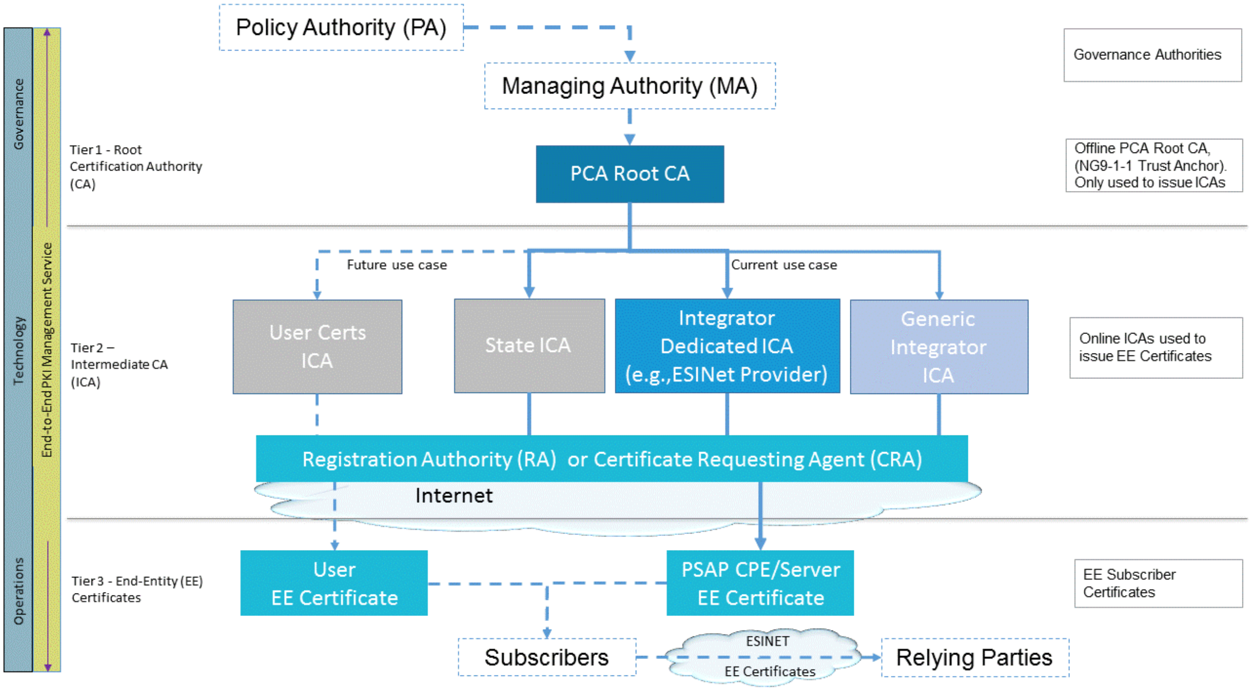
Governance
Technology
Operations
End-to-End PKI Management Service
Policy Authority (PA)
Managing Authority (MA)
Governance Authorities
Tier 1 - Root Certification Authority (CA)
PCA Root CA
Offline PCA Root CA, (NG9-1-1 Trust Anchor). Only used to issue ICAs
Future use case
Current use case
Tier 2 – Intermediate CA (ICA)
User Certs ICA
State ICA
Integrator Dedicated ICA (e.g.,ESINet Provider)
Generic Integrator ICA
Online ICAs used to issue EE Certificates
Registration Authority (RA) or Certificate Requesting Agent (CRA)
Internet
Tier 3 - End-Entity (EE) Certificates
User EE Certificate
PSAP CPE/Server EE Certificate
EE Subscriber Certificates
Subscribers
ESINET
EE Certificates
Relying Parties

Figure 1: PCA PKI Architecture

Throughout this CP, the words that are used to define the significance of particular requirements are capitalized. These words are defined in [RFC 2119].

These words are:

"MUST"	This word, or the terms "REQUIRED" OR "SHALL", means that the definition is an absolute requirement of the specification.

"MUST NOT"	This phrase, or the phrase "SHALL NOT", means that the definition is an absolute prohibition of the specification.
"SHOULD"	This word, or the adjective "RECOMMENDED", means that there MAY exist valid reasons in particular circumstances to ignore a particular item, but the full implications MUST be understood and carefully weighed before choosing a different course.
"SHOULD NOT"	This phrase, or the phrase "NOT RECOMMENDED", means that there MAY exist valid reasons in particular circumstances when the particular 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, or the adjective "OPTIONAL", means that an item is truly optional. One Subscriber MAY choose to include the item because a particular marketplace requires it, or because the Subscriber enhances the product, while another Subscriber MAY omit the same item.

This CP uses tables in Section 6: Technical Security Controls, and Section 7: Certificate, CRL, and OCSP Profiles. In order to make these tables easier to follow, they are color coded as follows:

🟦	General tables (applying to this CP or to all Certificates)
🟦	PCA
🟪	ICAs
🟨	All CAs
🟥	End-Entity Certificates
🟩	Certificate Status Server (OCSP and CRL)

CA, RA, PA, MA, and Agency Representative responses are in italics and are color-coded as follows:

🟩	Certification Authority (CA)
🟪	Registration Authority (RA)
🟦	Policy Authority (PA) / Management Authority (MA) / Agency Representative

1.2 Document Name and Identification

1.2.1 Certificate Policy Name

This document is the PCA PKI Certificate Policy and has been approved for publication by the NIOC.

1.2.2 Object Identifier (OID)

Certificates issued by the PCA under this CP SHALL contain the PCA Object Identifier (OID), 1.3.6.1.4.1.55670.1. The OID SHALL be available to Relying Parties in each Certificate via the *certificatePolicies* extension.

NENA is requested to establish a Registry in the NENA Registry system (NRS) to maintain child OIDs under the PCA OID. The name of this sub-registry is “PCA Sub-registry”. A new entry to the PCA Sub-registry SHALL be approved by NIOC in a written policy made available at https://ng911ioc.org. This policy SHALL include an explanation of when the child OID will be used, and how its use distinguishes it from other child OIDs.

This registry SHALL include the following initial values:

Value	Purpose	Reference
1.3.6.1.4.1.55670.1.1	Quad for valid OtherName values for SubjectAlternativeName extension required in all NG9-1-1 PKI certificates.	This document.

PCA PA Response: Will comply.

1.3 PKI Participants

This section identifies PCA PKI Participants that are relevant to the administration and operation of the PKI under this CP, including the:

- PCA Policy Authority - NIOC;
- ICA Policy Authority – Tier 2 (or lower) ICA operator Policy Authority (PA) approved by NIOC;
- Management Authority – NENA, delegated to Eonti;
- Certification Authority – DigiCert for the PCA;
- Registration Authority – Eonti for the PCA;
- Subscribers – PCA PKI Certificate holders (inclusive of both ICAs and entity Certificate holders), for example, agencies, elements, services, and agents;
- Relying Parties – NG9-1-1 community and;
- Agency Representatives – See the VP.

1.3.1 Policy Authority (PA)

NENA, at the direction of its standards development community, including the NENA Development Steering Council, 9-1-1 Core Services Committee, and the NENA Executive Board, has established the NIOC, according to the bylaws of the NIOC.

The NIOC is the PA for the PCA PKI.

The PA is the owner of the PCA PKI and is responsible for setting up and approving policies and practices governing the PKI.

Responsibilities of the PA include:

- Establishing and approving this CP;
- Governing the PKI according to this CP;
- Approving the establishment of trust relationships with external PKIs;

- Approving the CPS for CAs that issue Certificates under this CP;
- Approving the Audits for CAs operating under this CP;
- Approving any revisions to this CP, and;
- Performing MA activities listed below in the absence of a MA.

ICAs MAY employ an ICA PA to institute additional policies that apply to their ICA and any Certificates issued by that ICA, such as changes to the CPS for that ICA. The CPS for an ICA that has a PA SHALL describe the authority, responsibilities and powers of that PA. Any policies adopted by the ICA PA SHALL conform with the CP. ICA PA polices MAY be more stringent than the CP, but SHALL NOT be less stringent than the CP. Unless stated otherwise, "PA" in the CP means NIOC.

1.3.2 Management Authority (MA)

The PA oversees the MA to provide trust management services to support the NG9-1-1 ecosystem in meeting its security goals in using the PCA PKI. The PA MAY perform the MA duties itself or designate a trusted third party to act as the MA on its behalf to provide operational support and maintain the PKI in accordance with this CP. The PA has designated NENA to be the MA for the PCA PKI. While NENA retains overall responsibility for the PCA to ensure the responsibilities of the MA are fulfilled, day-to-day function of the MA is delegated to Eonti Inc. (Eonti). For any ICA (i.e., hosted or discrete), the MA is designated in the CPS for the ICA.

The MA's primary focus is to ensure that policies for secure physical and logical Access, data sharing, and communications across the ecosystem are realized through the execution and management of the CP requirements and its participants. The MA is responsible for the following:

- The Process for CAs to submit CPSs;
- Approval of the process for recognizing Prospective Subscribers, their authorized representatives, and their agreements;
- Ensuring continued conformance of each CA that issues Certificates under this CP with applicable requirements as a condition for allowing continued participation;
- Approval of the process for Revocation requests;
- Approval of the process for Audits, and;
- Approval of the process to approve Subscriber authorizations.

1.3.3 Certification Authority (CA)

The CA is the collection of hardware, software and operating personnel that create, sign, and issue Public Key Certificates to Subscribers. Within this CP, the acronym "CA or CAs" includes the Root and ICAs. If a requirement only applies to the PCA, it will denote PCA. If it only applies to ICAs hosted by DigiCert, it will denote Hosted ICA. If it only applies to ICAs operated by the Subscriber or a third party on behalf of the Subscriber, it will be denoted as a Discrete ICA.

The CA is responsible for:

- Approving the issuance of all Certificates it issues, including those issued to next tier ICAs;
- Revoking Certificates;
- Providing the PA, MA, and RA with CA Certificates it has issued;
- Generating, protecting, operating, and destroying its CA Private Keys;
- Establishing and maintaining its CPS;
- Certificate Status Servers (CSS) including Online Certificate Status Protocol (OCSP) responder and Certificate Revocation List (CRL) generation and distribution;
- Repository management of Certificate related items;
- Managing all aspects of the CA services, operations and infrastructure related to Certificates (e.g., security Audit, configuration management, and Archive);
- Onboarding Prospective Subscribers to the Certificate issuance process, and;
- Securing delivery of Certificates to its Subscriber.

DigiCert, Inc. (DigiCert) operates the PCA and any hosted ICAs under contract to NENA, at the direction of NIOC. Stand-alone ICAs MAY be hosted by the Subscriber or by a third party on behalf of the Subscriber with a signed ICA Certificate from the PCA or the appropriate upper-level ICA. The first tier must be approved by NIOC. All other ICAs in the NG9-1-1 PKI must also conform with this CP and develop a CPS approved by the appropriate PA for that CA, regardless of operator.

1.3.4 Registration Authority (RA)

The RA is an authority that performs Certificate management functions on behalf the CA, such as collection and verification of a Prospective Subscriber’s identity and information that is to be entered into the Subscriber’s Public Key Certificate. The RA performs its function in accordance with this CP, as well as any additional relevant policies and procedures included in the CA’s CPS. Eonti is the RA for the Hosted ICAs. Discrete ICAs MAY employ an RA to assist the CA in its Certificate management functions. In this document, if a requirement only applies to the CA, it will denote CA. If it applies to the RA on behalf of the CA, it will denote RA.

The RA is responsible for:

- Control over the account registration process;
- Verifying the identity of the Prospective Subscriber for their respective ICA;
- Onboarding Prospective Subscribers to the Certificate issuance process, converting them to a Subscriber;
- Requesting Certificates on behalf of the Subscriber, and;
- Delivery of End-Entity Certificates to the Subscriber.

1.3.5 Subscribers

A Subscriber is the entity whose name appears as the Subject in an End-Entity Certificate (also known as a Subscriber Certificate), who agrees to use its Private Key and Certificate in accordance with the Certificate Policy asserted in the Certificate, and that does not itself issue Certificates.

Subscribers are responsible for:

- Executing the applicable Subscriber agreement (i.e., the Digital Certificate Subscriber Agreement (DCSA));
- Completing the requested Certificate Application information;
- Responding to verification requests in a timely manner;
- Generating the asymmetric Key Pair and protecting their Private Key;
- Delivering the Public Key of the Key Pair to the RA as part of their Certificate request, and;
- Using the Certificate and corresponding Private Key in compliance with this CP.

CAs are sometimes technically considered "Subscribers" in a PKI. However, the term "Subscriber" as used in this document refers only to those who request Certificates for uses other than signing and issuing Certificates or Certificate status information.

1.3.6 Relying Parties

A Relying Party is an entity that relies on the validity of the Binding of the Subscriber's name to a Public Key. The Relying Party uses a Subscriber's Certificate to verify or establish the identity and status of the Subscriber. A Relying Party is responsible for deciding whether or how to check the validity of the Certificate by checking the appropriate Certificate status information. A Relying Party MAY use information in the Certificate to determine the suitability of the Certificate for a particular use.

1.3.7 Other Participants

The PCA PKI MAY require the services of other security, community, and application authorities. If required, the appropriate PA SHALL identify the parties, define the services, and designate the mechanisms used to support these services.

PCA PA Response: Will comply.

1.3.7.1 *ICA Policy Authority*

An ICA must have a corresponding PA, which is referred to as an ICA PA. The NIOC is the PA for an ICA that does not have its own PA.

1.3.7.2 *Agency*

An Agency is a Public Safety Entity[4] that is eligible to hold an Agency Certificate.[5] The PCA's RA MUST authenticate the Agency according to the VP. The Agency MAY then designate an Agency Representative to act on its behalf, to authorize PKI Sponsors or for other purposes outlined in future versions of this CP.

[4] See VP section 3.7.

[5] See VP section 3.2.

RA Response: The RA will validate all identities, including organizations (agencies), devices and agents according to the requirements contained within the NIOC PSAP Credentialing Agency (PCA) Certificate Validation Guidelines (Validation Policy).

1.3.7.3 *Agency Representative*

An Agency Representative is a Legal Agent[6] for an Agency.

1.3.7.4 *PKI Sponsor*

A PKI Sponsor is an individual who is to be explicitly responsible for managing access to the private key associated with a device certificate when the Subscriber is a device. The Agency or its Agency Representative SHALL authorize the PKI Sponsor and MAY provide identifying information for the device during the Certificate request for the device.

Agency Representative Response: The Agency Representative will authenticate itself to the RA and provide a signed request and contact information of the designated PKI Sponsor(s) for the Agency.

1.3.7.5 *Compliance Auditor*

The Compliance Auditor is an individual or entity who is responsible for Auditing the security of CAs, including reviewing, maintaining, and archiving Audit logs; and performing or overseeing Audits of CAs. The Compliance Auditor MUST have expertise in information security, cryptography, and PKI, Risk mitigation strategies, and industry best practices. A single individual MAY perform the Audit, but MUST NOT be affiliated with the entity being Audited. The CA SHALL identify in the CPS the parties responsible for providing such services, and the mechanisms used to support these services.

PCA Response: The PCA will identify the Compliance Auditor service provider and provide it to the PA upon request.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

Certificates issued under this CP represent a high level of assurance[7], as defined in the VP, which is relevant to environments where Risks and consequences of identity and data Compromise are severe.

Two types of Certificates are issued to End-Entities conforming to this CP; End-Entity Authentication Certificates and End-Entity Signing Certificates. Certificates SHOULD be issued in pairs, one Authentication and one Signing Certificate with the same Certificate Validity Period, Distinguished Name and Subject Alternative Name).

Certificates issued within the NG9-1-1 PKI are to be used for Authentication and signing purposes, as designated by the *keyUsage* and *extKeyUsage* fields found within the

[6] See VP section 3.7.

[7] Commensurate with NIST SP-800-63 [SP 800-63] series Identity Assurance Level 3.

Certificate, for entities connected to an Emergency Services IP Network (ESInet) to protect services for, or ancillary to, public safety or processing emergency calls. Specifically, applicable Certificate uses include:

- PCA issuance of ICA Certificates, CSS Certificates, and CRLs;
- ICA, which are CAs subordinate to the PCA, issuance of ICA CRLs. ICAs MAY issue other ICA Certificates and Subscriber End-Entity Certificates, as well as local CSS Certificates;
- CSSs sign OCSP responses; and
- End-Entity Certificates are used for purposes described in NENA-STA-010.3-2020 and other applicable NENA Standards as determined by NIOC.
    - End-Entity Authentication Certificates issued by the PCA are to be used for Authentication purposes, *as designated* by the *keyUsage* and *extKeyUsage* fields found within the Certificate, for entities connected to an ESInet to protect services for, or ancillary to, public safety or processing emergency calls.
    - End-Entity Signing Certificates issued by the PCA are to be used for signing purposes, as designated by the *keyUsage* and *extKeyUsage* fields found within the Certificate, for entities connected to an ESInet to protect services for, or ancillary to, public safety or processing emergency calls.

The PA MAY allow additional permitted uses not included in this CP by an affirmative vote of its members in accordance with its bylaws. In such cases, the PA SHOULD update this CP with those permitted activities within a reasonable period of time.

1.4.2 Prohibited Certificate Uses

Certificates issued by the PCA are generally not appropriate for use in commercial transactions. In limited cases, they MAY be used in commercial transactions related to public safety. Other prohibited applications include:

- Any export, import, use, or activity that contravenes any local or international laws or regulations;
- Any usage of Certificates in conjunction with illegal activities;
- Any usage of Certificates for personal use or purposes not related to the community's operation;
- Any use of a Certificate after it has been Revoked;
- Any use of a Certificate after it has expired; and
- Any use not expressly permitted in Section 1.4.1.

Additionally, Subscribers and Relying Parties SHALL NOT use, Certificates issued by the PCA for Authentication outside of communications directly related to NG9-1-1, unless expressly permitted by the PA. The PA MAY add prohibited uses not included in this CP by an affirmative vote of its members in accordance with its bylaws. In such cases, the PA SHOULD update this CP with those prohibited activities no later than 60 days from the date of the affirmative vote.

PCA PA Response: While no additional prohibited uses exist, the PCA PA may approve additional prohibited uses in the future, at its discretion.

1.5 Policy Administration

1.5.1 Organization Administering the Document

This CP is administered by the NIOC as the PA. It owns this CP and represents the interest of its members in developing the policies that govern the PCA PKI. Additional policies or exceptions to these policies enacted by the PA under an affirmative vote of its members in accordance with its own bylaws and updating this CP with these changes within a reasonable period of time.

1.5.2 Contact Person

The following individual is responsible for accepting comments on this CP on behalf of NIOC:

NG9-1-1 Interoperability Oversight Commission
c/o NENA
Director of Technology
1700 Diagonal Blvd
Suite 1700
Alexandria, VA 22314
admin@ng911ioc.org
+1 202 466 4911

1.5.3 Person Determining CPS Suitability for this CP

The PCA PA SHALL approve the CPS for the PCA and all lower-tier ICAs.

PCA PA Response: Will comply.

1.5.4 CPS Approval Procedures

CAs SHALL submit their CPS to the appropriate MA. The MA SHALL evaluate CAs against all facets of this CP.

MA Response: Will comply.

The appropriate PA SHALL approve the CPS if it determines that the CPS complies with this CP. The CA MUST meet all requirements of an approved CPS before commencing operations.

PCA PA Response: If the MA determines that the CPS submitted by the PCA or Tier 2 ICA complies with the CP, the PCA PA will review and approve the CPS. Only then may the ICA commence operations.

1.6 Definitions, Acronyms

See Appendices A and B.

1.7 References

See Appendix C.

2. Publication and Repository Responsibilities

2.1 Repositories

All CAs that issue Certificates under this CP MUST post all CRLs issued by the CA in a Repository that is Accessible through Uniform Resource Identifier (URI) references asserted in valid Certificates issued by that CA. The PKI Repositories containing Certificates and Certificate status information SHALL be deployed so as to provide high levels of availability as appropriate for the entity's environment and service level agreement. This service level agreement MUST be included in every CPS. To promote consistent Access to Certificates and CRLs, the Repository SHALL implement Access Controls and communication mechanisms to prevent unauthorized Modification or deletion of information.

CAs SHALL provide their CA Certificate and any CA Certificates they have issued in a Repository that is available to the PKI Participants.

PCA Response: The PCA makes its Root Certificate, ICA Certificates the PCA has issued, and Revocation data for issued Certificates available to its PKI Participants via its publicly available PCA Repository.

2.2 Publication of Certification Information

2.2.1 Publication of CA Information

The PA SHALL make the CP publicly available, and the CA SHALL make CRLs, and CA Certificates available as shown on Table 1. In general, the CPS for CAs are Confidential, but it SHALL be made available to participating members, in a redacted version, from the appropriate PA. The CA SHALL protect information not intended for public dissemination.

Table 1 below is a matrix of the various PKI practice documents, showing whether or not they are publicly available, and their locations. The list is not intended to be exhaustive, nor will each document listed be applicable to every CA. Documents not expressly made public are confidential to preserve the security of the PCA PKI.

Table 1: Publication Requirements

Item	Classification	Available From	Available At:
PCA PKI CP	Public	PA	https://ng911ioc.org/library
Bylaws	Public	PA	https://ng911ioc.org/library
PCA Certificate	Public	PA	https://ng911ioc.org/library
ICA Certificates	Public	PA	https://ng911ioc.org/library
PCA CRLs	Public	CA	<CA Repository URI>

ICA CRLs	Public	CA	<CA Repository URI>
PCA CPS	Portions Confidential	PA	https://ng911ioc.org/library (redacted version)
ICA CPS	Portions Confidential	CA	<CA Repository URI> (redacted version)
Subscriber guides	Public	RA	<RA Repository URI>

PCA Response: Will comply.

PCA PA Response: Will comply.

2.2.2 Availability of Information

CAs SHALL make all information published in the Repository available on a twenty-four (24) hour per day, seven (7) day per week basis, save for periods of scheduled or unscheduled downtime, as negotiated between relevant parties as part of a commercial contract.

CAs SHALL retain all information in the Repository, including non-public information, specifically all End-Entity Certificates, for a period of ten (10) years from the expiration of the information.

PCA Response: Will comply.

2.3 Time or Frequency of Publication

The PA SHALL make updated versions of this CP publicly available within ten (10) business days of the incorporation of changes.

CA Certificates SHALL be made publicly available within ten (10) business days after issuance.

CAs MUST publish CRLs as specified in Section 4.9.7.

All other information to be published in the Repository SHALL be published promptly after such information becomes available to the CA. The maximum time for publication of information SHALL be specified in the CPS.

PCA Response: Will comply.

PCA PA Response: Will comply. The maximum time for publication of all other information in the Repository is ten (10) business days.

2.4 Access Controls on Repositories

2.4.1 Certificate Policy

The PA SHALL make this CP publicly available as shown in Table 1 for read-only Access.

PCA PA Response: Will comply.

2.4.2 Certificates and CRLs

The CA SHALL protect information not intended for public dissemination or Modification. CA Certificates and CRLs in the Repository SHALL be publicly available for read-only Access through the Internet. The CPS SHALL detail what information in the Repository SHALL be exempt from automatic availability and to whom, and under what conditions the restricted information MAY be made available.

PCA Response: <redacted response>.

PCA PA Response: Security information detailed in this CPS is exempt from automatic, public availability and is only available to the PCA PA, and its corresponding MA and RA.

3. Identification and Authentication

3.1 Naming

3.1.1 Types of Names

The CAs SHALL assign non-empty X.500 Distinguished Names (DNs) [X.500] to the issuer and *subjectDN* fields of the Certificates issued as shown in Table 2. CAs MAY create Subscriber Certificates that contain any name type appropriate to the application. The CA MUST assign DNs in the form of a X.500 *printableString* to the issuer and *subjectDN* fields. If the CA cannot encode the string as a *printableString*, it MUST encode it as a UTF8String [**Error! Reference source not found.**].

Table 2: Certificate Names

Certificate	Issuer DN	Subject DN

PCA Certificate	c=<two-letter ISO 3166-1 country code>
	o=<Organization Name>
	ou=PCA-<serial number>
	cn=PCA Root
		c=<two-letter ISO 3166-1 country code>
		o=<Organization Name>
		ou=PCA-<serial number>
		cn=PCA Root

ICA Certificate	c=<two-letter ISO 3166-1 country code>
	o=<Organization Name>
	ou=PCA-<serial number>
	cn=PCA Root
		c=<two-letter ISO 3166-1 country code>
		o=<Organization Name> or <state, regional, local 9-1-1 defined>
		ou=CA-<serial number>
		st=<state, regional, local 9-1-1 defined>
		l=<state, regional, local 9-1-1 defined>
		cn=CA

End-Entity Certificate	c=<two-letter ISO 3166-1 country code>
	o=<Organization Name> or <state, regional, local 9-1-1 defined>
	ou=CA-<serial number>
	st=<state, regional, local 9-1-1 defined>
	l=<state, regional, local 9-1-1 defined>
	cn=CA
		c=<two-letter ISO 3166-1 country code>
		o=<Subscriber Organization Name>
		[ou=<Organization Unit Name>]
		cn=<End-Entity idType/iD >

PCA Response: Will comply.

3.1.2 Need for Names to be Meaningful

The RA MUST ensure that names used in all PCA PKI Certificates represent an unambiguous identifier for the Subject and that the Subject contains the verified organization name of the PKI Sponsor responsible for the Certificate. The RA MUST use the verified organization name as the *organizationName* field in the DN of the issued Certificate.

Relying Parties SHOULD use the *subjectAltName* (SAN) extension, as defined in Section 7.1.2.11, to assert the identity and role of the entity (e.g., person, organization, device, or object). Relying Parties SHALL use the Subject DN to verify the organization the

Certificate was issued to. Relying Parties SHOULD use the Issuer DN to verify the issuer of the Certificate.

The *Organization Name* or *o* field SHOULD be the display name of the Owner, such as "NG9-1-1 Interoperability Oversight Commission" or "State of Virginia".

The *Organizational Unit* or *ou* field SHOULD be descriptive, down to an instance, of what the entity issued a certificate does. For example, "PCA-1" or "State of Virginia ECRF-01". It MAY also be the iD for the Certificate, such as "ecrf01.ngcs.virginia.gov" or "tom.jones@psap.alexandria.gov", as defined in Section 7.1.2.11.

The *Common Name* or *cn* field SHOULD be a display name, such as "PCA" or "Virginia ECRF".

RA Response: The Certificates issued contain subjectDN attributes that appear in the Certificates which can be understood and used by Relying Parties. Names used in the Certificates identify the Agency, Agent or Device to which they are assigned in a meaningful way.

3.1.3 Anonymity or Pseudonymity of Subscribers

The PCA and its RA, and ICAs and their RAs, SHALL NOT issue Anonymous or Pseudonymous Certificates.

PCA Response: Will comply.

3.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting DN forms are specified in X.500 [X.500].

3.1.5 Uniqueness of Names

The PCA and ICAs SHALL ensure that NENA ID Quad values in the Subject Alternative Name (SAN) extension in the Certificate are unique.

PCA Response: Will comply.

3.1.6 Recognition, Authentication, and Role of Trademarks

The PCA and its RA, and ICAs and their RAs, SHALL NOT knowingly issue a Certificate including the name that a court of competent jurisdiction has determined infringes upon a third party's trademark. Prospective Subscribers SHALL NOT use names in their Certificate Applications that infringe upon the Intellectual Property Rights of others.

A CA or RA SHALL NOT knowingly issue a Certificate including the name of any entity, such as a government agency, that a court of competent jurisdiction would determine that the Prospective Subscriber is not a legitimate agent of, such as through employment (for Certificates issued to individual identities) or ownership/responsibility to operate (for Certificates issued to devices or software).

A CA or RA is not required to determine whether a Prospective Subscriber has Intellectual Property Rights or otherwise has Legal Agency 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, including, without limitation, rights in a domain name, trade name, trademark, or service mark; and the PA, and any CA SHALL be entitled, without liability to any Prospective Subscriber, to reject or suspend any DCSA because of such dispute. The PA SHALL attempt to resolve disputes involving names and trademarks.

PCA Response: Will comply.

RA Response: Will comply.

PCA PA Response: Will comply.

3.2 Initial Identity Validation

This section provides the requirements for the issuance of high assurance Certificates under this CP. The word "Assurance" means how well a Relying Party can be certain of the identity Binding between the Public Key and the entity whose Subject name is cited in the Certificate. In addition, it also reflects how well the Relying Party can be certain that the entity whose name is cited in the Subject of the Certificate is controlling the use of the Private Key that corresponds to the Public Key in the Certificate.

The level of Assurance associated with a Public Key Certificate describes the procedures and controls involved in validating a Subscriber's identity and Binding that identity to a Public Key. It is the responsibility of the Relying Party to assess that level of Assurance and determine if it meets their security requirements for some particular use. The level of Assurance depends on the proper generation and management of the Certificate and associated Private Keys, in accordance with the stipulations of this CP. Personnel, physical, procedural, and technical security controls contribute to the Assurance level of the Certificates issued.

3.2.1 Method to Prove Possession of Private Key

The Authentication of the Subscriber, as defined in Section 3.2.3, is required prior to the proof of possession process described in this section.

In all cases where the Subscriber generates its own keys, that Subscriber SHALL prove possession of the Private Key, which corresponds to the Public Key in the Certificate Signing Request (CSR). For example, this may be done by the Subscriber, using its Private Key to sign the CSR or a value assigned by the RA. The RA SHALL then validate the signature using the Subscriber's Public Key provided in the CSR.

For cases where a trusted account administrator submits the CSR on behalf of the Subscriber, proof of possession MAY be done by the Subscriber using its private key to sign a value supplied by the CA. The CA SHALL describe in its CPS how it validates possession of the Private Key.

The PCA or ICA, and any RA on behalf of the CAs, SHALL prove that the Subscriber possesses the Private Key by verifying the Subscriber's Digital Signature on the PKCS #10 CSR with the Public Key in the CSR.

The PA MAY approve other methods to prove possession of a Private Key by a Subscriber that are at least as secure as those here.

PCA Response: The PCA establishes that the Prospective Subscriber holds the Private Key corresponding to the Public Key by performing signature verification on the CSR file submitted by the Prospective Subscriber or the RA on behalf of the Subscriber.

RA Response: Will comply.

3.2.2 Authentication of Organization Identity

The RA SHALL conform to the requirements contained within the VP to validate all identities, including organizations (agencies), devices and agents.

RA Response: Will comply.

3.2.3 Authentication of Subscriber Identity

See the VP.

3.2.4 Non-verified Subscriber Information

Information that is not verified by a CA or RA SHALL NOT be included in Certificates.

3.2.5 Validation of Authority

See the VP.

3.2.6 Criteria for Interoperation

This CP provides for interoperability with third party CAs (i.e., CAs external to the PCA PKI) through cross certification. The PA SHALL determine the criteria for cross certification with other entities in accordance with the PCA PKI Cross Certification Methodology and Criteria [forthcoming]. Interoperability will be established when directed by the PA and will require a Memorandum of Agreement (MOA) between the PCA and the third parity CA.

PCA PA Response: The forthcoming PCA PKI Cross Certification Methodology and Criteria will define the process for cross-signing with third party CAs and the criteria in which cross-signing is allowed.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-Key

For Re-Key of any CA Certificate issued under this CP, the CA SHALL follow the same procedures as the initial registration process described in Section 3.2.

For Re-Key of any End-Entity Certificate issued under this CP, the RA SHALL follow the same procedures as the initial registration described in Section 3.2.

PCA Response: Will comply.

RA Response: Will comply.

3.3.2 Identification and Authentication for Re-Key after Revocation

Once a Certificate has been Revoked for Compromise, the RA SHALL require a root cause analysis of the issue that led to Revocation, and a documented plan to address the issue with committed dates. Issuance of a new Certificate and the Re-Key SHALL require completion of the plan and SHALL require following the same process as the initial registration process, described in Section 3.2.

RA Response: Will comply.

3.4 Identification and Authentication for Revocation Request

Revocation requests MUST be Authenticated by the PCA or ICAs, or their corresponding RAs, prior to the request being accepted. Requests to Revoke a Certificate MAY be Authenticated using that Certificate's Public Key, regardless of whether or not the associated Private Key has been Compromised. If the request cannot be Authenticated with the Certificate’s Public Key, the CA or RA SHALL validate the information provided by the Revocation requestor and document those details prior to determining if the Revocation will be completed or not. The CA, or RA acting on its behalf, SHALL Authenticate a request for Revocation of a Certificate based on the information provided by the requestor. Authentication mechanisms used by the CA or RA SHALL balance the need to prevent unauthorized Revocation requests against the need to quickly Revoke Certificates. Revocation requests Authenticated on the basis of the current Key Pair SHALL always be accepted as valid, even if this Key Pair is the one suspected of being Compromised. Other Revocation request Authentication mechanisms MAY be used with the permission of the CA, such as challenge-response questions combined with a completed standard CA Revocation Request form that was sent to the Certificate holder at the time of the Revocation request. All Revocation requests SHALL be logged by the CA or RA.

After a Certificate has been Revoked, other than during a Renewal or update action, the Subscriber SHALL go through the initial Certificate Application process to obtain a new Certificate.

PCA Response: Will comply.

RA Response: Will comply.

4. Certificate Life-cycle Operational Requirements

4.1 Certificate Application

The Certificate Application consists of the Subscriber agreement (i.e., the DCSA) and the accompanying Naming Application provided with the DCSA and an accompanying PKCS #10 CSR. A copy of the DCSA can be requested from the RA.

4.1.1 Who Can Submit a Certificate Application

No stipulation.

4.1.2 Enrollment Process and Responsibilities

Prospective Subscribers SHOULD submit sufficient information to allow the PCA or ICAs, or their corresponding RAs, to successfully perform the required verification.

The CA or RA SHALL develop processes that sufficiently verify the Prospective Subscriber's identity for all Certificate types generated for the PCA PKI according to Section 3.2.3.

Prospective Subscribers SHALL:

- Agree to the applicable Subscriber agreement (i.e., the DCSA);
- Complete the Certificate Application provided in the DCSA;
- Provide the requested information;
- Respond to verification requests in a timely manner;
- Generate the Key Pair;
- Deliver the Public Key of the Key Pair to the RA; and
- Submit payment, if required.

The items in the list above MAY be completed in any order that is convenient for the RA and Prospective Subscribers that does not defeat security, but all SHALL be completed before Certificate issuance.

PCA Response: Will comply.

RA Response: Will comply.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

The RA SHALL perform the identification and Authentication validation functions for Prospective Subscribers requesting PCA PKI Certificates, as specified in Sections 3.2 and 3.3 in this CP.

RA Response: Will comply.

4.2.2 Approval or Rejection of Certificate Applications

The RA SHALL approve a Certificate Application if all of the following conditions are met:

- Receipt of a fully executed DCSA;
- Receipt of a signed Certificate Application;
- Successful validation per the VP;
- Receipt of all requested supporting documentation; and
- Payment (if applicable) has been received.

The RA SHALL reject any Certificate Application for which such validation cannot be completed, or when the RA has cause to lack confidence in the application. The RA MAY reject a Certificate Application if any one or more of the following conditions arise:

- The Prospective Subscriber fails to execute the required DCSA;
- An authorized representative fails to sign the Certificate Application;
- Unable to successfully validate per the VP;
- The Prospective Subscriber fails to furnish requested supporting documentation;
- The Prospective Subscriber fails to respond to notices within a specified time;
- The Prospective Subscriber is not in good standing with the RA or CA;
- The RA believes that issuing the Certificate MAY bring the RA or CA into disrepute; or
- Payment (if applicable) has not been received;

RA Response: Will comply.

The CA MAY reject any Certificate Application if the CA believes that issuing a Certificate MAY bring the CA into disrepute.

4.2.3 Time to Process Certificate Applications

RAs SHALL process Certificate Applications within a reasonable time of receipt of all necessary documents as specified in the CPS.

RA Response: Once all Certificate Application materials are received, the RA will process the Application within five (5) business days.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

A Certificate is created and issued by a CA following its RA's approval of a Certificate Application. Upon receiving the request, the CA SHALL:

- Authenticate the RA using a Certificate provided to the RA by the CA;
- Receive the PKCS #10 CSR generated by the Subscriber from the RA;
- Generate a Certificate using the information in the CSR, along with any additional Certificate profile information provided by the RA; and
- Ensure delivery of the Certificate to the Subscriber.

PCA Response: Upon receiving the Certificate request, the PCA will:

- *Verify the identity of the requester;*
- *Validate the information in the Certificate request by checking the signature on the CSR;*

- *Create and sign a Certificate if all Certificate requirements have been met; and*
- *Make the Certificate available to the Subscriber directly or via the RA.*

4.3.2 Notification to Subscriber by the CA of Issuance of Certificates

CAs issuing Certificates SHALL notify the RA of the creation of a Subscriber Certificate. The RA SHALL inform the Subscriber, through information submitted during the Certificate enrolment process, that their Certificate is available and the means for obtaining the Certificate.

PCA Response: The PCA delivers issued Certificates in a secure manner to Subscribers directly or via the RA within a reasonable time after issuance.

RA Response: <redacted response>.

4.4 Certificate Acceptance

Once downloaded, the Subscriber SHALL check the contents of the Certificate without delay. If the Subscriber detects any problems, the Subscriber SHALL notify the CA, or the RA on behalf of the CA, about the problem. The Certificates are considered accepted thirty (30) days after the Certificate's issuance, unless the CA, or the RA on behalf of the CA, is notified of a problem.

4.4.1 Conduct Constituting Certificate Acceptance

An issued Certificate SHALL be deemed to have been accepted when it has been downloaded, installed, and used, and the Subscriber has not notified the RA of a problem with the Certificate or its contents.

4.4.2 Publication of the Certificate by the CA

CAs SHALL publish CA Certificates, as specified in Section 2.2.

This CP makes no stipulation regarding publication of Subscriber Certificates.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

CAs operating under this CP SHALL notify PKI Participants whenever it issues a CA Certificate by updating its CA Repository.

PCA Response: Will comply.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Subscriber use of the Private Key corresponding to the Public Key in the Certificate SHALL only be permitted once the Subscriber has agreed to the DCSA and accepted the Certificate, as described in Section 4.4.1. Subscriber key use SHALL be consistent with the *keyUsage* and *extKeyUsage* extensions, in the associated Certificate.

Subscribers SHALL protect their Private Keys from unauthorized use and SHALL discontinue use of the Private Key following expiration or Revocation of the Certificate.

Subscriber Certificate use SHALL be in lawful accordance with the DCSA and the terms of this CP.

The RA SHALL provide guidance to Subscribers on its responsibilities on use of their Private Key and obtain the Subscriber's acknowledgement, as defined in Section 9.6.3.

RA Response: Will comply.

4.5.2 Relying Party Public Key and Certificate Usage

Before any act of reliance, Relying Parties SHALL independently assess the following:

- The appropriateness of the use of a Certificate for any given purpose and determine that the Certificate will, in fact, be used for an appropriate purpose that is not prohibited or otherwise restricted by Section 1.4;
- That the Certificate is being used in accordance with the *keyUsage* and *extKeyUsage* extensions included in the Certificate; and
- The status of the Certificate and all the CAs in the chain that issued the Certificate. If any of the Certificates in the Certificate chain have been Revoked, the Relying Party SHALL NOT rely on the Certificate or other Revoked Certificates in the Certificate chain.

4.6 Certificate Renewal

Renewing a Certificate means creating a new Certificate with the same name, key, and other information as the old one, but a new, extended Validity Period and a new serial number is created.

4.6.1 Circumstances for Certificate Renewal

Any Certificate MAY be Renewed if the Public Key has not reached the end of its Validity Period, the associated Private Key has not been Revoked or Compromised, and the Subscriber name and attributes are unchanged. In addition, the Validity Period of the Certificate MUST NOT exceed the remaining lifetime of the Private Key, as specified in Section 6.3.2.

Certificates MAY be Renewed as long as the aggregated lifetime of the Public Key does not exceed the Certificate lifetime specified in Section 6.3.2.

4.6.2 Who May Request Renewal

The following MAY request a Certificate Renewal:

- The Subscriber of the Certificate or an authorized representative of the Subscriber,
- A CA, to request a Renewal of its own Certificate, or
- A CA, to Renew its issued Certificates during recovery from a CA key Compromise.

4.6.3 Processing Certificate Renewal Requests

A CA MAY require a revalidation prior to Renewal of a Certificate.

4.6.4 Notification of Certificate Renewal to Subscriber

The RA SHALL inform the Subscriber of the Renewal of its Certificate, in accordance with Section 4.3.2.

RA Response: Will comply.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Acceptance of the Renewed Certificate or its contents constitutes acceptance of the Certificate, as per Section 4.4.

4.6.6 Publication of the Renewal Certificate by the CA

Publication of Renewed Certificates is subject to the requirements in Section 2 of this CP.

4.6.7 Notification of Certificate Renewal by the CA to Other Entities

See Section 4.4.3.

4.7 Certificate Re-Key

Subscribers SHALL identify themselves to the RA for the purpose of Re-Keying as required in Section 3.

Certificate Re-Key consists of creating a new Certificate for a different Key Pair (and serial number) but can retain the contents of the original Certificate's *subjectName*. Certificate Re-Key does not violate the requirement for name uniqueness. The new Certificate MAY be assigned a different Validity Period, key identifiers, and/or be signed with a different key.

4.7.1 Circumstances for Certificate Re-key

When a CA Re-Keys a certificate, the new certificate MUST include a new key. A CA SHALL NOT process a Re-Key if the key is the same as the original. Any Certificate holder MAY request a Re-Key at any time.

A Certificate MAY be Re-Keyed after Revocation, for example, due to a Compromised Private Key. A Certificate MAY also be Re-Keyed before expiration to maintain continuity of Certificate usage. A Certificate MAY be Re-Keyed after expiration.

PCA Response: Will comply.

4.7.2 Who May Request Certification of a New Public Key (Re-Key)

Requests to the RA for a new Public Key SHALL be considered for the following:

- Subscribers with a currently valid Certificate MAY request a new Public Key;
- The RA MAY request a new Public Key on behalf of a Subscriber;
- A CA MAY request a Re-Key of its own Certificate;
- A CA MUST Re-Key its issued Certificates during recovery from a CA key Compromise; or

- The appropriate PA MAY request Re-Key of CA Certificate.

PCA Response: Will comply.

4.7.3 Processing Certificate Re-Keying Requests

A CA MAY require a revalidation prior to Renewal of a Certificate.

4.7.4 Notification of New Certificate Issuance to Subscribers

A CA SHALL inform the Subscriber of the Re-Key of its Certificate, as per Section 4.3.2.

PCA Response: Will comply.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

Acceptance of the Renewed Certificate or its contents constitutes acceptance of the Certificate, as per Section 4.4.

4.7.6 Publication of the Re-Keyed Certificate by the CA

Publication of Re-Keyed Certificates is subject to the requirements in Section 2 of this CP.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3.

4.8 Certificate Modification

A CA SHALL treat all requests for Certificate Modification as new Certificate Applications, subject to the provisions of Sections 4.1 and 4.2.

Modifying a Certificate means creating a new Certificate that has the same or a different key and a different serial number, and that differs in one or more other fields from the old Certificate.

PCA Response: Will comply.

4.8.1 Circumstance for Certificate Modification

The RA MAY accept Certificate Modification requests only for Subscribers whose characteristics have changed in a way which would not invalidate the verification of identity used to issue the Certificate.

If the Modified Certificate will have the same Public Key as the original Certificate, the requirements for Renewal as stated in Section 4.6.1 also apply.

Certificates MAY be Modified:

- For a Subscriber organization name change or other Subscriber characteristic change; or
- For Validity Period.

A Certificate MAY be Modified after Certificate expiration.

4.8.2 Who May Request Certificate Modification

Requests to the RA for Certificate Modification SHALL be considered for the following:

- Subscribers with a currently valid Certificate MAY request Certificate Modification;
- The RA MAY request Certificate Modification on behalf of a Subscriber;
- A CA MAY request a Certificate Modification of its own Certificate; or
- The appropriate PA MAY request Modification of CA Certificates.

4.8.3 Processing Certificate Modification Requests

CA Certificate Modification SHALL be approved by the PA for the CA performing the certificate modification.

For Certificate Modification requests, the RA SHALL confirm the identity of the Subscriber in accordance with the requirements, as specified in the VP.

PCA PA Response: Will comply.

RA Response: Will comply.

4.8.4 Notification of Modified Certificate Issuance to Subscriber

A CA SHALL inform the Subscriber of the Modification of its Certificate, in accordance with Section 4.3.2.

PCA Response: Will comply.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Acceptance of the Modified Certificate or its contents constitutes acceptance of the Certificate, as per Section 4.4.

4.8.6 Publication of the Modified Certificate by the CA

Publication of Modified Certificates is subject to the requirements in Section 2 of this CP.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3.

4.9 Certificate Revocation and Suspension

Revocation of a Certificate permanently ends the operational period of the Certificate prior to the Certificate reaching the end of its stated Validity Period.

CAs SHALL issue CRLs covering all unexpired Certificates issued under this CP, except for OCSP responder Certificates that include the *id-pkix-ocsp-nocheck* extension.

CAs SHALL make public a description of how to obtain Revocation information for the Certificates they publish. The RA SHALL provide this information to Subscribers during the Certificate request or issuance and SHALL be readily available to any potential Relying Party.

The RA SHALL validate any Revocation requests subject to the requirements in Section 3.4. The RA MAY Authenticate requests to Revoke a Certificate using that Certificate's associated Public Key, regardless of whether the Private Key has been Compromised.

PCA Response: The PCA's CRLs include all Revoked Certificates on all new publications of the CRL until the Certificates expire.

4.9.1 Circumstances for Revocation

The RA SHALL request from its corresponding CA that a Certificate be Revoked when the Binding between the Subject and the Subject's Public Key defined within the Certificate is no longer considered valid. When this occurs, the associated Certificate SHALL be Revoked. The CA SHALL include all Revoked Certificates on all new publications of the Certificate Status Service (CSS) information (see Section 4.10) until the Certificates expire.

Revocation SHALL occur on decision of the CA when reasonable and credible evidence exists to establish at least one of the following:

- A determination by the CA that Revocation is appropriate and/or needed;
- Identifying information or affiliation components of any names in the Certificate becomes invalid;
- Any information in the Certificate becomes invalid, subject to the terms of the CPS the Certificate is issued under;
- The Subscriber can be shown to have violated the stipulations of its DCSA or one or more sections of this CP;
- The original Certificate request was not authorized;
- The Subscriber or other authorized party asks for its Certificate to be Revoked;
- The Subscriber is no longer eligible to obtain a Certificate from a CA operating under this CP;
- The Certificate has been delivered based upon wrong or falsified information;
- There is reason to believe the Confidentiality of a Private Key is no longer ensured or has been Compromised; or
- The media holding the Private Key is suspected or known to have been Compromised.

If there is a Risk of a Private Key disclosure, then the CA SHALL Revoke the Certificate, and measures SHALL be taken to invalidate or securely erase the Private Key associated with the Certificate.

PCA Response: Will comply.

RA Response: Will comply.

4.9.2 Who Can Request Revocation

Within the PKI, the Revocation of a Certificate MAY be requested by any one of the PKI Participants.

4.9.3 Procedure for Revocation Request

The Certificate Revocation requestor SHALL identify the date of the request, the Certificate to be Revoked, the reason for Revocation, and allow the requestor to be Authenticated.

Upon receipt of a Revocation request, the RA SHALL Authenticate the request and establish circumstances per Section 4.9.1.

The MA shall publicly disclose the instructions through a readily accessible online means, and in the CPS. The Issuer CA shall maintain a continuous 24/7 ability to internally respond to any high priority Revocation requests.

Once Authenticated, the RA SHALL inform its corresponding CA and MA of the request. If the request for Revocation comes from someone other than the entities listed in Section 4.9.2, then the RA SHALL investigate the alleged basis for the Revocation request prior to informing the CA and MA of the request. In the event a Private Key is Compromised, time is of the essence to Revoke a Certificate. In that event, the CA may perform a Revocation without consulting the RA and MA.

The MA, at its discretion, MAY take whatever measures it deems appropriate to verify the need for Revocation. If the MA approves the Revocation, the MA SHALL direct the CA to Revoke the Certificate.

RA Response: <redacted response>.

MA Response: Once the MA approves a Revocation, the MA will inform the RA and direct the CA to Revoke the Certificate

PCA Response: The PCA will respond to a high priority Revocation within 24hrs.

4.9.4 Revocation Request Grace Period

There is no grace period for Revocation under this CP.

Responsible parties SHALL request Revocation as soon as they identify the need for Revocation.

4.9.5 Time Within Which CA Must Process the Revocation Request

CAs SHALL process Certificate Revocation requests as quickly as practical upon receipt of a proper Revocation request from the RA. There is no stipulation about when Certificate Revocation requests are completed because such timing depends largely on the availability of information supporting authorization of the Revocation request. The Issuer CA shall maintain a continuous 24/7 ability to internally respond to any high priority Revocation requests.

PCA Response: The PCA will process a Certificate Revocation request within twenty-four (24) hours of receipt of a PA approved Certificate Revocation request.

4.9.6 Revocation Checking Requirement for Relying Parties

A Relying Party MUST obtain the current CRL or employ the CSS provided by its CA to determine if a Certificate has been Revoked.

CAs, MAs, and RAs SHALL provide Relying Parties with information on how to find the appropriate CRL or web-based Repository, or CSS to check the Revocation status of Certificates issued by the CA.

PCA Response: The PCA will provide Relying Parties with information on how to find the appropriate CRL or OCSP responder (if available) via the URLs provided in the cRLDistributionPoints and authorityInformationAccess extension in the Certificate.

MA Response: The MA will provide Relying Parties with information on how to find the appropriate CRL or OCSP responder (if available) via the URLs provided in the cRLDistributionPoints and authorityInformationAccess extension in the Certificate.

RA Response: The RA will provide Relying Parties with information on how to find the appropriate CRL or OCSP responder (if available) via the URLs provided in the cRLDistributionPoints and authorityInformationAccess extension in the Certificate.

Relying Parties SHOULD maintain a local OCSP Server in the event Certificate status checking is not available (which can be caused by any number of different reasons such as lack of local network connectivity or Internet outage, no CRL/OCSP Server availability, missing CRL file at the CSS, etc.). A cache of the CRL MAY be maintained locally.

Fallback operation, in the event Certificate status checking is not available, SHOULD use the cached version of the CRL until the latest CRL can be downloaded or the online availability of CSS is restored. If a cached version of the CRL is not available, the Certificate SHOULD be considered valid until its status can be checked in the next available CRL or via the online CSS.

4.9.7 CRL Issuance Frequency

A CA SHALL generate and publish (a.k.a. issue) CRLs 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. A CA SHALL ensure that superseded Certificate status information is removed from the PKI Repository upon posting of the latest Certificate status information.

Certificate status information SHALL be published no later than the next scheduled update. This will facilitate the local caching of Certificate status information for offline or remote operation. The CA SHALL update its PKI Repositories to which they post Certificate status information to reduce latency between creation and availability.

Table 3 below provides CRL issuance frequency requirements.

Table 3: CRL Issuance Frequency

Type of CRL	Issuance Frequency
Routine	At least once every twenty-four (24) hours
Loss/Compromise of Private Key (Emergency)	Within four (4) hours of notification
CA Compromise (Emergency)	Immediately, but no later than within fifteen (15) minutes of generation.

CRL issuance frequency requirements MAY be further constrained by applicable jurisdictional regulatory law.

The CAs that issue routine CRLs less frequently than the requirement for emergency CRL issuance (i.e., CRL issuance for loss or Compromise of key or for Compromise of CA) SHALL meet the requirements specified above for issuing emergency CRLs.

PCA Response: Will comply.

4.9.8 Maximum Latency for CRLs

A CA SHALL publish CRLs within four (4) hours of generation, except for CA Compromise emergencies, which shall be published immediately, but no later than within 15 minutes of generation. Furthermore, each CRL SHALL be published no later than the time specified in the *nextUpdate* field of the previously issued CRL for the same scope.

The maximum delay between the time a Certificate Revocation is performed by a CA and the time that this Revocation information is available to Relying Parties SHALL be no greater than fifteen (15) minutes.

PCA Response: Will comply.

4.9.9 Online 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.

All online CRLs SHALL have service availability of not less than 99.95% with scheduled downtime notification of at least thirty (30) hours in advance. Scheduled downtime for online CRLs SHALL NOT exceed four (4) hours in any single calendar week, or sixteen (16) hours in a calendar year.

PCA Response: The PCA maintains an online 24x7 Repository that Relying Parties can use to check the current status of all unexpired Certificates issued by the PCA.

4.9.10 Online Revocation Checking Requirements

Relying Party Client software SHOULD support online status checking. Client software using online status checking is NOT required to obtain or process CRLs.

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 online Repository or by requesting Certificate status using the applicable OCSP responder.

4.9.11 Other Forms of Revocation Advertisements Available

Any alternate forms used to disseminate Revocation information SHALL be described in the CA's CPS and SHALL be implemented in a manner consistent with the security and latency requirements for the implementation of CRLs and online Revocation and status checking. CRL and OCSP Certificate status checking SHALL be supported even if alternate mechanisms are provided.

PCA Response: The PCA only uses CRLs and OCSP responders to publicize status of Revoked Certificates.

4.9.12 Special Requirements Regarding Key Compromise

See Section 4.9.3.

A CA SHALL notify its senior management in the event of Compromise, or suspected Compromise, of the CA Private Key.

PCA Response: Will comply.

4.9.13 Circumstances for Suspension

Suspension is not supported by this CP.

4.9.14 Who Can Request Suspension

No stipulation.

4.9.15 Procedure for Suspension Request

No stipulation.

4.9.16 Limits on Suspension Period

No stipulation.

4.10 Certificate Status Services (CSS)

The PCA PKI MUST include a service that provides status information about Certificates on behalf of a CA through online transactions. In particular, the PCA PKI includes CRLs and OCSP responders to provide online status information. Such a service is termed a Certificate Status Service (CSS). Where the CSS is identified in Certificates as an authoritative source for Revocation information or issued a delegated responder

Certificate, the operations of that authority are considered within the scope of this CP. A CSS SHALL assert all the policy OIDs for which it is authoritative, including OCSP Servers that are identified in the Authority Information Access (AIA) extension. OCSP Servers that are locally trusted, as described in [RFC 2560], are not required to meet Section 4.10.2 below.

The CSS is considered an integral part of the CAs and, except where expressly noted, all requirements imposed on CAs apply.

PCA Response: The PCA maintains an online 24x7 Repository that Relying Parties can use to check the current status of all unexpired Certificates issued by the PCA.

4.10.1 Operational Characteristics

A CSS SHALL meet the following requirements:

- The CSS SHALL be operated in compliance with this CP;
- Information exchanged between a CA and the CSS SHALL be Authenticated and protected from Modification using mechanisms commensurate with the requirements of the data to be protected by the Certificate being issued;
- Accurate and up-to-date information from the associated CA SHALL be used to provide the Revocation status;
- Revocation status responses SHALL provide Authentication and Integrity services commensurate with the requirements of the data to be protected by the Certificates being issued, to include the status of the Certificate and the time the status indication was generated; and
- Latency of Certificate status information SHALL meet or exceed the requirements for CRL issuance stated in Section 4.9.7.

Certificate status can be ascertained by querying the CRL maintained and published in its Repository by the CA, or by querying an authorized OCSP responder.

PCA Response: Will comply.

4.10.2 Service Availability

Relying parties SHOULD establish instances of a trusted OCSP responder. A CA’s OCSP service SHALL be available twenty-four (24) hours a day, seven (7) days a week, fifty-two (52) weeks a year, with the following availability:

- Outside declared maintenance window: 99.99%
- Within declared maintenance window: 99.9%

Declared maintenance windows SHALL NOT exceed four (4) hours in any single calendar week.

Relying Parties MAY locally cache CRLs for cases where the Relying Party is not able to Access the Certificate status online.

PCA Response: Will comply.

4.10.3 Operational Features

No stipulation.

4.11 End of Subscription

Subscription is synonymous with the Certificate Validity Period. The subscription ends when the Certificate is Revoked or expired.

For Certificates that have expired prior to or upon end of subscription, Revocation is not required. Issuing CAs SHALL always Revoke unexpired CA Certificates at the end of the subscription.

PCA Response: Will comply.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

No stipulation.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5. 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.

5.1 Physical Controls

The CA SHALL protect all CA equipment, including Cryptographic Modules from theft, loss, and unauthorized Access. Unauthorized use of CA equipment is prohibited. The CA SHALL dedicate CA equipment to performing CA functions. The CA SHALL implement physical Access Controls to reduce the Risk of equipment tampering, even when the Cryptographic Module is not installed and activated.

All the physical control requirements specified below apply equally to the PCA and ICAs.

PCA Response: Will comply.

5.1.1 Site Location and Construction

The CA SHALL conduct all CA operations within a physically protected environment that deters, prevents, and detects unauthorized use of, Access to, or disclosure of sensitive information and systems. The CA SHALL select its site location and construction, so that when combined with other physical security protection mechanisms such as guards, high security locks, and intrusion sensors, it SHALL provide robust protection against unauthorized Access to the CA equipment and Records.

PCA Response: <redacted response>.

5.1.2 Physical Access

5.1.2.1 *Physical Access for CA Equipment*

The CA SHALL have physical Access Controls for CA equipment, as well as remote workstations used to administer the CAs, to:

- Protect all CA equipment from unauthorized Access;
- Manually or electronically monitor CA equipment for unauthorized intrusion;
- Ensure an Access log is maintained and available for inspection;
- Store all removable media and paper containing sensitive plain-text information in secure containers; and
- Except for remote workstations, require two-person physical Access Control to both the Cryptographic Module and computer systems.

The CA SHALL place all removable Cryptographic Modules and the activation information used to Access or enable Cryptographic Modules in secure containers when not in use. Activation Data SHALL be either memorized or recorded and stored in a manner commensurate with the security afforded the Cryptographic Module, and SHALL NOT be stored with the Cryptographic Module or removable hardware associated with remote workstations used to administer the CA. Access to the contents of the locked containers SHALL be restricted to individuals holding CA Trusted Roles, as defined in

Section 5.2.1, utilizing two-person Access Controls, and two-person Integrity while the container is unlocked.

When in active use, the Cryptographic Module SHALL be locked into the system or container (rack, reader, Server, etc.) using a physical lock under the control of the CA Operations Staff to prevent unauthorized removal.

A security check of the CA Facility, or remote workstations used to administer the CAs, SHALL occur prior to leaving the CA Facility unattended. 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/CSS is shut down);
- Any containers housing the Cryptographic Module are properly secured;
- Physical security systems (e.g., door locks, vent covers) are functioning properly; and
- The area is secured against unauthorized Access.

PCA Response: Will comply.

5.1.2.2 *Physical Access for RA Equipment*

The RA SHALL protect its RA equipment from unauthorized Access.

RA Response: Will comply.

5.1.3 Power and Air Conditioning

The CA SHALL have facilities equipped with primary and Backup power systems to ensure continuous, uninterrupted Access to electric power 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.

PCA Response: Will comply.

5.1.4 Water Exposures

The CA SHALL install its equipment such that it prevents damage from exposure to water. The CA SHALL construct its facilities and SHALL implement procedures 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.

PCA Response: Will comply.

5.1.5 Fire Prevention and Protection

The CA SHALL equip its facilities and SHALL implement procedures to prevent damaging exposure to flame or smoke. These measures SHALL meet all local applicable safety regulations.

PCA Response: Will comply.

5.1.6 Media Storage

The CA SHALL store its media to protect it from accidental damage (water, fire, electromagnetic) and prevent unauthorized physical Access. The CA SHALL store media not required for daily operation, or not required by policy, to remain with the CA that contains security Audit, Archive, or Backup information in a securely stored location separate from the CA equipment.

PCA Response: Will comply.

5.1.7 Waste Disposal

The CA and RA SHALL destroy sensitive media and documentation that are no longer needed for operations in a secure manner, for example, sensitive documentation SHALL be shredded, burned, or otherwise rendered unrecoverable.

Destruction of media and documentation containing sensitive information, such as Private Key material, SHALL employ methods commensurate with those in the NIST Guidelines for Media Sanitization [SP 800-88-1].

PCA Response: Will comply.

RA Response: Will comply.

5.1.8 Off-Site Backup

The CA SHALL maintain full system Backups, sufficient to recover from system failure, on a periodic schedule. The CA SHALL store at least one full Backup copy at an off-site location (separate from CA equipment). The CA SHALL store the Backup at a site with physical and procedural controls commensurate to that of the operational CA system.

PCA Response: Will comply.

5.2 Procedural Controls

Procedural controls are requirements on Trusted Roles that perform functions that can introduce security problems, either accidentally or maliciously, if not carried out properly. The functions performed in these roles form the basis of trust for the entire PKI.

5.2.1 Trusted Roles

Trusted Persons are personnel identified to fill Trusted Roles and are designated to manage the PKI’s trustworthiness.

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. Trusted Persons include all employees, contractors, and consultants that have Access to or control Authentication or cryptographic operations that MAY materially affect:

- The validation, Authentication, and handling 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 workstations) personnel having Access to restricted portions of its Repository;
- Access to safe combinations and/or keys to security containers that contain materials supporting production services;
- Access to Hardware Security Modules (HSMs), their associated keying material, and the secret share splits of the Personal Identification Numbers (PINs) that protect Access to the HSMs;
- Installation, configuration, and maintenance of the CA;
- Access to restricted portions of the Certificate Repository;
- The handling of Subscriber information or requests; and
- The ability to grant physical and/or logical Access to the CA equipment.

A Trusted Role is one who performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. Thus, it is essential that the people selected to fill these roles SHALL be held accountable to perform designated actions correctly or the Integrity of the CA is weakened. The functions performed in these roles form the basis of trust in the CA.

Multiple people MAY hold the same Trusted Role, with collective privileges sufficient to fill the role. CAs MAY use different titles to describe these roles, or break out the duties in different ways, as long as the requirements for separation of duties are met (see Sections 5.2.2 and 5.2.4). Other Trusted Roles MAY be defined by the organization administering the PKI, in which case they will be described as additional subsections below.

5.2.1.1 *CA Administrator*

The CA Administrator SHALL maintain lists, including names, organizations, contact information, and organizational affiliation for those who perform CA Administrator functions.

The CA SHALL ensure a separation of duties into Trusted Roles for critical CA functions to prevent an individual from maliciously using the CA system without detection. Each such Trusted Role’s system Access is to be limited to those actions which they are REQUIRED to perform in fulfilling their responsibilities.

The CA Administrator role is responsible for:

- Installation, configuration, and maintenance of the CA;
- Establishing and maintaining CA system accounts;
- Configuring CA Audit parameters;

- Configuring Certificate status information;
- Generating and backing up CA keys;
- Controlling and managing CA Cryptographic Modules;
- System Backups and recovery;
- Changing recording media; and
- Posting Certificates and CRLs.

The individual with Access to the Private Keys SHALL NOT have security Audit responsibilities, nor be able to generate system Backups and recovery. The person who generates system Backups and recovery SHALL NOT have Access to the Private Keys, and SHALL NOT have security Audit responsibilities.

PCA Response: Will comply.

5.2.1.2 *CA Operations Staff*

The CA Operations Staff role is responsible for issuing Certificates. The CA SHALL maintain lists, including names, organizations, contact information, and organizational affiliation for those who act in CA Administrator, CA Operations Staff, and Security Auditor Trusted Roles.

PCA Response: Will comply.

The CA Operations Staff role includes:

- Managing operations of hosted CAs;
- Authenticating RAs;
- Executing the issuance of Certificates requested by the RA;
- Approving and executing Certificate Revocation requests;
- Approving Certificates issued to support the operations of the CA;
- Providing Certificate Revocation status information;
- Generating Certificate issuance reports; and
- Configuring Certificate profiles or templates.

5.2.1.3 *Security Auditor*

Security Auditors are responsible for internal Auditing of CAs and RAs. This sensitive role SHALL NOT be combined with any other sensitive role, e.g. the Security Auditor SHALL NOT also be part of the CA Operations Staff or CA Administrator. Security Auditors SHALL review, maintain, and Archive Audit logs, and perform or oversee internal Audits (independent of formal Compliance Audits) to ensure that CAs are operating in accordance with this CP.

PCA Response: Will comply.

5.2.1.4 *RA Staff*

RA Staff are the individuals holding Trusted Roles that operate and manage RA components. The RA SHALL maintain lists, including names, organizations, and contact information of those who act in RA Staff, RA Administrator, and RA Security Auditor Trusted Roles for that RA.

RA Staff is responsible for the following:

- Installation, configuration, and maintenance of RA equipment;
- Establishing and maintaining RA operating system and application accounts;
- Routine operation of the RA equipment such as system Backup and recovery or changing recording media;
- Registering new Subscribers and requesting the issuance of Certificates;
- Verifying the identity of Subscribers;
- Verifying the accuracy of information included in Certificates;
- Approving and executing the issuance of End-Entity Certificates;
- Requesting, approving, and executing Revocation of Certificates;
- Securely communicating requests to, and responses from, the CA; and
- Receiving and distributing Subscriber Certificates.

The RA SHALL ensure a separation of duties into Trusted Roles for critical RA functions to prevent an individual from maliciously using the RA system without detection. Each such Trusted Role's system Access is to be limited to those actions which they are REQUIRED to perform in fulfilling their responsibilities.

RA Response: Will comply.

5.2.2 Number of Persons Required per Task

Multi-person control procedures are designed to ensure that, at a minimum, two (2) Trusted Persons are present to gain either physical or logical Access to the CA. The CA SHALL enforce multi-person Access to CA Cryptographic Modules, from incoming receipt and inspection to final logical and/or physical destruction. Once a CA is activated with operational keys, further Access Controls SHALL be invoked to maintain split control over both physical and logical Access to the CA. Persons with physical Access to CA modules SHALL NOT hold credentials 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 Private Key activation; and
- CA Private Key Backup.

Where multi-person control is required, at least one of the PKI Participants SHALL be an administrator. The PKI Participants defined in Section 5.2.1 SHALL serve in a trusted role. Multi-person control SHALL NOT be achieved using personnel that serve in the Auditor Trusted Role.

PCA Response: <redacted response>.

5.2.3 Identification and Authentication for Each Role

Individuals assigned to Trusted Roles SHALL be appointed to the Trusted Role by an appropriate approving authority. Identity proofing of Trusted Roles SHALL be performed by the approving authority. The identity proofing of the RA SHALL be performed by the CA. Verification of identity SHALL include the personal (physical) presence of such personnel before human resources or other personnel performing security functions through either a face to face meeting or through a trusted video conferencing process approved by the PA and a check of well-recognized forms of identification, such as passports and driver's licenses. These appointments SHALL be annually reviewed for continued need and renewed if appropriate. The CA SHALL record the Trusted Role approvals in a secure and Auditable fashion. Individuals holding Trusted Roles SHALL accept the responsibilities of the Trusted Role, and the CA SHALL record this acceptance in a secure and Auditable fashion.

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 CA Facilities; and
- Given electronic credentials to Access and perform specific functions on CA systems.

CA equipment SHALL require, at a minimum, strong Authenticated Access Control for remote Access using multi-factor Authentication. Examples of multi-factor Authentication include: use of a password or PIN along with a time-based token, digital Certificate, or other device that enforces a policy of what a user has and what a user knows.

PCA Response: Will comply.

5.2.4 Roles Requiring Separation of Duties

An individual that performs any Trusted Role SHALL only have one identity when Accessing CA or RA equipment. The PCA, ICAs, and the corresponding RAs on their behalf SHALL have procedures to ensure that no user identity can assume multiple roles.

Roles requiring separation of duties include, but are not limited to:

- Acceptance, rejection, or other processing of Certificate Applications, Revocation requests, Renewal requests, or enrollment information;
- Issuance or Revocation of Certificates, including personnel having Access to restricted portions of the Repository;
- Generation of Backups;
- Generation, issuance, or destruction of a CA Certificate Private Key;
- Loading of a CA to a production environment; and
- Security Auditor role.

Role separation, when required as mentioned above, MAY be enforced by either the CA or RA equipment, or procedurally, or by both means.

PCA Response: <redacted response>.

RA Response: <redacted response>.

5.3 Personnel Controls

Personnel controls plays a critical role in the PKI's overall system security to prevent unauthorized Access to CA and RA systems and CA/RA operations.

5.3.1 Qualifications, Experience, and Clearance Requirements

Personnel seeking Trusted Roles SHALL present proof of the requisite qualifications and experience to perform their duties, or be provided the training needed, to perform their prospective job responsibilities competently and satisfactorily.

Individuals appointed to any Trusted Role SHALL:

- Have no other duties that would interfere or conflict with their responsibilities, as defined in Section 5.2.1;
- Have demonstrated the ability to perform their duties;
- If necessary, have successfully completed the appropriate training; and
- Have not been previously relieved of Trusted Role duties for reasons of negligence or non-performance of duties.

5.3.2 Background Check Procedures

The CA and RA SHALL select persons filling Trusted Roles on the basis of loyalty, trustworthiness, and Integrity, and SHALL subject the persons to a background investigation.

The CA and RA SHALL conduct background checks (in accordance with local Privacy laws) for the previous five (5) years, which MAY include a combination of the following:

- The person is an employee of, or contractor of, the CA or RA and is bound by terms of employment or contract;
- Confirmation of employment history;
- Check of previous places of residences over the past three (3) years;
- Check of professional reference;
- Confirmation of the highest or most relevant educational degree obtained;
- Search of criminal Records (local, state or provincial, and national);
- Search of driver's license Records;
- Identification verification (e.g., driver's license, passport); and
- Any other applicable procedures followed by a public safety agency for critical employees in the jurisdiction the CA/RA covers.

CAs and RAs SHALL have a process in place to ensure employees in Trusted Roles undergo background checks at least every ten (10) years.

PCA Response: <redacted response>.

RA Response: <redacted response>.

5.3.3 Training Requirements

The CA and RA SHALL provide their personnel with the training needed to perform their job responsibilities competently and satisfactorily. The CA and RA SHALL conduct training in the following areas:

- Basic PKI knowledge;
- Next Generation 9-1-1;
- Security principles and mechanisms;
- PKI hardware and software versions in use on the CA systems;
- PKI duties the Trusted Role is expected to perform;
- Disaster recovery and business continuity procedures; and
- Stipulations of this CP.

The CA and RA SHALL document the identity of all personnel who received training and the level of training completed.

PCA Response: Will comply.

RA Response: Will comply.

5.3.4 Retraining Frequency and Requirements

The CA and RA SHALL provide refresher training and updates, at least annually, for all individuals in Trusted Roles to ensure that such personnel maintain the required level of proficiency to perform their role. The CA and RA SHALL:

- Make individuals in Trusted Roles aware of changes in the operations of the PKI, this CP, or the CPS;
- Plan and document training for any significant change to the PKI operations, this CP, or the CPS and;
- Document the identity of all personnel who receive training and the level of training completed.

PCA Response: Will comply.

RA Response: Will comply.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

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

PCA Response: Will comply.

RA Response: Will comply.

5.3.7 Independent Contractor Requirements

The CA and RA MAY permit independent contractors or consultants to become Trusted Persons only to the extent necessary to accommodate clearly defined outsourcing needs. Contractors fulfilling Trusted Roles SHALL follow all personnel requirements stipulated in this CP and SHALL establish procedures to ensure that their duties are in accordance with this CP.

The CA SHALL escort independent contractors and consultants not fulfilling a Trusted Role and directly supervise them with Trusted Persons when they are given Access to the CA Facility, or CA and RA systems.

PCA Response: Will comply.

RA Response: Will comply.

5.3.8 Documentation Supplied to Personnel

The CA and RA SHALL make available to its personnel this CP, the corresponding CPS, and any relevant statutes, policies, or contracts needed for the Trusted Persons to perform their duties.

PCA Response: Will comply.

RA Response: Will comply.

5.4 Audit Logging Procedures

The CA and RA SHALL generate Audit log files for all events relating to the security of the CA and RA.

PCA Response: Will comply.

RA Response: Will comply.

5.4.1 Types of Events Recorded

The CA and RA SHALL include in each Audit Record the following information (either recorded automatically or manually for each Auditable event):

- The type of event;
- The date and time the event occurred;
- Success or failure; and
- The identity of the entity and/or person that caused the event.

The CA and RA SHALL enable all security Auditing capabilities of the CA and RA operating systems and applications to record the following events (where these events cannot be electronically logged, the CA and RA SHALL supplement the electronic Audit logs with physical logs as necessary):

Table 4: Auditable Events Recorded

Auditable Event	CA	RA
Physical Access to CA Facility:		
Personnel Access to room housing CA	X	
Access to the CA Server	X	
Known or suspected violations of physical security	X	
Any removal or addition of equipment to the CA enclosure	X	
System Configuration:		
Installation of the operating system	X	
Installation of the CA software	X	
Installation and removal of hardware Cryptographic Modules	X	
System startup	X	
Any security-relevant changes to the configuration of the CA	X	
CA hardware configuration	X	
System configuration changes and maintenance	X	
Cryptographic Module lifecycle management-related events (e.g., receipt, use, de-installation, and retirement)	X	
Account Administration:		
Roles and users are added or deleted	X	
The Access Control privileges of a user account or a role are modified	X	
Appointment of an individual to a Trusted Role	X	
Designation of personnel for multi-person control	X	
System administrator accounts	X	
Attempts to create, remove, set passwords or change the system privileges of the privileged users (Trusted Roles)	X	
Attempts to delete or modify Audit logs	X	
Changes to the value of maximum Authentication attempts	X	
Resetting operating system clock	X	
CA Operational Events:		
Key generation	X	
Start-up and shutdown of CA systems and applications	X	
Changes to CA details or keys	X	
Records of the destruction of media containing key material, Activation Data, or personal Subscriber information	X	
Successful and unsuccessful attempts to log into the CA system	X	

Auditable Event	CA	RA
The value of maximum Authentication attempts is changed	X	
Maximum unsuccessful Authentication attempts occur during user login	X	
A CA Administrator unlocks an account that has been locked as a result of unsuccessful Authentication attempts	X	
Attempts to set passwords	X	
Attempts to modify passwords	X	
End-Entity Certificate Lifecycle Events:		
Certificate Application requests		X
Certificate requests	X	X
Issuance	X	
Re-Key	X	X
Renewal	X	X
Certificate Revocation requests	X	X
Revocation	X	X
Trusted Person Events:		
Logon and logoff to the CA system	X	X
Attempts to create, remove, set passwords or change the system privileges of the privileged users	X	X
Unauthorized attempts to Access the CA system	X	X
Unauthorized attempts to Access system files	X	X
Failed read and write operations on the Certificate	X	
Personnel changes	X	X
Account Administrator Certificates	X	X
Data Events:		
Any attempt to delete or modify the Audit logs	X	X
All successful and unsuccessful requests for confidential and security-relevant Information	X	X

PCA Response: Will comply.

RA Response: Will comply.

5.4.2 Requirements for Time-Stamping of Audit Records

The CA and RA SHALL automatically time-stamp Audit Records as they are created. The CA and RA SHALL describe how system clocks used for time-stamping are maintained in synchrony with an authoritative time standard.

PCA Response: Will comply.

RA Response: Will comply.

5.4.3 Frequency of Processing Log

The CA SHALL review the Audit log at least once every sixty (60) days, unless the CA is offline, in which case the Audit logs SHALL be reviewed when the system is activated or every sixty (60) days, whichever is later.

The RA SHALL review its Audit logs at least once per quarter.

The CA and RA external Audit reviews SHALL involve verifying that the logs have not been tampered with, that there is no discontinuity or other loss of Audit Data, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs.

PCA Response: Will comply.

RA Response: Will comply.

5.4.4 Retention Period for Audit Log

The CA and RA SHALL retain Audit logs for at least ten (10) years and thereafter MAY be Archived.

The Security Auditor shall be only the entity who removes Audit logs from the CA system.

The CA and RA SHALL make all Audit logs, both electronic and non-electronic, available during a Compliance Audit.

PCA Response: Will comply.

RA Response: Will comply.

5.4.5 Protection of Audit Logs

The CA and RA SHALL protect Audit logs from unauthorized viewing, modification, deletion, or other tampering. CA and RA system configuration and procedures SHALL be implemented together to ensure that only authorized people Archive or delete Audit logs. The CA and RA SHALL implement procedures to protect Archived data from deletion or destruction.

System configuration and operational procedures SHALL be implemented together to ensure that:

- Only authorized personnel have read Access to the logs;
- Only authorized personnel MAY Archive Audit logs;
- Audit logs are not modified; and
- Audit logs are stored in a secure storage.

PCA Response: Will comply.

RA Response: Will comply.

5.4.6 Audit Log Backup Procedures

The CA and RA SHALL Backup their Audit logs and Audit summaries at least monthly, unless the CA is offline, in which case Audit logs and Audit summaries SHALL be backed up every time the system is activated, or at least every thirty (30) days.

PCA Response: Will comply.

RA Response: Will comply.

5.4.7 Audit Collection System (Internal vs. External)

The Audit log collection system MAY or MAY NOT be external to the CA or RA system.

Where possible, the CA and RA SHALL automatically collect Audit logs. Where this is not possible, the CA and RA SHALL use a logbook, paper form, or other physical mechanism. Automated Audit processes SHALL be invoked at system or application start-up, and cease only at system or application shutdown. Audit collection systems SHALL be configured such that the Audit log is protected against loss (e.g., overwriting or overflow of automated log files). Should it become apparent that an automated Audit system has failed; CA and RA operations SHALL be suspended until the Audit capability can be restored.

PCA Response: Will comply.

RA Response: Will comply.

5.4.8 Notification to Event-Causing Subject

This CP has no stipulation to notify the individual, organization, or device that caused an event that an event was Audited.

5.4.9 Procedures to Obtain and Verify Audit Log Information

After receiving a request made for a proper entity, its agent, or a party involved in a dispute over a transaction involving the PKI, the CA or RA MAY elect to retrieve the information from its Audit Log system. The CA or RA SHALL verify the Integrity of the Audit Log information. The CA or RA MAY elect to transmit the relevant information via a secure electronic method or courier.

PCA Response: Will comply.

RA Response: Will comply.

5.4.10 Vulnerability Assessments

The CA and RA SHALL perform routine self-assessments of security controls for vulnerabilities that identify and assess reasonably foreseeable internal and external Threats that could result in unauthorized Access, disclosure, misuse, alteration, or destruction of any Certificate data or Certificate issuance process. The CA and RA

SHALL perform their assessments, at least on an annual basis, as input into their annual Audit.

PCA Response: Will comply.

RA Response: Will comply.

5.5 Records Archival (Retention)

5.5.1 Types of Records Archived

Archived (or retained) Records SHALL be sufficiently detailed to determine that functions of the MA, CA, and RA have been properly executed. At a minimum, the following data SHALL be recorded and retained:

Table 5: Records Retention

Records to be Retained	CA	RA	MA
CP releases			X
CAs issued and key generation	X		
Export of CA Private Keys	X		
CPS reviews	X		X
Contractual obligations	X	X	X
Modifications and updates to CA system or configuration	X		
Subscriber identity verification data as per Section 3.2.3		X	
CRLs issuance	X		
Certificate issuance, Re-Key, Renew, and Revoke	X		
Audit logs	X	X	
Compliance Auditor reports	X		
Any attempt to delete or modify the Audit logs	X		
Remedial action taken as a result of violations of physical security	X		
Certificate request documentation		X	
Appointment of an individual to a Trusted Role	X	X	
Destruction of Cryptographic Modules	X		
Certificate Compromise notifications	X	X	

PCA Response: Will comply.

RA Response: Will comply.

MA Response: Will comply.

5.5.2 Retention Period for Archive

The CA, RA, and MA MUST keep Records for a minimum of ten (10) years and six (6) months.

PCA Response: Will comply.

RA Response: Will comply.

MA Response: Will comply.

5.5.3 Protection of Archive

The CA, RA, and MA SHALL protect the Records so that only the their authorized Trusted Persons are able to obtain Access to the Records. The Records SHALL be protected against unauthorized viewing, modification, deletion, or other tampering. The Recorded media and the applications required to process the Records SHALL be maintained to ensure that the Records can be Accessed for the retention time period.

PCA Response: Will comply.

RA Response: Will comply.

MA Response: Will comply.

5.5.4 Archive Backup Procedures

CAs and RAs compiling Records information SHALL incrementally back up the Records information at least on a weekly basis and perform full Backups at least on a monthly basis. Copies of paper-based Records SHALL be maintained in secure storage.

PCA Response: Will comply.

RA Response: Will comply.

5.5.5 Requirements for Time-Stamping of Records

The CA and RA SHALL automatically time-stamp Records as they are created. The CA and RA SHALL describe how system clocks used for time-stamping are maintained in synchrony with an authoritative time standard.

PCA Response: <redacted response>.

RA Response: <redacted response>.

5.5.6 Archive Collection System (Internal or External)

The CA SHALL collect Records information internally.

PCA Response: Will comply.

5.5.7 Procedures to Obtain and Verify Archive Information

After receiving a request made for a proper entity, its agent, or a party involved in a dispute over a transaction involving the PKI, the CA or RA MAY elect to retrieve the information from its Records system. The CA or RA SHALL verify the Integrity of the

Records information. The CA or RA MAY elect to transmit the relevant information via a secure electronic method or courier.

PCA Response: Will comply.

RA Response: Will comply.

5.6 Key Changeover

To minimize Risk from Compromise of a CA's Private Key, that key MAY be changed in accordance with the CPS. From that time on, only the new key will be used to sign Certificates. If the old Private Key is used to sign OCSP responder Certificates or CRLs that cover Certificates signed with that key, the old key MUST be retained and protected.

The CA's Private Key SHALL have a Validity Period as described in Section 6.3.2.and MAY be Re-Keyed at any time during its Validity Period, as per Section **Error! Reference source not found.**.

If an Intermediate CA is to be Re-Keyed, the Intermediate CA SHALL generate a new Public Key Pair and submit a CSR to the PCA to request its Intermediate CA Certificate. The Intermediate CA SHALL notify entities relying on its Certificate that its CA Certificate has been Re-Keyed. The PCA SHALL publish the issued CA Certificate in its Repository. The new Intermediate CA Private Key is used to re-sign all active End-Entity Certificates it has issued.

When the PCA Certificate is to be Re-Keyed, the PCA SHALL generate a new Key Pair and two key rollover Certificates:

- One key rollover Certificate where the new Public Key is signed by the old Private Key, indicating that this is the new PCA Public Key; and
- The other key rollover Certificate where the old Public Key is signed with the new Private Key, indicating that this is the old Public Key being replaced.

The new PCA Certificate will be available for download from the new PCA's Repository. The Relying Party will validate both Certificates and replace the old PCA Certificate with the published new PCA Certificate. This permits acceptance of newly issued Certificates and CRLs without distribution of the new self-signed Certificate to current users.

The new PCA Private Key is used to re-sign all existing active Intermediate CAs, which then issue new End-Entity Certificates. There is no need to re-sign existing active End-Entity Certificates, unless the Intermediate CA is also Re-Keyed.

PCA Response: Will comply.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

The CA and RA SHALL have an Incident Response Plan and a Disaster Recovery Plan (DRP).

If Compromise of a CA is suspected, the CA SHALL stop Certificate issuance and follow the procedures outlined in Section 5.7.3. The CA SHALL assess the scope of potential damage in order to determine appropriate remediation procedures.

In case of a CSS key Compromise, all Certificates issued to the CSS SHALL be Revoked and the Revocation information SHALL be published immediately in the most expeditious manner. Subsequently, the CSS SHALL be Re-Keyed.

The CA SHALL notify the MA, PA and (if applicable) ICA PA if any CAs operating under this CP experiences the following:

- Suspected or detected Compromise (including Compromise of the CA's Private Key) of the CA systems;
- Physical or electronic penetration of CA systems;
- Successful denial of service attacks on CA components;
- Any incident preventing the CA from issuing a CRL within twenty-four (24) hours of the issuance of the previous CRL; or
- Any incident preventing the CA from updating the CSS within fifteen (15) minutes of performing an operation on the CA.

The CA SHALL re-establish operational capabilities as quickly as possible.

PCA Response: <redacted response>.

RA Response: The RA maintains incident response procedures to guide personnel in response to security incidents, natural disasters, and similar events that may give rise to system Compromise. It reviews, tests, and updates its incident response plans and procedures on at least an annual basis.

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

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

- Notify the MA, PA and (if applicable) ICA PA and other CAs as soon as possible;
- Ensure that the system's Integrity has been restored prior to returning to operation and determine the extent of loss of data since the last point of Backup;
- Re-establish CA operations, giving priority to the ability to generate Certificate status information within the CSS and CRL issuance schedule;
- If the CA Private Keys are not destroyed, CA operation SHALL be re-established, giving priority to the ability to generate Certificate status information within the CSS and CRL issuance schedule;
- If the CA Private Keys are destroyed, re-establish CA operations as quickly as possible, giving priority to the generation of a new CA Key Pair;
- If the Integrity of the system cannot be restored, or if the Risk is deemed substantial, re-establish system Integrity before returning to operation;
- If a CA cannot issue a CRL prior to the time specified in the next update field of its currently valid CRL, then all CAs that have been issued Certificates by the CA

SHALL be securely notified immediately. This will allow other CAs to protect their Subscribers' interests as Relying Parties;

- If the CA cannot, within fifteen (15) minutes of corruption of computing resources, software, and/or data, correctly reflect the status of Certificates issued by the CA, then all CAs that have been issued Certificates by the CA SHALL be securely notified immediately. This will allow other CAs to protect their Subscribers' interests as Relying Parties; and
- If the ability to Revoke Certificates is inoperative or damaged, the CA SHALL re-establish Revocation capabilities as quickly as possible in accordance with procedures set forth in the respective CPS. If the CA's Revocation capability cannot be established in the time-frame specified in the CPS, the CA SHALL determine whether to request Revocation of its Certificate(s). If the CA is the PCA, the CA SHALL determine whether to notify all Subscribers using the CA as a Trust Anchor to delete the Trust Anchor.

PCA Response: <redacted response>.

5.7.3 Entity (CA) Private Key Compromise Procedures

If a CA's Private Keys are Compromised, lost, or suspected of Compromise, the CA SHALL:

- Notify the MA, PA and (if applicable) ICA PA immediately;
- Generate new keys;
- If the CA can obtain accurate information on the Certificates it has issued and that are still valid (i.e., not expired or Revoked), the CA MAY re-issue (i.e., Renew) those Certificates with the *notAfter* date in the Certificates remaining the same as in original Certificates; and
- If the CA is the PCA, it SHALL provide all Subscribers with the new Trust Anchor using secure means.

The CPS SHALL specify the maximum time during which these procedures MUST be completed.

PCA Response: <redacted response>.

5.7.3.1 *PCA Compromise Procedures*

In the case of the PCA Compromise, the CA SHALL notify the MA, PA, Relying Parties, and any cross-certified PKIs, of the PCA Compromise so that they MAY Revoke any Cross-Certificates issued to the PCA or any ICAs and notify all Subscribers and Relying Parties to remove the trusted self-signed Certificate from their trust stores. Notification SHALL be made in an Authenticated and trusted manner. Initiation of notification to the MA and PA and any cross-certified PKIs SHALL be made at the earliest feasible time, which SHALL NOT be longer than the time specified in the CPS, beyond the determination of Compromise or loss unless otherwise required by law enforcement. Initiation of notification to Relying Parties and Subscribers MAY be made after mediations are in place to ensure continued operation of applications and services. If the cause of the Compromise can be adequately addressed, and it is determined that the PKI can be securely re-established, the CA SHALL then generate a new PCA Certificate, solicit requests and issue new ICA Certificates, securely distribute the new PCA Certificate, and re-establish any Cross-Certificates.

PCA Response: <redacted response>.

5.7.3.2 *Intermediate CA Compromise Procedures*

In the event of an ICA key Compromise, the issuing CA SHALL notify the MA, PA, ICA PA (if applicable), and any lower level ICAs. The issuing CA SHALL Revoke the Compromised CA's Certificate, and the Revocation information SHALL be published immediately in the most expedient, Authenticated, and trusted manner after the notification. The Compromised CA SHALL also investigate and report to the MA, PA, ICA PA (if applicable) and any lower level ICAs what caused the Compromise or loss, and what measures have been taken to preclude recurrence. If the cause of the Compromise can be adequately addressed and it is determined that the CA can be securely re-established, then, the CA SHALL be re-established. Upon re-establishment of the CA, new Subscriber Certificates SHALL be requested and issued.

For ICAs, when a Subscriber Certificate is Revoked because of Compromise, suspected Compromise, or loss of the Private Key, a Revocation notice as specified in Section 4.9, SHALL be published at the earliest feasible time by the supporting CA after notification.

5.7.3.3 *CSS Compromise Procedures*

In case of a CSS key Compromise, the CA that issued the CSS a Certificate SHALL Revoke that Certificate, and the Revocation information SHALL be published immediately in the most expedient, Authenticated, and trusted manner. The CSS SHALL subsequently be Re-Keyed. If the CSS is self-signed and the CSS Certificate expiration is more than twenty-four (24) hours away, the CA SHALL immediately notify the MA, PA, Relying Parties, and any cross-certified PKIs of the CSS Compromise so that they can notify all Subscribers and Relying Parties to remove trust in the CSS Certificate from each Relying Party application, and install the Re-Keyed Certificate.

PCA Response: <redacted response>.

5.7.3.4 *RA Compromise Procedures*

In case of a RA Compromise, the CA SHALL disable the RA. In the case that a RA's key is Compromised, the CA that issued the RA Certificate SHALL Revoke it, and the Revocation information SHALL be published in the most expedient, Authenticated, and trusted manner. The Compromise SHALL be investigated by the CA in order to determine the actual or potential date and scope of the RA Compromise. All Certificates approved by that RA since the date of actual or potential RA Compromise SHALL be Revoked. In the event that the scope is indeterminate, then the CA Compromise procedures in Section 5.7.3.2 SHALL be followed.

PCA Response: <redacted response>.

5.7.4 Business Continuity Capabilities after a Disaster

The CA and RA SHALL develop, test, and maintain a DRP designed to mitigate the effects of any kind of natural or man-made disaster. The DRP 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. The CA SHALL provide an alternate secure facility that conforms to all the provisions of the present document for resumption of the CA following any CA service interruption.

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;
- Publication of Revocation information; and
- CA Private Key Compromise.

The disaster recovery equipment SHALL have physical security protections comparable to the production CA system.

The CA SHALL have the ability to fully test its abilities under this section. The CPS SHALL specify a minimum time period where this capability SHALL be demonstrated.

PCA Response: <redacted response>.

RA Response: <redacted response>.

5.8 CA or RA Termination

When a CA operating under this CP terminates operations before all Certificates have expired, entities SHALL be given as much advance notice as circumstances permit.

Prior to CA termination, and in coordination with the MA, the CA SHALL:

- Provide notice to all cross-certified CAs and request Revocation of all Certificates issued to it;
- Issue a CRL revoking all unexpired Certificates prior to termination. This CRL SHALL be available until all Certificates issued by the CA expire;
- Archive all Audit logs and other Records prior to termination;
- Destroy all Private Keys upon termination;
- Archive Records SHALL be transferred to an appropriate authority specified in the CPS; and
- If the PCA is terminated, use secure means to notify the Subscribers to delete all Trust Anchors representing the terminated CA.

Before terminating RA activities, the RA SHALL:

- Provide notice and information about the termination by sending notice by email to Subscribers, Relying Parties, and cross-certifying entities and by posting such information on its web site; and
- Transfer all responsibilities to a successor designated by the MA.

PCA Response: Will comply.

RA Response: Will comply.

PCA PA Response: Prior to its termination, the PCA being terminated SHALL transfer its Archive Records to the PCA PA.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

CAs SHALL generate Key Pairs using at a minimum the FIPS 140-2 Level described in Table 6 for the hardware Cryptographic Modules and Key Pair generation processes that provide the required cryptographic strength of the generated keys and prevent the loss, disclosure, Modification, or unauthorized use of Private Keys.

Table 6: Key Pair Generation

Entity	Minimum FIPS 140-2 Level	Hardware Or Software	Key Storage Restricted To the Module on Which the Key was Generated
PCA	3	Hardware	Yes
ICA	2 or higher	Hardware	Yes
CSS	2 or higher	Hardware	Yes
End-Entity	1 or higher	Hardware or Software	No stipulation

PCA Response: Will comply.

6.1.1.1 *CA Key Pair Generation*

CAs SHALL generate CA Key Pairs in a Key Generation Ceremony, using multi-person control, and HSMs validated to the minimum FIPS level specified above. The CA's Key Pair generation MUST create a verifiable Audit trail demonstrating that the security requirements for the procedure was followed. The CA's documentation of the procedure MUST show that appropriate role separation was used. A witness SHALL validate the execution of the key generation procedures by witnessing the key generation and examining the signed and documented Record of the key generation.

PCA Response: Will comply.

6.1.1.2 *Subscriber Key Pair Generation*

Subscribers SHALL perform Key Pair generation by using a FIPS-approved method or equivalent international standard and either a validated hardware or software Cryptographic Module, as shown in Table 6. Subscribers SHALL generate the random numbers and parameters used for key generation material by a FIPS-approved method or equivalent international standard.

6.1.1.3 *CSS Key Pair Generation*

CAs SHALL generate the cryptographic keying material used by CSSs to sign CRLs or OCSP status information in [FIPS 140-2] Level 2 (or higher) validated Cryptographic Modules.

PCA Response: Will comply.

6.1.2 Private Key Delivery to Subscribers

Subscribers SHALL generate their own Key Pairs, so there is no stipulation for delivering Private Keys to Subscribers.

6.1.3 Public Key Delivery to Certificate Issuer

The Subscriber SHALL deliver the Public Key to the RA in a PKCS #10 CSR file, or an equivalent method ensuring that the Public Key has not been altered during transit. The RA SHALL verify the Subscriber's identity and Authenticate the delivery of the Subscriber's Public Key to the RA. The RA Authenticates to the CA's Certificate issuance portal and sends the Public Key CSR file to the CA to request a Certificate on behalf of the Subscriber.

RA Response: Will comply.

6.1.4 CA Public Key Delivery to Relying Parties

The CA SHALL provide their CA Public Key Certificate to Relying Parties in a secure manner to preclude substitution attacks. Acceptable methods for secure delivery are:

- Secure distribution of CA Certificates through secure Out-of-Band mechanisms; and
- Downloading the CA Certificate from trusted websites.

PCA Response: The PCA provides CA Public Key Certificates to Relying Parties via secure communication via the RA or through its PCA Repository.

6.1.5 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.

PCA Certificates SHALL meet or exceed the following requirements for key size:

Table 7: Key Sizes

Certificate	Key Size
PCA Certificate	4096 – bit RSA
ICA Certificate	3072 – bit RSA
CSS Certificate	2048 – bit RSA
End-Entity Authentication Certificate	2048 – bit RSA
End-Entity Signing Certificate	256 – bit ECC

PCA Response: Will comply.

6.1.6 Public Key Parameters Generation and Quality Checking

Public Key parameters SHALL always be generated and validated in accordance with [FIPS 186-4]. RAs SHALL only use CSRs containing a Public Key that meets the required key sizes for the requested Certificate.

RA Response: Will comply.

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

The use of a specific key is constrained by the *keyUsage* extension in the X.509 Certificate.

The extended key usage SHALL meet the requirements stated in Section 7.1.2. *extKeyUsage* OIDs SHALL be consistent with *keyUsage* bits asserted.

PCA Response: Will comply.

6.1.7.1 *keyUsage Extension for CA Certificates*

Table 8 shows the specific *keyUsage* extension settings for CA Certificates (i.e., the PCA and ICAs) and specifies that all CA Certificates:

- SHALL include a *keyUsage* extension;
- SHALL set the criticality of the *keyUsage* extension to TRUE;
- SHALL assert the *digitalSignature* bit.
- SHALL assert the *nonRepudiation* bit.
- SHALL assert the *keyCertSign* bit; and
- SHALL assert the *cRLSign* bit.

Table 8: *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)		1	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

PCA Response: Will comply.

6.1.7.2 *keyUsage Extension for all End-Entity Device Certificates*

Table 9 shows the specific *keyUsage* extension settings for End-Entity device Certificates and specifies that all End-Entity device Certificates:

- SHALL include a *keyUsage* extension;
- SHALL set the criticality to TRUE; and
- SHALL set the *digitalSignature, nonRepudiation, keyEncipherment, and keyAgreement* bits.

Table 9: *keyUsage* Extension for all End-Entity Certificates

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

6.2 Private Key Protection and Cryptographic Module Engineering Controls

Private Key holders SHALL take necessary precautions to prevent the loss, disclosure, Modification, or unauthorized use of such Private Keys in accordance with this section of the CP.

6.2.1 Cryptographic Module Standards and Controls

Table 6, in Section 6.1.1, summarizes the minimum requirements for Cryptographic Modules; higher levels MAY be used. In addition, Private Keys SHALL NOT exist outside the Cryptographic Module in plaintext form.

PCA Response: Will comply.

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

A single person SHALL NOT be permitted to activate or Access any Cryptographic Module that contains the complete CA Private Key. CA Private Keys SHALL be backed up only under multi-person control. Access to CA Private Keys backed up for disaster recovery SHALL be under multi-person control.

PCA Response: Will comply.

6.2.3 Private Key Escrow

No stipulation.

6.2.4 Private Key Backup

6.2.4.1 ***Backup of CA Private Keys***

The CA Private Keys SHALL be transported and backed up under the same multi-person control as the original Private Key. At least one copy of the Private Key SHALL be stored off-site. All copies of the CA Private Key SHALL be accounted for and protected in the same manner as the original.

PCA Response: Will comply.

6.2.4.2 ***Backup of Subscriber Private Keys***

Subscriber Private Keys MAY be backed up or copied, but SHALL be held under the control of the Subscriber or other authorized administrator. Subscriber backed up Private Keys SHALL NOT be stored in plaintext format outside the Cryptographic Module. Storage SHALL ensure security controls consistent with the protection provided by the Certificate's Cryptographic Module.

6.2.5 Private Key Archival

The PCA, ICAs, and Subscribers SHALL NOT Archive Private Keys.

PCA Response: Will comply.

6.2.6 Private Key Transfer into or from a Cryptographic Module

PCA and ICA Private Keys MAY be exported from the Cryptographic Module only to perform CA key Backup procedures as described in Section 6.2.4.1. At no time SHALL the CA Private Key exist in plaintext form outside the Cryptographic Module.

In the event that a Private Key is to be transported from one Cryptographic Module to another, the Private Key MUST be encrypted during transport; Private Keys MUST 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.

PCA Response: <redacted response>.

6.2.7 Private Key Storage on Cryptographic Module

No stipulation beyond that specified in [FIPS 140-2] (or equivalent standard).

PCA Response: Will comply.

6.2.8 Method of Activating Private Key

Subscribers MUST be Authenticated to the Cryptographic Module before the activation of their 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 (i.e., the data SHOULD NOT be displayed while it is entered).

A device MAY be configured to activate its Private Key without requiring Activation Data, provided that appropriate physical and logical Access Controls are implemented for the device and its Cryptographic Module. The Device's PKI Sponsor SHALL be responsible for ensuring that the system has security controls commensurate with the level of Threat in the device's environment. These controls SHALL protect the device's hardware, software, and the cryptographic token and its Activation Data from Compromise.

The PCA and all ICAs SHALL protect the Activation Data for their Private Keys against loss, theft, Modification, disclosure, or unauthorized use.

PCA Response: Will comply.

6.2.8.1 *CA Administrator Activation*

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

- Use of a smart card, Biometric Access device, and/or password in accordance with Section 6.4.1, or security of equivalent strength to Authenticate the CA Administrator before the activation of the Private Key; and
- Commercially reasonable measures for the physical protection of the CA Administrator's workstation to prevent use of the workstation and its associated Private Key without the CA Administrator's authorization.

PCA Response: The CA Administrator is activated according to the above activation requirements. Activation Data entry is protected from disclosure.

6.2.8.2 *Offline CAs Private Key*

Once the CA system has been activated, a threshold number of Multi-Person Private Key holders SHALL be REQUIRED to supply their Activation Data in order to activate an offline CA's Private Key, as defined in Section 6.2.2. Once the Private Key is activated, it SHALL only be active until termination of the session.

PCA Response: Will comply.

6.2.8.3 *Online CAs Private Keys*

An online CA's Private Key SHALL be activated by a threshold number of Multi-Person Private Key holders, as defined in Section 6.2.2, 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.

6.2.9 Method of Deactivating Private Key

After use, Private Key holders SHALL deactivate the Cryptographic Module, e.g., via a manual logout procedure or automatically after a period of inactivity. When deactivated, Private Keys SHALL be kept in encrypted form only. Private Keys SHALL be cleared from memory before the memory is de-allocated. Any disk space where Private Keys were stored SHALL be overwritten before the space is released to the operating system. CA and CSS Cryptographic Modules SHALL be stored in a secure container when not in use.

PCA Response: <redacted response>.

6.2.10 Method of Destroying Private Key

Private Key holders SHALL 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.

CA Private Key destruction procedures SHALL be sufficient to ensure that it is impossible to recover any part of the Private Key from any Cryptographic Module, memory or disk space.

If proper destruction of a Private Key cannot be guaranteed, then the key SHALL be treated as Compromised and its corresponding Public Key Certificate Revoked.

PCA Response: <redacted response>.

6.2.11 Cryptographic Module Rating

See Section 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

The Public Key is Archived as part of the Certificate archival described in Section 5.5.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The usage period for the PCA Key Pair is a maximum three (3) years. For ICAs operating under this CP, the usage period for a CA Key Pair is a maximum of three (3) years. The CA Private Key MAY be used to sign Certificates for at most three (3) years, but MAY be used to sign CRLs and Certificates for the entire usage period.

To minimize Risk from Compromise of a CA's Private Key, that key MAY be changed often; from that time on, only the new key SHALL be used for Certificate signing purposes. The older, but still valid, Certificate will be available to verify old signatures until all the Certificates signed using the associated Private Key have also expired. If the old Private Key is used to sign OCSP responder Certificates or CRLs, then the old key SHALL be retained and protected.

When a CA updates its Private Key and thus generates a new Public Key, the CA SHALL notify all CAs and Subscribers that rely on the CA's Certificate that it has been changed.

Table 10 provides the lifetimes for the Private Keys and Certificates issued to the owner of that Private Key.

Table 10: Certificate Validity Periods

Certificate	Certificate Validity	Key Validity Period
PCA	Up to 3 Years	3 years
Intermediate CA	Up to 3 Years	3 years
End-Entity Authentication Certificates	Up to 3 Years	3 years
End-Entity Signing Certificates	Up to 3 Years	10 years

Validity Periods SHALL be nested such that the Validity Periods of issued Certificates SHALL be contained within the Validity Period of the issuing CA. In other words, CAs SHALL NOT issue Certificates that extend beyond the expiration date of their own Certificates and Public Keys. All Certificates signed by a specific CA Key Pair MUST expire before the end of that Key Pair's usage period. There is a difference between the Certificate Validity Period and the Key Validity Period. The Validity Period of the Certificate indicates a period for which the Public Key bound to the Certificate may be used. The key Validity Period indicates the usage period for the Private Key, which is dependent on key size and usage.

ICA CPSs SHOULD NOT allow End-Entity Certificates to have a Validity Period of over one (1) year, and SHOULD limit End-Entity Certificate validity to no more than three (3) months. Where an ICA CPS provides for End-Entity Certificates that are valid for more than one (1) year, the CPS SHALL justify the purposes for a longer Validity Period.

PCA PKI Participants SHALL cease all use of their Private Key Pairs after their Validity Period has expired.

Notwithstanding the above table, in all cases the CA Private Key MAY be used to sign OCSP responder Certificates (if applicable) and CRLs until the CA Certificate expires.

PCA Response: Will comply.

PCA PA Response: The PCA key validity period and certificate validity are both three (3) years.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Private Key holders SHALL use Activation Data to unlock Private Keys, in conjunction with any other Access Control, which have an appropriate level of strength for the keys or data to be protected and SHALL meet the applicable Security Policy requirements of the Cryptographic Module used to store the keys. Two-factor Authentication SHALL be used to Authenticate users prior to unlocking Private Keys. To the extent passwords are used as Activation Data, the PCA's and ICAs' activation participants SHALL generate passwords that cannot easily be guessed or cracked. Participants MAY NOT need to generate Activation Data, for example, if they use Biometric Access devices.

CAs SHALL either entail the use of Biometric data or satisfy the policy-enforced at/by the Cryptographic Module. If the CA MUST transmit Activation Data, it SHALL be via an appropriate protected channel, and distinct in time and place from the associated Cryptographic Module. The CA SHALL change its Activation Data upon CA Re-Key.

RA and Subscriber Activation Data MAY be user-selected. The strength of the Activation Data SHALL meet or exceed the requirements for Authentication mechanisms stipulated for Level 1 or higher in [FIPS 140-2], or some other equivalent standard. If the Activation Data MUST be transmitted, it SHALL be via an appropriately protected channel, and distinct in time and place from the associated Cryptographic Module.

PCA Response: <redacted response>.

6.4.2 Activation Data Protection

Private Key holder Activation Data used to unlock Private Keys SHALL be protected from disclosure by a combination of cryptographic and physical Access Control mechanisms, such as:

- Memorization;
- Biometric in nature; or
- Recorded and secured at the level of assurance associated with the activation of the Cryptographic Module, and SHALL NOT be stored with the Cryptographic Module.

In all cases, the protection mechanism implemented by Private Key holders SHALL include a facility to temporarily lock the account, or terminate the application, after a predetermined number of failed login attempts.

PCA Response: Will comply.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

CA computer security functions SHALL:

- Require Authenticated logins;
- Require users to select strong passwords;
- Provide Security Audit capability;
- Lock the Access to CA services after a determined amount of unsuccessful login attempts;
- Restrict Access Control to CA services;
- Enforce separation of duties for Trusted Roles;
- Require identification and Authentication of Trusted Roles;
- Archive history and Audit Data;

- Employ malicious code protection mechanisms to mitigate the Risk of malicious code on CA system components;
- Employ technical and procedural controls to prevent and detect unauthorized changes to firmware and software on CA systems;
- Require Backups for recovery of keys and the CA system; and
- Enforce domain Integrity boundaries for security critical CA processes.

RA computer security functions SHALL:

- Require Authenticated logins;
- Require users to select strong passwords;
- Provide Security Audit capability;
- Lock Access to RA services after a determined amount of unsuccessful login attempts;
- Restrict Access Control to RA services;
- Enforce separation of duties for Trusted Roles;
- Require identification and Authentication of Trusted Roles; and
- Archive history and Audit Data.

The CA and RA functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards.

PCA Response: Will comply.

RA Response: Will comply.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The system development controls address various aspects related to the development and change of the PCA and ICA systems through aspects of its life-cycle. The system development controls for CAs SHALL:

- Use software that has been designed and developed under a formal, documented development methodology;
- Procure hardware and software in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase);
- Develop hardware and software in a controlled and documented environment to demonstrate that security requirements were achieved through a combination of software verification & validation, structured development approach, and controlled development environment;
- Deliver all hardware and software via controlled methods that provide a continuous chain of accountability from the purchase location to the operations location;

- Dedicate hardware and software to performing PKI activities;
- Prevent malicious software from being loaded onto the equipment by implementing and testing in a non-production environment prior to implementation in a production environment.
- Obtain applications required to perform PKI operations from sources authorized by local policy.
- Scan CA hardware and software for malicious code on first use and periodically thereafter; and
- Purchase or develop hardware and software updates in the same manner as original equipment, and installed using trusted and trained personnel.

PCA Response: Will comply.

6.6.2 Security Management Controls

A list of acceptable products and their versions for each individual PCA and ICA system component SHALL be maintained and kept up-to-date within a configuration management system.

To reduce the available attack surface of a CA system, only those ports, protocols, and services that are necessary to the CA system architecture are permitted to be installed or operating. The CA system SHALL maintain a list of ports, protocols, and services that are necessary for the correct function of each component within the CA system.

The configuration of the CA system, in addition to any modifications and upgrades, SHALL be documented and controlled. 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.

The CA system SHALL provide a mechanism to periodically verify the Integrity of the software.

The CA SHALL also have mechanisms and policies in place to control and monitor the configuration of the CA system.

PCA Response: Will comply.

6.6.3 Life Cycle Security Controls

The PCA and ICAs SHALL have a plan for receiving notification of software and firmware updates, for obtaining and testing those updates, for deciding when to install them, and finally for installing them without undue disruption. A log SHALL be kept of the notifications, the decision to apply/not apply including reason, and the application of relevant updates/patches.

From time to time, the CA MAY discover errors in configuration files, either because of human error, source data error, or changes in the environment which have made an entry erroneous. The CA SHALL correct such errors and document the reason for the error, and the associated correction. In the event a vulnerability is detected with a rated severity value of 9 or higher on the US-CERT CVSS 3.1 [CVSS] rating scale, remediation SHALL be effected within 45 days after patch availability.

Remediation activities SHOULD NOT cause unavailability of Revocation information.

PCA Response: Will comply.

6.7 Network Security Controls

Many components of a CA are connected to each other and their customers via various forms of networks. While it is necessary for connections to customers and administrative systems, care needs to be taken to ensure those connections do not adversely impact the security of those components. Guidelines for effective CA networking security are discussed in the following sections.

The CPS SHALL describe how network security is configured and validated.

PCA Response: <redacted response>.

6.7.1 Isolation of Networked Systems

The PCA and its Private Keys SHALL be offline.

Communication channels between the network-connected ICA components and the trusted CA processing components SHALL be protected against attack. Furthermore, information flowing into these CA components from the network-connected CA components SHALL NOT lead to any Compromise or disruption of these components.

The components of a CA requiring direct network connections SHALL be minimized. Those networked components SHALL be protected from attacks by adequate means to filter unwanted protocols (utilizing Access rules, whitelists, blacklists, protocol checkers, etc., as necessary). Data loss prevention tools SHALL be employed to detect inappropriate leakage of sensitive information. Such components SHOULD be secure without the use of a Firewall.

PCA Response: Will comply.

6.7.2 Boundary Protection

Any boundary control devices used to protect a CA's Repository or CA's local area network SHALL deny all but the necessary services to the PKI equipment even if those services are enabled for other devices on the network.

The PCA and ICAs, the RAs on their behalf, Repositories, remote workstations used to administer the CAs, and CSS 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.

PCA Response: Will comply.

RA Response: Will comply.

6.7.2.1 *Transmission Confidentiality*

Intra-CA communications that cross the physical protection barrier of the Certificate signing portion of a CA system SHALL be Confidentiality-protected. Services used by a CA system that are not administered by its CA Administrator SHALL provide protection commensurate with this CP.

Confidentiality of Subscriber data SHALL be maintained as negotiated between the RA and the Subscriber or the Subscriber's organization.

PCA Response: Will comply.

RA Response: Will comply.

6.7.3 Network Monitoring

The CA SHALL monitor the CA system to detect attacks and indicators of potential attacks.

PCA Response: Will comply.

6.8 Time-Stamping

Certificates, CRLs, and other Revocation database entries SHALL contain time and date information.

Asserted times SHALL be accurate to within 100ms. Electronic or manual procedures MAY be used to maintain system time. Clock adjustments are Auditable events (see Section 5.4.1).

All CA components SHALL regularly synchronize with a time service such as National Institute of Standards and Technology (NIST) Atomic Clock or NIST Network Time Protocol Service, a master clock it operates, or is operated by a public safety entity. Time derived from the time service SHALL be used for establishing the time of:

- Initial validity type of a Certificate;
- Revocation of a Certificate;
- Posting of CRL updates; and
- OCSP responses.

PCA Response: Will comply.

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

Certificates issued by a CA under this CP SHALL conform to [RFC 5280] Internet X.509 Public Key Infrastructure Certificate and CRL Profile, May 2008.

CA Certificates SHALL contain the identity and attribute data of a Subject using the base Certificate with applicable extensions. The base Certificate SHALL contain the version number of the Certificate, the Certificate's identifying serial number, the signature algorithm used to sign the Certificate, the issuer's DN, the Validity Period of the Certificate, the Subject's DN, information about the Subject's Public Key, and extensions (See Table 11).

Table 11: Certificate Profile Basic Fields

Field	[RFC 5280] Section	Requirement or Recommendation
tbsCertificate	4.1.1.1	Follows [RFC 5280] guidance
version	4.1.2.1	See CP Section 0.
serialNumber	4.1.2.2	SHALL be a unique positive integer assigned by the CA and SHALL NOT be longer than 20 octets.
signature	4.1.2.3	See CP Section 7.1.3.
issuer	4.1.2.4	See CP Section 3.1.1.
validity	4.1.2.5	See CP Section 6.3.2.
subject	4.1.2.6	See CP Section 7.1.4.
subjectPublicKeyInfo	4.1.2.7	See CP Section 7.1.3.
extensions	4.1.2.9	See CP Section 7.1.2.
signatureAlgorithm	4.1.1.2	Follows [RFC 5280] guidance
algorithmIdentifier	4.1.1.2	See CP Section 7.1.3.
algorithm	4.1.1.2	See CP Section 7.1.3.
parameters	4.1.1.2	See CP Section 7.1.3.
signatureValue	4.1.1.3	Follows [RFC 5280] guidance

PCA Response: Will comply.

7.1.1 Certificate Version Number(s)

The PCA and ICAs SHALL issue X.509 v3 Certificates. The CA SHALL set the Certificate version number to the integer value of "2" to designate a version 3 Certificate.

PCA Response: Will comply.

7.1.2 Certificate Extensions

CA Certificate extensions provide methods for associating additional attributes with Public Keys and for managing relationships between CAs. CA Certificates SHALL follow the guidance in [RFC 5280] and SHALL contain the standard extensions shown in the tables below, unless they are denoted as optional.

PCA Response: Will comply with all requirements in the tables and sub-sections below.

7.1.2.1 ***Standard Extension for PCA Certificates***

Table 12 shows the Certificate extensions for all PCA Certificates.

Table 12: PCA Certificate Standard Extensions

Field	Referenced Standard	Section	Requirement or Recommendation
basicConstraints	[RFC 5280]	4.2.1.9	SHALL be included in PCA Certificate. Criticality SHALL be set to TRUE.
keyUsage	[RFC 5280]	4.2.1.3	SHALL be included in PCA Certificate. Criticality SHALL be set to TRUE.
subjectAltName	[RFC 5280]	4.2.1.6	MAY be included in PCA Certificate. Criticality SHALL be set to FALSE.
subjectKeyIdentifier	[RFC 5280]	4.2.1.2	SHALL be included in PCA Certificate. Criticality SHALL be set to FALSE.

7.1.2.2 ***Standard Extension for ICA Certificates***

Table 13 shows the Certificate extensions for all ICA Certificates.

Table 13: ICA Certificate Standard Extensions

Field	Referenced Standard	Section	Requirement or Recommendation
authorityInformationAccess	[RFC 5280]	4.2.2.1	SHALL be included in ICA Certificates. Criticality SHALL be set to FALSE.
authorityKeyIdentifier	[RFC 5280]	4.2.1.1	SHALL be included in ICA Certificates. Criticality SHALL be set to FALSE.
basicConstraints	[RFC 5280]	4.2.1.9	SHALL be included in ICA Certificates. Criticality SHALL be set to TRUE.
certificatePolicies	[RFC 5280]	4.2.1.4	MAY be included in ICA Certificates. Criticality SHALL be set to FALSE.
crlDistributionPoints	[RFC 5280]	4.2.1.13	SHALL be included in all ICA Certificates. Criticality SHALL be set to FALSE.
keyUsage	[RFC 5280]	4.2.1.3	SHALL be included in ICA Certificates. Criticality SHALL be set to TRUE.
subjectAltName	[RFC 5280]	4.2.1.6	MAY be included in ICA Certificates. Criticality SHALL be set to FALSE.
subjectKeyIdentifier	[RFC 5280]	4.2.1.2	SHALL be included in ICA Certificates. Criticality SHALL be set to FALSE.

7.1.2.3 *Standard Extensions for End-Entity Certificates*

Table 14 shows the Certificate extensions for all End-Entity Certificates.

Table 14: End-Entity Certificate Standard Extensions

Field	Referenced Standard	Section	Requirement or Recommendation
authorityInformationAccess	[RFC 5280]	4.2.2.1	SHALL be included in End-Entity Certificates. Criticality SHALL be set to FALSE
authorityKeyIdentifier	[RFC 5280]	4.2.1.1	SHALL be included in End-Entity Certificates. Criticality SHALL be set to FALSE.
certificatePolicies	[RFC 5280]	4.2.1.4	MAY be included in End-Entity Certificates. Criticality SHALL be set to FALSE.
crlDistributionPoints	[RFC 5280]	4.2.1.13	SHALL be included in End-Entity Certificates. Criticality SHALL be set to FALSE.
extKeyUsage	[RFC 5280]	4.2.1.12	SHALL be included in End-Entity Certificates. Criticality SHALL be set to TRUE in End-Entity Certificates.
keyUsage	[RFC 5280]	4.2.1.3	SHALL be included in End-Entity Certificates. Criticality SHALL be set to TRUE.
subjectAltName	[RFC 5280]	4.2.1.6	SHALL be included in End-Entity Certificates. Criticality SHALL be set to FALSE.
subjectKeyIdentifier	[RFC 5280]	4.2.1.2	SHALL be included in End-Entity Certificates. Criticality SHALL be set to FALSE.

7.1.2.4 *Authority Information Access Extension*

The *authorityInformationAccess* extension indicates how to Access OCSP information for the Certificate issuer.

Table 15 shows the *authorityInformationAccess* extension settings for ICA Certificates and specifies that all ICA Certificates:

- SHALL include the *authorityInformationAccess* extension;
- SHALL set the criticality of the *authorityInformationAccess* extension to FALSE;
- SHALL set the *accessMethod* OID to 1.3.6.1.5.5.7.48.1 for OCSP; and
- SHALL set the *accessLocation* to the URL of the OCSP responder.

Table 15: *authorityInformationAccess* Extension for ICA Certificates

Field	Format	Criticality	Value	Comment
authorityInformationAccess		FALSE	{ id-pe 1 }	Included in all ICA Certificates.
accessMethod	OID		1.3.6.1.5.5.7.48.1	OCSP {id-pkix-ocsp}
accessLocation	General Name		URL	Address of the OCSP responder

Table 16 shows the *authorityInformationAccess* extension settings for End-Entity Certificates and specifies that all End-Entity Certificates:

- SHALL include the *authorityInformationAccess* extension;
- SHALL set the criticality of the *authorityInformationAccess* extension to FALSE;
- SHALL set the *accessMethod* OID to 1.3.6.1.5.5.7.48.1 for OCSP; and
- SHALL set the *accessLocation* to the URL of the OCSP responder.

Table 16: *authorityInformationAccess* Extension for End-Entity Certificates

Field	Format	Criticality	Value	Comment
authorityInformationAccess		FALSE	{ id-pe 1 }	Included in all End-Entity Certificates.
accessMethod	OID		1.3.6.1.5.5.7.48.1	OCSP {id-pkix-ocsp}
accessLocation	General Name		URL	Address of the OCSP responder

7.1.2.5 *Authority Key Identifier Extension*

The *authorityKeyIdentifier* extension provides a means to identify the identity of the Public Key corresponding to the Private Key used to sign a Certificate.

Table 17 shows the *authorityKeyIdentifier* extension settings for ICA Certificates and specifies that all ICA Certificates:

- SHALL include the *authorityKeyIdentifier* extension;
- SHALL set the criticality of the *authorityKeyIdentifier* extension to FALSE; and
- SHALL calculate the *keyIdentifier* of the *authorityKeyIdentifier* per Method 1.

Table 17: *authorityKeyIdentifier* Extension for ICA Certificates

Field	Format	Criticality	Value	Comment
authorityKeyIdentifier		FALSE	{ id-ce 35 }	Included in all ICA Certificates.
keyIdentifier	OCTET STRING		<keyIdentifier>	Calculated per Method 1

Table 18 shows the *authorityKeyIdentifier* extension settings for End-Entity Certificates and specifies that all End-Entity Certificates:

- SHALL include the *authorityKeyIdentifier* extension;
- SHALL set the criticality of the *authorityKeyIdentifier* extension to FALSE; and
- SHALL calculate the *keyIdentifier* of the *authorityKeyIdentifier* per Method 1.

Table 18: *authorityKeyIdentifier* Extension for End-Entity Certificates

Field	Format	Criticality	Value	Comment
authorityKeyIdentifier		FALSE	{ id-ce 35 }	Included in all End-Entity Certificates.
keyIdentifier	OCTET STRING		<keyIdentifier>	Calculated per Method 1

7.1.2.6 *Basic Constraints Extension*

The *basicConstraints* extension identifies whether the Subject of a Certificate is a CA and the maximum depth of valid certification paths that include the Certificate.

NOTE: The *pathLenConstraint* field gives the maximum number of ICA Certificates that MAY follow this Certificate in the certification path. A value of 0 indicates that only an End-Entity Certificate MAY follow in the path. If the *pathLenConstraint* value is set, it has to be greater than or equal to 0. If it is not set, then the certification path MAY be of any length.

Table 19 shows the *basicConstraints* extension settings for Root CA Certificates (for example, the PCA) and specifies that all Root CA Certificates:

- SHALL include the *basicConstraints* extension;
- SHALL set the criticality of the *basicConstraints* extension to TRUE;
- SHALL set the cA field of the *basicConstraints*; and
- SHALL set the *pathLenConstraint* field of the *basicConstraints* to “None”.

Table 19: *basicConstraints* Extension for Root CA Certificates

Field	Format	Criticality	Value	Comment
basicConstraints		TRUE	{ id-ce 19 }	Included in all Root CA Certificates.
cA	BOOLEAN		TRUE	Set
pathLenConstraint	INTEGER		None	Not Set

Table 20 shows the *basicConstraints* extension settings for Tier-2 ICA Certificates and specifies that all ICA Certificates:

- SHALL include the *basicConstraints* extension;
- SHALL set the criticality of the *basicConstraints* extension to TRUE;
- SHALL set the cA field of the *basicConstraints*; and
- SHALL set the *pathLenConstraint* field of the *basicConstraints* to “3” for a Tier-2 ICA.

Table 20: *basicConstraints* Extension for Tier-2 ICA Certificates

Field	Format	Criticality	Value	Comment
basicConstraints		TRUE	{ id-ce 19 }	Included in all ICA Certificates.
cA	BOOLEAN		TRUE	Set
pathLenConstraint	INTEGER		3	Set

Table 21 shows the *basicConstraints* extension settings for Tier-3 ("Tier-n") and above (Tier-N) ICA Certificates and specifies that all ICA Certificates:

- SHALL include the *basicConstraints* extension;
- SHALL set the criticality of the *basicConstraints* extension to TRUE;
- SHALL set the cA field of the *basicConstraints*; and
- CA SHALL set *pathLenConstraint* field of any ICA Certificate it issues to its own *pathLenConstraint* -1.

Table 21: *basicConstraints* Extension for Tier-n ICA Certificates

Field	Format	Criticality	Value	Comment
basicConstraints		TRUE	{ id-ce 19 }	Included in all ICA Certificates.
cA	BOOLEAN		TRUE	Set
pathLenConstraint	INTEGER		5 – n	Set

7.1.2.7 *Certificate Policies Extension*

See Section 7.1.6.

7.1.2.8 *CRL Distribution Points Extension*

The *cRLDistributionPoints* extension identifies how CRL information is obtained.

Table 22 shows the *cRLDistributionPoints* extension settings for ICA Certificates and specifies that all ICA Certificates:

- SHALL include the *cRLDistributionPoints* extension;
- SHALL set the criticality of the *cRLDistributionPoints* extension to FALSE; and
- SHALL set the *distributionPointName* to the URL of the CRL.

Table 22: *cRLDistributionPoints* Extension for ICA Certificates

Field	Format	Criticality	Value	Comment
cRLDistributionPoints		FALSE	{ id-ce 31 }	Included in all ICA Certificates.
distributionPoint				
distributionPointName	GeneralNames		URL	Address of the CRL

Table 23 shows the *cRLDistributionPoints* extension settings for End-Entity Certificates and specifies that all End-Entity Certificates:

- SHALL include the *cRLDistributionPoints* extension;
- SHALL set the criticality of the *cRLDistributionPoints* extension to FALSE; and
- SHALL set the *distributionPointName* to the URL of the CRL.

Table 23: *cRLDistributionPoints* Extension for End-Entity Certificates

Field	Format	Criticality	Value	Comment
cRLDistributionPoints		FALSE	{ id-ce 31 }	Included in all End-Entity Certificates.
distributionPoint				
distributionPointName	GeneralNames		URL	Address of the CRL

7.1.2.9 *Extended Key Usage Extension*

The *extendedKeyUsage* (or *extKeyUsage*) extension indicates one or more purposes for which the Public Key MAY be used, in addition to, or in place of, the purposes indicated in the *keyUsage* extension.

CA Certificates SHALL NOT include the *extKeyUsage* extension.

Table 24 shows the *extKeyUsage* extension settings for Client Certificates and specifies that all Client Certificates:

- SHALL include the *extKeyUsage* extension;
- SHALL set the criticality of the *extKeyUsage* extension to TRUE; and
- SHALL set the *keyPurposeId* field to *id-kp-clientAuth.*

Table 24: *extKeyUsage* Extension for Client Certificates

Field	Format	Criticality	Value	Comment
extKeyUsage		TRUE	{ id-ce 37 }	Included in Client Certificates.
keyPurposeID	OID		1.3.6.1.5.5.7.3.2	id-kp-clientAuth. Included in Authentication Certificates
keyPurposeID	OID		1.3.6.1.5.5.7.3.3	Id-kp-codeSigning. Included in ECC signing Certificates

Table 25 shows the *extKeyUsage* extension settings for Server Certificates and specifies that all Server Certificates:

- SHALL include the *extKeyUsage* extension;
- SHALL set the criticality of the *extKeyUsage* extension to TRUE; and
- SHALL set the *keyPurposeId* field to *id-kp-serverAuth*.

Table 25: *extKeyUsage* Extension for Server Certificates

Field	Format	Criticality	Value	Comment
extKeyUsage		TRUE	{ id-ce 37 }	Included in all Server Certificates.
keyPurposeID	OID		1.3.6.1.5.5.7.3.1	id-kp-serverAuth
keyPurposeID	OID		1.3.6.1.5.5.7.3.2	id-kp-clientAuth

7.1.2.10 *Key Usage Extension*

See Section 6.1.7.

7.1.2.11 *Subject Alternative Name Extension*

The *subjectAlternativeName* (or *subjectAltName*) extension allows identities to be bound to the Subject of the Certificate.

The *otherName* field SHALL include a single quad that includes fields “idType”, “iD”, “role”, and “owner” using UTF-8 encoding, delimited by a forward slash. For idTypes of AgencyID, there may be no logical owner, so the "Owner" field may be null.

The idType SHALL include the values as allowed in the NENA i3 standard (e.g., AgentId, AgencyId, ServiceId, ElementId)[8] or the value “CAId” if the Certificate is a CA Certificate.

The CAId value for CA Certificates SHALL be an FQDN under the CA owner’s control, subject to validation as documented in the VP.

The Owner field SHALL contain the iD of the issuing Agency. For an ICA, the owner field SHALL contain the iD of the issuing CA.

The whole of the otherName field SHALL be globally unique.

Role SHALL include a list of comma delimited roles as defined in the NENA i3 Standard and appropriate registries;[9] for CA iD, roles SHALL be one of either “PCA” for the PCA or “ICA” for any ICA. The OID for the quad SHALL be the child OID specified for this quad in 1.2.2.

An example of a valid *otherName* element for an agency that processes emergency calls and includes a local police, fire and EMS function is below:

```
OBJECT IDENTIFIER 1.3.6.1.4.1.55670.1.1
          [0] (1 elem)
                    UTF8String
                    agencyId/foo.allegheny.pa.us/urn:emergency:service:responder.psap,
                    urn:emergency:service:responder.police.local,
                    urn:emergency:service:responder.fire.local,
                    urn:emergency:service:responder.ems.local/
```

[8] See i3 at Section 2.1.

[9] See i3 at Section 5.3

An example of a valid *otherName* element for an individual named John Smith who processes emergency calls and also dispatches resources is below:

```
OBJECT IDENTIFIER 1.3.6.1.4.1.55670.1.1
        [0] (1 elem)
                UTF8String agentID/jsmith@psap.allegheny.pa.us/Dispatching,CallTaking/
                psap.allegheny.pa.us
```

Table 26 shows the *subjectAltName* extension settings for all Root Certificates and specifies that all Root Certificates:

- MAY include the *subjectAltName* extension;
- SHALL set the criticality of the *subjectAltName* extension to FALSE; and
- SHALL set the *directoryName* with the appropriate information.

Table 26: *subjectAltName* Extension for Root Certificates

Field	Format	Criticality	Value	Comment
subjectAltName		FALSE	{ id-ce 17 }	MAY be included in all PCA Certificates.
otherName	OtherName (UTF8 String)		[forthcoming]	Single triplet that includes fields “idType”, “iD”, and “role” in UTF-8 encoding, delimited by a forward slash

Table 27 shows the *subjectAltName* extension settings for all ICA Certificates and specifies that all ICA Certificates:

- MAY include the *subjectAltName* extension;
- SHALL set the criticality of the *subjectAltName* extension to FALSE; and
- SHALL set the *otherName* with the appropriate information.

Table 27: *subjectAltName* Extension for ICA Certificates

Field	Format	Criticality	Value	Comment
subjectAltName		FALSE	{ id-ce 17 }	MAY be included in all CA Certificates.
otherName	OtherName (UTF8 String)		Quad ID OID	Single quad that includes fields “idType”, “iD”, and “role” in UTF-8 encoding, delimited by a forward slash

Table 28 shows the *subjectAltName* extension settings for End-Entity Certificates and specifies that End-Entity Certificates:

- SHALL include the *subjectAltName* extension;
- SHALL set the criticality of the *subjectAltName* extension to FALSE; and
- SHALL set the *otherName* with the appropriate information.

Table 28: *subjectAltName* Extension for End-Entity Certificates

Field	Format	Criticality	Value	Comment
subjectAltName		FALSE	{ id-ce 17 }	SHALL be included in End-Entity Certificates.
otherName	OtherName (UTF8 String)		[forthcoming]	ID that includes fields "idType", "iD", "role", and "owner", if applicable, in UTF-8 encoding, delimited by a forward slash

7.1.2.12 *Subject Key Identifier Extension*

The *subjectKeyIdentifier* extension provides a means of identifying Certificates that contain a particular Public Key.

Table 29 shows the *subjectKeyIdentifier* extension settings for CA Certificates and specifies that all CA Certificates:

- SHALL include the *subjectKeyIdentifier* extension;
- SHALL set the criticality of the *subjectKeyIdentifier* extension to FALSE; and
- SHALL calculate the *keyIdentifier* of the *subjectKeyIdentifier* per Method 1.

Table 29: *subjectKeyIdentifier* Extension for CA Certificates

Field	Format	Criticality	Value	Comment
subjectKeyIdentifier		FALSE	{ id-ce 14 }	SHALL be included in all CA Certificates.
keyIdentifier	OCTET STRING		<key identifier>	Calculated per Method 1

Table 30 shows the *subjectKeyIdentifier* extension settings for End-Entity Certificates, and specifies that all End-Entity Certificates:

- SHALL include the *subjectKeyIdentifier* extension;
- SHALL set the criticality of the *subjectKeyIdentifier* extension to FALSE; and
- SHALL calculate the *keyIdentifier* of the *subjectKeyIdentifier* per Method 1.

Table 30: *subjectKeyIdentifier* Extension for End-Entity Certificates

Field	Format	Criticality	Value	Comment
subjectKeyIdentifier		FALSE	{ id-ce 14 }	Included in all End-Entity Certificates.
keyIdentifier	OCTET STRING		<key identifier>	Calculated per Method 1

7.1.3 Algorithm Object Identifiers (OIDs)

Certificates issued under this CP SHALL use the following OIDs for signatures:

sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
sha384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12}
sha512withRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha512WithRSAEncryption(13)}
ecdsa-with-Sha256	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-Sha2(3) 2}
ecdsa-with-Sha384	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-Sha2(3) 3}
ecdsa-with-Sha512	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-Sha2(3) 3 ecdsa-with-Sha512(4)}

Certificates issued under this CP SHALL use the following OIDs to identify the algorithm associated with the Subject key:

rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
id-ecPublicKey	{iso(1) member-body(2) us(840) ansi-X9-62(10045) id-publicKeyType(2) 1}

Where the Certificate contains an elliptic curve Public Key, the parameters SHALL be specified as one of the following named curves:

secp256r1	{iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 7}
secp384r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 34 }
Secp521r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 35 }

PCA Response: Will comply.

7.1.4 Name Forms

The Subject field in Certificates issued under this CP SHALL be populated with an X.500 DN as specified in Section 3.1.1.

The issuer field of Certificates issued under this CP SHALL be populated with a non-empty X.500 DN as specified in Section 3.1.1.

PCA Response: Will comply.

7.1.4.1 *PCA*

The following naming attributes SHALL be used to populate the PCA Certificate Subject fields issued under this CP:

Table 31: PCA Certificate Subject Fields

Name	Field	Value	Requirement
country	(C=)	<Country Name>	(Optional) MAY contain the two-letter ISO 3166-1 country code for the country in which the PCA's service provider's place of business is located.
organizationName	(O=)	<Organization>	SHALL contain the organization name (or abbreviation thereof), trademark, or other meaningful identifier.
organizationalUnitName	(OU=)	<CA type> CA-<Id#>	SHALL contain the CA type (e.g., PCA) and unique ID, e.g., PCA – 1.
commonName	(CN=)	<Name> CA	SHALL contain a name that accurately identifies the PCA (e.g., Organization Name Root CA).

PCA Response: Will comply.

7.1.4.2 *ICAs*

All attributes permitted by RFC 5280 MAY be populated in the ICA Certificate Subject fields issued under the CP. The following attributes MUST be populated:

Table 32: ICA Certificate Subject Fields

Name	Field	Value	Requirement
country	(C=)	<Country Name>	(Optional) MAY contain the two-letter ISO 3166-1 country code for the country in which the PCA's service provider's place of business is located.
organizationName	(O=)	<Organization>	SHALL contain the organization name (or abbreviation thereof), trademark, or other meaningful identifier.
organizationalUnitName	(OU=)	<CA type> CA-<Id#>	SHALL contain the CA type (e.g., Intermediate or I) and unique ID, e.g., ICA–1.
commonName	(CN=)	<Name> CA	SHALL contain a name that accurately identifies the ICA (e.g., Organization Name ICA).

7.1.4.3 *End-Entity Certificates*

The following naming attributes SHALL be used to populate the Subject in End-Entity Certificates issued under this CP:

Table 33: End-Entity Certificate Subject Fields

Name	Field	Value	Requirement
countryName	(C=)	<Country Name>	SHALL be the two-letter ISO 3166-1 country code for the country in which the Subscriber's place of business is located.
organizationName	(O=)	<Organization>	SHALL contain the organization name (not to exceed 64 characters).
localityName	[l=]	<Location>	[Optional] <City>
stateOrProvinceName	[st=]	<state or province>	[Optional] <state or province name>
organizationalUnitName	[OU=]	<subsidiary/location>	[Optional] subsidiary/location (not to exceed 64 characters)
commonName	(CN=)	<Name>	[Optional] MAY contain a name that accurately identifies the Subscriber and includes the idType and iD.

7.1.5 Name Constraints

No stipulation.

7.1.6 Certificate Policy Object Identifier

ICA Certificates issued under this CP SHALL assert the policy OID listed in Section 1.2.2 of this CP.

Table 34 shows the *certificatePolicies* extension settings for ICA Certificates and specifies that these Certificates:

- SHALL include the *certificatePolicies* extension; and
- SHALL set the criticality of the *certificatePolicies* extension to FALSE.

Table 34: *certificatePolicies* Extension for ICA Certificates

Field	Format	Criticality	Value	Comment
certificatePolicies		FALSE	{ id-ce 32 }	SHALL be included in ICA Certificates.
policyIdentifier	OID			See Section 1.2.2.

End-Entity Certificates issued under this CP SHALL assert the policy OID listed in Section 1.2.2 of this CP.

Table 35 shows the *certificatePolicies* extension settings for End-Entity Certificates and specifies that these Certificates:

- SHALL include the *certificatePolicies* extension; and
- SHALL set the criticality of the *certificatePolicies* extension to FALSE.

Table 35: *certificatePolicies* Extension for End-Entity Certificates

Field	Format	Criticality	Value	Comment
certificatePolicies		FALSE	{ id-ce 32 }	SHALL be included in End-Entity Certificates.
policyIdentifier	OID			See Section 1.2.2.

7.1.7 Usage of Policy Constraints Extension

None.

7.1.8 Policy Qualifiers Syntax and Semantics

Certificates issued under this CP SHALL NOT contain policy qualifiers.

PCA Response: Will comply.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

Certificates issued under this CP SHALL NOT contain a critical Certificate policies extension.

PCA Response: Will comply.

7.2 CRL Profile

CRLs issued by a CA under this CP SHALL conform to the CRL profile specified in [RFC 5280].

CRLs SHALL contain the basic fields and contents specified in the table below:

Table 36: CRL Profile Basic Fields

Field	Referenced Standard	Section	Requirement or Recommendation
version	[RFC 5280]	5.1.2.1	MUST specify version 2 (the integer value is 1).
signature	[RFC 5280]	5.1.2.2	This CP requires use of RSA signatures.
issuer	[RFC 5280]	5.1.2.3	This field details the entity that has signed and issued the CRL.
thisUpdate	[RFC 5280]	5.1.2.4	This field indicates the issue date of this CRL.
nextUpdate	[RFC 5280]	5.1.2.5	This field indicates the date by which the next CRL will be issued.
revokedCertificates	[RFC 5280]	5.1.2.6	When there are no Revoked Certificates, the revokedCertificates list MUST be absent. Otherwise, Revoked Certificates are listed by their serial numbers.
authorityKeyIdentifier	[RFC 5280]	5.2.1	
cRLNumber	[RFC 5280]	5.2.3	
signatureAlgorithm	[RFC 5280]	5.1.1.2	The signatureAlgorithm field contains the algorithm identifier for the algorithm used by the CRL issuer to sign the Certificate List. This field MUST contain the same algorithm identifier as the signature field in the sequence tbsCertList (RFC 5280, Section 5.1.2.2).
signatureValue	[RFC 5280]	5.1.1.3	

PCA Response: Will comply.

7.2.1 CRL Version Number(s)

The PCA and ICAs SHALL support the issuance of X.509 Version 2 CRLs. The CRL version number SHALL be set to the integer value of "1" for Version 2 [RFC 5280, Section 5.1.2.1].

PCA Response: Will comply.

7.2.2 CRL and CRL Entry Extensions

Detailed CRL profiles addressing the use of each extension are specified in [RFC 6960].

Critical CRL extensions SHALL NOT be used.

PCA Response: Will comply.

7.3 OCSP Profile

OCSP is a way to obtain timely information about the Revocation status of a particular Certificate. OCSP responses issued by a CA under this CP SHALL conform to the OCSP profile specified in [RFC 5280].

OCSP responses SHALL conform to [RFC 5019] and SHALL 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 Certificate SHALL contain the extension *id-pkix-ocsp-nocheck* as defined by [RFC 6960]. This extension indicates that the End-Entity need not obtain a CRL for the OCSP responder's Certificate. The OCSP responder should be a highly trusted component.

PCA Response: Will comply.

7.3.1 OCSP Version Number(s)

CSSs operated under this CP SHALL use OCSP version 1 as defined by [RFC 6960] and [RFC 5019].

PCA Response: Will comply.

7.3.2 OCSP Extensions

Detailed CRL profiles addressing the use of each extension are specified in [RFC 6960].

8. Compliance Audit and Other Assessments

The PCA and ICAs, and the RAs on their behalf, SHALL have a Compliance Audit mechanism in place to ensure that the requirements of this CP are being implemented and enforced. CAs SHOULD have self-Auditing capability and SHOULD complete self-Audits quarterly.

This CP does not impose a requirement for any particular assessment methodology other than that noted below.

PCA Response: <redacted response>.

RA Response: The RA Compliance Audit is covered as part of the annual DigiCert Private PKI Service Audit.

8.1 Frequency or Circumstances of Assessment

CAs and RAs SHALL be subject to a periodic Compliance Audit at least once per year. In addition, the appropriate PA MAY require an Audit should circumstances dictate.

PCA Response: The PCA, receives an annual Audit by an independent external Auditor.

RA Response: The RA Compliance Audit is covered as part of the annual DigiCert Private PKI Service Audit.

8.2 Identity and Qualifications of Assessor

The Compliance Auditor MUST demonstrate competence in the field of Compliance Audits, and MUST be thoroughly familiar with CAs, RAs, and CPs. The Compliance Auditor MUST perform such Compliance Audits as a regular ongoing business activity. In addition to the previous requirements, the Compliance Auditor MUST be a Certified Information Systems Auditor or IT security specialist, and a PKI subject matter specialist who can offer input regarding acceptable Risks, mitigation strategies, and industry best practices. The CA and RA MAY identify the parties responsible for providing such services, and the mechanisms used to support these services.

PCA Response: For the PCA Audit, WebTrust Auditors must meet the following requirements:

1. Qualifications and experience: Auditing must be the Auditor's primary business function. The individual, or at least one member of the Audit group, must be qualified as a Certified Information Systems Auditor (CISA), an AICPA Certified Information Technology Professional (CPA.CITP), a Certified Internal Auditor (CIA), or have another recognized information security Auditing credential. Auditors must be subject to disciplinary action by its licensing body.

2. Expertise: The individual or group must be trained and skilled in the Auditing of secure Information Systems and be familiar with PKI, certification systems, and internet security issues.

3. Rules and standards: The Auditor must conform to applicable standards, rules, and best practices promulgated by the American Institute of Certified Public Accountants (AICPA), Information Systems Audit and Control Association (ISACA), the Institute of Internal Auditors (IIA), or another qualified Auditing standards body.

4. Reputation: The firm must have a reputation for conducting its Auditing business competently and correctly.

5. Insurance: Auditors must maintain Professional Liability/Errors and Omissions Insurance, with policy limits of at least $1 million in coverage.

RA Response: The RA Compliance Audit is covered as part of the annual DigiCert Private PKI Service Audit. And thus complies with the DigiCert Audit requirements.

8.3 Assessor's Relationship to Assessed Entity

The Compliance Auditor either SHALL be a private firm that is independent from the entities (CA or RA) being Audited, or it SHALL be sufficiently and organizationally separated from those entities to provide an unbiased, independent evaluation. To ensure independence and objectivity, the Compliance Auditor MUST NOT have served the entity in developing or maintaining the to-be-Audited CA Facility. The appropriate PA SHALL determine whether a Compliance Auditor meets this requirement.

PCA Response: Will comply.

RA Response: Will comply.

PCA PA Response: Will comply.

8.4 Topics Covered by Assessment

The Audit MUST conform to industry standards, cover the CA’s and RA’s compliance with this CP and the relevant CPS, and evaluate the Integrity of the CA’s PKI operations and RA’s operations. The Audit MUST verify that each CA and RA is compliant with this CP.

8.5 Actions Taken as a Result of Deficiency

When the Compliance Auditor finds a discrepancy between the requirements of this CP and the design, operation, or maintenance of the PKI, the following actions SHALL be performed:

- The Compliance Auditor SHALL note the discrepancy;
- The Compliance Auditor SHALL notify the responsible party promptly of the discrepancy;
- The party responsible for correcting the discrepancy SHALL determine what further notifications or actions are necessary pursuant to the requirements of the applicable CPS, create a written plan with committed dates and then proceed to make such notifications and take such actions without delay. This plan, with dates, SHALL be given to the appropriate PA, which MUST approve it;

- The responsible party SHALL provide the appropriate PA with regular progress reports and notify the appropriate PA when corrective actions have been completed; and
- The Compliance Auditor SHALL be notified when corrective actions have been completed and MAY repeat portions or the entirety of the Audit to confirm the discrepancy has been addressed to the satisfaction of the Compliance Auditor.

Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the appropriate PA MAY decide to temporarily halt operation of its corresponding CA, to Revoke a Certificate issued by the CA or its corresponding RA, or take other actions it deems appropriate. The appropriate PA SHALL provide to the CA its procedures for making and implementing such determinations.

PCA PA Response: Will comply.

8.6 Communication of Results

See Section 8.5

8.7 Internal Audits

The PCA and ICAs SHALL perform regular internal Audits of its operations, personnel, and compliance with this CP. Results of these Audits SHALL be made available to the Compliance Auditor.

PCA Response: Will comply.

9. Other Business and Legal Matters

9.1 Fees

Any fees SHALL be approved by the PA and (if applicable) the ICA PA, if the ICA PA institutes fees in addition to those instituted by the PA.

Fees for services defined in this CP are agreed to by the PA and PCA in their Master Service Agreement (MSA). Any changes to the services required in the CP (e.g., cross-certification with another CA) will be evaluated by the PCA upon request from the PA. The scope and cost to implement the change will be negotiated in good faith and the MSA will be amended accordingly.

PCA PA Response: Will comply.

9.1.1 Certificate Issuance or Renewal Fees

Subscribers MAY be charged a fee for the issuance, management, and Renewal of Certificates. These fees will be proposed by the MA, agreed to by the appropriate PA, and will be available to Prospective Subscribers.

9.1.2 Certificate Access Fees

Section 2.4 of this CP requires that CA Certificates and CRLs be publicly available. The PCA and ICAs operating under this CP MUST NOT charge additional fees for Access to this information.

PCA Response: Will comply.

9.1.3 Revocation or Status Information Access Fees

CAs operating under this CP MUST NOT charge additional fees for Access to Certificate status information.

PCA Response: Will comply.

9.1.4 Fees for other Services

No stipulation.

9.1.5 Refund Policy

To be proposed by the MA and agreed to by the appropriate PA.

PCA PA Response: Will comply.

9.2 Financial Responsibility

This CP contains no limits on the use of Certificates issued by CAs under the policy. The CA, RA, PA, ICA PA and MA assume no liability for any use of the Certificates.

9.2.1 Insurance Coverage

To be addressed in the MSA between the PA and the PCA for the PCA. For ICAs, to be addressed in the agreement between the MA and the ICA.

9.2.2 Other Assets

Not Applicable.

9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3 Confidentiality of Business Information

The PCA and ICAs, and the RAs on their behalf, SHALL protect the Confidentiality of sensitive information stored or processed on CA systems that could lead to abuse or fraud. RAs SHALL protect customer data that could allow an attacker to impersonate a customer.

Public Access to organizational information SHALL be determined by the respective organization.

PCA Response: Will comply.

RA Response: Will comply.

9.3.1 Scope of Confidential Information

Confidential Information means all information in written or oral form that the disclosing party identifies as confidential, and any trade secret or other proprietary information that the recipient knows or reasonably should know is intended to be treated as confidential.

9.3.2 Information Not Within the Scope of Confidential Information

Information that is generally known to the public or properly known by the receiving party at the time of disclosure and other typical exceptions is not within the scope of Confidential Information.

9.3.3 Responsibility to Protect Confidential Information

Any party that collects, transmits, or stores confidential information SHALL be responsible for ensuring it SHALL NOT be released except as required by law.

9.4 Privacy of Personal Information

It is the responsibility of all parties to ensure Privacy of personal information under their control. No personal information is registered or certified. Information about ICA operators is retained by the PCA as part of the certification request, which is subsequently logged and later Archived. If a party collects, transmits, or stores personal information, its practices will comply with all applicable laws.

9.4.1 Privacy Plan

The PCA and ICAs, and the RAs on their behalf, SHALL each develop, implement, and maintain a Privacy plan. The Privacy plan SHALL document what personally identifiable information is collected, how it is stored and processed, and under what conditions the information MAY be disclosed.

PCA Response: Will comply.

RA Response: Will comply.

9.4.2 Information Treated as Private

CAs and RAs SHALL protect all Subscriber personally identifiable 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 CP SHALL NOT be released, except as required by the Privacy plan.

PCA Response: Will comply.

RA Response: Will comply.

9.4.3 Information Not Deemed Private

Information included in Certificates is not subject to protections outlined in Section 9.4.1.

9.4.4 Responsibility to Protect Private Information

Sensitive information MUST be stored securely, and MAY be released only in accordance with other stipulations in Section 9.4.

9.4.5 Notice and Consent to Use Private Information

CAs or RAs MAY NOT provide any notice or obtain the consent of the Subscriber in order to release private information in accordance with other stipulations of Section 9.4.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

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

PCA Response: Will comply.

RA Response: Will comply.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property Rights

No party will use any property owned by any other party, including, without limitation, any trademark, copyright, trade secret or other proprietary right, unless they have been licensed that use

PKI Participants SHALL NOT knowingly violate Intellectual Property Rights held by others and SHALL NOT knowingly claim to represent an agency or role that the party does not credibly represent. Without limitation, except as the intellectual property owner or a Trusted Person credibly representing an agency MAY expressly authorize in writing, it is prohibited to:

- Reverse engineer, translate, disassemble, decompile the whole or any part of any software or system or any part thereof, or otherwise attempt to Access any software source code embedded in or used in the operation of any system;
- Assign, transfer, sell, license, sub-license, lease, rent, charge or otherwise deal in or encumber, any software or system or any part thereof, or use same on behalf of or for the benefit of any third party, or make available the same in any way whatsoever to any third party without prior written consent;
- Remove or alter any trademark or any copyright or other proprietary notice on any software, system or any other materials;
- Distribute, create derivative works of or modify any materials, software or systems or any part thereof in anyway, or use, copy, duplicate or display same on a commercial or development basis; and
- Provide any service using a Certificate provided under this CP except as authorized and provided in this CP and an approved CPS.

These restrictions SHALL NOT be construed in a manner that would violate any applicable law.

The PA SHALL be deemed the owner of the keys for all hosted ICAs.

PCA PA Response: Will comply.

9.6 Representations and Warranties

The PA SHALL:

- Approve the CPS for CAs issued by the PCA under this CP;

The obligations described below pertain to the MA, on behalf of the PA.

The MA SHALL:

- Review name space control procedures to ensure that DNs are uniquely assigned for all Certificates issued under this CP;
- Distribute this CP; and
- Coordinate modifications to this CP to ensure continued compliance by CAs operating under approved CPSs.

PCA PA Response: Will comply.

MA Response: Will comply.

9.6.1 CA Representations and Warranties

CAs operating under this CP SHALL comply with the stipulations of this CP, and comply with a CPS approved by the PA for use with this CP. The CA warrants that any

Certificates issued that assert the policy OIDs identified in this CP were issued in accordance with the stipulations of this CP.

A CA that issues Certificates that assert a policy defined in this CP SHALL conform to the stipulations of this CP, including:

- Providing a CPS to the appropriate PA, as well as any subsequent changes, for conformance assessment;
- Maintaining its operations in conformance to the stipulations of the CPS;
- Ensuring that registration information is accepted only from approved RAs operating under an approved CPS;
- Including only valid and appropriate information in Certificates, and maintaining evidence that due diligence was exercised in validating the information contained in the Certificates;
- Revoking the Certificates of Subscribers found to have acted in a manner counter to their obligations in accordance with Section 9.6.3; and

Operating or providing for the services of an online Repository, and informing the Repository service provider of their obligations if applicable.

PCA Response: Will comply.

9.6.2 RA Representations and Warranties

A RA that performs registration functions as described in this CP SHALL comply with the stipulations of this CP, and comply with a CPS approved by the appropriate PA for use with this CP. A RA who is found to have acted in a manner inconsistent with these obligations is subject to Revocation of RA responsibilities. A RA supporting this CP SHALL conform to the stipulations of this document, including:

- Maintaining its operations in conformance to the stipulations of the approved CPS;
- Including only valid and appropriate information in Certificate requests, and maintaining evidence that due diligence was exercised in validating the information contained in the Certificate; and
- Ensuring that obligations are imposed on Subscribers in accordance with Section 9.6.3, and that Subscribers are informed of the consequences of not complying with those obligations.

To the extent permitted by applicable law, the RA disclaims any warranties, including any warranty of merchantability or fitness for a particular purpose.

RA Response: Will comply.

9.6.3 Subscriber Representations and Warranties

A Subscriber SHALL sign a DCSA to acknowledge acceptance of the requirements the Subscriber SHALL meet, including protection of their Private Keys and use of the Certificates before being issued the Certificate.

In addition, Subscribers SHALL:

- Accurately represent themselves in all communications with the PKI authorities;
- Protect their Private Key(s) at all times, in accordance with this CP, and as stipulated in their DCSA;
- Promptly notify the appropriate CA upon suspicion of loss or Compromise of their Private Key(s).Such notification SHALL be made directly or indirectly through mechanisms consistent with the CA's CPS; and
- Abide by all the terms, conditions, and restrictions levied on the use of their Private Key(s) and Certificate(s).

DCSAs MAY include additional representations and warranties.

9.6.4 Relying Parties Representations and Warranties

This CP does not specify the 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.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

PAs, MAs, CAs, RAs, and Subscribers operating under this CP SHALL NOT disclaim any of their responsibilities described in this CP.

PCA PA Response: Will comply.

MA Response: Will comply.

PCA Response: Will comply.

RA Response: Will comply.

9.8 Limitations of Liability

The PCA SHALL NOT be liable for any indirect damages of any kind, including consequential, incidental, special, punitive, or other damages whatsoever arising out of or related to this CPS, even if advised of the possibility of such damages.

The liability (and/or limitations thereof) of Subscribers SHALL be as set forth in the applicable DCSAs.

PCA Response: Will comply.

9.9 Indemnities

No stipulation.

9.10 Term and Termination

9.10.1 Term

This CP SHALL be effective from the PA approval date, and SHALL remain effective until replaced. Amendments to this CP become effective upon publication.

9.10.2 Termination

Termination of this CP is at the discretion of the PA.

9.10.3 Effect of Termination and Survival

The requirements of this CP remain in effect through the end of the Archive period for the last Certificate issued.

9.11 Individual Notices and Communications with PKI Participants

The PA SHALL establish appropriate procedures for communications with CAs operating under this CP via contracts or memoranda of agreements as applicable.

For all other communications, no stipulation.

PCA PA Response: Will comply.

9.12 Amendments

9.12.1 Procedure for Amendment

The PA SHALL review this CP at least once every year. Corrections, updates, or changes to this CP SHALL be made publicly available. Suggested changes to this CP SHALL be communicated to the contact in Section 1.5.2; such communication MUST include a description of the change, a change justification, and contact information for the person requesting the change.

PCA PA Response: Will comply.

9.12.2 Notification Mechanism and Period

Whenever the CP is amended, the PA SHALL published it within five (5) days of the date the amendment took place and all known concerned parties (CA staff, Relying Parties, Subscribers, etc.) SHALL be notified.

PCA PA Response: Will comply.

9.12.3 Circumstances Under Which OID Must be Changed

CP OIDs SHALL be changed if the CA determines that a change in this CP decreases the level of assurance provided.

9.13 Dispute Resolution Provisions

The PA SHALL facilitate the resolution between entities when conflicts arise as a result of the use of Certificates issued under this CP.

PCA PA Response: Will comply.

9.14 Governing Law

The construction, validity, performance and effect of Certificates issued under this CP for all purposes SHALL be governed by United States Federal, state or local law, or applicable national law (statute, case law, or regulation), as appropriate.

9.15 Compliance with Applicable Law

All CAs operating under this CP SHALL comply with applicable law.

PCA Response: Will comply.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

Except where specified by contract, no party MAY assign or delegate this CP or any of its rights or duties under this CP, without the prior written consent of the other party (such consent not to be unreasonably withheld), except that the PA MAY assign and delegate this CP to any party of its choosing.

9.16.3 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 this CP is updated. The process for updating this CP is described in Section 9.12.

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

Any failure to exercise any right hereunder SHALL NOT be construed as a relinquishment of any future exercise of such right.

9.16.5 Force Majeure

No stipulation.

9.17 Other Provisions

No stipulation.

Appendices

Appendix A – Abbreviations and Acronyms

This document uses the following abbreviations and acronyms:

AIA	Authority Information Access
CA	Certification Authority
CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CSS	Certificate Status Server
DCSA	Digital Certificate Subscriber Agreement
DN	Distinguished Name
DRP	Disaster Recovery Plan
ESInet	Emergency Services IP Network
FIPS	Federal Information Processing Standards
FPKI	Federal Public Key Infrastructure
HSM	Hardware Security Module
HTTPS	Hypertext Transfer Protocol Secure
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
MA	Management Authority
MOA	Memorandum of Agreement
MSA	Master Service Agreement
NENA	National Emergency Number Association
NG9-1-1	Next Generation 9-1-1
NIOC	NG9-1-1 Interoperability Oversight Commission
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol

OID	Object Identifier
PA	Policy Authority
PCA	PSAP Credentialing Agency
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
PSAP	Public Safety Answering Point
RA	Registration Authority
RFC	Request for Comments
RSA	Rivest-Shamir-Adleman
SHA	Secure Hash Algorithm
SP	Special Publication
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

Appendix B – Glossary

This document uses the following terms and definitions:

Term	Definition
Access	Ability to make use of any Information System resource. [CNSSI 4009]
Access Control	Process of granting Access to Information System resources only to authorized users, programs, processes, or other systems. [CNSSI 4009]
Account Administrator	An employee or other Trusted Person authorized to perform PKI tasks via the RA on behalf of the Subscriber.
Activation Data	Private data, other than keys, that are required to Access Cryptographic Modules (i.e., unlock Private Keys for signing or decryption events).
Anonymous	Having an unknown or undisclosed name.
Applicant	See “Prospective Subscriber.”
Archive	Long-term, physically separate storage.

Term	Definition
Audit	Independent review and examination of Records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. [CNSSI 4009]
Audit Data	Chronological Record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. [CNSSI 4009, "Audit trail"]
Authenticate	To confirm the identity of an entity when that identity is presented.
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [CNSSI 4009]
Backup	Copy of files and programs made to facilitate recovery if necessary.
Binding	Process of associating two related elements of information. [CNSSI 4009]
Biometric	A physical or behavioral characteristic of a human being.
CA Administrator	An employee or other Trusted Person authorized to perform PKI tasks on behalf of the CA.
CA Facility	The collection of equipment, personnel, procedures, and structures that are used by a CA to perform Certificate issuance and Revocation.
CA Operations Staff	CA components are operated and managed by individuals holding trusted, sensitive roles.
Certificate	A digital representation of information which at least: • Identifies its issuing CA • Names or identifies the Subscriber of the Certificate • Contains the Subscriber’s Public Key • Identifies its operational period • Is digitally signed by the issuing CA As used in this CP, the term “Certificate” refers to X.509 Certificates that expressly reference the OID of this CP in the *certificatePolicies* extension.
Certificate Application	A request from a Prospective Subscriber that is also called the Naming Application (which is part of the DCSA), containing the naming information that will be included in the End-Entity Certificates (customer profile information and Naming Application that will set the Subject DN in the Certificates).
Certificate Policy (CP)	A CP is a specialized form of administrative policy that conforms to RFC 3647 and consists of a named set of rules that indicates the applicability of a Certificate to a particular community and/or class of application with common security requirements.
Certificate Revocation List (CRL)	A list maintained by a CA of the Certificates that is has issued that are Revoked prior to their stated expiration date.

Term	Definition
Certificate Signing Request (CSR)	A message conveying a request to have a Certificate issued.
Certificate Status Server (CSS)	A trusted entity that provides online verification to a Relying Party of a Subject Certificate's Revocation status, and MAY also provide additional attribute information for the Subject Certificate.
Certification Authority (CA)	An authority trusted by one or more users to issue and manage X.509 Public Key Certificates and CRLs.
Certification Practice Statement (CPS)	A statement of the practices which a CA employs in issuing Certificates.
Client (application)	A system entity, usually a computer process acting on behalf of a service provided by a Server.
Compliance Audit	A periodic Audit that a CA system undergoes to determine its conformance with PKI requirements that apply to it.
Compliance Auditor	An individual (e.g. employee, contractor, consultant, third party) who is responsible for Auditing the security of CAs or RAs, including reviewing, maintaining, and archiving Audit logs; and performing or overseeing internal Audits of CAs or RAs. A single individual MAY Audit both CAs and RAs. Compliance Auditor is an external role that is designated as trusted.
Compromise	Disclosure of information to unauthorized persons, or a violation of the Security Policy of a system in which unauthorized intentional or unintentional disclosure, Modification, destruction, or loss of an object may have occurred. [CNSSI 4009]
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes. [CNSSI 4009]
Cross-Certificate	A Certificate used to establish a trust relationship between two CAs.
Cryptographic Module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [FIPS 140-2]
Digital Certificate Subscriber Agreement (DCSA)	An agreement setting forth the terms and conditions under which an organization acts as a Subscriber. The DCSA contains the Certificate Application.
Digital Signature	The result of a transformation of a message by means of a cryptographic system using keys such that a Relying Party can determine (1) whether the transformation was created using the Private Key that corresponds to the Public Key in the signer’s digital Certificate; and (2) whether the message has been altered since the transformation was made.
Disaster Recovery Plan (DRP)	A documented process or set of procedures to recover and protect an infrastructure in the event of a disaster.
Discrete ICA	An ICA operated by the Subscriber or a third-party PKI service provider on behalf of the Subscriber.

Term	Definition
Distinguished Name (DN)	Identification fields in a Certificate that are input by the CA when issuing Certificates. The information is obtained from the Subscriber's Certificate Application.
End-Entity Authentication Certificate	A Certificate used for Authentication in which the Subject is not a CA (also known as a Subscriber Certificate).
End-Entity Signing Certificate	A Certificate used for Signing in which the Subject is not a CA (also known as a Subscriber Certificate).
End-Entity Certificate	An End-Entity Authentication Certificate or an End-Entity Signing Certificate
Firewall	Gateway that limits Access between networks in accordance with local Security Policy. [CNSSI 4009]
Hardware Security Module (HSM)	A physical computing device that safeguards and manages digital keys for strong Authentication and provides crypto processing.
Hosted ICA	An ICA that is hosted by DigiCert in its PKI facilities.
Information System	An integrated set of components for collecting, storing, and processing data and for providing information, knowledge, and digital products.
Integrity	Protection against unauthorized modification or destruction of information. [CNSSI 4009] A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.
Intellectual Property Rights	Rights under one or more of the following: copyright, patent, trade secret, trademark, trade name, or any other Intellectual Property Rights.
Intermediate CA (ICA)	A CA subordinate to the PCA or another ICA and operates according to this CP.
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.
Key Pair	Two mathematically related keys having the properties that (1) one (Public) Key can be used to encrypt a message that can only be decrypted using the other (Private) Key; and (2) even knowing the Public Key, it is computationally infeasible to discover the Private Key.
Key Rollover Certificate	The Certificate that is created when a CA signs a new Public Key for itself with its old Private Key, and vice versa.
Management Authority (MA)	An entity whose role is to provide management services to support the ecosystem in meeting its security goals.
Modification (of a Certificate)	The act or process by which data items bound in an existing Public Key Certificate, especially authorizations granted to the Subject, are changed by issuing a new Certificate.
Naming Application	A form, included in the Certificate Application, that is completed by the Prospective Subscriber and contains the information to be loaded into the Certificate Subject DN which will set the Certificate profile.

Term	Definition
Object Identifier (OID)	A specialized formatted number that is registered with an internationally recognized standards organization, the unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In this PKI, OIDs are used to uniquely identify Certificate policies and cryptographic algorithms.
Online Certificate Status Protocol (OCSP)	An Internet protocol used for obtaining the Revocation status of a X.509 digital Certificate.
Out-of-Band	Communication between parties utilizing a means or method that differs from the current method of communication (e.g., one party uses U.S. Postal Service mail to communicate with another party where current communication is occurring online).
PKCS #10	Public-Key Cryptography Standard #10, developed by RSA Security Inc., which defines a structure for a CSR.
PKI Participant	An individual or organization that is one or more of the following within the PKI: a CA, a Subscriber, or a Relying Party.
PKI Sponsor	When the Subscriber is a device, an authorized representative of the device will act as the PKI Sponsor.
Policy Authority (PA)	Body established to oversee the creation and update of Certificate policies, review CPSs, review the results of CA Audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI Certificate policies.
Privacy	Restricting Access to Subscriber or Relying Party information in accordance with Federal law.
Private Key	The key of a signature Key Pair used to create a Digital Signature. This key MUST be kept secret.
Prospective Subscriber	The Subscriber, sometimes called an "Applicant", is known as a Prospective Subscriber while going through the Certificate issuance process, until the point when the Certificate issuance procedure is completed (e.g. when the Certificate has been issued).
Pseudonym	A Subscriber name that has been chosen by the Subscriber that is not verified as meaningful by identity proofing. [CNSSI 4009]
Public Key	The key of a signature Key Pair used to validate a Digital Signature. This key is normally made publicly available in the form of a digital Certificate.
Public Key Infrastructure (PKI)	A set of policies, processes, service platforms, software and workstations used for the purpose of administering Certificates and Public-Private Key Pairs, including the ability to issue, maintain, and Revoke Public Key Certificates.
Records	A thing constituting a piece of evidence about the past, especially an account of an act or occurrence kept in writing or some other permanent form.

Term	Definition
Registration Authority (RA)	An entity in a PKI (separate from the CA) that is responsible for identification and Authentication of Certificate Subjects, but that does not sign or issue Certificates (i.e., a RA is delegated certain tasks on behalf of an authorized CA). The RA MAY also perform other Certificate management functions for the CA.
Re-Key (a Certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new Certificate that contains the new Public Key.
Relying Party	A person or entity that receives a Certificate with a Digital Signature verifiable with the Public Key listed in the Certificate, and is in a position to assess the trust in the Authentication information provided by the Certificate depending on the CP governing the PKI and the Certificate verification.
Renew (a Certificate)	The act or process of extending the validity of the data Binding asserted by a Public Key Certificate by issuing a new Certificate.
Repository	A database containing information and data relating to Certificates as specified in this CP; MAY also be referred to as a directory.
Revocation	The process of canceling (or revoking) a Certificate.
Revoke (a Certificate)	To prematurely end the operational period of a Certificate effective at a specific date and time.
Risk	An expectation of loss expressed as the probability that a particular Threat will exploit a particular vulnerability with a particular harmful result.
Root CA	In a hierarchical PKI, the CA whose Public Key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain. A Root CA is the highest level CA of a PKI. It generates a self-signed Certificate, which means that the Root CA validates itself (self-validating). A Root CA can issue ICAs that effectively trust it. The ICAs receive a Certificate signed by the Root CA, so the ICAs can issue Certificates that are validated by the Root CA. This establishes a CA hierarchy and chain of trust.
Security Auditor	An individual (e.g. employee, contractor, consultant, third party) who is responsible for Auditing the security of CAs or RAs, including reviewing, maintaining, and archiving Audit logs; and performing or overseeing internal Audits of CAs or RAs. A single individual MAY Audit both CAs and RAs. Security Auditor is an internal role that is designated as trusted.
Security Policy	The highest-level document describing an organization's Security Policies.
Server	A system entity that provides a service in response to requests from Clients.
Subject	The holder of a Private Key corresponding to a Public Key. The term "Subject" can refer to the Subscriber who is issued the Certificate.

Term	Definition
Subscriber	A Subscriber is an entity that (1) is the Subject named or identified in a Certificate issued to that entity, (2) holds a Private Key that corresponds to the Public Key listed in the Certificate, and (3) does not itself issue Certificates to another party. This includes, but is not limited to, an individual, an application, or a network device.
Threat	Any circumstance or event with the potential to cause harm to an Information System in the form of destruction, disclosure, adverse modification of data, and/or denial of service. [CNSSI 4009]
Trust Anchor	The Root Certificate from which the chain of trust for a PKI is derived.
Trusted Person	An employee, contractor, or consultant of an entity within a PKI, responsible for managing infrastructural trustworthiness of the entity, its products, its services, its facilities, and/or its practices.
Trusted Role	Those roles Identified in Section 5.2.1.
Validity Period	The period starting with the date and time a Certificate is issued and ending with the date and time on which the Certificate expires or is Revoked.

Appendix C – References

This document uses the following references:

Doc Number	Reference Title
CNSSI 4009	CNSSI 4009, Committee on National Security Systems Glossary, April 6, 2015 https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf
CVSS	Common Vulnerability Scoring System v3.1: Specification Document. https://www.first.org/cvss/v3.1/specification-document
FIPS 140-2	Security Requirements for Cryptographic Modules, FIPS 140-2, May 25, 2001; (Change Notice 2, 12/3/2002), is available at: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf
FIPS 186-4	Digital Signature Standards (DSS), FIPS 186-4, July 2013. http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf
FPKIPA	X.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework, version 1.31, February 8, 2019. https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/fpki-x509-cert-policy-common.pdf
NENA i3	NENA i3 Standard for Next Generation 9-1-1, STA-010.3-202x, https://dev.nena.org/higherlogic/ws/public/document?document_id=16133&wg_id=eca27a3d-a4c7-4d67-bb06-b3bb241df44e
RFC 2119	Key words for use in RFCs to Indicate Requirement Levels (Bradner), March 1997 https://www.ietf.org/rfc/rfc2119.txt
RFC 2560	X.509 Internet Public Key Infrastructure: Online Certificate Status Protocol – OCSP, Michael Myers, Rich Ankney, Ambarish Malpani, Slava Galperin, and Carlisle Adams, June 1999. http://www.ietf.org/rfc/rfc2560.txt

Doc Number	Reference Title
RFC 3647	Internet X.509 PKI Certificate Policy and Certification Practices Framework, IETF (Chokhani, Ford, Sabett, Merrill, and Wu), November 2003. https://www.ietf.org/rfc/rfc3647.txt
RFC 5019	The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments, IETF (Deacon, and Hurst), September 2007. https://www.ietf.org/rfc/rfc5019.txt
RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008 https://www.ietf.org/rfc/rfc5280.txt
RFC 6960	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, June 2013 https://www.ietf.org/rfc/rfc6960.txt
SP 800-63	NIST Special Publication 800-63, Digital Identity Guidelines document suite, https://pages.nist.gov/800-63-3/
SP 800-88-1	NIST Special Publication 800-88, Rev 1: Guidelines for Media Sanitization https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf
Validation Policy	NIOC PSAP Credentialing Agency (PCA) Certificate Validation Guidelines, February 2022. https://ng911ioc.org/wp-content/uploads/2022/02/NIOC-PCA-Validation-Policy-v1.0-02-09-2022-CLEAN.pdf
X.500	ITU-T Recommendation X.500 Series (1994) – ISO/IEC 9594,1-9:1994, *Information Technology – Open Systems Interconnection – The Directory*