DigiCert Electric Vehicle (EV) Public Key Infrastructure (PKI) – Certificate Policy (CP)

- SAE EVPKI CP, ISO15118-2, and ISO15118-20

V1.0

February 6th, 2026

Disclaimer

This document is furnished on an "AS IS" basis. DigiCert, Inc. and its affiliates ("DigiCert") do not provide any representation or warranty, express or implied, regarding the accuracy, completeness, noninfringement, or fitness for a particular purpose of this document, or any document referenced herein. Any use or reliance on the information or opinion in this document is at the risk of the user, and DigiCert shall not be liable for any damage or injury incurred by any person arising out of the completeness, accuracy, or utility of any information or opinion contained in the document.

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

DOCUMENT REVISION HISTORY

The following revisions have been made to the original document.

Version	Date	Remarks
V1.0	02/06/2026	Initial Draft

TABLE OF CONTENTS

TABLE OF TABLES

TABLE OF FIGURES

1 Introduction

1.1 Overview

This document is the DigiCert, Inc. (DigiCert) Certificate Policy (CP) for the issuance and management of an Electric Vehicle Public Key Infrastructure (PKI) (DigiCert EV PKI CP) as part of DigiCert's Private PKI Services defined in DigiCert's "Certificate Policy/Certification Practices Statement for Private PKI Services" [DigiCert Private PKI CP/CPS]. This service is also aligned with [ISO 15118-2], [ISO 15118-20], and the SAE International EVPKI – Certificate Policy [SAE EVPKI CP], as applicable. In the event of any inconsistency between:

- [DigiCert Private PKI CP/CPS] and this document, i.e., the DigiCert EV PKI CP, the inconsistency will be reconciled by the DigiCert Policy Authority (DCPA).
- [ISO 15118-2] and this document, the DigiCert EV PKI CP requirements take precedence in this document.
- [ISO 15118-20] and this document, the DigiCert EV PKI CP requirements take precedence in this document.
- [SAE EVPKI CP] and this document, the inconsistency will be reconciled between the [SAE EVPKI CP] Policy Authority and the DCPA.

This document provides the governance, technology, and operations requirements in accordance with [RFC 3647] to facilitate the comparison with other Certificate Policies. This CP includes all sections of the framework and will state "no stipulation" in sections that are left up to the discretion of the individual Certification Authority (CA) and the CP has no specific requirements or guidance.

The DCPA owns this document and MAY update these requirements from time to time, in order to address any additional PKI security service needs of the ecosystem.

These requirements are applicable to all CAs within the DigiCert EVPKI chain of trust. They flow down from the PA to the Root CA through successive Subordinate Certification Authorities (Sub-CAs) and down to the End-Entity Certificates.

The DigiCert EVPKI architecture provided in Figure 1 is aligned with [ISO 15118-2] and [SAE EVPKI CP].

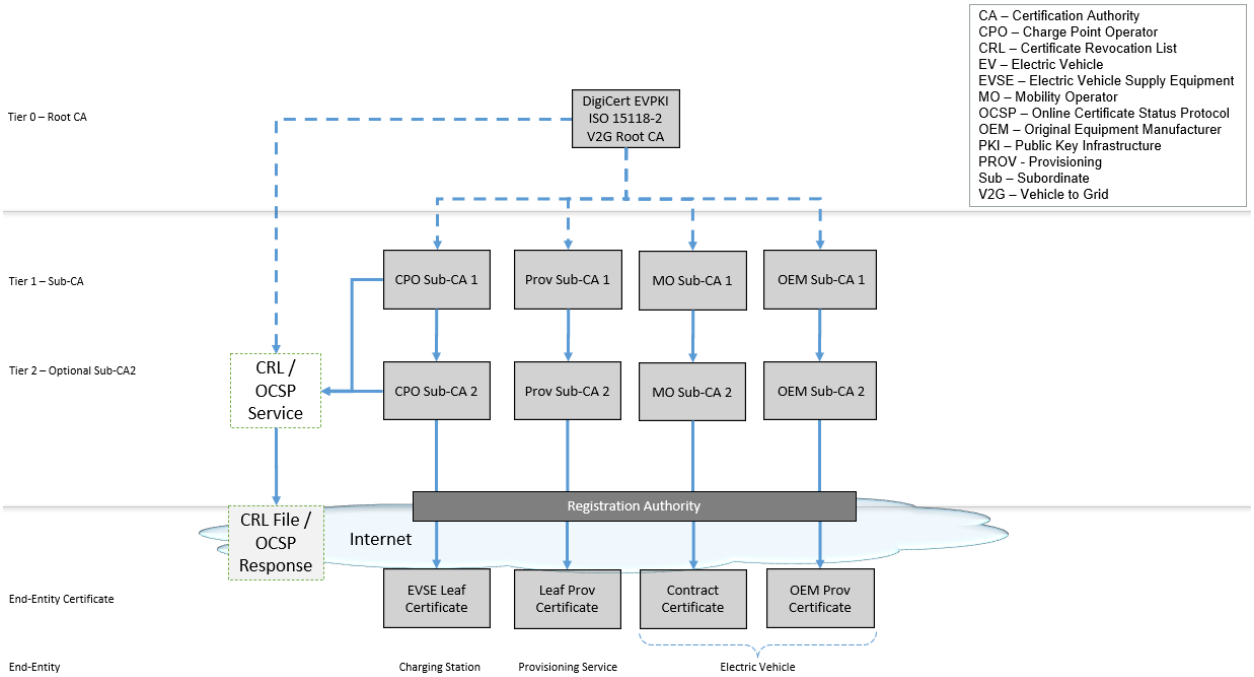

Figure 1: DigiCert EVPKI Architecture aligned with [ISO 15118-2] and [SAE EVPKI CP]

The DigiCert EVPKI architecture provided in Figure 2 is aligned with [ISO 15118-20] and [SAE EVPKI CP].

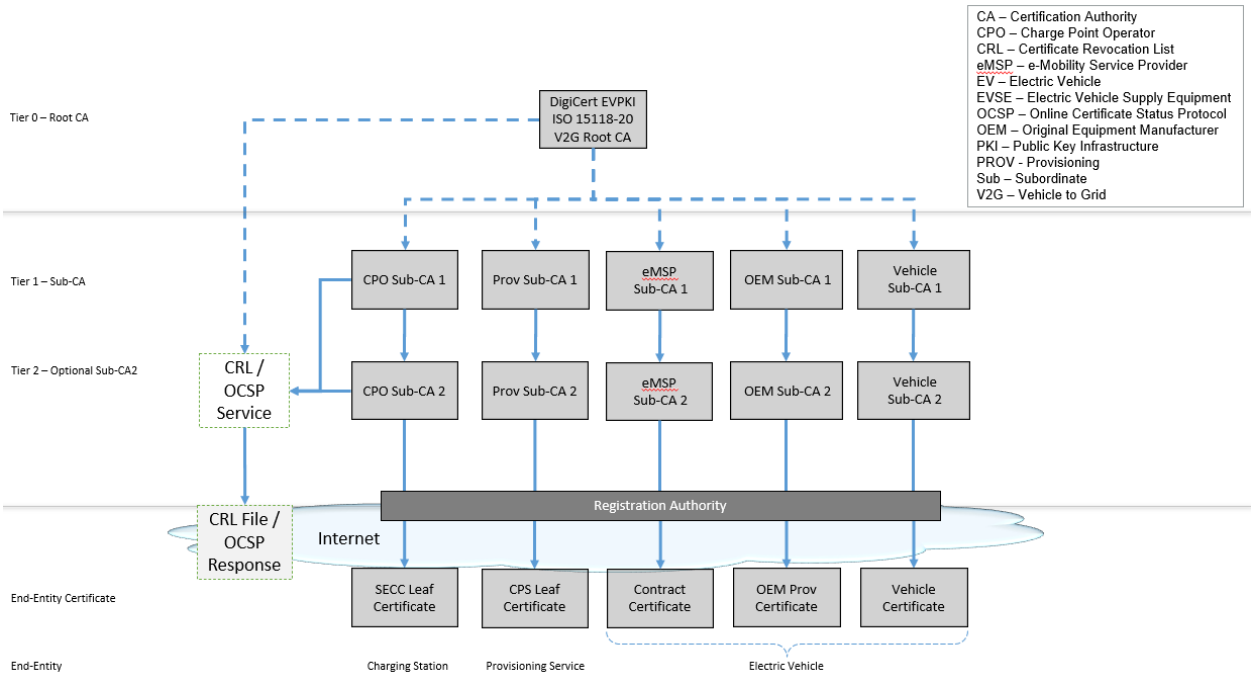

Figure 2: DigiCert EVPKI Architecture compliant with [ISO 15118-20] and [SAE EVPKI CP]

This document uses the words defined in [RFC 2119] to signify the requirements for this document. Throughout this document, the following capitalized words are used to define the significance of particular requirement:

“SHALL”	This word, or the terms “REQUIRED” or “MUST”, mean that the item is an absolute requirement in this document.
“SHALL NOT”	This phrase, or the phrase “MUST NOT”, mean that the item is an absolute prohibition in this document.
“SHOULD”	This word, or the adjective “RECOMMENDED”, mean 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”, mean 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 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 document 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 the document or to all Certificates)
	Root CA
	Subordinate CAs (Sub-CAs)
	All CAs
	End-Entity Certificates
	Certificate Revocation List (CRL)
	Online Certificate Status Protocol (OCSP)

1.2 Document Name and Identification

1.2.1 Certificate Policy Name

This document is the DigiCert Electric Vehicle (EV) Public Key Infrastructure (PKI) Certificate Policy (CP), a private PKI for issuing Certificates to the EV charging ecosystem, and has been approved for publication by DCPA as of the date indicated on the cover page.

1.3 PKI Participants

The PKI Participants that are relevant to the administration and operation of the DigiCert EVPKI include the:

- DigiCert Policy Authority (DCPA)
- Certification Authority (CA)
- Registration Authority (RA)
- Subscribers
- Relying Parties

1.3.1 DigiCert Policy Authority (DCPA)

The DigiCert Policy Authority (DCPA) is the owner of the DigiCert EVPKI and is responsible for setting up and approving policies and practices governing the PKI.

The PA SHALL have the following responsibilities:

- Establishing and approving this CP;
- Governing the EVPKI according to this CP;
- Approving the establishment of trust relationships with external PKIs;
- Approving the Audits for Root CAs operating under this CP; and
- Approving any revisions to this CP.

1.3.2 Certification Authority (CA)

DigiCert performs the functions of the CAs associated with the DigiCert EVPKI, including receiving applicable Certificate requests, issuing, Revoking and Renewing a digital Certificate, and maintaining, issuing, and publishing CRLs and OCSP responses.

The CA SHALL have the following responsibilities:

- Approving the issuance of Certificates;
- Revoking Certificates it has issued;
- Providing PKI Participants, e.g., via a CA Repository, with access to CA Certificates it has issued;
- Generating, protecting, operating, and destroying its CA Private Keys;
- Establishing and maintaining its CP and associated CPS;
- Managing its Online Certificate Status Protocol (OCSP) responder and Certificate Revocation List (CRL) generation and distribution;
- Managing its Repository of Certificate related items;
- Managing all aspects of its CA services, operations and infrastructure related to Certificates (e.g., configuration management, and Archive);
- Securing delivery of Sub-CA Certificates to Sub-CAs;
- On-boarding Prospective Subscribers or Sub-CAs to the Certificate issuance process; and
- Securing delivery of Certificates to its Subscriber.

Within this CP, the acronym “CA or CAs” includes the Root and its Sub-CAs. If a requirement only applies to the Root CA, it will denote Root CA. If it only applies to Sub-CAs, it will denote Sub-CA.

1.3.3 Registration Authority (RA)

The Registration Authority (RA) is a trusted entity that can perform specific Certificate management functions on behalf of the CA. DigiCert MAY delegate the performance of certain Certificate lifecycle management functions to its RA including Certificate request processing and/or Subscriber identification verification.

The RA SHALL perform its functions in accordance with the requirements contained in this CP, as well as any additional relevant policies and procedures included in the CA's CPS.

In this document, if a requirement only applies to the CA, it SHALL denote CA. If a requirement applies to the RA on behalf of the CA, it SHALL denote RA.

1.3.4 Subscribers

A Subscriber is the entity whose identity attributes (e.g., organization name, common name, etc.) appear in the Subject Distinguished Name of the Certificate. The Subscriber agrees to use its Private Key and Public Key Certificate in accordance with the requirements contained in this CP, asserted in the Subscriber's Certificate *certificatePolicies* extension. The Subscriber's Certificate itself does not issue other Certificates.

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.

1.3.5 Relying Parties

A Relying Party is the entity that depends on the binding of the Certificate Subscriber's name to its corresponding Public Key. The Relying Party is responsible for deciding whether or how to check the status of the Certificate by checking the appropriate Certificate status information. The Relying Party can use the Certificate to determine the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the holder of the Certificate. A Relying Party MAY use information in the Certificate (such as Certificate Policy identifiers) to determine the suitability of the Certificate for a particular use.

1.3.6 Other Participants

Other Participants are defined in their respective CPs, guidelines, and by contract with DigiCert.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

Appropriate Certificate uses SHALL include:

- Self-signed Root CA issuance of Tier-1 CA Certificates and OCSP Responder Certificates;
- Tier-1 CA issuance of Tier-2 CA Certificates or End-Entity Certificates, as well as OCSP Responder Certificates;
- Tier-2 CA Certificates issuance of End-Entity Certificates, as well as OCSP Responder Certificates; and
- End-Entity Certificates are used for:
  - Authentication purposes, as designated by the *keyUsage* and *extKeyUsage* fields found within the Certificate; and
  - Identification purposes, as designated by the *keyUsage* and *extKeyUsage* fields found within the Certificate.

The DCPA MAY allow additional permitted uses not included in this CP at the discretion of the DCPA.

1.4.2 Prohibited Certificate Uses

Certificates do not guarantee that the Subject is trustworthy, honest, reputable in its business dealings, compliant with any laws, or safe to do business with. A Certificate only establishes that the information in the Certificate was verified as reasonably correct when the Certificate was issued. The following applications MUST NOT be used:

- 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, unless permitted by the DCPA.

The DCPA MAY add prohibited uses not included in this CP at the discretion of the DCPA.

1.5 Policy Administration

1.5.1 Organization Administering the Document

This CP is owned and administered by the DCPA and represents the interest of its members in developing the policies that govern the DigiCert EV PKI.

1.5.2 Contact Person

This CP is maintained by the DCPA, which can be contacted at:

DigiCert Policy Authority
Suite 500
2801 N. Thanksgiving Way
Lehi, UT 84043 USA
Tel: 1-801-701-9600
Fax: 1-801-705-0481
policy@digicert.com

1.5.3 Person Determining CPS Suitability for the CP

The DCPA determines the suitability and applicability of this CP and is responsible for the PKI's compliance with this CP.

1.5.4 CP and CPS Approval Procedures

The DCPA is responsible for approving this CP and any amendments. Amendments are made after the DCPA has reviewed the amendments' consistency with technical requirements and the relevant contracts. The DCPA determines whether an amendment to this document is consistent with a contract, technical requirements, requires notice, or requires an OID change.

1.6 References, Definitions, and Acronyms

1.6.1 References

This document uses the following references:

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
DigiCert Private PKI CP/CPS	DigiCert Legal Repository, available at https://www.digicert.com/legal-repository/, as updated from time to time
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 186-5	Digital Signature Standards (DSS), FIPS 186-5, February 2023, Digital Signature Standard (DSS) (nist.gov)
ISO 15118-1	*Road vehicles — Vehicle to grid communication interface — Part 1: General information and use-case definition (2019)*
ISO 15118-2	Road Vehicles – Vehicles-to-Grid Communication Interface – Part 2: Network and application protocol requirements (2014-04-01)
ISO 15118-20	Road Vehicles – Vehicles-to-Grid Communication Interface – Part 20: 2nd generation network layer and application layer requirements (2022-04)

ISO 27001	Information technology – Security techniques – Information security management systems – Requirements (ISO/IEC 27001:2022)
ISO 3166-1	Codes for the representation of names of countries and their subdivisions – Part 1: Country codes, https://www.iso.org/iso-3166-country-codes.html
RFC 2119	Key words for use in RFCs to Indicate Requirement Levels (March 1997), https://www.ietf.org/rfc/rfc2119.txt
RFC 3647	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (November 2003), https://www.ietf.org/rfc/rfc3647.txt
RFC 5019	The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments (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 6818	Updates to Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (January 2013) – Updates RFC 5280, rfc-editor.org/rfc/rfc6818.txt
RFC 6960	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP (June 2013), https://www.ietf.org/rfc/rfc6960.txt
RFC 7748	Elliptic Curves for Security (January 2016), https://www.rfc-editor.org/rfc/rfc7748
RFC 8032	Edwards-Curve Digital Signature Algorithm (EdDSA) (January 2017), https://www.rfc-editor.org/rfc/rfc8032
RFC 8954	Online Certificate Status Protocol (OCSP) Nonce Extension; Update RFC 6960 (November 2020), RFC 8954: Online Certificate Status Protocol (OCSP) Nonce Extension (rfc-editor.org)
RFC 9549	Internationalization Updates to RFC 5280 (March 2024), https://www.rfc-editor.org/rfc/rfc9549.txt
RFC 9598	Internationalized Email Addresses in X.509 Certificates (May 2024), https://www.rfc-editor.org/rfc/rfc9598.txt
RFC 9608	No Revocation Available for X.509 Public Key Certificates (June 2024), https://www.rfc-editor.org/rfc/rfc9608.txt
RFC 9618	Updates to X.509 Policy Validation (August 2024), https://www.rfc-editor.org/rfc/rfc9618.txt
SAE EVPKI CP	SAE Electric Vehicle Public Key Infrastructure Certificate Policy (CP) v1.2 (2024-11-12)
SP 800-63-3	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
SSAE 18	Replaces Statement of Auditing Standards 70 (SAS 70). Statement on Standards for Attestation Engagements No. 18 (April 2016), https://www.aicpa-cima.com/resources/download/aicpa-statement-on-standards-for-attestation-engagements-no-18
X.500	ITU-T Recommendation X.500 Series (1994) – ISO/IEC 9594, 1-9:1994, *Information Technology – Open Systems Interconnection – The Directory*

1.6.2 Definitions

This document uses the following terms and definitions:

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]
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.
Archive	Long-term, physically separate storage.
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]
Authorized Entity	An entity that is Authenticated to act on behalf of an organization or Subscriber.
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 of 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 Certificate Repository	A database containing information and data relating to the CA's Certificate and any Sub-CA Certificates issued by 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 the CA that issued it; • Names or identifies the Subscriber of the Certificate; • Contains the Subscriber's Public Key; • Identifies its operational period; and • It is digitally signed by the CA that issued it. 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 contains the naming information that will be included in the Certificate.
Certificate Policy (CP)	A specialized form of administrative requirements 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 it has issued that are Revoked prior to their stated expiration date.
Certificate Signing Request (CSR)	A message conveying a request to have a Certificate issued.
Certificate Status Services (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.
Competent	Having the necessary ability, knowledge, or skill to do something successfully.
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 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.
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 Certificate	An End-Entity Authentication Certificate or an End-Entity Identity Certificate.
End-Entity Identity Certificate	An End-Entity Certificate used to identify the Subscriber to a Relying Party (e.g., Mobility Operator (MO)).
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.
Intermediate CA (ICA)	A CA subordinate to the Root CA 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.
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.
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.
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 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.
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 Intermediate CAs (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.
Subordinate CA (Sub-CA)	In a hierarchical PKI, a CA whose Certificate signature key is certified by another CA, and whose activities are constrained by that other CA.
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.
Superior CA	In a hierarchical PKI, a CA who has certified the Certificate signature key of another CA, and who constrains the activities of that CA.
Superior Entity	An entity that has a governance relationship to a CA and constrains the activities of that CA via the governance requirements.
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	Personnel, designated to manage the PKI's trustworthiness, identified to perform functions that can introduce security problems into a PKI if not carried out properly, whether accidentally or maliciously.
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.
WebTrust	An assurance service jointly developed by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA). WebTrust relies on a series of principles and criteria designed to promote confidence and trust between consumers and companies conducting business on the Internet.

1.6.3 Abbreviations and Acronyms

This document uses the following abbreviations and acronyms:

CA	Certification Authority
CP	Certificate Policy
CPO	Charge Point Operator
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CRP	(SAE International) Collaborative Research Project
CSR	Certificate Signing Request
CSS	Certificate Status Services
DN	Distinguished Name
DRP	Disaster Recovery Plan
eMSP	e-Mobility Service Provider
EV	Electric Vehicle

EVSE	Electric Vehicle Supply Equipment
FIPS	Federal Information Processing Standards
HSM	Hardware Security Module
ICA	Intermediate Certification Authority
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
MA	Management Authority
MO	Mobility Operator
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OEM	Original Equipment Manufacturers
OID	Object Identifier
PA	Policy Authority
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKCS	Public Key Cryptography Standards
Prov	Provisioning
RA	Registration Authority
RFC	Request for Comment
SECC	Supply Equipment Communication Controller
SP	Special Publication
Sub-CA	Subordinate CA
TLS	Transport Layer Security
URI	Uniform Resource Identifier
V2G	Vehicle-to-Grid

2 Publication and Repository Responsibilities

2.1 Repositories

CA Repositories, CRLs, and OCSP responses are available through online resources twenty-four (24) hours a day, seven (7) days a week. To promote consistent access to Certificates and CRLs, the CA Repository SHALL implement Access Controls to prevent unauthorized modification or deletion of information.

2.2 Publication of Certification Information

This CP, CRLs, CA Certificates and CPS SHALL be available as shown on Table 1.

Table 1: Publication Requirements

Item	Classification	Available From:
DigiCert EV PKI CP	Public	https://www.digicert.com/legal-repository
Root CA Certificates	Public	CA Repository
Sub-CA Certificates	Public	CA Repository
Root CA CRLs	Public	The location listed in the *cRLDistributionPoint* extension of Certificates issued by the Root CA
Sub-CA CRLs	Public	The location listed in the *cRLDistributionPoint* extension of Certificates issued by the Sub-CA
CA CPS	Public	https://www.digicert.com/legal-repository
Audit results	Confidential	https://www.digicert.com/webtrust-audits

A CA MAY redact any information it deems confidential from its publicly available CPS and Audit results.

The CA SHALL protect information not intended for public dissemination.

2.3 Time or Frequency of Publication

The PA SHALL make updates to this CP publicly available within seven (7) business days of the incorporation of changes.

The CA SHALL make any CA Certificate it issues publicly available within seven (7) business days after issuance.

The CA SHALL generate and publish its CRL as specified in Section 4.9.7.

The CA SHALL make updates to its CPS publicly available within seven (7) business days of the incorporation of changes.

2.4 Access Controls on Repositories

2.4.1 Certificate Policy

The DCPA SHALL make this CP publicly available for read-only Access.

2.4.2 Certificates, CPS, and CRLs

The CA SHALL make the CA Certificates and CRLs in the Repository publicly available for read-only Access to protect Certificate, CPS and CRL information from Modification or deletion.

3 Identification and Authentication

3.1 Naming

3.1.1 Type of Names

The CAs SHALL assign non-empty X.509 Distinguished Names (DNs) [X.500] to the *issuer* and *subjectDN* fields of the Certificates issued as shown in Table 2.

Table 2: Certificate Names

Certificate	Attribute	Issuer DN	Subject DN
Root CA Certificates	Country (c=) Organization (o=) Organizational Unit (ou=) Common name (cn=) Domain Component (dc=)	[c=<2-letter ISO 3166-1 country code>] o=<Organization Name> [ou=<optional field>] cn= < Root CA name> [dc=<Domain Component>]	[c=<2-letter ISO 3166-1 country code>] o=<Organization Name> [ou=<optional field>] cn=< Root CA name> [dc=<Domain Component>]
Sub-CA Certificates	Country (c=) Organization (o=) Organizational Unit (ou=) Common name (cn=) Domain Component (dc=)	[c=<2-letter ISO 3166-1 country code>] o=<Organization Name> [ou=<optional field>] cn=<Superior CA common name> [dc=<Domain Component>]	[c=<2-letter ISO 3166-1 country code>] o=<Organization Name> [ou=<additional identifying information>] cn=<Sub-CA common name> [dc=<Domain Component>]
End-Entity Certificates	Country (c=) Organization (o=) Organizational Unit (ou=) Common name (cn=) Domain Component (dc=)	[c=<2-letter ISO 3166-1 country code>] o=<Organization Name> [ou=<additional identifying information>] cn=<Sub-CA common name> [dc=<Domain Component>]	[c=<2-letter ISO 3166-1 country code>] o=<Organization Name> [ou=<additional information>] cn=<unique identifying information> [dc=<Domain Component>]

Note that in the table above:

- "[ ]"denotes an optional field. Certificate validation ignores the absence of this field.
- "< >" denotes an input value that the parameter is set to.

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 *UTF8* to the *issuer* and *subjectDN* fields.

3.1.2 Need for Names to be Meaningful

The CA or RA MUST verify that names used in to-be-issued DigiCert EV PKI Certificates represent an unambiguous identifier for the Subject and that the Subject contains the verified identification of the Sub-CA or Subscriber. The RA MUST use the verified company name or Subscriber name as the *organizationName* field in the Subject DN of the issued Certificate. The Subject DN of a Certificate is verified as described in Section 3.2.

3.1.3 Anonymity or Pseudonymity of Subscribers

The CA, or a RA on behalf of the CA, SHALL NOT issue Anonymous or Pseudonymous Certificates.

3.1.4 Rules for Interpreting Various Name Forms

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

3.1.5 Uniqueness of Names

Subscriber Subject DNs in a Certificate SHALL be unique per each Subject entity certified by the CA within a Root CA domain. CAs MAY issue Certificates with the same Subject DN to the same Subject entity such as in cases involving Renewing, Revoking, Re-Key, Modification, expiring Certificates, etc.

3.1.6 Recognition, Authentication, and Role of Trademarks

The CA, and its RAs, SHALL NOT knowingly issue a Certificate including a name that a court of Competent jurisdiction has determined infringes upon a third party's trademark and/or Intellectual Property Rights.

Prospective Subscribers SHALL NOT knowingly use names in their Certificate Applications that infringe upon the Intellectual Property Rights of others.

The CA or RA SHALL NOT knowingly issue a Certificate including the name of any entity, such as an organization name, 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).

The 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 trademark and/or Intellectual Property Rights, including, without limitation, rights in a domain name, trade name, trademark, or service mark.

DigiCert and any CA SHALL be entitled, without liability to any Prospective Subscriber, to reject or suspend any Subscriber agreement because of such dispute.

The CA or RA SHALL correct, if necessary, any disputes regarding names brought to its attention.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

The Authentication of the Sub-CA or 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 Sub-CA or Subscriber generates its own keys, that Sub-CA or Subscriber SHALL prove possession of the Private Key, which corresponds to the Public Key in the PKCS #10 Certificate Signing Request (CSR). For example, this MAY be done by the Sub-CA or Subscriber using its Private Key to sign the CSR. The RA SHALL then validate the signature using the Sub-CA or Subscriber's Public Key provided in the CSR.

For cases where a trusted administrator submits the CSR on behalf of the Subscriber for an End-Entity Certificate, proof of possession MAY be done via a challenge-response mechanism between the EV (storing the Subscriber Private Key) and the Electric Vehicle Supply Equipment (EVSE) at a later time.

The CA SHALL describe in its CPS how it validates possession of the Private Key.

3.2.2 Authentication of Organization Identity

The RA SHALL verify the identity of the organization by confirming that the organization:

- Exists in a business database (e.g., Dun & Bradstreet), or alternatively, has organizational documentation issued by or filed with the applicable government (e.g., government issued business credentials) that confirms the existence of the organization, such as Articles of Incorporation, Certificate of Formation, Charter Documents, or a business license that allows it to conduct business.

The RA SHALL verify that the identity of the organization:

- Is not on a government watch list at the CA's location;
- If the organization is on a watch list, the RA will comply with applicable law and exercise discretion in determining whether to continue with the Authentication;
- Conducts business at the address provided; and
- The verified organization or trade name is used in the *organizationName* field of the Certificate as a way for Relying Parties to Authenticate the organization name.

3.2.3 Authentication of Individual Identity

For Authentication of PKI Sponsors and Authorized Entities, prior to them requesting Certificates on behalf of Subscribers, the RA SHALL verify:

- The organization that the PKI Sponsor or Authorized Entity is representing;

- That the individual is an employee, partner, member, agent, etc. authorized to act on behalf of the organization;
- That the email address of the individual is controlled by the organization; and
- That the individual can be reached through another communication channel of the organization (e.g., a central number) obtained by the RA and not just by the information provided by the individual.

For individuals (e.g., Subscribers) requesting Certificates, the RA SHALL verify:

- That the individual is authorized by the organization to be named in the Certificate;
- That the individual's identity has been verified by the RA or Authorized Entity; and
- That the request was received from a certified/approved organization or Authorized Entity.

3.2.4 Non-verified Subscriber Information

Subscriber information that is not verified by the CA or RA SHALL NOT be included in Certificates.

3.2.5 Validation of Authority

The RA SHALL confirm that the:

- End-Entity Certificates are only issued to authorized Subscribers; and
- PKI Sponsors and Authorized Entities submitting Certificate Applications are authorized to act on behalf of the organization/Subscriber to be listed in the Certificate.

3.2.6 Criteria for Interoperation

The DCPA SHALL determine the criteria for cross certification with other entities.

3.3 Identification and Authentication for Re-Key Requests

Certificate Re-Key consists of creating a new Certificate with 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.

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.

3.3.2 Identification and Authentication for Re-Key after Revocation

Once a CA Certificate has been Revoked, the Superior Entity 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 CA Certificate and the Re-Key SHALL require completion of the aforementioned plan, in the requirement above, and SHALL require following the same process as the initial registration process, described in Section 3.2.

Issuance of a new End-Entity Certificate for Re-Key SHALL require following the same process as the initial registration process, described in Section 3.2.

3.4 Identification and Authentication for Revocation Request

Revocation requests MUST be Authenticated by the CA or the RA 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. The Revocation request mechanisms MAY include challenge-response questions combined with a completed CA provided Revocation request form that was sent to the Certificate holder at the time of the Revocation request. The CA SHALL document those details in its CPS showing how or if the Revocation will be completed or not. 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. 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.

4 Certificate Life Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

The following Prospective Subscribers or Sub-CAs MAY request Certificates:

- Any entity that participates in providing EV charging services (e.g., EV OEMs, EVSE Manufacturers, Engine Control Unit (ECU) manufacturers, etc.);
- Any administrator or agent of any such entity above;
- Any Prospective Subscriber (Sub-CA, PKI Sponsor, or Authorized Entity;
- Any RA on behalf of the Prospective Subscriber or Sub-CA; or
- Any CA on behalf of the Prospective Subscriber or Sub-CA.

4.1.2 Enrollment Process and Responsibilities

Prospective Subscribers SHALL submit sufficient information to allow the CA or RA to successfully perform the required verification.

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

Prospective Subscribers or an Authorized Entity SHALL:

- Agree to the applicable Subscriber agreement, if required;
- Complete the Certificate Application;
- Provide the requested information;
- Respond to verification requests in a timely manner;
- Generate the Key Pair, if required;
- Deliver the Public Key of the Key Pair to the RA, if required; 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.

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 or Sub-CAs requesting Certificates, as specified in Sections 3.2 and 3.3.

4.2.2 Approval or Rejection of Certificate Applications

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

- Receipt of a fully executed Subscriber agreement, if applicable;
- Receipt of a signed Certificate Application;
- Successful validation per Section 3.2;
- Receipt of all requested supporting documentation; and
- Receipt of payment (if applicable).

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 or Sub-CA fails to execute the required Subscriber agreement, if applicable;
- An authorized representative fails to sign the Certificate Application;
- Unable to successfully validate the organization;
- The Prospective Subscriber or Sub-CA fails to furnish requested supporting documentation;

- The Prospective Subscriber or Sub-CA fails to respond to notices within a specified time;
- The Prospective Subscriber or Sub-CA 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.

The CA MAY reject any Certificate Application if the CA believes that issuing a Certificate MAY bring the CA into disrepute. The CA SHALL log all Certificate Application rejections and the reason for the rejection.

4.2.3 Time to Process Certificate Applications

CAs or RAs SHALL process Certificate Applications within a reasonable time of receipt of all necessary documents as specified in their CPS. Events outside of the control of DigiCert can delay the issuance process.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

A Certificate is issued by the CA following the approval of a Certificate Application.

If using a RA, the CA, upon receiving the Certificate request, SHALL:

- Authenticate the RA using a credential provided to the RA by the CA;
- Receive the PKCS #10 CSR generated by the Subscriber or Sub-CA from the RA, if applicable;
- Generate a CSR, if necessary;
- Generate a Certificate using the Public Key in the CSR, along with any additional Certificate profile information provided by the Subscriber or Sub-CA, or the RA on behalf of the Subscriber or Sub-CA; and
- Ensure delivery of the Certificate to the Subscriber or Sub-CA.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificates

CAs issuing Certificates SHALL notify the Subscriber or Sub-CA, or the RA on behalf of the Subscriber or Sub-CA, of the issuance of a Subscriber or Sub-CA Certificate.

The CA or RA SHALL inform the Subscriber or Sub-CA, through information submitted during the Certificate enrollment process, that their Certificate is available and the means for obtaining the Certificate. The details of the process employed by the CA or RA SHALL be detailed in the CPS.

4.4 Certificate Acceptance

Once downloaded, the Subscriber or Sub-CA SHOULD check the contents of the Certificate without delay. If the Subscriber or Sub-CA detects any problems with the issued Certificate (e.g., incorrect information, wrong Validity Period, etc.), the Subscriber or Sub-CA SHALL notify the RA about the problem.

4.4.1 Conduct Constituting Certificate Acceptance

An issued Certificate SHALL be deemed to have been accepted when the Subscriber or Sub-CA has downloaded and used the Certificate, and the Subscriber or Sub-CA has not notified the CA or RA of a problem with the Certificate or its contents, or thirty (30) days after the Certificate's issuance, whichever comes first.

4.4.2 Publication of Certificate by the CA

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

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

CAs operating under this CP MAY notify the PKI Participants, through the RA, PA or Management Authority (MA), whenever it issues a CA Certificate.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Subscriber or Sub-CA use of the Certificate SHALL only be permitted once the Subscriber or Sub-CA has agreed to a Subscriber agreement (if applicable) and accepted the Certificate, as described in Section 4.4.1. Subscriber or Sub-CA SHALL use the Private Key consistent with the *keyUsage* and *extKeyUsage* extensions, in the associated Certificate.

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

Subscriber or Sub-CA SHALL use the Certificate(s) in lawful accordance with the Subscriber agreement, if applicable, and the terms of this CP.

4.5.2 Relying Party Public Key and Certificate Usage

Before any act of reliance, Relying Parties MAY 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 SHOULD NOT rely on the Certificate or other Revoked Certificates in the Certificate chain to establish trust.

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 all the following conditions are met:

- The Public Key has not reached the end of its Validity Period (as described in Section 6.3.2);
- The associated Private Key has not been Revoked or Compromised; and
- The Subscriber name and attributes are unchanged.

Certificates MAY be Renewed as long as the lifetime of the Public Key validity exceeds the aggregate Certificate lifetime (i.e., the original Certificate Validity Period plus the Renewal Validity Period) specified in accordance with 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 Entity of the Subscriber;
- The CA, to request a Renewal of its own Certificate; or
- The 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 validation of the Renewal request 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.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Acceptance of the Renewed Certificate 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

Certificate Re-Key consists of creating a new Certificate for a new 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.

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

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

Re-Key of a Certificate SHALL include a new Public Key. A Re-Key request SHALL NOT be processed if the Public Key is same as the Public Key in the currently active Certificate which is being requested to be Re-Keyed. Any Certificate holder MAY request a Re-Key for a valid Certificate.

A CA MAY Re-Key a Certificate even after Revocation. A Certificate MAY also be Re-Keyed before expiration to maintain continuity of Certificate usage.

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

Requests to the RA for Re-Key SHALL be considered for the following:

- Subscribers with a currently valid Certificate;
- The RA MAY request a new Public Key on behalf of a Subscriber;
- The CA MAY request a Re-Key of its own Certificate;
- The CA MUST Re-Key its issued CA Certificates during recovery from a CA key Compromise;
- The CA MAY resign Subscriber Certificates that are long-lived (greater than five (5) years) and had the Key Pair generated by the Subscriber (e.g., OEM) at the time of manufacture, otherwise the Subscriber Certificates MUST be Re-Keyed; or
- The Superior CA MAY request Re-Key of Sub-CA Certificate.

4.7.3 Processing Certificate Re-Keying Requests

A CA SHALL require revalidation of the Subscriber or Sub-CA prior to Re-Key of a Certificate.

4.7.4 Notification of New Certificate Issuance to Subscribers

The CA SHALL inform the Subscriber or Sub-CA of the Re-Key of the Subscriber's Certificate, as per Section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

Acceptance of the Re-Keyed Certificate 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

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.

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

4.8.1 Circumstance for Certificate Modification

The RA MAY accept Certificate Modification requests only for Subscriber or Sub-CA's characteristics that 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;
- The CA MAY request a Certificate Modification of its own Certificate; or
- The PA MAY request Modification of CA Certificates.

4.8.3 Processing Certificate Modification Requests

CA Certificate Modification SHALL be approved by its Superior CA.

For Certificate Modification requests, the RA SHALL confirm the identity of the Subscriber or Sub-CA in accordance with the requirements, as specified in Section 3.

4.8.4 Notification of Modified Certificate Issuance to Subscriber

The CA SHALL inform the Subscriber or Sub-CA of the Modification of its Certificate, in accordance with Section 4.3.2.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

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

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

CAs that issue CRLs, SHALL make public a description of how to obtain Revocation information for the Certificates they issue via the issued Certificate's *cRLDistributionPoints* extension.

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.

4.9.1 Circumstances for Revocation

The RA SHALL request from the 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. The CA SHALL include all Revoked Certificates on all new publications of the CSS (see Section 4.10) until the Certificates expire.

Revocation SHALL occur on the decision of the CA when reasonable and credible evidence exists to establish one (1) or more 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 or Sub-CA can be shown to have violated the stipulations of its Subscriber agreement, if applicable, or one or more sections of this CP;
- The original Certificate request was not authorized;
- The Subscriber, Sub-CA or other authorized party asks for its Certificate to be Revoked;
- The Subscriber or Sub-CA 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 the Private Key associated with the Certificate is no longer ensured or Private Key associated with the Certificate has been Compromised; or
- The media holding the Private Key associated with the Certificate is suspected or known to have been Compromised.

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 (i.e., Certificate serial number, issuer CA), 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 RA SHALL disclose the Revocation instructions to PKI Participants through a readily accessible online means. Once Authenticated, the RA SHALL inform the CA 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.

The CA, MA, or RA at their discretion, MAY take whatever measures they deem appropriate to verify the need for Revocation. If the RA approves the Revocation, the RA SHALL direct the CA to Revoke the Certificate.

4.9.4 Revocation Request Grace Period

PKI Participants SHALL request Revocation as soon as they identify the need for Revocation and at least within twenty-four (24) hours after detecting 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 an Authenticated Revocation request. Once a Certificate has been Revoked the Revocation SHALL be reflected in supported OCSP responses issued within one (1) hour, and in supported CRLs within twenty-four (24) hours.

The Issuer CA SHALL maintain a continuous 24/7 ability to internally respond to any high priority Revocation requests.

4.9.6 Revocation Checking Requirement for Relying Parties

A Relying Party SHOULD obtain the current CRL or employ the CSS (i.e., OCSP responder) provided by the 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, web-based Repository, or CSS to check the Revocation status of Certificates issued by the CA.

.

Fallback operation: In the event Certificate status checking is not available, Relying Parties SHOULD use the cached version of the CRL until the latest CRL can be downloaded or the online availability of CSS is restored.

4.9.7 CRL/CSS Issuance Frequency

The CA SHALL generate and publish (a.k.a. issue) CRLs or CSS information periodically. Certificate status information MAY be issued more frequently than the issuance frequency described below. A CA SHALL ensure that obsoleted 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.

Table 3 below provides CRL/CSS issuance frequency requirements.

Table 3: CRL Frequency

Type of CRL	Issuance Frequency
Routine	At least quarterly, i.e., the CRL SHALL be published at least every three (3) months
Loss/Compromise of End-Entity Certificate Private Key (Emergency)	Within twenty-four (24) hours of notification
Loss/Compromise of CA Private Key (Emergency)	Immediately, but no later than within twenty-four (24) hours of notification

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

The CAs that issue routine CRLs/CSSs less frequently than the requirement for emergency CRL/CSS 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/CSSs.

4.9.8 Maximum Latency for CRLs/CSSs

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

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.

CAs SHALL provide Relying Parties with information in the Certificate on how to find the appropriate Repository to check Certificate status, or how to find the correct OCSP responder.

All online CRLs/CSSs SHALL have service availability of not less than 99.9% with scheduled downtime notification of at least thirty (30) hours in advance, under normal operating circumstances.

4.9.10 Online Revocation Checking Requirements

Relying Parties 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 by using the path validation algorithm in Section 6 of the Internet Engineering Task Force (IETF) Request for Comments [RFC 5280].

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

No stipulation.

4.9.12 Special Requirements Regarding Key Compromise

See Section 4.9.3.

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

4.9.13 Circumstances for Suspension

Suspension is not supported by this CP.

4.9.14 Who Can Request Suspension

Suspension is not supported by this CP.

4.9.15 Procedure for Suspension Request

Suspension is not supported by this CP.

4.9.16 Limits on Suspension Period

Suspension is not supported by this CP.

4.10 Certificate Status Services (CSS)

DigiCert MUST include a service that provides status information about Certificates on behalf ofCAs through online transactions (i.e., CRLs and OCSP). In particular, the EVPKI CAs include CRLs and/or 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.

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

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 the 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.

Relying Parties MAY ascertain the Certificate status by querying the CRL maintained and published in its Repository by the CA, or by querying an authorized OCSP responder.

4.10.2 Service Availability

The 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: 99.9%
- 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 a maximum of seven (7) days (168 hours) for cases where the Relying Party is not able to Access the Certificate status online.

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

Subscription is synonymous with the Subscriber's agreement, if applicable. The subscription ends when the Subscriber's agreement terminates.

For Certificates that have expired prior to or upon end of the Subscriber's agreement, Revocation is not required.

CAs SHALL always Revoke unexpired Certificates at the end of the subscription.

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

5.1 Physical Controls

The CA SHALL physically protect all CA equipment, including Cryptographic Modules from theft, loss, and unauthorized Access as specified in Section 5.1.2. Unauthorized use of CA equipment is prohibited. The CA SHALL dedicate CA equipment to performing CA functions only.

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 CA physical control requirements specified below apply equally to the Root CA and Sub-CAs.

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.

5.1.2 Physical Access

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;
- 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
- Require multi-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 by 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 multi-person Access Controls, and multi-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.

Physical Access for RA Equipment

The RA SHALL protect its RA equipment from theft, loss, and unauthorized Access.

5.1.3 Power and Air Conditioning

The CA SHALL have facilities equipped with primary and Backup power systems to ensure continuous (i.e., 24x7), uninterrupted Access to electric power sufficient for the operations of its Server and network connections to meet its service level agreements and also sufficient to lock out input, finish any pending actions, and record the state of the equipment automatically in case of a shutdown.

5.1.4 Water Exposures

The CA SHALL install its equipment in a manner that 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.

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. The fire prevention and protection measures SHALL meet all local applicable safety regulations.

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 Audit, Archive, or Backup information in a securely stored location separate from the CA equipment.

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].

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 as specified in Section 5.1.2.

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 CA Certificate Repository;
- The handling of Subscriber or Sub-CA 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 or RA is weakened. The functions performed in these roles form the basis of trust in the CA or RA. Multiple people MAY hold the same Trusted Role, with collective privileges sufficient to fill the role. CAs or RAs 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.

Each such Trusted Role's system Access is to be limited to those actions which they are REQUIRED to perform in fulfilling their responsibilities.

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 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
- If applicable, posting Certificates and CRLs.

The individual(s) with Access to the Private Keys SHALL NOT have Security Audit responsibilities, nor be able to generate system Backups and perform system recovery.

5.2.1.2 CA Operations Staff

The CA Operations Staff role is responsible for issuing Certificates.

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.

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.

5.2.1.3 Internal Auditor

Internal Auditors are responsible for internal Auditing of CAs and RAs and SHOULD have similar qualifications as the Compliance Auditor specified in Section 1.3.6. This sensitive role SHALL NOT be combined with any other sensitive role, e.g., the internal Auditor SHALL NOT also be part of the CA Operations Staff or CA Administrator or RA Staff. Internal 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.

5.2.1.4 RA Administration and Operations Staff

RA Administration 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 Internal Auditor Trusted Roles for that RA.

RA Administration Staff are 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; and
- Registering new Subscribers or Sub-CAs and requesting the issuance of Certificates.

RA Operations Staff are responsible for the following:

- 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.

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 multi-person 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 for CA/RA operations, at least one of the PKI Participants SHALL be a CA or RA administrator. Multi-person control SHALL NOT be achieved using personnel that serve in the Auditor Trusted Role. The internal Auditor MAY serve to fulfill the requirement of multi-party control for physical Access to the CA system but not logical Access.

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 within the organization managing Trusted Roles. 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. Any necessary security checks, as defined by the DCPA and/or the approving authority, for Trusted Role appointments/approvals SHALL also be performed at the discretion of the DCPA. If a continued need of these appointments is identified and all defined security checks pass, the appointment MAY be Renewed, if appropriate. The CA or RA SHALL record the Trusted Role approvals and Renewals in a secure and Auditable fashion. Individuals holding Trusted Roles SHALL accept the responsibilities of the Trusted Role in writing, and the CA or RA SHALL record this acceptance in a secure and Auditable fashion.

CAs or RAs 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, multi-person 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.

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 CA and RA SHALL have procedures to ensure that no user identity can assume multiple roles.

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

- CA Operations Staff:
  - 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, issuance, or destruction of a CA Certificate Private Key;
- CA Administration Staff:
  - Generation of CA Backups;
  - Loading of a CA to a production environment; and
  - Internal Auditor role.

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

- RA Operations Staff:
  - Acceptance, rejection, or other processing of Certificate Applications, Revocation requests, Renewal requests, or enrollment information;
  - Generation, issuance, or destruction of a Subscriber or Sub-CA Certificate Private Key;
- RA Administration Staff:
  - Generation of RA Backups;
  - Loading of a RA to a production environment; and
  - Internal 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.

5.3 Personnel Controls

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;
- Have not been previously relieved of Trusted Role duties for reasons of negligence or non-performance of duties (e.g., unauthorized disclosure of confidential information, theft, embezzlement, destruction of property, etc.); and
- Do not have any other disqualifications as documented by the CA in its CPS.

5.3.2 Background Check Procedures

The CA and RA SHALL select persons filling Trusted Roles on the basis of loyalty to the CA and RA organization, 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 references;
- 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; and
- Identification verification (e.g., driver's license, passport).

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

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;
- 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. If the CA and RA training uses a grading system (e.g., pass/fail) for testing, then the CA and RA SHALL include the training test results as part of the material to be reviewed during an Audit.

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.

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.

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.

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.

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.

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 and description 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/RA Facility:		
Personnel Access to room housing CA/RA equipment	X	X
Access to the CA/RA Server	X	X
Known or suspected violations of physical security	X	X
Any removal or addition of equipment to the CA/RA enclosure	X	X
System Configuration:		
Installation of the operating system	X	X

Auditable Event	CA	RA
Installation of the CA/RA software	X	X
Installation and removal of hardware Cryptographic Modules	X	
System startup	X	X
Any security-relevant changes to the configuration of the CA/RA	X	X
CA/RA hardware configuration	X	X
System configuration changes and maintenance	X	X
Cryptographic Module life cycle management-related events (e.g., receipt, use, de-installation, and retirement)	X	
Account Administration:		
Roles and users are added or deleted	X	X
The Access Control privileges of a user account or a role are modified	X	X
Appointment of an individual to a Trusted Role	X	X
Designation of personnel for multi-person control	X	X
System administrator accounts	X	X
Attempts to create, remove, set passwords or change the system privileges of the privileged users (Trusted Roles)	X	X
Attempts to delete or modify Audit logs	X	X
Changes to the value of maximum Authentication attempts	X	X
Resetting operating system clock	X	X
CA/RA Operational Events:		
Key generation	X	X
Start-up and shutdown of CA/RA systems and applications	X	X
Changes to CA/RA details or keys	X	X
Records of the destruction of media containing key material, Activation Data, or personal Subscriber information	X	X
Successful and unsuccessful attempts to log into the CA/RA system	X	X
The value of maximum Authentication attempts is changed	X	X
Maximum unsuccessful Authentication attempts occur during user login	X	X
A CA/RA Administrator unlocks an account that has been locked as a result of unsuccessful Authentication attempts	X	X
Attempts to set passwords	X	X
Attempts to modify passwords	X	X
Certificate Life Cycle Events:		
Certificate Application requests		X
Certificate requests	X	X
Issuance	X	
Refusal to issue Certificates	X	X
Re-Key	X	
Renewal	X	
Certificate Revocation requests	X	X
Revocation	X	

Auditable Event	CA	RA
Trusted Person Events:		
Logon and logoff to the CA/RA 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/RA system	X	X
Unauthorized attempts to Access system files	X	X
Failed read and write operations on the Certificate	X	
Personnel changes	X	X
RA 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

5.4.2 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 Compliance 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.

5.4.3 Retention Period of Audit Log

Audit Records MUST be accessible until reviewed, in addition to specific Records being Archived as described in Section 5.5.

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

5.4.4 Protection of Audit Logs

The CA and RA SHALL protect Audit logs from unauthorized viewing (i.e., viewing without permission from the CA, RA, or Internal Auditor), 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 by the CA/RA to ensure that:

- Only authorized personnel (i.e., CA, RA, or Internal Auditor) have read Access to the logs;
- Only authorized personnel (i.e., CA, RA, or Internal Auditor) MAY Archive Audit logs;
- Audit logs are not modified; and
- Audit logs are stored in a secure storage.

5.4.5 Audit Log Backup Procedures

No stipulation.

5.4.6 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 Audit logs SHALL be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism SHALL be used. Automated Audit processes SHALL be invoked at system or application start-up, and cease only at system or application shutdown. It SHALL NOT be possible to terminate automated Audit

logging processes while the CA/RA system is powered ON or still running. 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; affected CA (or RA) operations, except Revocation status services, SHALL be suspended until the Audit capability can be restored.

5.4.7 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 logged or Audited.

5.4.8 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.

5.5 Records Archival

5.5.1 Types of Records Archived

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

Table 5: Archival Events

Data to be Archived	CA	RA	MA
CP releases			X
CAs issued and key generation	X		
Export of CA Private Keys	X		
CPS reviews			X
Contractual obligations	X	X	X
Modifications and updates to CA system or configuration	X		
Subscriber identity verification data		X	
CRL issuance	X		
All Certificates issued, Re-Keyed, Renewed, and Revoked	X		
Audit logs	X	X	
Compliance Auditor reports	X		
Any attempt to delete or modify the Audit logs	X	X	
Remedial action taken as a result of violations of physical security	X		
Certificate request documentation	X	X	
Appointment of an individual to a Trusted Role	X	X	
Destruction of Cryptographic Modules	X		
All Certificate Compromise notifications	X	X	

5.5.2 Retention Period for Archive

Archive retention periods begin at the key generation event for any CA. For CAs that leverage key-rollover procedures a new retention period begins for each subsequent key generation event.

CAs SHALL maintain all Archived Records related to that CA, in an accessible fashion, for two (2) years after CA expiration or CA termination.

Individual RA Records associated with Certificate request Authorization, Certificate Revocation, Subscriber Authentication, or Subscriber Certificate acceptance MUST be maintained for a minimum of two (2) years after the Subject Certificate expiration date. Issuance of new Certificates with extended Validity Periods (i.e., Renewal, Re-Key or Modification) supported by existing Subscriber Authentication Records (i.e., Authentication using an existing

valid Certificate) will result in a new retention period for those initial Records, based on the new Certificate expiration date.

5.5.3 Protection of Archive

An entity maintaining Records SHALL protect the Records so that only the entity's 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.

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.

5.5.5 Requirements for Time-Stamping of Records

Records SHALL be automatically time-stamped 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.

5.5.6 Archive Collection (Internal or External)

The CA or RA SHALL collect Records information internally.

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/RA SHALL verify the Integrity of the Records information. The CA/RA MAY elect to transmit the relevant information via a secure electronic method or courier.

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 4.7.

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

When the Root CA Certificate is to be Re-Keyed, the Root CA SHALL generate a new Key Pair and two (2) key rollover Certificates:

- One (1) key rollover Certificate where the new Public Key is signed by the old Private Key, indicating that this is the new Root CA 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 Root CA Certificate SHALL be available for download from the new Root CA's Repository. The Relying Party SHOULD validate both Certificates and replace the old Root CA Certificate with the published new Root CA Certificate. This permits acceptance of newly issued Certificates and CRLs without distribution of the new self-signed Certificate to current users.

The new Root CA Private Key SHALL be used to re-sign all existing active Tier-1 CAs. There is no need to re-sign existing active Sub-CA or End-Entity Certificates issued by the Tier-1 CA, unless the Tier-1 CA is also Re-Keyed.

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 Private Key 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.

The CA SHALL notify its Superior Entity if it experiences one or more of 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: or
- Any incident preventing the CA from issuing a CRL within twenty-four (24) hours of the issuance of the previous CRL.

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

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 its Superior Entity Sub-CAs, and any cross certified 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 *nextUpdate* 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 a reasonable time 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 a Root CA, the CA SHALL determine whether to notify all Subscribers using the CA as a Trust Anchor to delete the Trust Anchor.

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 its Superior Entity immediately;
- Generate new keys;
- If the CA can obtain accurate information on the Certificates it has issued which 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 a Root CA, it SHALL provide all Relying Parties with the new Trust Anchor using secure means.

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

5.7.3.1 Root CA Compromise Procedures

In the case of the Root CA Compromise, the Root CA SHALL notify:

- The MA and PA;
- Any cross certified PKIs so that they MAY Revoke any Cross-Certificates issued to the Root CA;
- Any Tier-1 CAs; and
- Relying Parties so they can remove the trusted self-signed Root CA 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 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 remediations 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 Root CA SHALL then generate a new Root CA Certificate, solicit requests and issue new Tier-1 CA Certificates, securely distribute the new Root CA Certificate, and re-establish any Cross-Certificates. Tier-1 CAs SHALL follow the procedure for Sub-CA Compromise for their issued Certificates.

5.7.3.2 Sub-CA Compromise Procedures

In the event of a CA key Compromise, the CA SHALL notify the MA, PA, its Superior Entity, and any lower level Sub-CAs. The Superior CA SHALL Revoke the Compromised CA's Certificate, and the Revocation information SHALL be published via a CRL, if supported, or via an emergency CSS update immediately in the most expedient, Authenticated, and trusted manner after the notification. The Compromised CA SHALL also investigate and report to the MA, PA, Superior CA (if applicable) and any lower level Sub-CAs 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 Sub-CA (if applicable) and Subscriber Certificates SHALL be requested and issued.

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 via a CRL, if supported, or via an emergency CSS update 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 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.

5.7.3.4 RA Compromise Procedures

In case of a RA Compromise, the CA SHALL disable the RA. In the case 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 this section SHALL be followed.

5.7.3.5 Subscriber Compromise Procedures

When a Subscriber Certificate is Revoked because of Compromise, suspected Compromise, or loss of the Private Key, the CA SHALL publish a Revocation notice via a CRL, if supported, or via a CSS update at the earliest feasible time by the supporting CA after notification as defined in Section 4.9.

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 following a disaster with, at a minimum, support for the following functions:

- Certificate issuance;
- Certificate Revocation;
- Publication of Revocation information; and
- CA Private Key issuance.

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.

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 its Superior Entity, the CA SHALL:

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

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 CA.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Key Pair generation SHALL be performed 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 Level	Hardware Or Software	Key Storage Restricted to the Module on Which the Key was Generated
Root CA Certificate	FIPS 140-2Level 3+	Hardware	Yes
Sub-CA Certificates	FIPS 140-2 Level 3+	Hardware	Yes
CSS	FIPS 140-2 Level 3+	Hardware	Yes
End-Entity Certificate	FIPS 140-2 Level 1+	Hardware or Software	No stipulation

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 in Table 6. The CA's Key Pair generation MUST create a verifiable Audit trail demonstrating that the security requirements for the procedure were followed. The CA's documentation of the procedure MUST show that appropriate role separation was used. One or more witnesses 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.

6.1.1.2 Subscriber Key Pair Generation

Subscribers, or their Authorized Entity, 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.

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, as shown in Table 6.

6.1.2 Private Key Delivery to Subscribers

Subscribers MAY generate their own Key Pairs, so there is no stipulation for delivering Private Keys to Subscribers when the Subscriber generates their own Keys.

When a CA, RA, or Authorized Entity generates Key Pairs on behalf of a Subscriber, the Private Keys MUST be delivered securely to the Subscriber and:

- The entity who generates a Private Key for a Subscriber SHALL NOT retain any copy of the key after delivery of the Private Key to the Subscriber;
- The Private Key SHALL be protected from activation, Compromise, or Modification during the delivery process; and
- Delivery SHALL be accomplished in a way that ensures that the Certificates and associated Private Keys are provided to the correct Subscriber.

6.1.3 Public Key Delivery to Certificate Issuer

The Subscriber, the CA, RA, or an Authorized Entity 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 deliver the Subscriber's Public Key to the CA. The RA SHALL Authenticate to the CA and send the Public Key CSR file to the CA to request a Certificate on behalf of the Subscriber.

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 SHALL include:

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

6.1.5 Key Sizes

Key Pairs SHALL be of sufficient length, as per Table 7, to prevent others from determining the Key Pair's Private Key using cryptanalysis during the period of expected utilization of such Key Pairs.

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

Table 7: Key Size

Certificate	[SAE EVPKI CP]	[ISO 15118-2]	[ISO 15118-20]
Root CA Certificates	At least ECC 256-bit or higher	ECC 256-bit	ECC 521-bit
Sub-CA Certificates	At least ECC 256-bit or higher	ECC 256-bit	ECC 521-bit
End-Entity Certificates	At least ECC 256-bit or higher	ECC 256-bit	ECC 521-bit
OCSP Responder Certificates	At least ECC 256-bit or higher	ECC 256-bit	ECC 521-bit

6.1.6 Public Key Parameters Generation and Quality Checking

Public Key parameters SHALL always be generated and validated in accordance with [FIPS 186-5].

CAs or RAs SHALL verify that CSRs contain a Public Key that meets the required key sizes for the requested Certificate.

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

The use of a specific key SHALL be constrained by the *keyUsage* and *extKeyUsage* extensions in the X.509 Certificate.

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

6.1.7.1 keyUsage Extension for CA Certificates

Table 8 shows the specific *keyUsage* extension settings for CA Certificates (i.e., Root CAs, Sub-CAs) and specifies that all CA Certificates:

- SHALL include a *keyUsage* extension;
- SHALL set the criticality of the *keyUsage* extension to TRUE; and
- SHALL assert the *keyUsage* bits below according to the appropriate specification.

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)		x	[ISO 15118-2] not set (x = 0) [ISO 15118-20] optional (x = 0/1) [SAE EVPKI CP] optional (x = 0/1)
nonRepudiation (contentCommitment)	(1)		x	[ISO 15118-2] not set (x = 0) [ISO 15118-20] optional (x = 0/1) [SAE EVPKI CP] optional (x = 0/1)

Field	Format	Criticality	Value	Comment
keyEncipherment	(2)		x	[ISO 15118-2] not set (x = 0) [ISO 15118-20] optional (x = 0/1) [SAE EVPKI CP] optional (x = 0/1)
dataEncipherment	(3)		0	Not Set
keyAgreement	(4)		x	[ISO 15118-2] not set (x = 0) [ISO 15118-20] optional (x = 0/1) [SAE EVPKI CP] not set (x = 0)
keyCertSign	(5)		x	[ISO 15118-2] optional (x = 0/1) [ISO 15118-20] set (x = 1) [SAE EVPKI CP] set (x = 1)
cRLSign	(6)		x	[ISO 15118-2] optional (x = 0/1) [ISO 15118-20] optional (x = 0/1) [SAE EVPKI CP] set (x = 1)
encipherOnly	(7)		0	Not Set
decipherOnly	(8)		0	Not Set

6.1.7.2 keyUsage Extension for all End-Entity Certificates

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

- SHALL include a *keyUsage* extension;
- SHALL set the criticality to TRUE;
- SHALL set the *digitalSignature* bit; and
- SHALL assert the other *keyUsage* bits below according to the appropriate specification.

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 (contentCommitment)	(1)		x	[ISO 15118-2] not set (x = 0), except for Contract Cert (x = 1) [ISO 15118-20] optional (x = 0/1) [SAE EVPKI CP] set (x = 1)
keyEncipherment	(2)		x	[ISO 15118-2] not set (x = 0), except for Contract Cert (x = 1) [ISO 15118-20] optional (x = 0/1) [SAE EVPKI CP] not set (x = 0)
dataEncipherment	(3)		0	Not Set
keyAgreement	(4)		x	[ISO 15118-2] not set (x = 0), except for Contract Cert (x = 1) [ISO 15118-20] • SECC & OEM Prov Certs set (x = 1) • CPS, Contract & Vehicle Certs optional (x = 0/1) [SAE EVPKI CP] Optional (x =0/ 1)
keyCertSign	(5)		0	Not Set
cRLSign	(6)		0	Not Set
encipherOnly	(7)		0	Not Set

decipherOnly	(8)		0	Not Set

6.1.7.3 keyUsage Extension for all OCSP Responder Certificates

Table 10 shows the specific *keyUsage* extension settings for OCSP responder Certificates and specifies that all OCSP responder Certificates:

- SHALL include a *keyUsage* extension;
- SHALL set the criticality of the *keyUsage* extension to TRUE; and
- SHALL assert the *keyUsage* bits below according to the appropriate specification.

Table 10: keyUsage Extension for OCSP Responder Certificates

Field	Format	Criticality	Value	Comment
keyUsage	BIT STRING	TRUE	{ id-ce 15 }	Included in all OCSP responder Certificates.
digitalSignature	(0)		x	[ISO 15118-2] not set (x = 0) [ISO 15118-20] optional (x = 0/1) [SAE EVPKI CP] set (x = 1) (Note: *digitalSignature* MUST be set to allow the OCSP responder to sign the response)
nonRepudiation	(1)		x	[ISO 15118-2] not set (x = 0) [ISO 15118-20] optional (x = 0/1) [SAE EVPKI CP] not set (x = 0)
keyEncipherment	(2)		x	[ISO 15118-2] not set (x = 0) [ISO 15118-20] optional (x = 0/1) [SAE EVPKI CP] not set (x = 0)
dataEncipherment	(3)		0	Not Set
keyAgreement	(4)		x	[ISO 15118-2] not set (x = 0) [ISO 15118-20] optional (x = 0/1) [SAE EVPKI CP] not set (x = 0)
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 this 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.

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.

6.2.3 Private Key Escrow

No stipulation.

6.2.4 Private Key Backup

6.2.4.1 Backup of CA Private Keys

The Backup 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 CA 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.

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

Private Keys SHALL NOT be Archived.

6.2.6 Private Key Transfer into or from a Cryptographic Module

CA Private Keys MAY be exported from the Cryptographic Module only to perform CA key Backup procedures as described in Section 6.2.4 or for transferring CRL/CSS operations to a Superior Entity when the CA terminates operations (as defined by Section 5.8). 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 duringtransport; 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.

6.2.7 Private Key Storage on Cryptographic Module

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

6.2.8 Method of Activating Private Key

CAs 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 by the CA 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 the physical and logical Access Controls are implemented as specified in Section 5. The Device's PKI Sponsor SHALL be responsible for ensuring that the end-entity system has security controls as specified in Section 6. These controls SHALL protect the device's hardware, software, and the cryptographic token and its Activation Data from Compromise.

All CAs SHALL protect the Activation Data for their Private Keys against loss, theft, Modification, disclosure, or unauthorized use.

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.

6.2.8.2 Offline CAs Private Key

Once the CA system has been activated, a m-of-n 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 CA's session.

6.2.8.3 Online CAs Private Key

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, CAs SHALL deactivate the Cryptographic Module, e.g., via a manual logout procedure or automatically after a period of inactivity as defined in the CPS but no more than thirty (30) minutes. When deactivated, Private Keys SHALL be kept in encrypted form or protected in an HSM. 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.

6.2.10 Method of Destroying Private Key

CAs 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 employ methods commensurate with those in the NIST Guidelines for Media Sanitization [SP 800-88-1] and 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 CA Private Key cannot be guaranteed, then the key SHALL be treated as Compromised and its corresponding Public Key Certificate Revoked.

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 Root CA Key Pair is a maximum of fifty (50) years. For all other CAs operating under this CP, the usage period for a CA Key Pair is a maximum of forty (40) years. The CA Private Key MAY be used to sign Certificates for as long as the Validity Period of the issued Certificate does not exceed the Certificate Validity Period of the CA, but the CA's Private Key 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 to the same level as the new Private Key.

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

Table 11: Certificate Validity Periods

Certificate	Certificate Validity Period	Key Validity Period
Root CA Certificates	[ISO 15118-2] 40 years [ISO 15118-20] 40 years [SAE EVPKI CP] Up to 50 years	Up to 50 years
[ISO 15118-2] Sub-CA Certificates	CPO Tier-1 CA: 4 years CPO Tier-2 CA: 1-2 years SECC Leaf: 2-3 months Prov Tier-1 CA: 4 years Prov Tier-2 CA: 1-2 years Prov Leaf: 2-3 months MO Tier-1 CA: up to MO MO Tier-2 CA: up to MO Contract: 4 weeks to 2 years OEM Tier-1 CA: up to OEM OEM Tier-2 CA: up to OEM OEM Prov Leaf: up to OEM	Same as Certificate Validity Period
[ISO 15118-20] Sub-CA Certificates	Up to the Subscriber (CPO, Prov, OEM, Vehicle, eMSP)	Same as Certificate Validity Period
[SAE EVPKI CP] Sub-CA Certificates	Up to 40 years	Up to 40 years
End-Entity Certificates	Up to 20 years	Up to 20 years
OCSP Responder Certificates	Up to 1 year	Up to 1 year

Validity Periods SHALL be nested such that the Validity Periods of issued Certificates SHALL be contained within the Validity Period of the CA. CAs SHALL NOT issue Certificates with Validity Periods that extend beyond the expiration date of their own CA Certificate.

All Certificates signed by a specific CA Private Key MUST expire before the end of that Private Key's usage period. End-Entity Certificates SHALL have a Validity Period as specified in Table 11.

DigiCert EVPKI Participants SHALL cease all use of their Private Key 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.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

CAs 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 CA Staff prior to unlocking the CA's Private Keys. To the extent passwords are used as Activation Data, the CA's 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 (e.g., password). The strength of the Activation Data SHALL meet or exceed the requirements for Authentication mechanisms stipulated for Level 3 or higher in [FIPS 140-2], or some other equivalent standard (see Table 6).

6.4.2 Activation Data Protection

CA 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 CA Private Key holders SHALL include a facility to temporarily lock the account, or terminate the application, after at maximum ten (10) unsuccessful login attempts.

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 [SP 800-63-3];
- Provide Security Audit capability;
- Lock the Access to CA services after at maximum ten (10) 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 at maximum ten (10) 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.

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 CA system through aspects of its life cycle.

The system development controls for the CA 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.

6.6.2 Security Management Controls

A list of acceptable products and their versions for each individual CA 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.

6.6.3 Life Cycle Security Controls

CAs 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. CAs SHALL document any 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 configuration file 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 nine (9) or higher on the US-CERT CVSS 3.1 [CVSS] rating scale, or equivalent, remediation SHALL be effected within forty-five (45) days after patch availability.

Remediation activities applied to requirements and SHOULD NOT cause unavailability of Revocation information.

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 the CA network security is configured and validated.

6.7.1 Isolation of Networked Systems

The Root CA and its Private Keys SHALL be offline.

Communication channels between the network-connected CA components and the offline Root CA processing components SHALL be protected against attacks. Information flowing into offline Root 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. Online CA networked components SHALL be protected from attacks by adequate means to filter unwanted protocols (utilizing Access rules, protocol checkers, etc., as necessary). Data loss prevention tools SHALL be employed to detect inappropriate leakage of sensitive information from CA components.

6.7.2 Boundary Protection

Any boundary control devices used to protect the CA Repository or CA 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.

CAs, RAs, 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.

6.7.2.1 Transmission Confidentiality

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

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

6.7.3 Network Monitoring

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

6.8 Time-Stamping

Certificates, CRLs, and other Revocation database entries SHALL contain time and date information based a trustable and traceable time source. Asserted times SHALL be accurate to within 100 milliseconds. 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, or equivalent.

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;
- Audit logs; and
- OCSP responses.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

Certificates issued by a CA under this CP SHALL conform to Internet X.509 Public Key Infrastructure Certificate and CRL Profile [RFC 5280] and its updates [RFC 6818], [RFC 9549], [RFC 9598], [RFC 9608], and [RFC 9618].

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 12).

Table 12: 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 7.1.1.
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

Table 13 shows the size limitations of each Certificate for its respective standard to which it is compliant.

Table 13: Certificate Size Limitations

Standard	Section within the Standard	Description
[ISO 15118-2]	[V2G2-010]	The size of a Certificate in DER encoded form shall be not bigger than 800 Bytes
[ISO 15118-20]	[V2G20-1234]	Each Certificate in a Certificate chain shall be DER encoded and the size of each Certificate in DER encoded form shall be limited to a maximum of 1 600 bytes.
[SAE EVPKI CP]		No size limitations.

7.1.1 Certificate Version Number(s)

The CA 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 (see Section 7.2 for CRL Certificate version number and Section 7.3.1 for OCSP Certificate version number).

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.

7.1.2.1 Standard Extension for Root CA Certificates

Table 14 shows the Certificate extensions for all Root CA Certificates.

Table 14: Root CA Certificate Standard Extensions

Field	Referenced Standard	Section	Requirement or Recommendation
authorityInfoAccess	[RFC 5280]	4.2.2.1	[ISO 15118-2] Optional. Criticality SHALL be set to FALSE. [ISO 15118-20] Not included. [SAE EVPKI CP] Not included. (Note: This extension SHOULD NOT be included in Root CA Certificates.)
authorityKeyIdentifier	[RFC 5280]	4.2.1.1	[ISO 15118-2] Optional. Criticality SHALL be set to FALSE. [ISO 15118-20] Not included. [SAE EVPKI CP] Not included. (Note: This extension is typically omitted from Root CA Certificates that contain the *subjectKeyIdentifier* extension because the values are the same.)
basicConstraints	[RFC 5280]	4.2.1.9	SHALL be included in Root CA Certificates. Criticality SHALL be set to TRUE.
certificatePolicies	[RFC 5280]	4.2.1.4	[ISO 15118-2] Optional. Criticality SHALL be set to FALSE. [ISO 15118-20] Not included. [SAE EVPKI CP] Not included. (Note: This extension is typically omitted from Root CA Certificates.)
cRLDistributionPoint	[RFC 5280]	4.2.1.13	[ISO 15118-2] Optional. Criticality SHALL be set to FALSE. [ISO 15118-20] Not included. [SAE EVPKI CP] Not included. (Note: This extension SHOULD NOT be included in Root CA Certificates.)
keyUsage	[RFC 5280]	4.2.1.3	SHALL be included in Root CA Certificates. Criticality SHALL be set to TRUE.
subjectKeyIdentifier	[RFC 5280]	4.2.1.2	[ISO 15118-2] Optional. [ISO 15118-20] SHALL be included. [SAE EVPKI CP] SHALL be included. Criticality SHALL be set to FALSE.

7.1.2.2 Standard Extension for Sub-CA Certificates

Table 15 shows the Certificate extensions for all Sub-CA Certificates.

Table 15: Sub-CA Certificate Standard Extensions

Field	Referenced Standard	Section	Requirement or Recommendation
authorityInfoAccess	[RFC 5280]	4.2.2.1	[ISO 15118-2] MAY be included in Sub-CA Certificates. Criticality SHALL be set to FALSE. [ISO 15118-20]: • SHALL be included in CPO Sub-CA Certificates. Criticality SHALL be set to TRUE.

			• May be included in Prov Sub-CA Certificate. Criticality SHALL be set to FALSE. • May be included in eMSP, OEM, and Vehicle Sub-CA Certificates. Criticality SHALL be set to TRUE. [SAE EVPKI CP] MAY be included in Sub-CA Certificates. Criticality SHALL be set to TRUE or FALSE, depending on compliance to -2 or -20.
authorityKeyIdentifier	[RFC 5280]	4.2.1.1	[ISO 15118-2] MAY be included in Sub-CA Certificates. Criticality SHALL be set to FALSE. [ISO 15118-20]: • SHALL be included in Sub-CA Certificates. • Criticality SHALL be set to FALSE in CPO Sub-CA Certificates. • Criticality SHALL be set to TRUE in Prov, eMSP, OEM, and Vehicle Sub-CA Certificates. [SAE EVPKI CP] SHALL be included in Sub-CA Certificates. Criticality SHALL be set to TRUE or FALSE, depending on compliance to -2 or -20.
basicConstraints	[RFC 5280]	4.2.1.9	SHALL be included in Sub-CA Certificates. Criticality SHALL be set to TRUE.
certificatePolicies	[RFC 5280]	4.2.1.4	[ISO 15118-2] SHALL NOT be included in Sub-CA Certificates. [ISO 15118-20] MAY be included in Sub-CA Certificates. Criticality SHALL be set to FALSE. [SAE EVPKI CP] MAY be included in Sub-CA Certificates. Criticality SHALL be set to FALSE.
cRLDistributionPoints	[RFC 5280]	4.2.1.13	[ISO 15118-2] MAY be included in all Sub-CA Certificates. Criticality SHALL be set to TRUE or FALSE. [ISO 15118-20]: • SHALL NOT be included in CPO Sub-CA Certificates. • MAY be included in Prov Sub-CA Certificates. Criticality SHALL be set to FALSE. • MAY be included in eMSP, OEM, and Vehicle Sub-CA Certificates. Criticality SHALL be set to TRUE. [SAE EVPKI CP] MAY be included in Sub-CA Certificates. Criticality SHALL be set to TRUE or FALSE, depending on compliance to -2 or -20.
keyUsage	[RFC 5280]	4.2.1.3	SHALL be included in Sub-CA Certificates. Criticality SHALL be set to TRUE.
subjectKeyIdentifier	[RFC 5280]	4.2.1.2	[ISO 15118-2] MAY be included in Sub-CA Certificates. Criticality SHALL be set to FALSE. [ISO 15118-20]: • SHALL be included in Sub-CA Certificates. • Criticality SHALL be set to FALSE in CPO Sub-CA Certificates. • Criticality SHALL be set to TRUE in Prov, eMSP, OEM, and Vehicle Sub-CA Certificates. [SAE EVPKI CP] SHALL be included in Sub-CA Certificates. Criticality SHALL be set to TRUE or FALSE, depending on compliance to -2 or -20.

7.1.2.3 Standard Extension for End-Entity Certificates

Table 16 shows the Certificate extensions for all End-Entity Certificates.

Table 16: End-Entity Certificate Standard Extensions

Field	Referenced Standard	Section	Requirement or Recommendation
authorityInfoAccess	[RFC 5280]	4.2.2.1	[ISO 15118-2] MAY be included in End-Entity Certificates. Criticality SHALL be set to FALSE. [ISO 15118-20]: • SHALL be included in CPO End-Entity Certificates. Criticality SHALL be set to TRUE. • May be included in Prov End-Entity Certificates. Criticality SHALL be set to FALSE. • May be included in eMSP, OEM, and Vehicle End-Entity Certificates. Criticality SHALL be set to TRUE. [SAE EVPKI CP] MAY be included in End-Entity Certificates. Criticality SHALL be set to TRUE or FALSE, depending on compliance to -2 or -20.
authorityKeyIdentifier	[RFC 5280]	4.2.1.1	[ISO 15118-2] MAY be included in End-Entity Certificates. Criticality SHALL be set to FALSE. [ISO 15118-20]: • SHALL be included in End-Entity Certificates. • Criticality SHALL be set to FALSE in CPO End-Entity Certificates. • Criticality SHALL be set to TRUE in Prov, eMSP, OEM, and Vehicle End-Entity Certificates. [SAE EVPKI CP] SHALL be included in End-Entity Certificates. Criticality can be set to TRUE or FALSE, depending on compliance to -2 or -20.
basicConstraints	[RFC 5280]	4.2.1.9	[ISO 15118-2] SHALL be included in End-Entity Certificates. Criticality SHALL be set to TRUE. [ISO 15118-20] SHALL be included in End-Entity Certificates. Criticality SHALL be set to TRUE. [SAE EVPKI CP] MAY be included in End-Entity Certificates. Criticality SHALL be set to TRUE.
certificatePolicies	[RFC 5280]	4.2.1.4	[ISO 15118-2] SHALL NOT be included in End-Entity Certificates. [ISO 15118-20] MAY be included in End-Entity Certificates. Criticality SHALL be set to FALSE. [SAE EVPKI CP] MAY be included in End-Entity Certificates. Criticality SHALL be set to FALSE.
cRLDistributionPoints	[RFC 5280]	4.2.1.13	[ISO 15118-2] MAY be included in all End-Entity Certificates. Criticality SHALL be set to TRUE or FALSE. [ISO 15118-20]: • SHALL NOT be included in CPO End-Entity Certificates. • MAY be included in Prov End-Entity Certificates. Criticality SHALL be set to FALSE. • MAY be included in eMSP, OEM, and Vehicle End-Entity Certificates. Criticality SHALL be set to TRUE. [SAE EVPKI CP] MAY be included in End-Entity Certificates. Criticality SHALL be set to TRUE or FALSE, depending on compliance to -2 or -20.
extKeyUsage	[RFC 5280]	4.2.1.12	[ISO 15118-2] SHALL NOT be included in End-Entity Certificates. [ISO 15118-20]: • MAY be included in CPO and Vehicle End-Entity Certificates. Criticality SHALL be set to TRUE.

Field	Referenced Standard	Section	Requirement or Recommendation
			• SHALL NOT be included in Prov, eMSP, and OEM End-Entity Certificates. [SAE EVPKI CP] MAY 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.
subjectKeyIdentifier	[RFC 5280]	4.2.1.2	[ISO 15118-2] MAY be included in End-Entity Certificates. Criticality SHALL be set to FALSE. [ISO 15118-20]: • SHALL be included in End-Entity Certificates. • Criticality SHALL be set to FALSE in CPO End-Entity Certificates. • Criticality SHALL be set to TRUE in Prov, eMSP, OEM, and Vehicle End-Entity Certificates. [SAE EVPKI CP] SHALL be included in End-Entity Certificates. Criticality SHALL be set to TRUE or FALSE, depending on compliance to -2 or -20.

7.1.2.4 Standard Extension for OCSP Responder Certificates

Table 17 shows the Certificate extensions for all End-Entity Certificates.

Table 17: OCSP Responder Certificate Standard Extensions

Field	Referenced Standard	Section	Requirement or Recommendation
authorityInfoAccess	[RFC 5280]	4.2.2.1	[ISO 15118-2] MAY be included in OCSP responder Certificates. [ISO 15118-20] SHALL NOT be included in OCSP responder Certificates. [SAE EVPKI CP] MAY be included in OCSP responder Certificates. Criticality SHALL be set to FALSE.
authorityKeyIdentifier	[RFC 5280]	4.2.1.1	[ISO 15118-2] MAY be included in OCSP responder Certificates. [ISO 15118-20] SHALL be included in OCSP responder Certificates. [SAE EVPKI CP] MAY be included in OCSP responder Certificates. Criticality SHALL be set to FALSE.
basicConstraints	[RFC 5280]	4.2.1.9	SHALL be included in OCSP responder Certificates. Criticality SHALL be set to TRUE.
certificatePolicies	[RFC 5280]	4.2.1.4	[ISO 15118-2] SHALL NOT be included in OCSP responder Certificates. [ISO 15118-20] SHALL NOT be included in OCSP responder Certificates. [SAE EVPKI CP] MAY be included in OCSP responder Certificates.
cRLDistributionPoints	[RFC 5280]	4.2.1.13	[ISO 15118-2] MAY be included in OCSP responder Certificates. [ISO 15118-20] SHALL NOT be included in OCSP responder Certificates. [SAE EVPKI CP] MAY be included in OCSP responder Certificates. Criticality SHALL be set to FALSE.
extendedKeyUsage	[RFC 5280]	4.2.1.12	[ISO 15118-2] SHALL be included in OCSP responder Certificates. [ISO 15118-20] SHALL be included in OCSP responder Certificates. [SAE EVPKI CP] MAY be included in OCSP responder Certificates. Criticality SHALL be set to TRUE.
keyUsage	[RFC 5280]	4.2.1.3	SHALL be included in OCSP responder Certificates. Criticality SHALL be set to TRUE.
noCheck	[RFC 5280]	4.2.2.2.1	MAY be included in OCSP responder Certificates. Criticality SHALL be set to FALSE.
subjectKeyIdentifier	[RFC 5280]	4.2.1.2	[ISO 15118-2] MAY be included in OCSP responder Certificates.

			[ISO 15118-20] SHALL be included in OCSP responder Certificates. Calculated per Method 2. [SAE EVPKI CP] MAY be included in OCSP responder Certificates. Criticality SHALL be set to FALSE. Calculated per Method 1 or 2.

7.1.2.5 Authority Information Access Extension

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

Table 18 shows the *authorityInfoAccess* extension settings for CA Certificates and specifies that all CA Certificates:

- MAY include the *authorityInfoAccess* extension;
- SHALL set the criticality of the *authorityInfoAccess* extension to TRUE or FALSE, depending on compliance to -2 or -20;
- 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 18: authorityInfoAccess Extension for CA Certificates

Field	Format	Criticality	Value	Comment
authorityInfoAccess		TRUE or FALSE	{ id-pe 1 }	MAY be included in all Sub-CA Certificates. (For Root CA see Table 14) (For Sub-CAs see Table 15)
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 19 shows the *authorityInfoAccess* extension settings for End-Entity Certificates and specifies that all End-Entity Certificates:

- MAY include the *authorityInfoAccess* extension;
- SHALL set the criticality of the *authorityInfoAccess* extension to TRUE or FALSE, depending on compliance to -2 or -20;
- 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 19: authorityInfoAccess Extension for End-Entity Certificates

Field	Format	Criticality	Value	Comment
authorityInfoAccess		TRUE or FALSE	{ id-pe 1 }	MAY be included in all End-Entity Certificates. (see Table 16)
accessMethod	OID		1.3.6.1.5.5.7.48.1	OCSP {id-pkix-ocsp}
accessLocation	General Name		URL	Address of the OCSP responder

7.1.2.6 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 20 shows the *authorityKeyIdentifier* extension settings for CA Certificates and specifies that all CA Certificates:

- MAY include the *authorityKeyIdentifier* extension;
- SHALL set the criticality of the *authorityKeyIdentifier* extension to TRUE or FALSE, depending on compliance to -2 or -20; and
- SHALL calculate the *keyIdentifier* of the *authorityKeyIdentifier* per Method 1 or Method 2.

Table 20: authorityKeyIdentifier Extension for CA Certificates

Field	Format	Criticality	Value	Comment
authorityKeyIdentifier		TRUE or FALSE	{ id-ce 35 }	MAY be included in all CA Certificates. (For Root CA see Table 14) (For Sub-CAs see Table 15)
keyIdentifier	OCTET STRING		<keyIdentifier>	Calculated per Method 1 or Method 2

Table 21 shows the *authorityKeyIdentifier* extension settings for End-Entity Certificates and specifies that all End-Entity Certificates:

- MAY include the *authorityKeyIdentifier* extension;
- SHALL set the criticality of the *authorityKeyIdentifier* extension to TRUE or FALSE, depending on compliance to -2 or -20; and
- SHALL calculate the *keyIdentifier* of the *authorityKeyIdentifier* per Method 1 or Method 2.

Table 21: authorityKeyIdentifier Extension for End-Entity Certificates

Field	Format	Criticality	Value	Comment
authorityKeyIdentifier		TRUE or FALSE	{ id-ce 35 }	MAY be included in all End-Entity Certificates. (see Table 16)
keyIdentifier	OCTET STRING		<keyIdentifier>	Calculated per Method 1 or Method 2

Table 22 shows the *authorityKeyIdentifier* extension settings for OCSP responder Certificates and specifies that all OCSP responder Certificates:

- MAY 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 or Method 2.

Table 22: authorityKeyIdentifier Extension for OCSP Responder Certificates

Field	Format	Criticality	Value	Comment
authorityKeyIdentifier		FALSE	{ id-ce 35 }	MAY be included in all OCSP responder Certificates. (see Table 17)
keyIdentifier	OCTET STRING		<keyIdentifier>	Calculated per Method 1 or Method 2

7.1.2.7 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 Sub-CA 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 23 shows the *basicConstraints* extension settings for Root CA Certificates 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 to TRUE*; and
- SHALL set the *pathLenConstraint* field of the *basicConstraints* to “None”.

Table 23: 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 24 shows the *basicConstraints* extension settings for Tier-1 CA Certificates and specifies that all Tier-1 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 to TRUE*; and
- SHALL set the *pathLenConstraint* field of the *basicConstraints* to "1" or "0" for a Tier-1 CA.

Table 24: basicConstraints Extension for Tier-1 CA Certificates

Field	Format	Criticality	Value	Comment
basicConstraints		TRUE	{ id-ce 19 }	Included in all Tier-1 CA Certificates.
cA	BOOLEAN		TRUE	Set
pathLenConstraint	INTEGER		x	Set to "1", if the CA is to only issue Tier-2 CAs. Set to "0", if the CA is to only issue End-entity Certificates.

Table 25 shows the *basicConstraints* extension settings for Tier-2 CA Certificates and specifies that all Tier-2 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 to TRUE*; and
- CA SHALL set pathLenConstraint field of any CA Certificate it issues to a *pathLenConstraint* of 0.

Table 25: basicConstraints Extension for Tier-2 CA Certificates

Field	Format	Criticality	Value	Comment
basicConstraints		TRUE	{ id-ce 19 }	Included in all Tier-2 CA Certificates.
cA	BOOLEAN		TRUE	Set
pathLenConstraint	INTEGER		0	Set

Table 26 shows the *basicConstraints* extension settings for End-Entity Certificates and specifies that all End-Entity Certificates:

- MAY include the *basicConstraints* extension;
- SHALL set the criticality of the *basicConstraints* extension to TRUE;
- SHALL set the cA field of the *basicConstraints to FALSE*; and
- SHALL set pathLenConstraint field to "NONE".

Table 26: basicConstraints Extension for End-Entity Certificates

Field	Format	Criticality	Value	Comment
basicConstraints		TRUE	{ id-ce 19 }	Included in all End-Entity Certificates. (see Table 16)
cA	BOOLEAN		FALSE	Set
pathLenConstraint	INTEGER		NONE	Not Set

Table 27 shows the *basicConstraints* extension settings for OCSP responder Certificates and specifies that all OCSP responder Certificates:

- MAY include the *basicConstraints* extension;
- SHALL set the criticality of the *basicConstraints* extension to TRUE;
- SHALL set the *cA* to FALSE; and
- SHALL set the *pathLenConstraint* field of the *basicContraints* to "None".

Table 27: basicConstraints Extension for OCSP Responder Certificates

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

7.1.2.8 Certificate Policies Extension

See Section 7.1.6.

7.1.2.9 CRL Distribution Points Extension

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

Table 28 shows the *cRLDistributionPoints* extension settings for CA Certificates and specifies that all CA Certificates:

- MAY include the *cRLDistributionPoints* extension; and if included
- SHALL set the criticality of the *cRLDistributionPoints* extension to TRUE or FALSE, depending on compliance to -2 or -20; and
- SHALL set the *distributionPointName* to the URL of the CRL.

Table 28: cRLDistributionPoints Extension for Sub-CA Certificates

Field	Format	Criticality	Value	Comment
cRLDistributionPoints		TRUE or FALSE	{ id-ce 31 }	MAY be included in all Sub-CA Certificates. (For Root CA see Table 14) (For Sub-CAs see Table 15)
distributionPoint				
distributionPointName	GeneralNames		URL	Address of the CRL

Table 29 shows the *cRLDistributionPoints* extension settings for End-Entity Certificates and specifies that all End-Entity Certificates:

- MAY include the *cRLDistributionPoints* extension; and if included
- SHALL set the criticality of the *cRLDistributionPoints* extension to TRUE or FALSE, depending on compliance to -2 or -20; and
- SHALL set the *distributionPointName* to the URL of the CRL.

Table 29: cRLDistributionPoints Extension for End-Entity Certificates

Field	Format	Criticality	Value	Comment
cRLDistributionPoints		TRUE or FALSE	{ id-ce 31 }	MAY be included in all End-Entity Certificates. (see Table 16)
distributionPoint				
distributionPointName	GeneralNames		URL	Address of the CRL

7.1.2.10 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 30 shows the *extKeyUsage* extension settings for End-Entity Certificates and specifies that all Certificates:

- MAY include the *extKeyUsage* extension; and if included
- SHALL set the criticality of the *extKeyUsage* extension to TRUE; and
- SHALL set the *keyPurposeId* field to *id-kp-clientAuth and/or id-kp-serverAuth.*

Table 30: extKeyUsage Extension for End-Entity Certificates

Field	Format	Criticality	Value	Comment
extKeyUsage		TRUE	{ id-ce 37 }	May be included in End-Entity Certificates. (see Table 16)
keyPurposeID	OID		1.3.6.1.5.5.7.3.2	id-kp-clientAuth
keyPurposeID	OID		1.3.6.1.5.5.7.3.1	id-kp-serverAuth

Table 31 shows *extendedKeyUsage* the extension settings for OCSP responder Certificates and specifies that all OCSP responder Certificates:

- MAY include the *extendedKeyUsage* extension;
- If included, SHALL set the criticality of the *extendedKeyUsage* extension to TRUE; and
- SHALL set the *keyPurposeId* field of the *extendedKeyUsage* to OCSP Signing.

Table 31: extendedKeyUsage Extension for OCSP Responder Certificates

Field	Format	Criticality	Value	Comment
extendedKeyUsage		TRUE	{ id-ce 37 }	MAY be included in OCSP responder Certificates. (see Table 17)
keyPurposeID	OID		1.3.6.1.5.5.7.3.9	OCSP Signing

7.1.2.11 Key Usage Extension

See Section 6.1.7.

7.1.2.12 OCSP noCheck Extension

***Table** 32* shows the OCSP *noCheck* extension for OCSP responder Certificates and specifies that all OCSP responder Certificates:

- MAY include a *noCheck* extension;
- SHALL set the criticality of the *noCheck* extension to FALSE; and
- SHALL set the *value* to NULL.

Table 32: OCSP noCheck Extension

Field	Format	Criticality	Value	Comment
id-pkix-ocsp-nocheck		FALSE	NULL	{id-pkix-ocsp 5}

7.1.2.13 Subject Key Identifier Extension

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

Table 33 shows the *subjectKeyIdentifier* extension settings for CA Certificates and specifies that all CA Certificates:

- MAY include the *subjectKeyIdentifier* extension; and if included
- SHALL set the criticality of the *subjectKeyIdentifier* extension to TRUE or FALSE, depending on compliance to -2 or -20; and
- SHALL calculate the *keyIdentifier* of the *subjectKeyIdentifier* per Method 1 or Method 2.

Table 33: subjectKeyIdentifier Extension for CA Certificates

Field	Format	Criticality	Value	Comment
subjectKeyIdentifier		TRUE or FALSE	{ id-ce 14 }	MAY be included in all CA Certificates. (For Root CA see Table 14) (For Sub-CAs see Table 15)
keyIdentifier	OCTET STRING		<key identifier>	Calculated per Method 1 or Method 2

Table 34 shows the *subjectKeyIdentifier* extension settings for End-Entity Certificates, and specifies that all End-Entity Certificates:

- MAY include the *subjectKeyIdentifier* extension;
- SHALL set the criticality of the *subjectKeyIdentifier* extension to TRUE or FALSE, depending on compliance to -2 or -20; and
- SHALL calculate the *keyIdentifier* of the *subjectKeyIdentifier* per Method 1 or Method 2.

Table 34: subjectKeyIdentifier Extension for End-Entity Certificates

Field	Format	Criticality	Value	Comment
subjectKeyIdentifier		TRUE or FALSE	{ id-ce 14 }	MAY be included in all End-Entity Certificates. (see Table 16)
keyIdentifier	OCTET STRING		<key identifier>	Calculated per Method 1 or Method 2

Table 35 shows the *subjectKeyIdentifier* extension settings for OCSP responder Certificates, and specifies that all OCSP responder Certificates:

- MAY 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 or Method 2.

Table 35: subjectKeyIdentifier Extension for OCSP Responder Certificates

Field	Format	Criticality	Value	Comment
subjectKeyIdentifier		FALSE	{ id-ce 14 }	MAY be included in all OCSP responder Certificates. (see Table 17)
keyIdentifier	OCTET STRING		<key identifier>	Calculated per Method 1 or Method 2. (see Table 17)

7.1.2.14 Subject Information Access Extension

Table 19 shows the subject*InfoAccess* extension settings for [ISO 15118-20] End-Entity Contract Certificates and specifies that all [ISO 15118-20] End-Entity Contract Certificates:

- MAY include the subject*InfoAccess* extension;
- SHALL set the criticality of the subject*InfoAccess* extension to FALSE, for compliance to -20;
- SHALL set the *accessMethod* to:
- id-contractOperatorName (1.0.20.0.1) for Contract Mobility Operator Name;
- id-contractTariffName (1.0.20.02) for Contract Tariff Name;
- id-contractDynamicInformationUrl (1.0.20.0.3) for Contract Dynamic Information URL; and
- SHALL set the *accessLocation* to the URL of the OCSP responder:
- Friendly name – alphanumeric string for Contract Mobility Operator Name;
- Friendly name – alphanumeric string for Contract Tariff Name;
- URL for Contract Dynamic Information URL.

Table 36: subjectInfoAccess Extension for End-Entity Certificates

Field	Format	Criticality	Value	Comment
subjectInfoAccess		FALSE	{ id-pe 11 }	MAY be included in [ISO 15118-20] Contract Certificates. (see Table 16)
accessMethod	OID			id-contractOperatorName (1.0.20.0.1) for Contract Mobility Operator Name; id-contractTariffName (1.0.20.02) for Contract Tariff Name; id-contractDynamicInformationUrl (1.0.20.0.3) for Contract Dynamic Information URL
accessLocation	General Name			Friendly name – alphanumeric string for Contract Mobility Operator Name. Friendly name – alphanumeric string for Contract Tariff Name. URL for Contract Dynamic Information URL.

7.1.3 Algorithm Object Identifiers (OIDs)

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

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) ecdsa-with-Sha512(4)}

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

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

The elliptic curve Public Key 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 }

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.

7.1.4.1 Root CAs

The following naming attributes SHALL specify the Root CA Certificate Subject fields issued under this CP:

Table 37: Root CA Certificate Subject Fields

Name	Field	Value	Requirement
countryName	(C=)	<Country Name>	MAY contain the country name field. If included, it SHALL use the two-letter ISO 3166-1 country code for the country in which the Root CA'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#>	MAY contain the organizational unit name field. If included, it SHALL contain the CA type (e.g., Root) and unique ID, e.g., Root CA – 1.
commonName	(CN=)	<Name> CA	SHALL contain a name that accurately identifies the Root CA (e.g., Organization Name Root CA).
domainComponent	(DC=)	<Domain Component>	MAY contain the domain component field. If included, it SHALL contain a string with a desired domain component (e.g., "V2G").

7.1.4.2 Sub-CAs

All attributes permitted by [RFC 5280] MAY be populated in the Sub-CA Certificate Subject fields issued under this CP.

The following attributes apply to Sub-CAs:

Table 38: Sub-CA Certificate Subject Fields

Name	Field	Value	Requirement
countryName	(C=)	<Country Name>	MAY contain the two-letter ISO 3166-1 country code for the country in which the Root CA's service provider's place of business is located.

Name	Field	Value	Requirement
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 and unique ID, e.g., Sub-CA–1.
commonName	(CN=)	<Name> <CA type> CA	SHALL contain a name that accurately identifies the Sub-CA (e.g., Organization Name Sub-CA).
domainComponent	(DC=)	<Domain Component>	MAY contain a string with a desired domain component (e.g., “V2G").

7.1.4.3 End-Entity Certificates

The following naming attributes SHALL specify the Subject fields in End-Entity Certificates issued under this CP:

Table 39: End-Entity Certificate Subject Fields

Name	Field	Value	Requirement
countryName	(C=)	<Country Name>	MAY contain the country name. If included it 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).
organizationalUnitName	[OU=]	<optional entry>	[Optional] subsidiary/location (not to exceed 64 characters).
commonName	(CN=)	<Name>	[Optional] MAY contain a name that accurately identifies the Subscriber.
domainComponent	(DC=)	<Domain Component>	MAY contain a string with a desired domain component (e.g., “V2G").

7.1.4.4 OCSP Responder Certificates

The following naming attributes SHALL specify the Subject fields in OCSP responder Certificates issued under this CP:

Table 40: OCSP Responder Certificate Subject Fields

Name	Field	Value	Requirement
countryName	[C=]	<Country Name>	[ISO 15118-] Optional, if included, SHALL be the two-letter ISO 3166-1 country code for the country in which the Subscriber’s place of business is located. [ISO 15118-20] SHALL NOT be included. [SAE EVPKI CP] Optional, if included, 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 include the organization name of the responder.
organizationalUnitName	[OU=]	<optional field>	[Optional field] (not to exceed 64 characters).
commonName	(CN=)	<Common Name>	SHALL include the common name for the responder.
domainComponent	(DC=)	<Domian Component>	[Optional field]

7.1.5 Name Constraints

No stipulation.

7.1.6 Certificate Policy Object Identifier

CA Certificates issued under this CP MAY assert the policy OIDs described in Section 1.2.2 of this CP.

Table 40 shows the *certificatePolicies* extension settings for CA Certificates and specifies that these Certificates:

- MAY include the *certificatePolicies* extension; and if included
- SHALL set the criticality of the *certificatePolicies* extension to FALSE; and;
- MAY set the *policyIdentifier* to the OID of one or more CP OIDs that apply to the issued Certificate.

Table 41: certificatePolicies Extension for CA Certificates

Field	Format	Criticality	Value	Comment
certificatePolicies		FALSE	{ id-ce 32 }	SHALL be included in Sub-CA Certificates. (For Root CA see Table 14) (For Sub-CAs see Table 15)
policyIdentifier	OID			See Section 1.2.2.
policyIdentifier	OID			See Section 1.2.2.

End-Entity Certificates issued under this CP MAY assert the policy OIDs described in Section 1.2.2.

Table 41 shows the *certificatePolicies* extension settings for End-Entity Certificates and specifies that these Certificates:

- MAY include the *certificatePolicies* extension; and if included
- SHALL set the criticality of the *certificatePolicies* extension to FALSE and;
- MAY set the *policyIdentifier* to the OID of one or more CP OIDs that apply to the issued Certificate.

Table 42: certificatePolicies Extension for End-Entity Certificates

Field	Format	Criticality	Value	Comment
certificatePolicies		FALSE	{ id-ce 32 }	MAY include in End-Entity Certificates. (see Table 16)
policyIdentifier	OID			See Section 1.2.2.
policyIdentifier	OID			See Section 1.2.2.

OCSP responder Certificates issued under this CP MAY assert the policy OIDs described in Section 1.2.2.

Table 42 shows the *certificatePolicies* extension settings for OCSP responder Certificates and specifies that these Certificates:

- MAY include the *certificatePolicies* extension;
- If included, SHALL set the criticality of the *certificatePolicies* extension to FALSE; and
- If included, SHALL set the value to the appropriate *policyIdentifier* values listed in Section 1.2.2.

Table 43: certify

icatePolicies Extension for Operational OCSP Responder Certificates

Field	Format	Criticality	Value	Comment
certificatePolicies		FALSE	{ id-ce 32 }	MAY be included in OCSP responder Certificates. (see Table 17)
policyIdentifier	OID			See Section 1.2.2.
policyIdentifier	OID			See Section 1.2.2.

7.1.7 Usage of Policy Constraints Extension

Certificates issued under this CP SHALL NOT contain policy constraints extension.

7.1.8 Policy Qualifiers Syntax and Semantics

Certificates issued under this CP SHALL NOT contain policy qualifiers.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

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

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 44: 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 field details the signature algorithm.
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 in *generalizedTime* in GMT (Zulu) format.
nextUpdate	[RFC 5280]	5.1.2.5	This field indicates the date by which the next CRL will be issued in *generalizedTime* in GMT (Zulu) format.
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	

7.2.1 CRL Version Number(s)

The CAs MAY support the issuance of X.509 Version 2 CRLs. If the CA supports CRL issuance, the CRL version number SHALL be set to the integer value of “1” for Version 2 [RFC 5280, Section 5.1.2.1].

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.

7.3 OCSP Profile

OCSP is a way to obtain timely information about the Revocation status of a particular Certificate.

OCSP responses, if supported by a CA, SHALL conform to the OCSP profile specified in [RFC 6960] as updated by [RFC 8954].

OCSP responses SHALL conform to [RFC 6960] and SHALL either be:

- Signed by the CA that issued the Certificates whose Revocation status is being checked; or
- Signed by an OCSP responder Certificate signed by the Root CA; or
- Signed by an OCSP responder Certificate signed by the CA that issued the Certificate whose Revocation status is being checked. Such OCSP responder Certificate, with a short Validity Period (e.g., fourteen (14) days), MAY contain the extension *id-pkix-ocsp-nocheck* as defined by [RFC 6960]. This extension indicates that the End-Entity Certificate need not obtain a CRL for the OCSP responder's Certificate. The OCSP responder SHOULD be a highly trusted component.

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].

7.3.2 OCSP Extensions

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

8 Compliance Audit and Other Assessments

CAs SHALL have a Compliance Audit mechanism in place.

8.1 Frequency or Circumstances of Assessment

The Subordinate CA's and RA SHALL be subject to a periodic Compliance Audit at least once per year.

8.2 Identity and Qualifications of Assessor

The Compliance Auditor MUST demonstrate competence in the field of Compliance Audits. 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, and:

- Be an independent public accounting or Auditing firm that has proficiency in examining PKIs, security Auditing, and third-party attestation and be currently licensed to perform WebTrust for CA Audits [SSAE 18] or [ISO 27001] standards, or to perform such alternate equivalent Audits approved by the PA; and
- Be a member of the American Institute of Certified Public Accountants (AICPA) or equivalent that requires that Audits be completed under defined standards.

8.3 Assessor's Relationship to Assessed Entity

The Compliance Auditor SHALL be a private firm that is independent from the entities (CA or RA) being Audited.

To ensure independence and objectivity, the Compliance Auditor MUST NOT have served the entity in developing or maintaining the to-be-Audited CA/RA Facility.

The Superior Entity SHALL determine whether a Compliance Auditor meets the Audit qualification requirements including checking that the CA is reviewing the Audits of its Sub-CAs for compliance to the requirements contained in this CP and their CPS.

8.4 Topics Covered by Assessment

The Audit MUST conform to industry standards (e.g., WebTrust for CA Audits [SSAE 18] or [ISO 27001]), cover the Subordinate CA's and RA's compliance with the requirements contained in this CP and the relevant CPS, and evaluate the Integrity of the CA's and RA's PKI operations.

The Audit MUST verify that each Subordinate CA is compliant with requirements contained in this CP.

The Superior CA SHOULD check that the CA it approved is performing similar checks on any Sub-CAs approved by this CA. For example, the Root CA Audit checks that the Root CA properly checked the Audit results of Sub-CA 1 below it and that the Root CA responded appropriately to any deficiencies that were found and reported. Sub-CA 1 will do the same for any Sub-CAs it has issued.

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 Superior Entity 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 Superior Entity, which MUST approve it;
- The responsible party MAY provide the Superior Entity with progress reports and notify the 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, which will notify the Superior Entity.

Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the Superior Entity MAY decide to temporarily halt operation of the CA, to Revoke a Certificate issued by the CA, or take other actions it deems appropriate.

The Superior Entity SHALL provide to the CA its procedures for making and implementing such determinations.

8.6 Communication of Results

See Section 8.5.

8.7 Internal Audits

Results of a CA's internal Audits SHALL be made available to the Compliance Auditor.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

DigiCert charges fees in connection to certificate issuance and renewal. DigiCert may change its pricing for future purchases at any time in accordance with the applicable customer agreement.

9.1.2 Certificate Access Fees

CAs operating under this CP MUST NOT charge additional fees for Access to CA Certificates, CRLs or OCSP responses.

9.1.3 Revocation or Status Information Access Fees

CA shall not charge a Certificate Revocation fee or a fee for checking the validity status of an issued Certificate using a CRL.

9.1.4 Fees for other Services

No stipulation.

9.1.5 Refund Policy

Subscribers must request refunds, in writing, within 30 days after the purchase of an entitlement to issue a Certificate. After receiving the refund request, DigiCert may revoke the certificate. Refunds are discretionary and may be subject to applicable application processing fees.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

CAs maintain Commercial General Liability insurance with a policy limit of at least $2 million in coverage and Professional Liability/Errors & Omissions insurance with a policy limit of at least $5 million in coverage. Insurance is carried through companies rated no less than A- as to Policy Holder's Rating in the current edition of Best's Insurance Guide (or with an association of companies, each of the members of which are so rated).

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3 Confidentiality of Business Information

The CA and RA SHALL protect the Confidentiality of sensitive information stored or processed on CA systems that could lead to abuse or fraud.

The CA and RA SHALL protect customer data that could allow an attacker to impersonate a customer.

9.3.1 Scope of Confidential Information

The following information is considered confidential and protected against disclosure using a reasonable degree of care:

- Private Keys;
- Activation Data used to Access Private Keys or to gain Access to the CA system;
- Business continuity, incident response, contingency, and disaster recovery plans;
- Other security practices used to protect the Confidentiality, Integrity, or availability of information;
- Information held by CA as private information in accordance with Section 9.4;
- Audit logs and Archive Records; and

- Transaction Records, financial Audit Records, and Audit trail Records and any Audit reports (with the exception of an Auditor's letter confirming the effectiveness of the controls set forth in this CP).

9.3.2 Information Not Within the Scope of Confidential Information

Any information not listed as confidential is considered public information. Published Certificate and Revocation data is considered public 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 permitted by applicable agreement or 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. Information about CA operators is retained by the CA 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

CAs shall create and follow a publicly posted Privacy policy that specifies how the CA handles personal information.

DigiCert follows the Privacy Notices posted on its website when handling personal information. See https://www.digicert.com/digicert-privacy-policy

9.4.2 Information Treated as Private

DigiCert treats all personal information about an individual that is not publicly available in the contents of a certificate or CRL as private information. DigiCert protects private information using appropriate safeguards and a reasonable degree of care. Information Not Deemed Private

Information included in Certificates or CRLs is not subject to the protections outlined in this CP.

9.4.3 Responsibility to Protect Private Information

DigiCert employees and contractors are expected to handle personal information in strict confidence and meet the requirements outlined in DigiCert's Data Privacy Framework Policy. All sensitive information is securely stored and protected against accidental disclosure Notice and Consent to Use Private Information

Personal information obtained from an applicant during the application or identity verification process is considered private information if the information is not included in a Certificate or CRL. CA will only use private information after obtaining the subject's consent or as required by applicable law or regulation. All Subscribers must consent to the global transfer and publication of any personal data contained in a Certificate.

9.4.4 Disclosure Pursuant to Judicial or Administrative Process

The CA or RA 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.

9.4.5 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property Rights

CA and/or its business partners own the intellectual property rights in CA's services, including the Certificates, trademarks used in providing the services, and this CP/CPS.

Certificate and Revocation information are the property of CA. CA grants permission to reproduce and distribute Certificates on a non-exclusive and royalty-free basis, provided that they are reproduced and distributed in full. CA does not allow derivative works of its Certificates or products without prior written permission. Private and Public

Keys remain the property of the Subscribers who rightfully hold them. All secret shares (distributed elements) of the CA Private Keys are the property of CA.

All intellectual property of entities participating in the CA private PKI remains the property of its respective owners as per the relevant legal agreements.

9.6 Representations and Warranties

The PA SHALL approve the CPS of Root CAs trusted to issue Tier-1 CAs as part of the DigiCert EVPKI.

9.6.1 CA Representations and Warranties

Except as expressly stated in this CP or in a separate agreement with a Subscriber, CA does not make any representations regarding its products or services. CA represents, to the extent specified in this CP, that the CA:

- Complies, in all material aspects, with this CP and all applicable laws and regulations;
- Publishes and updates CRLs and OCSP responses on a regular basis;
- Does not warrant the accuracy, authenticity, completeness, or fitness of any unverified information;
- Is not responsible for information contained in a Certificate except as stated in this CP/CPS;
- Does not warrant the quality, function, or performance of any software or hardware device; and
- Is not responsible for failing to comply with this CP because of circumstances outside of CA's control.

9.6.2 RA Representations and Warranties

RAs represent that:

- The RA's Certificate issuance and management services conform to this CP;
- Information provided by the RA does not contain any false or misleading information;
- Translations performed by the RA are an accurate translation of the original information; and
- All Certificates requested by the RA meet the requirements of this CP. CA's agreement with the RA may contain additional representations.

9.6.3 Subscriber Representations and Warranties

Subscribers are solely responsible for any misrepresentations they make to third parties and for all transactions that use the Subscriber's Private Key, regardless of whether such use was authorized.

Subscribers are required to notify CA, and any applicable RA, if a change occurs that could affect the status of the Certificate. Subscribers represent to the CA, Application Software Vendors, and Relying Parties that, for each Certificate, the Subscriber will:

- Securely generate its Private Keys and protect its Private Keys from Compromise;
- Provide accurate and complete information when communicating with CA and RAs;
- Confirm the accuracy of the Certificate data prior to using the Certificate;
- Promptly cease using a Certificate and notify CA if (i) any information that was submitted to the CA/RA or is included in a Certificate change or becomes misleading, or (ii) there is any actual or suspected misuse or Compromise of the Private Key associated with the Certificate;
- Ensure that individuals using Certificates on behalf of an organization have received security training appropriate to the Certificate;
- Use the Certificate only for authorized and legal purposes, consistent with the Certificate purpose, this CP, the relevant CPS, any applicable guidelines, and the relevant Subscriber Agreement; and
- Promptly cease using the Certificate and related Private Key after the Certificate's expiration.

Subscriber Agreements may include additional representations and warranties.

9.6.4 Relying Parties Representations and Warranties

Each Relying Party represents that, prior to relying on a CA Certificate, it:

- Obtained sufficient knowledge on the use of digital Certificates and PKI;

- Studied the applicable limitations on the usage of Certificates and agrees to CA's limitations on liability related to the use of Certificates;
- Has read, understands, and agrees to the CA Relying Party Agreement and this CP;
- Verified both the CA Certificate and the Certificates in the Certificate chain using the relevant CRL or OCSP;
- Will not use a CA Certificate if the Certificate has expired or been Revoked; and
- Will take all reasonable steps to minimize the Risk associated with relying on a Digital Signature, including only relying on a CA Certificate after considering:
  - Applicable law and the legal requirements for identification of a party, protection of the Confidentiality or Privacy of information, and enforceability of the transaction;
  - The intended use of the Certificate as listed in the Certificate or this CP/CPS;
  - The data listed in the Certificate;
  - The economic value of the transaction or communication;
  - The potential loss or damage that would be caused by an erroneous identification or a loss of Confidentiality or Privacy of information in the application, transaction, or communication;
  - The Relying Party's previous course of dealing with the Subscriber;
  - The Relying Party's understanding of trade, including experience with computer-based methods of trade; and
  - Any other indicia of reliability or unreliability pertaining to the Subscriber and/or the application, communication, or transaction.

Any unauthorized reliance on a Certificate is at a party's own Risk.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

EXCEPT AS EXPRESSLY STATED IN SECTION 9.6.1, ALL CERTIFICATES AND ANY RELATED SOFTWARE AND SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE". TO THE MAXIMUM EXTENT PERMITTED BY LAW, CA DISCLAIMS ALL EXPRESS AND IMPLIED WARRANTIES, INCLUDING ALL WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. CA DOES NOT WARRANT THAT ANY SERVICE OR PRODUCT WILL MEET ANY EXPECTATIONS OR THAT ACCESS TO CERTIFICATES WILL BE TIMELY OR ERROR-FREE. CA does not guarantee the availability of any products or services and may modify or discontinue any product or service offering at any time. A fiduciary duty is not created simply because an entity uses CA's services.

9.8 Limitations of Liability

NOTHING HEREIN LIMITS LIABILITY RELATED TO (I) DEATH OR PERSONAL INJURY RESULTING FROM CA'S NEGLIGENCE OR (II) FRAUD COMMITTED BY CA. EXCEPT AS STATED ABOVE, ANY ENTITY USING A CA CERTIFICATE OR SERVICE WAIVES ALL LIABILITY OF CA RELATED TO SUCH USE, PROVIDED THAT CA HAS MATERIALLY COMPLIED WITH THIS CP/CPS IN PROVIDING THE CERTIFICATE OR SERVICE. Subscriber agreements and agreements with Relying Parties may contain different limitations on liability, in which case the agreement controls.

All liability is limited to actual and legally provable damages. CA is not liable for:

- Any indirect, consequential, special, or punitive damages or any loss of profit, revenue, data, or opportunity, even if CA is aware of the possibility of such damages;
- Liability related to fraud or wilful misconduct of the Applicant;
- Liability related to use of a Certificate that exceeds the limitations on use, value, or transactions as stated either in the Certificate or this CP/CPS;
- Liability related to the security, usability, or Integrity of products not supplied by CA, including the Subscriber's and Relying Party's hardware; or
- Liability related to the Compromise of a Subscriber's Private Key.

The limitations in this section apply to the maximum extent permitted by law and apply regardless of (i) the reason for or nature of the liability, including tort claims, (ii) the number of claims of liability, (iii) the extent or nature of the

damages, (iv) whether CA failed to follow any provision of this CP, or (v) whether any provision of this CP was proven ineffective.

The disclaimers and limitations on liabilities in this CP are fundamental terms to the use of CA's Certificates and services.

9.9 Indemnities

As set forth in the relevant customer agreement.

9.10 Term and Termination

9.10.1 Term

This CP SHALL be effective from the DCPA approval date and SHALL remain effective until replaced.

9.10.2 Termination

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

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 CA accepts digitally signed or paper notices related to this CP that are addressed to the locations specified in section 2.2 of this CP. Notices are deemed effective after the sender receives a valid and digitally signed acknowledgment of receipt from CA. If an acknowledgement of receipt is not received within five (5) days, the sender must resend the notice in paper form to the street address specified in section 2.2 using either a courier service that confirms delivery or via certified or registered mail with postage prepaid and return receipt requested.

9.12 Amendments

9.12.1 Procedures for Amendment

The DCPA SHALL review this CP at its discretion.

Corrections, updates, or changes to this CP SHALL be made publicly available.

9.12.2 Notification Mechanism and Period

Whenever a material change of the CP occurs, the CP SHALL be published within seven (7) days of the date the amendment took place and all known concerned parties (CA staff, Relying Parties, Subscribers, etc.) SHALL be notified. The DCPA SHALL be responsible for determining what constitutes a material change of the CP.

9.12.3 Circumstances Under Which OID Must be Changed

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

9.13 Dispute Resolution Provisions

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall contain a dispute resolution clause. Unless otherwise approved by CA, the procedure to resolve disputes involving CA require an initial negotiation period of sixty (60) days followed by litigation in the federal or state court encompassing Salt Lake County, Utah, in the case of claimants who are U.S. residents, or, in the case of all other claimants, arbitration administered by the International Chamber of Commerce ("ICC") in accordance with the ICC Rules of Conciliation and Arbitration.

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

9.14 Governing Law

The (i) laws that govern the interpretation, construction, and enforcement of this Agreement and all matters, claims or disputes related to it, including tort claims, and (ii) the courts or arbitration bodies that have exclusive jurisdiction over any of the matters, claims or disputes contemplated in sub-Section (i) above, will each depend on where Customer is domiciled as set forth in the table below; provided, for clarity, that rights and obligations arising from other applicable local laws continue to be governed by such laws. In instances where the International Chamber of Commerce is designated below as the court or arbitration body with exclusive jurisdiction of such matters, claims or disputes, then the parties hereby agree that (x) all matters, claims or disputes arising out of or in connection with this Agreement shall be finally settled under the Rules of Arbitration of the International Chamber of Commerce (Rules) by one or more arbitrators appointed in accordance with the Rules, (y) judgment on the award rendered by such arbitration may be entered in any court having jurisdiction, and (z) this arbitration clause shall not preclude parties from seeking provisional remedies in aid of arbitration from a court of appropriate jurisdiction.

Customer is Domiciled in or the Services are:	**Governing Law is laws of:**	**Court or arbitration body with exclusive jurisdiction:**
The United States of America, Canada, Mexico, Central America, South America, the Caribbean, or any other country not otherwise included in the rest of the table below	Utah state law and United States federal law	State and Federal courts located in Salt Lake County, Utah
Europe, Switzerland, the United Kingdom, Russia, the Middle East or Africa	England	International Chamber of Commerce, International Court of Arbitration, with seat of arbitration in London.
Japan	Japan	International Chamber of Commerce, International Court of Arbitration, with seat of arbitration in Tokyo
Australia or New Zealand	Australia	International Chamber of Commerce, International Court of Arbitration, with seat of arbitration in Melbourne

A Country in Asia or the Pacific region, other than Japan, Australia or New Zealand	Singapore	International Chamber of Commerce, International Court of Arbitration, with seat of arbitration in Singapore

9.15 Compliance with Applicable Law

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

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

The CA contractually obligates any entity operating under this CP to comply with this CP and relevant CPS. The CA also requires each party using its products and services to enter into an agreement that delineates the terms associated with the product or service. If an agreement has provisions that differ from this CP, then the agreement with that party controls, but solely with respect to that party. Third parties may not rely on or bring action to enforce such an agreement.

9.16.2 Assignment

The DCPA 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.

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

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

9.16.5 Force Majeure

The CA is not liable for any delay or failure to perform an obligation under this CP to the extent that the delay or failure is caused by an occurrence beyond CA's reasonable control. The operation of the Internet is beyond the CA's reasonable control. Clauses for force majeure will be added to the extent of applicable law for relevant parties and affiliates within the associated legal agreements.

9.17 Other Provisions

No stipulation.