California ISO

# Certificate Policies for the California Independent System Operator Public Key Infrastructure

---

**Version 3.8**
**Last Updated August 2023**

Table of Contents

## 1.1 INTRODUCTION

## 1.2 Overview

This document defines four certificate policies for use in the California Independent System Operator Public Key Infrastructure (ISO PKI), representing four different assurance levels (Rudimentary, Basic, Medium, and High) for Identity Authentication, Message Origin Authentication and Key Agreement certificates. This document follows and conforms to the Internet Engineering Task Force (IETF) Request for Comment (RFC) 3647. RFC 3647 was published in November 2003 and replaces RFC 2527. The RFC is entitled: *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.*

The California ISO, through a Managed PKI Service, operates a two-level certification authority hierarchy as depicted in Figure 1 below. The Root CA is a self signed certification authority named *CAISO_Root_CA*. The Root CA issues certificates to operational Certification Authorities (CAs) according to one or more of the policies described in this document. The Operational Certification Authorities then issue certificates to all ISO PKI Subscribers.

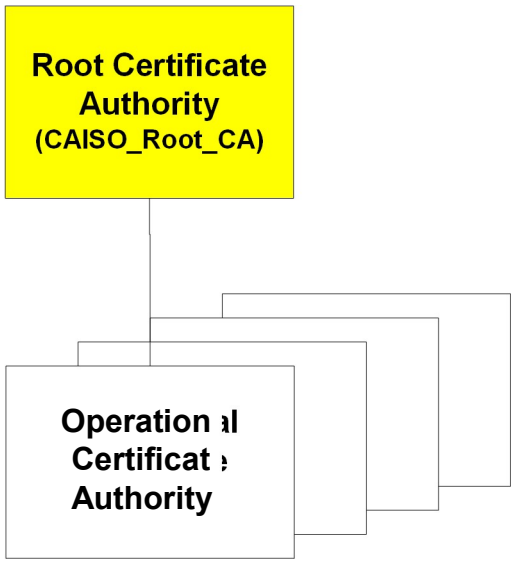


**Figure 1 California ISO Certification Authority Hierarchy**

Under normal operating conditions the Root CA is an off-line system. Circumstances that may warrant bringing the Root CA on-line include (but are not limited to):

1. Revoke the digital certificate of one of the operational CAs,
2. Create a new operational CA, or
3. Create a cross-certificate for another CA.

**The policies described in rest of this document apply to the operational Certificate Authorities (CAs) only. These CAs are on-line systems that issue end-entity certificates.**

The certificate policies defined in this document are intended for use by the ISO PKI and its Subscribers and Relying Parties. Users of this document are to consult the issuing Certification Authority and its related Certification Practice Statement (CPS) to obtain further details of the implementation of this Certificate Policy. There are four policies associated with ISO certificates that are used for Identity Authentication, Message Origin Authentication and Key Agreement. The applicability of these certificates, and the related policies, will depend on the application that uses or is relying on certificates for these purposes.

The four policies are for the management and use of certificates containing public keys used for identity authentication, message origin authentication and key agreement mechanisms. For instance, the certificates issued under these policies could be used for verifying the identity of a user or system for access to a California ISO application.

Issuance of a public key certificate under any of these policies does not imply that the Subscriber has any authority to conduct business transactions on behalf of the ISO.

The laws of the State of California and the California ISO Tariff concerning the enforceability, construction, interpretation and validity of this Certificate Policy will govern the CA.

The ISO reserves the right to accept or the decline offers to enter into a cross certification agreement with an external Certification Authority.

An overview of the four policies covered by this document follows.

**Rudimentary (Test) Assurance Policy**
The California ISO disclaims all liability for any use of this type of certificate. Any disputes concerning key or certificate management under this policy are to be resolved under the provisions of the California ISO Tariff.

Digital certificates may be issued under this policy without any authentication of a Subscriber's identity. Subscriber’s identification may be in any manner indicated by the CA.

Rudimentary (test) assurance digital certificates are only appropriate for use in testing identity authentication, testing message origin authentication and for testing establishment of a session key for secure communication as described in the Certificate Practice Statement for non-production based ISO systems.

A CA is not obliged to revoke certificates under this type of policy.

**Basic Assurance Policy**
This policy has been designed to be used in certain situations and identifies specific roles and responsibilities for CAs, which issue this type of certificate and for Registration Authorities (RA) which must perform tasks that may be assigned to them by the CA. Subscribers and Relying Parties also have specific obligations which are outlined in this policy.

A CA must ensure that it associates itself with and uses at least one Certificate and one CRL repository for this type of certificate. Digital certificates must be made available to the respective Subscribers. The repository may be used by other CAs of same or different assurance level.

Basic assurance digital certificates are appropriate for use in identity authentication, message origin authentication and for establishing a session key for secure communication as described in the Certification Practice Statement for appropriate production based ISO systems.

ISO disclaims all liability for any use of this type of certificate other than uses permitted by the CA. ISO limits its liability for permitted uses as stated in Section 14 of the California ISO Tariff. The subscriber identified within the certificate is liable for all transactions occurring with their respective certificate(s).

Certificates may be issued under this policy following authentication of a Subscriber's identity. Identification will be in the manner set out in this policy.

A CA will revoke certificates in the circumstances enumerated in this policy.

A CA is required to maintain records or information logs in the manner described in this policy.

Keys will have a validity period as indicated in this policy.

No personal information collected by a CA may be disclosed without the Subscriber's consent unless required by law or applicable regulation.

CA activities are subject to inspection.

**Medium Assurance Policy**
This policy has been designed to be used in certain situations and identifies specific roles and responsibilities for CAs, which issue this type of certificate, and for Registration Authorities (RA) which must perform tasks that may be assigned to them by the CA. Subscribers and Relying Parties also have specific obligations which are outlined in this policy.

A CA must ensure that it associates itself with and uses at least one Certificate and one CRL repository for this type of certificate. Digital certificates must be made available to

the respective Subscribers. The repository may be used by other CAs of same or different assurance level.

Medium assurance certificates are appropriate for use in identity authentication, message origin authentication and for establishing a session key for secure communication as described in the Certificate Practice Statement for appropriate production based ISO systems.

ISO disclaims all liability for any use of this type of certificate other than uses permitted by the CA. ISO limits its liability for permitted uses as stated in Section 14 of the California ISO Tariff. The subscriber identified within the certificate is liable for all transactions occurring with their respective certificate(s).

Certificates may be issued under this policy following authentication of a Subscriber's identity. Identification will be in the manner set out in this policy.

A CA will revoke certificates in the circumstances enumerated in this policy.

A CA is required to maintain records or information logs in the manner described in this policy.

Keys will have a validity period as indicated in this policy.

No personal information collected by a CA may be disclosed without the Subscriber's consent unless required by law or applicable regulation.

CA activities are subject to inspection.

**High Assurance Policy**

This policy has been designed to be used in certain situations and identifies specific roles and responsibilities for CAs, which issue this type of certificate, and for Registration Authorities (RA) which must perform tasks that may be assigned to them by the CA. Subscribers and Relying Parties also have specific obligations which are outlined in this policy.

A CA must ensure that it associates itself with and uses at least one Certificate and one CRL repository for this type of certificate. Digital certificates must be made available to the respective Subscribers. The repository may be used by other CAs of same or different assurance level.

High assurance certificates are appropriate for use in identity authentication, message origin authentication and for establishing a session key for secure communication as described in the Certificate Practice Statement for appropriate production based ISO systems.

ISO disclaims all liability for any use of this type of certificate other than uses permitted by the CA. ISO limits its liability for permitted uses as stated in Section 14 of the California ISO Tariff. The subscriber identified within the certificate is liable for all transactions occurring with their respective certificate(s).

Certificates may be issued under this policy following authentication of a Subscriber's identity. Identification will be in the manner set out in this policy.

A CA will revoke certificates in the circumstances enumerated in this policy.

A CA is required to maintain records or information logs in the manner described in this policy.

Keys will have a validity period as indicated in this policy

No personal information collected by a CA may be disclosed without the Subscriber's consent unless required by law or applicable regulation.

CA activities are subject to inspection

## 1.3 Document name and identification

This document is identified by name as *Certificate Policies for the California Independent System Operator Public Key Infrastructure*. This document describes four policies identified as follows:

1. Rudimentary (Test) Assurance, Policy identifier 1.3.6.1.4.1.3907.1.1.1.1
2. Basic Assurance, Policy identifier 1.3.6.1.4.1.3907.1.1.1.4
3. Medium Assurance, Policy identifier 1.3.6.1.4.1.3907.1.1.1.3
4. High Assurance, Policy identifier 1.3.6.1.4.1.3907.1.1.1.2

## 1.4 PKI participants

This section describes the identity or types of entities that fill the roles of participants in ISO PKI operations.

### 1.3.1. CERTIFICATION AUTHORITIES (CAs)

**Rudimentary (Test) Assurance**

A CA operating under this policy is responsible for the creation and signing of certificates binding Subscribers with their public encryption keys for use with non-production ISO systems.

**Basic, Medium, and High Assurance**

A CA operating under these policies is responsible for:

- creation and signing of certificates binding Subscribers and PKI personnel with their identity authentication and key agreement keys for use with appropriate production ISO systems;
- promulgating certificates, and certificate status including CRLs (or equivalent measures), in a repository; and
- ensuring adherence to this Certificate Policy.

### 1.3.2. Registration authorities

For all assurance levels enumerated in this Certificate Policy, the Registration Authorities (RAs) manage the certificate lifecycle for their respective CAs. RAs are responsible for requesting or approving requests to the CA to issue and revoke certificates in accordance with this Policy, as well as any additional relevant policies and procedures included in their respective Certification Practice Statements.

Establishing a Local RA (LRA) requires registration through a Registration Authority. An LRA operating under the all the policies enumerated in this Certificate Policy is responsible for all duties assigned to it by the CA.

An RA and an LRA may perform duties on behalf of more than one CA, provided that in doing so they satisfy all the requirements of this CP.

### 1.3.3. Subscribers

For all assurance levels enumerated in this Certificate Policy, Subscribers include individuals, organizations, devices, systems, and applications. Subscribers may be issued certificates for assignment to devices, groups, organizational roles or applications provided that responsibility and accountability is attributable to an individual or an organization. The Subscriber, identified within the certificate, is liable for all transactions occurring with their respective certificate(s).

ISO PKI certificates will only be issued after request or authorization for issuance from one or more Sponsors. They may be issued to employees, market participants, and related systems and organizations or others with whom the Sponsor has a relationship.

Eligibility for a certificate is at the sole discretion of the ISO. A CA may administer any number of Subscribers. Additional stipulations with respect to Subscribers for each Certificate Policy are as follows.

**Rudimentary (Test) Assurance**

The Subscribers include all internal and external organizations, users, applications and devices that interact with ISO and that require certificates for the purpose of testing their systems for interoperability and integration with non-production ISO applications and/or networks.

**Basic Assurance**

The Subscribers include all internal and external organizations, users, applications and devices that interact with ISO and that require certificates for the purpose of

authenticating identity, message origin authentication and establishing secure sessions with appropriate production ISO applications and/or the ISO network.

**Medium Assurance**
The Subscribers include all internal and external organizations, users, applications and devices that interact with ISO and that require certificates for the purpose of authenticating identity, message origin authentication and establishing secure sessions with appropriate production ISO applications and/or ISO networks.

**High Assurance**
The Subscribers include all internal and external organizations, users, applications and devices that interact with ISO and that require certificates for the purpose of authenticating identity, message origin authentication and establishing secure sessions with appropriate production ISO applications and/or ISO networks.

### 1.3.4. Relying parties

**Rudimentary (test) Assurance**
No stipulation.

**Basic, Medium, and High Assurance**
A Relying Party may be either a Subscriber of the ISO PKI or an entity that interacts with a Subscriber, which presents a ISO Certificate but does not require a reciprocal certificate to be presented to it.

### 1.3.5. Other participants

ISO PKI requires participation of repositories as follows.

**Rudimentary (Test) Assurance**
Not required.

**Basic, Medium, and High Assurance**
A CA must ensure that there is at least one certificate and CRL repository associated with it. This repository should be in the form of one or more directories that comply with the LDAP standards profile.

A repository may or may not be under the control of a CA. Where a repository is not under the control of a CA, the CA must ensure that the terms and conditions of its association include, but are not limited to, the subjects of availability, access control, data integrity, directory replication and directory chaining.

## 1.4 Certificate usage

### 1.4.1. Appropriate certificate uses

**Rudimentary (Test) Assurance**

Applications that leverage rudimentary certificates must be in non-production status.

**Basic, Medium, and High Assurance**

A CA must advise Subscribers which applications are intended to be used with the PKI system. These applications must, at a minimum, meet the following requirements:

- establish, transfer and use the public and private keys;
- capability to perform the appropriate certificate validity and verification checking;
- report appropriate information and warnings to the Subscriber

## 1.5 Policy administration

This section includes the name and mailing addresses of the organization and individuals responsible for creating and maintaining this Certificate Policy document.

### 1.5.1. Organization administering the document

The California Independent System Operator (ISO) is responsible for administering this document. The mailing address for the CAISO is:
California ISO
250 Outcropping Way
Folsom, CA 95630

### 1.5.2. Contact person

The points of contact for this Certificate Policy document are:
Manager, Information Security
California ISO
250 Outcropping Way
Folsom, CA 95630

CIO and VP, Information Technology
California ISO
250 Outcropping Way
Folsom, CA 95630

### 1.5.3. Person determining CPS suitability for the policy

The person determining CPS suitability for the policies enumerated in this Certificate Policy document is:
Hubert Hafner
Manager, Information Security
California ISO
250 Outcropping Way
Folsom, CA 95630

### 1.5.4. CPS approval procedures

A CA's accreditation into the ISO PKI must be in accordance with procedures specified by the Policy Management Authority (PMA). Where a CPS contains information relevant to the security of a CA, all or part of the CPS need not be made publicly available.

## 1.6 Definitions and acronyms

This section provides general definitions of terms and acronyms that are used throughout this document.

### 1.6.1. General definitions

**Certificate**

The public key of an entity together with related information, digitally signed with the private key of the Certification Authority that issued it. The certificate format is in accordance with ITU-T Recommendation X.509v3. An entity can be a human user, a device, or an application that is executed on a device.

**Certificate Revocation List (CRL)**

A list maintained by a Certification Authority of the certificates it has issued that are revoked before their natural expiry time.

**Certification Authority**

An authority trusted by one or more users to issue and manage X.509v3 public key certificates and CRLs. Each CA within the ISO PKI may issue certificates under one or more policies based on the assurance level the CA has been accredited to and the requirements and role of the Subscriber.

**Certification Authority Software**

The cryptographic software required for managing the lifecycle of keys and certificates of end entities.

**Data Integrity**

Assurance that data remains free of unauthorized change from its creation to reception.

**Digital Signature**

The result of a transformation of a message by means of a cryptographic system using keys such that a person who has the initial message can determine:

(a) Whether the transformation was created using the key that corresponds to the signer's key; and

(b) Whether the message has been altered since the transformation was made.

**End-Entity**

An Entity that uses the keys and certificates created within the PKI for purposes other than the management of the aforementioned keys and certificates. An end-entity may be a Subscriber or a Relying Party.

**Entity**

Any autonomous element within the Public Key Infrastructure. This may be a CA, an RA or an End-Entity.

**Issuing CA**

In the context of a particular certificate, the issuing CA is the CA that signed and issued the certificate.

**Root CA**

The highest level CA, or in CAISO's PKI, the CA that is named CAISO_Root_CA. The Root CA's certificate is self-signed.

**Registration Authority (RA)**

A person or organization that is responsible for the identification and authentication of certificate Subscribers before certificate issuance, but does not actually sign or issue the certificates. An RA is delegated certain tasks on behalf of a CA. RAs are also referred to as a Local Registration Authority (LRA).

**MD5**

One of the message digest algorithms developed by RSA Data Security Inc.

**Object Identifier (OID)**

The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the ISO PKI they are used to uniquely identify each of the four policies and cryptographic algorithms supported.

**Operational Authority**

Personnel who are responsible for the overall operations for the ISO PKI CAs.

**Operations Zone**

An area where access is limited to authorized personnel needing to work there and to properly escorted visitors. Operations Zones should be monitored at least periodically, based on a Threat Risk Assessment (TRA), and should preferably be accessible from a Reception Zone

**Organization**

A department, agency, corporation, partnership, trust, joint venture or other association or governmental body.

**Policy Management Authority (PMA)**

The body, ISO in this case, responsible for setting, implementing, and administering policy decisions regarding CPs and CPSs throughout the ISO PKI.

**Public Key Infrastructure (PKI)**

A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and keys.

**Reception Zone**

The entry to a facility where the initial contact between the public and the department occurs, where services are provided, information is exchanged and access to restricted (Operations, Security and High-security) zones is controlled. To varying degrees, activity in a Reception Zone is monitored by personnel who work there, by other personnel or by security staff. Access by the public may be limited to specific times of the day or for specific reasons. Entry beyond the Reception Zone is indicated by a recognizable perimeter such as a doorway or an arrangement of furniture and dividers in an open office environment.

**Relying Party**

An End Entity who uses a certificate signed by a ISO PKI CA to authenticate an identity or for key agreement to establish a secure session; May also be a Subscriber of the ISO PKI CA.

**Repository**

A location where CRLs and certificates are stored for access by End Entities with a need-to-know.

**Secure Hash Algorithm (SHA)**

One of the message digest algorithms developed by the US government under Federal Information Processing Standards (FIPS) publication.

**Security Zone**

An area to which access is limited to authorized personnel and to authorized and properly escorted visitors. Security Zones should preferably be accessible from an Operations Zone, and through a specific entry point. A Security Zone need not be separated from an Operations Zone by a secure perimeter. A Security Zone should be monitored 24 hours a day and 7 days a week by security staff, other personnel or electronic means.

**Sponsor**

A Sponsor in the ISO PKI is the department or employee that has nominated that a specific individual or organization be issued a certificate. (e.g., for an employee this may be the employee's manager). The Sponsor might suggest an appropriate DN for the certificate and will be responsible for either supplying or confirming the certificate attribute details to the RA. The Sponsor is also responsible for informing the CA or RA if the department's relationship with the Subscriber is terminated or has changed such that the certificate should be revoked or updated.

**Subscriber**

An individual, device or organization whose public key is certified in a public key certificate. In the ISO PKI this could be an employee, a market participant, a device, a system or an application.

### 1.6.2. Acronyms

| Acronym | Term |
|---|---|
| CA | Certification Authority |
| CAISO | The California Independent System Operator |
| CRL | Certificate Revocation List |
| LDAP | Lightweight Directory Access Protocol |
| LRA | Local Registration Authority |
| OID | Object Identifier |
| PKI | Public Key Infrastructure |
| RA | Registration Authority |

## 2.1 PUBLICATION AND REPOSITORY RESPONSIBILITIES

**Rudimentary (Test) Assurance**

No stipulation

**Basic, Medium, and High Assurance**

The repository should be available, on a need-to-know basis, for a significant portion of every 24-hour period. Certificates and CRLs must be available to Relying Parties, with a need-to-know, in accordance with the requirements of Section 2.3 of this policy.

## 2.2 Repositories

ISO and its Managed PKI Service provider operate all the repositories to which certificates and Certificate Revocation Lists (CRLs) are published.

## 2.3 Publication of certification information

**Rudimentary (Test) Assurance**

Not applicable

**Basic, Medium, and High Assurance**

An issuing CA must:

- Include within any certificate it issues the URL of a web site maintained by, or on behalf of, the CA;
- Ensure the publication of its CPs on a web site maintained by, or on behalf, of the CA. An electronic copy of this document, digitally signed by an authorized representative of the CA, is to be made available:
    - at the ISO World Wide Web site at the URL www.caiso.com;
    - via an e-mail request to the point of contact listed in Section 1.5.2.
- Ensure, directly or through agreement with a repository, that operating system and repository access controls will be configured so that only authorized CA personnel can write or modify the online version of the CPS; and
- Provide a full text version of the CPS when necessary for the purposes of any audit, inspection, or accreditation.
- Use a central repository for publishing digital certificates and CRLs.

## 2.4 Time and frequency of publication

**Rudimentary (Test) Assurance**

Not applicable.

**Basic, Medium, and High Assurance**

Certificates must be published promptly upon issuance. A CA must issue an up-to-date CRL at least every twenty-four hours. When a certificate is revoked due to key compromise the updated CRL must be issued immediately and published within 60 minutes.

## 2.5 Access controls on repositories

Access controls may be instituted at the discretion of the CA with respect to certificates or on-line certificate status (if the latter is provided as a service by the CA). Certificates must be published promptly upon issuance. CRL publication must be in accordance with Section 4.9.

# 3.1 IDENTIFICATION AND AUTHENTICATION

This section describes the procedures used to authenticate the identity and/or other attributes of an end-user certificate applicant to a CA or RA prior to certificate issuance.

## 3.2 Naming

### 3.2.1. Types of names

Each Entity must have a clearly distinguishable and unique X.500 Distinguished Name (DN) in the certificate subject name field and in accordance with PKIX Part 1. The DN must be in the form of a X.500 *printableString* and must not be blank.

### 3.2.2. Need for names to be meaningful

**Rudimentary (Test) Assurance**
No stipulation

**Basic, Medium, and High Assurance**
The contents of each certificate Subject and Issuer name fields must have an association with the authenticated name of the Entity.

In cases where multiple certificates are issued to the same Subscriber, the Subscriber's certificates will be differentiated using the certificates' serial numbers.

### 3.2.3. Anonymity or pseudonymity of subscribers

No stipulation

### 3.2.4. Rules for interpreting various name forms

No stipulation

### 3.2.5. Uniqueness of names

Distinguished names must be unique for all End-Entities of a CA. For each End-Entity additional numbers or letters may be appended to the `commonName` to ensure the RDN's uniqueness.

### 3.2.6. Recognition, authentication, and role of trademarks

The CA reserves the right to make all decisions regarding Entity names in all assigned certificates. A party requesting a certificate must demonstrate its right to use a particular name.

Where there is a dispute about a name in a repository not under its control, a CA must ensure that there is a name claim dispute resolution procedure in its agreement with that repository.

The use of trademarks will be reserved to registered trademark holders.

## 3.3 Initial identity validation

### 3.3.1. Method to prove possession of private key

**Rudimentary (Test) Assurance**
No stipulation

**Basic, Medium, and High Assurance**

When a subscriber generates its own private key it must prove possession of the private key by providing a signed request to the RA.

### 3.3.2. Authentication of organization identity

**Rudimentary (Test) Assurance**

No stipulation

**Basic, Medium, and High Assurance**

An application for an individual, a device, an application, or an organization to be a Subscriber may be made by an individual or an organization authorized to act on behalf of the prospective Subscriber.

Identification and authentication of the prospective Subscriber must be through one of the following means:

- The RA must examine documentation providing evidence of the existence of the organization; or
- Another department of ISO establishes the identity and existence of the organization using a process that satisfies the CA.

The RA must also verify the identity of the individual or organization acting on behalf of the prospective Subscriber and their authority to receive the initialized token on behalf of that organization.

The CA or RA must keep a record of identification details.

### 3.3.3. Authentication of individual identity

**Rudimentary (Test) Assurance**

No stipulation

**Basic, Medium, and High Assurance**

An application for an individual to be a Subscriber may be made by the individual, or by another person or organization authorized to act on behalf of the prospective Subscriber.

Identification and authentication of the individual must be through one of the following means:

- The RA will compare the identity of the individual with two pieces of identification. At least one of these must be an identification containing a photograph; or
- Another department of ISO establishes the identity and existence of the organization using processes and procedures that have been reviewed and approved by the RA and CA.

An application for a device, system or software application to be an End-Entity may be made by an individual or organization to which the device's, system's or application's signature is attributable for the purposes of accountability and responsibility. Identification and authentication of the applicant must follow Sections 3.2.2. of this policy as if that individual or organization was applying for the certificate on its own behalf. The RA must also verify the identity of the individual or organization making the application and its authority to receive the keys for that device or application.

The CA or RA must keep a record of identification details.

### 3.3.4. Non-verified subscriber information

The email address of the subscriber in the digital certificate is not verified. The email address may be empty, may have an incorrect user name and/or an incorrect domain name, or it may have an email address that belongs to an entity other than the Subscriber.

### 3.3.5. Validation of authority

An application for a device, system or software application to be an End-Entity may be made by an individual or organization to which the device's, system's or application's signature is attributable for the purposes of accountability and responsibility. Identification and authentication of the applicant must follow Sections 3.2.2. or 3.2.3. of this policy as if that individual or organization was applying for the certificate on its own behalf. The RA must also verify the identity of the individual or organization making the application and its authority to receive the keys for that device or application.

The CA or RA must keep a record of identification details.

### 3.3.6. Criteria for interoperation

Not applicable.

## 3.4 Identification and authentication for re-key requests

### 3.4.1. Identification and authentication for routine re-key

Not applicable

### 3.4.2. Identification and authentication for re-key after revocation

Where the information contained in a certificate has changed or there is a known or suspected compromise of the private key, a CA must authenticate a re-key in the same manner as for initial registration. The RA must verify any change in the information contained in a certificate before requesting that the CA issue the certificate.

## 3.5 Identification and authentication for revocation request

**Rudimentary (Test) Assurance**

No stipulation

**Basic, Medium, and High Assurance**

A CA, or RA acting on its behalf, must authenticate a request for revocation of a certificate. A CA must establish and make publicly available the process by which it addresses such requests and the means by which it will establish the validity of the request.

Requests for revocation of certificates must be logged.

## 4.1 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

This section specifies the requirements imposed upon issuing CAs, RAs, and Subscribers, with respect to the life-cycle of a certificate.

General obligations of the CAs are as follows:

**Rudimentary (Test) Assurance**

The CA will operate in accordance with this CP when managing the keys provided to RAs and Subscribers.

**Basic, Medium, and High Assurance**

The CAs will operate in accordance with their respective CPS, this CP, the laws of California and the California ISO Tariff when issuing and managing the keys provided to RAs and Subscribers under this CP. The CAs will ensure that all RAs operating on its behalf will comply with the relevant provisions of this CP concerning the operation of RAs. The CAs will take all reasonable measures to ensure that Subscribers and Relying Parties are aware of their respective rights and obligations with respect to the operation and management of any keys, certificates or End-Entity hardware and software used in connection with the PKI.

The CAs must provide notice by incorporation or reference within its CPS of limitations of liability established by the California ISO Tariff (Section 14) under which CAISO and the ISO PKI operates.

A CA must:

- Issue a CPS
- Have in place mechanisms and procedures to ensure that its RAs and Subscribers are aware of, and agree to abide with, the stipulations in this policy that apply to them.

CA personnel associated with PKI roles (e.g. PKI Administrators) must be individually accountable for actions they perform. “Individually accountable” means that there must be evidence that attributes an action to the person performing the action.

## 4.2 Certificate Application

### 4.2.1. Who can submit a certificate application

**Rudimentary (Test) Assurance**

The procedures and requirements for Certificate application will be established and published in the CPS or a publicly available document.

**Basic, Medium, and High Assurance**

A CA must ensure that all procedures and requirements with respect to an application for a certificate are set out in the CPS or a publicly available document. Bulk applications on behalf of End-Entities are permitted to be made only by persons authorized to make such applications.

### 4.2.2. Enrollment process and responsibilities

**Rudimentary (Test) Assurance**

The procedures and requirements for the enrollment process will be established and published in the CPS or a publicly available document.

**Basic, Medium, and High Assurance**

For ISO entities an RA must ensure that each application is accompanied by:

- Proof of the End-Entity's identity; and
- An acknowledgement of the conditions governing their use of the certificate.

For Non-ISO Subscribers an identical procedure will be enforced with authorization for certificate issuance being provided to the RA or by another department within ISO.

## 4.3 Certificate application processing

**Rudimentary (Test) Assurance**

When a CA issues a rudimentary certificate it certifies that the certificate is unique within its own system. The certificates issued are intended for use with non-production systems only.

The CA and the RA make no other representation.

**Basic, Medium, and High Assurance**

There is no stipulation for the period between the receipt of an application for a Certificate and the generation of the Entity's key material.

The Entity must notify the CA of completion of the initialization process.
The CA must ensure that the period for which the Entity has to complete its initialization process is no longer than five working days.

When an Issuing CA publishes a certificate it certifies that it has issued a certificate to a Subscriber and that the information stated in the certificate was verified in accordance with this CP. Publication of the certificate in a repository, to which the subscriber has access, constitutes notice of such verification. Additionally, use of the certificate by the Subscriber also constitutes such verification.

A CA will provide to each Subscriber notice of the Subscriber's rights and obligations under this Certificate Policy. Such notice may be in the form of incorporation within the CA's CPS or in Certificate Subscriber Agreement and publication of that CPS or Subscriber Agreement on a web site that is accessible to the Subscriber. Such notice will include a description of the allowed uses of certificates issued under this CP; the Subscriber's obligations concerning key protection; and procedures for communication between the Subscriber and the CA or RA, including communication of changes in service delivery or changes to this policy. Subscribers should also be notified as to procedures for dealing with suspected key compromise, certificate issuance, service cancellation, and dispute resolution.

A CA will ensure that any notice of the Subscriber's rights and obligations under this Certificate Policy includes a description of a Relying Party's obligations with respect to use, verification and validation of certificates.

When an RA submits Subscriber information to a CA, it must certify to the CA that it has authenticated the identity of that Subscriber in accordance with this section and Section 3.0 of this policy.

### 4.2.1. Performing identification and authentication functions

See Section 4.1.2.

### 4.2.2. Approval or rejection of certificate applications

An application for a certificate does not oblige a CA to issue a certificate.

### 4.2.3. Time to process certificate applications

**Rudimentary (Test) Assurance**
No stipulation

**Basic, Medium, and High Assurance**
The CPS of each CA must indicate the time to process certificate applications.

## 4.3 Certificate issuance

### 4.3.1. CA actions during certificate issuance

The issuance and publication of a certificate by a CA indicates a complete and final approval of the certificate application by the CA.

### 4.3.2. Notification to subscriber by the CA of issuance of certificate

An Issuing CA is required to make certificates available to the respective Subscribers.

## 4.4 Certificate acceptance

### 4.4.1. Conduct constituting certificate acceptance

**Rudimentary (Test) Assurance**
No stipulation

**Basic, Medium, and High Assurance**
A CA must ensure that an Entity acknowledges acceptance of a certificate. For a device or application the individual or organization responsible for the device or application may do this acknowledgement. Two forms of acknowledgement are:

- Downloading of the certificate, or
- Utilization of the delivered certificate.

### 4.4.2. Publication of the certificate by the CA

**Rudimentary (Test) Assurance**
Not applicable

**Basic, Medium, and High Assurance**
An issuing CA must publish the certificates it issues in a repository.

### 4.4.3. Notification of certificate issuance by the CA to other entities

No stipulation

## 4.5 Key pair and certificate usage

### 4.5.1. Subscriber private key and certificate usage

An Issuing CA must ensure that a Subscriber agrees to abide by an acceptable use policy which outlines the terms and conditions of use, including permitted applications and purposes. **By utilizing the delivered certificate, the Subscriber is agreeing that they have read, understood, and will abide by the terms and conditions as defined in either the CPS or Subscriber Agreement.**

### 4.5.2. Relying party public key and certificate usage

Prior to using a Subscriber's certificate, a Relying Party must ensure that it is appropriate for the intended use. A Relying Party should use certificates only in accordance with the certification path validation procedure specified in RFC 3280.

## 4.6 Certificate renewal

**Rudimentary (Test) Assurance**
No stipulation.

**Basic, Medium, and High Assurance**
Not applicable. The CAs operating at these assurance levels do not renew certificates. Every certificate issued from a conforming CAs follows the same procedure as issuing a new certificate.

### 4.6.1. Circumstance for certificate renewal
Not applicable.

### 4.6.2. Who may request renewal
Not applicable.

### 4.6.3. Processing certificate renewal requests
Not applicable.

### 4.6.4. Notification of new certificate issuance to subscriber
Not applicable.

### 4.6.5. Conduct constituting acceptance of a renewal certificate
Not applicable.

### 4.6.6. Publication of the renewal certificate by the CA
Not applicable.

### 4.6.7. Notification of certificate issuance by the CA to other entities
Not applicable.

## 4.7 Certificate re-key

**Rudimentary (Test) Assurance**
No stipulation.

**Basic, Medium, and High Assurance**
Not applicable. The CAs operating at these assurance levels do not re-key certificates. Every certificate issued from a conforming CAs follows the same procedure as issuing a new certificate.

### 4.7.1. Circumstance for certificate re-key
Not applicable.

### 4.7.2. Who may request certification of a new public key
Not applicable.

### 4.7.3. Processing certificate re-keying requests
Not applicable.

### 4.7.4. Notification of new certificate issuance to subscriber
Not applicable.

#### 4.7.5. Conduct constituting acceptance of a re-keyed certificate

Not applicable.

#### 4.7.6. Publication of the re-keyed certificate by the CA

Not applicable.

#### 4.7.7. Notification of certificate issuance by the CA to other entities

Not applicable.

### 4.8 Certificate modification

**Rudimentary (Test) Assurance**

No stipulation.

**Basic, Medium, and High Assurance**

Not applicable. The CAs operating at these assurance levels do not support issuance of modified certificates. Every certificate issued from a conforming CAs follows the same procedure as issuing a new certificate.

#### 4.8.1. Circumstance for certificate modification

Not applicable.

#### 4.8.2. Who may request certificate modification

Not applicable.

#### 4.8.3. Processing certificate modification requests

Not applicable.

#### 4.8.4. Notification of new certificate issuance to subscriber

Not applicable.

#### 4.8.5. Conduct constituting acceptance of modified certificate

Not applicable.

#### 4.8.6. Publication of the modified certificate by the CA

Not applicable.

#### 4.8.7. Notification of certificate issuance by the CA to other entities

Not applicable.

### 4.9 Certificate revocation and suspension

ISO PKI only revokes certificates. It does not suspend certificates.

**Rudimentary (Test) Assurance**

Not applicable.

**Basic, Medium, and High Assurance**
The Issuing CA must ensure that any procedures for the expiration and revocation of a certificate will conform to the relevant provisions of this CP and will be expressly stated in the Subscriber Agreement and any other applicable document outlining the terms and conditions of the certificate use**.** The Issuing CA will also ensure that notice of revocation of a certificate will be posted to the CRL within the time limits stated in Section 4.9.7. of this policy.

### 4.9.1. Circumstances for revocation

**Rudimentary (Test) Assurance**
No stipulation

**Basic, Medium, and High Assurance**
A certificate must be revoked:

- When any of the information in the digital certificate changes;
- When the Subscriber is an individual and leaves the organization or is otherwise terminated;
- When the Subscriber is assigned to other functions that no longer require the use of the digital certificate issued to them;
- Upon suspected or known compromise of the private key;
- Upon suspected or known compromise of the media holding the private key;
- Upon suspected or known loss of the private key.

The CA in its discretion may revoke a certificate when an Entity fails to comply with obligations set out in this CP, the CPS, any agreement or any applicable law.

### 4.9.2. Who can request revocation

**Rudimentary (Test) Assurance**
No stipulation

**Basic, Medium, and High Assurance**
The revocation of a certificate may only be requested by:

- The Subscriber in whose name the certificate was issued;
- An authorized individual within the organization who sponsored the Subscriber,
- The individual or organization that made the application for the certificate on behalf of a device or application;
- The Sponsor;
- The Policy Management Authority;
- Personnel of the Issuing CA;
- RA associated with the Issuing CA.

### 4.9.3. Procedure for revocation request

**Rudimentary (Test) Assurance**

No stipulation

**Basic, Medium, and High Assurance**

A CA must ensure that all procedures and requirements with respect to the revocation of a certificate are set out in the CPS, the Subscriber Agreement or are otherwise made publicly available. An authenticated revocation request, and any resulting actions taken by the CA, must be recorded and retained. In the case where a certificate is revoked, full justification for the revocation must also be documented by the RA.

Where an Entity certificate is revoked, the revocation will be published in the appropriate CRL, which is then in turn published to the standard repository available to Relying Parties.

### 4.9.4. Revocation request grace period

**Rudimentary (Test) Assurance**

No stipulation

**Basic, Medium, and High Assurance**

In the event of the compromise, or suspected compromise, of any Entity's private key, an Entity must notify the Issuing CA immediately.

### 4.9.5. Time within which CA must process the revocation request

**Rudimentary (Test) Assurance**

No stipulation

**Basic, Medium, and High Assurance**

Any action taken as a result of a request for the revocation of a certificate must be initiated within twenty-four (24) hours of receipt. There is no requirement for an RA to notify a Relying Party of the issuance or revocation of a certificate.

### 4.9.6. Revocation checking requirement for relying parties

**Rudimentary (Test) Assurance**

No stipulation.

**Basic, Medium, and High Assurance**

A Relying Party must check the status of all certificates in the certificate validation chain against the appropriate and current CRLs (including a previously cached CRL) prior to their use. A Relying Party must also verify the authenticity and integrity of the CRLs. As part of this verification process the digital signature of the CRL must also be validated. If CRLs are not being leveraged, an equivalent means of certificate validation must be made available.

### 4.9.7. CRL issuance frequency

The Root CA issues a CRL at least every two years with a validity period of 750 days.

**Rudimentary (Test) Assurance**

A CA is not required to make CRLs available to a Subscriber or a Relying Party unless otherwise stated in the Subscriber agreement.

**Basic, Medium, and High Assurance**

A CA must ensure that it issues an up-to-date CRL at least every twenty-four hours and is valid for at least thirty hours. When a certificate is revoked due to key compromise the updated CRL must be issued within 60 minutes of revocation. An Issuing CA is required to make certificates available to the respective Subscribers. An Issuing CA must make CRLs available to a Relying Party in accordance with this section of the CP, and on a need-to-know basis.

### 4.9.8. Maximum latency for CRLs

**Rudimentary (Test) Assurance**

Not applicable.

**Basic, Medium, and High Assurance**

A CRL must be posted to the appropriate repository immediately upon issuance.

### 4.9.9. On-line revocation/status checking availability

No stipulation.

### 4.9.10. On-line revocation checking requirements

No stipulation.

### 4.9.11. Other forms of revocation advertisements available

No stipulation.

### 4.9.12. Special requirements in reference to key compromise

No stipulation

### 4.9.13. Circumstances for suspension

Not applicable

### 4.9.14. Who can request suspension

Not applicable

### 4.9.15. Procedure for suspension request

Not applicable

### 4.9.16. Limits on suspension period

Not applicable

### 4.10 Certificate status services

ISO and its Managed PKI Service Provider do not provide a certificate status service. However, a CA must ensure that it issues an up-to-date CRL at least every twenty-four hours.

#### 4.10.1. Operational characteristics

No stipulation

#### 4.10.2. Service availability

No stipulation

#### 4.10.3. Optional features

No stipulation

### 4.11 End of subscription

A subscriber or the entity that sponsors the subscriber may inform the CA that the subscriber wishes to end its subscription. In this case, the CA should take the same actions that it would for revoking the subscriber's certificate.

### 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

## 5.1 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

### 5.2 Physical controls

#### 5.2.1. Site location and construction

**Rudimentary (Test) Assurance**

The CA site must:

- Satisfy at least the requirements for a Operations Zone; and
- Be manually or electronically monitored for unauthorized intrusion.

If RA workstations are employed, each RA workstation must be located in an area that satisfies the controls required for a Reception Zone.

Where a PIN or password is recorded, it must be stored in a locked filing cabinet or container accessible only to designated personnel.

**Basic, Medium, and High Assurance**
The CA site must:

- Satisfy at least the requirements for a Security Zone;
- Be manually or electronically monitored for unauthorized intrusion at all times;
- Ensure unescorted access to the CA server is limited to those personnel identified on an access list;
- Ensure personnel not on the access list are properly escorted and supervised;
- Ensure a site access log is maintained and inspected periodically; and
- Ensure all removable media and paper containing sensitive plaintext information are stored in containers either listed in, or of equivalent strength to those listed in, the Security Equipment Guide.

All RA sites must be located in areas that satisfy the controls required for a Reception Zone.

If an RA workstation is used for on-line Entity management with the CA, the workstation must be located in either:

- An Operations Zone; or
- A Reception Zone while attended with all media security protected when unattended.

The CA will ensure the operation of the RA site provides appropriate security protection of the RA Administrator's private key. For example, the RA Administrator's private key could be stored in a secure container or safe.

### 5.2.2. Physical access

**Rudimentary (Test) Assurance**
No stipulation

**Basic Assurance**
Where a PIN or password is recorded, it must be stored in a security container accessible only to authorized personnel.

Subscribers must not leave their workstations unattended when the cryptography is in an unlocked state (i.e., when the PIN or password has been entered). A workstation that contains private keys on a hard drive must be physically secured or protected with an appropriate access control product.

**Medium and High Assurance**
Where a PIN or password is recorded, it must be stored in a security container accessible only to designated personnel.

Subscribers must not leave their workstations unattended when the cryptography is in an unlocked state (i.e., when the PIN or password has been entered). A workstation that contains private keys on a hard drive must be physically secured or protected with an appropriate access control product.

The Subscriber's hardware crypto module must be protected physically. This may be done through site protection or being kept with the Subscriber.

### 5.2.3. Power and air conditioning

**Rudimentary (Test) Assurance**
No stipulation

**Basic, Medium, and High Assurance**
A CA must ensure that the power and air conditioning facilities are sufficient to support the operation of the CA system.

### 5.2.4. Water exposures

**Rudimentary (Test) Assurance**
No stipulation

**Basic, Medium, and High Assurance**
A CA must ensure that the CA system is protected from water exposure.

### 5.2.5. Fire prevention and protection

**Rudimentary (Test) Assurance**
No stipulation

**Basic, Medium, and High Assurance**
A CA must ensure that the CA system is protected with a fire suppression system.

### 5.2.6. Media storage

**Rudimentary (Test) Assurance**
No stipulation

**Basic, Medium, and High Assurance**
A CA must ensure that storage media used by the CA system is protected from environmental threats such as temperature, humidity and magnetism.

### 5.2.7. Waste disposal

**Rudimentary (Test) Assurance**
No stipulation

**Basic, Medium, and High Assurance**
The CA does not store private keys or activation data on a storage medium that is backed up. Other CA files containing sensitive data must be sanitized or destroyed before released for disposal

### 5.2.8. Off-site backup

**Rudimentary (Test) Assurance**
No stipulation

**Basic, Medium, and High Assurance**
A CA must ensure that facilities used for off-site back-up, if any, have the same level of security as the primary CA site.

## 5.3 Procedural controls

### 5.3.1. Trusted roles

#### 5.3.1.1 CA trusted roles

**Rudimentary (Test) Assurance**
A CA may permit all duties for critical CA operations to be performed by one individual.

**Basic, Medium, and High Assurance**
A CA must ensure a separation of duties for critical CA functions to prevent one person from maliciously using the CA system without detection.

A CA should provide for a minimum of two distinct PKI personnel roles, distinguishing between day-to-day operation of the CA system and the management and audit of those operations. One suggested division of responsibilities between the two roles is:

**PKI Master User**
- Configuration and maintenance of the CA system hardware and software;
- Commencement and cessation of CA services.

**PKI Administrator**
- Management of PKI Operators;
- Configuring CA security policies;
- Verification of audit logs;
- Verification of CP and CPS compliance;
- Management of Subscriber initialization process;
- Creation, renewal or revocation of certificates;
- Distribution of tokens (where applicable).

An alternative division of responsibilities is permitted so long as it provides the same degree of resistance to insider attack.

Only those personnel responsible for the duties outlined for PKI Master User and System Administrator should have access to the software that controls the CA operation.

#### 5.3.1.2 RA trusted roles

A CA must ensure that RA personnel understand their responsibility for the identification and authentication of prospective Subscribers and perform the following functions:

- Acceptance of subscription, certificates change and certificate revocation requests;
- Verification of an applicant's identity and authorizations or acceptance of verification made by other CAISO departments;
- Transmission of applicant information to the CA;
- Provision of authorization codes for on-line key exchange and certificate creation.

A CA may permit all duties for RA functions to be performed by one individual.

### 5.3.2. Number of persons required per task

**Rudimentary (Test) Assurance**
No stipulation

**Basic, Medium, and High Assurance**
Multi-user control is also required for CA key generation as outlined in Section 6.2.2. of this policy.

All other duties associated with CA roles may be performed by an individual operating alone. A CA must ensure that any verification process it employs provides for oversight of all activities performed by privileged CA role holders.

### 5.3.3. Identification and authentication for each role

All CA personnel must have their identity and authorization verified before they are:

- Included in the access list for physical access to the CA system;
- Given a certificate for the performance of their CA role;
- Given an account on the PKI system.

Each of these certificates and accounts (with the exception of CA signing certificates) must:

- Be directly attributable to an individual;
- Not be shared;
- Be restricted to actions authorized for that role through the use of CA software, operating system and procedural controls.

CA operations must be secured, using mechanisms such as token-based strong authentication and encryption, when accessed across a shared network.

### 5.3.4. Roles requiring separation of duties

See Section 5.2.2.

## 5.4 Personnel controls

A CA must ensure that all personnel performing duties with respect to the operation of a CA or LRA must:

- Be appointed in writing;
- Be bound by contract or statute to the terms and conditions of the position they are to fill;
- Have received comprehensive training with respect to the duties they are to perform;
- Be bound by statute or contract not to disclose sensitive CA security-relevant information or Subscriber information; and
- Not be assigned duties that may cause a conflict of interest with their CA or RA duties.

### 5.4.1. Qualifications, experience, and clearance requirements

A CA must ensure that all personnel performing duties with respect to the operation of a CA must have the appropriate clearance from ISO or its Managed PKI Service Provider. A CA must ensure that all personnel who operate an RA workstation for the purpose of on-line Entity management with the CA must have obtained the appropriate clearance from ISO which must include a drug check.

### 5.4.2. Background check procedures

All background checks must be performed in accordance with ISO Security Policy or a policy of the Managed PKI Service Provider that is deemed acceptable by ISO.

### 5.4.3. Training requirements

A CA must ensure that all personnel performing duties with respect to the operation of a CA or RA must receive comprehensive training in:

- The CA/LRA security principles and mechanisms;
- All PKI software versions in use on the CA system;
- All PKI duties they are expected to perform; and
- Disaster recovery and business continuity procedures. **This training is only required for personnel performing duties with respect to the operation of the CA.**

### 5.4.4. Retraining frequency and requirements

The requirements of Section 5.3.3. of this policy must be kept current to accommodate changes in the CA system. Refresher training must be conducted as required, and the CA must review these requirements at least once a year.

### 5.4.5. Job rotation frequency and sequence

No stipulation

### 5.4.6. Sanctions for unauthorized actions

In the event of actual or suspected unauthorized action by a person performing duties with respect to the operation of a CA or RA, a CA may suspend his or her access to the CA system in accordance with ISO policies and standards.

### 5.4.7. Independent contractor requirements

The CA must ensure that contractor access to the CA site is in accordance with Section 5.1.1. of this policy.

### 5.3.8. Documentation supplied to personnel

The CA must make available to its CA and RA personnel the certificate policies it supports, its CPS, and any specific statues, policies or contracts relevant to their position.

## 5.5 Audit logging procedures

### 5.5.1. Types of events recorded

**Rudimentary (Test) Assurance**

No stipulation

**Basic, Medium, and High Assurance**

A CA should record in audit log files all events relating to the security of the CA system. These include such events as:

- System start-up and shutdown;
- CA application start-up and shutdown;
- Changes to CA details and/or keys;
- Login and logoff attempts;
- Generation of own and subordinate Entity keys;
- Creation and revocation of certificates;
- Attempts to initialize remove, enable, and disable Subscribers, and update and recover their keys;
- Failed read-and-write operations on the certificate and CRL directory.

All logs, whether electronic or manual, should contain the date and time of the event, and the identity of the entity which caused the event.

Information captured that is not CA-system generated includes:

- Physical access logs;
- System configuration changes and maintenance;
- Personnel changes;
- Discrepancy and compromise reports;
- Records of the destruction of media containing key material, activation data, or personal Subscriber information.

A CA must ensure that the CPS indicates what information is logged.

### 5.5.2. Frequency of audit log processing

**Rudimentary (Test) Assurance**

No stipulation

**Basic, Medium, and High Assurance**

A CA must ensure that CA personnel review its audit log when issues arise and all significant events are explained. In case there are no issues that warrant review of the audit log, the CA personnel must review the audit log at least once a month with at least a random sample of no less than 5% of the logged information.

Actions taken following these reviews must be documented.

### 5.5.3. Retention period for audit log

**Rudimentary (Test) Assurance**

No stipulation

**Basic, Medium, and High Assurance**

A CA must retain its audit logs onsite for at least on year and subsequently retain them in the manner described in Section 5.5 of this policy.

### 5.5.4. Protection of audit log

**Rudimentary (Test) Assurance**

No stipulation

**Basic, Medium, and High Assurance**

The electronic audit log system must include mechanisms to protect the log files from unauthorized viewing, modification, and deletion.

Manual audit information must be protected from unauthorized viewing, modification and destruction.

### 5.5.5. Audit log backup procedures

**Rudimentary (Test) Assurance**
No stipulation

**Basic, Medium, and High Assurance**
Audit logs and audit summaries must be backed up or copied if in manual form.

### 5.5.6. Audit collection system (internal vs. external)

**Rudimentary (Test) Assurance**
No stipulation

**Basic, Medium, and High Assurance**
A CA must identify its audit collection systems in the CPS.

### 5.5.7. Notification to event-causing subject

**Rudimentary (Test) Assurance**
No stipulation

**Basic, Medium, and High Assurance**
Where an event is logged by the audit collection system no notice needs be given to the individual, organization, device or application which caused the event.

### 5.5.8. Vulnerability assessments

No stipulation

## 5.6 Records archival

### 5.6.1. Types of records archived

The following records will be archived:

- Digital Signature certificates stored by the CA.
- CRLs generated by the CA.
- Audit information as detailed in Section 5.4 of this policy.
- Any identification and authentication information.

### 5.6.2. Retention period for archive

Digital Signature certificates stored by the CA, and CRLs generated by the CA, must be retained for at least one year after the expiration of the key material. This requirement does not include the back up of private signature keys.

Audit information as detailed in Section 5.4 of this policy, and any identification and authentication information should be retained for at least four years.

### 5.6.3. Protection of archive

Archive records must be protected against accidental and malicious tampering

### 5.6.4. Archive backup procedures

A second copy of all material retained or backed up must be stored in a location other than the CA site and must be protected either by physical security alone, or a combination of physical and cryptographic protection. Any such secondary site must provide adequate protection from environmental threats such as temperature, humidity and magnetism.

### 5.6.5. Requirements for time-stamping of records

No stipulation

### 5.6.6. Archive collection system (internal or external)

No stipulation

### 5.6.7. Procedures to obtain and verify archive information

**Rudimentary (Test) Assurance**

No stipulation

**Basic, Medium, and High Assurance**

A CA should verify the integrity of the back-ups at least once every six months. Material stored off-site must be periodically verified for data integrity.

## 5.7 Key changeover

The CAISO system does not support key changeover. Upon or prior to expiration of an existing certificate the subscriber must apply for a new certificate in the same manner as the initial certificate.

## 5.8 Compromise and disaster recovery

### 5.8.1. Incident and compromise handling procedures

Incidents are handled according to managed PKI service provider incident handling procedures, which have been reviewed by CAISO.

### 5.8.2. Computing resources, software, and/or data are corrupted

**Rudimentary (Test) Assurance**

No stipulation

**Basic, Medium, and High Assurance**

A CA must establish business continuity procedures that outline the steps to be taken in the event of the corruption or loss of computing resources, software and/or data. Where a repository is not under the control of the CA, a CA must ensure any agreement with the repository provides that business continuity procedures be established and documented by the repository.

### 5.8.3. Entity private key compromise procedures

**Rudimentary (Test) Assurance**

No stipulation

**Basic, Medium, and High Assurance**

In the event of the compromise of a CA's Digital Signature key, prior to re-certification within the CAISO PKI, a CA must:

- Revoke all certificates issued using that key;
- Immediately notify:
  - The PMA;
    - All of its RAs;
    - All Subscribers;
    - All individuals or organizations who are responsible for a certificate used by a device or application.

After addressing the factors that led to key compromise, the CA may:

- Generate a new CA signing key pair;
- Re-issue certificates to all Entities and ensure all CRLs are signed using the new key.

In the event of the compromise, or suspected compromise, of any other Entity's Digital Signature key, the Entity must notify the Issuing CA immediately.

A CA must ensure that its CPS and appropriate agreements contain provisions outlining the means it will use to provide notice of compromise or suspected compromise.

### 5.8.4. Business continuity capabilities after a disaster

**Rudimentary (Test) Assurance**

No stipulation

**Basic, Medium, and High Assurance**

A CA must establish a disaster recovery plan outlining the steps to be taken to re-establish a secure facility in the event of a natural or other type of disaster. Where a repository is not under the control of the CA, a CA must ensure that any agreement with the repository provides that a disaster recovery plan be established and documented by the repository.

## 5.9 CA or RA termination

**Rudimentary (Test) Assurance**

No stipulation

**Basic, Medium, and High Assurance**
In the event that a CA ceases operation, it must notify its Subscribers immediately upon the termination of operations and arrange for the continued retention of the CA's keys and information.

In the event of a change in management of a CA's operations, the CA must notify all Entities for which it has issued certificates.

In the event of a transfer of a CA's operations to another CA operating at a lower level of assurance the certificates issued by the CA whose operations are being transferred must be revoked through a CRL signed by that CA prior to the transfer.

The CA archives should be retained in the manner and for the time indicated in Section 5.5 of this policy.

In the event of RA's termination the CA must revoke the RA's certificate according to the requirements of Section 4.9.

## 6.1 TECHNICAL SECURITY CONTROLS

## 6.2 Key pair generation and installation

### 6.2.1. Key pair generation

**Rudimentary (Test) Assurance**
No stipulation

**Basic, Medium, and High Assurance**
Each Subscriber's key pair must be generated using a PMA-approved algorithm. The following additional requirements apply.

**Basic Assurance**
CA digital signature key pairs must be generated in a hardware cryptographic module rated at **FIPS 140-1 level 2 or higher**. Key pairs for all other Entities may be generated in software or a hardware cryptographic module.

**Medium Assurance**
CA digital signature key pairs must be generated in a hardware cryptographic module rated at **FIPS 140-1 level 2 or higher**. Key pairs for all other entities must be generated in software or hardware cryptographic modules rated at FIPS **140-1 level 1.**

**High Assurance**
Key pairs for all entities must be generated in a hardware cryptographic module with a minimal rating of **FIPS 140-1 level 2 or higher.** Key pairs for all other entities must be

generated in software or hardware cryptographic modules rated at FIPS **FIPS 140-1 level 2 or higher.**

### 6.2.2. Private key delivery to subscriber

**Rudimentary (Test) Assurance**
No stipulation

**Basic, Medium, and High Assurance**
If the prospective certificate holder does not generate the private decryption key it must be delivered to the Entity in a secure manner approved by the PMA.

### 6.2.3. Public key delivery to certificate issuer

**Rudimentary (Test) Assurance**
No stipulation

**Basic, Medium, and High Assurance**
If the CA does not generate the public encryption key it must be delivered to the CA in a secure manner approved by the Policy Management Authority (PMA).

### 6.2.4. CA public key delivery to relying parties

**Rudimentary (Test) Assurance**
No stipulation

**Basic, Medium, and High Assurance**
The CA public verification key must be delivered to the prospective relying parties in a manner approved by the PMA.

### 6.2.5. Key sizes

**Basic, Medium, and High Assurance**
A CA must use a DSA or RSA 2048 bit key or longer. An RA must use a DSA or RSA 1024 bit key or longer. End users must use an RSA 1024 key or longer.

### 6.2.6. Public key parameters generation and quality checking

A CA that utilizes DSA must generate parameters in accordance with FIPS 186.

### 6.2.7. Key usage purposes (as per X.509 v3 key usage field)

**Rudimentary (Test) Assurance**
No stipulation

**Basic, Medium, and High Assurance**
The key usage purpose will be for Digital Signature (for purposes other than non-repudiation) and Key Encipherment and Key Agreement. Extended Key Usage may include Client Authentication, Server Authentication, Encrypted File System and Email Protection.

## 6.3 Private Key Protection and Cryptographic Module Engineering Controls

**Rudimentary (Test) Assurance**

A CA must ensure that its certificate signing private key is used only to sign certificates and CRLs. A CA may issue certificates to Subscribers, CA and RA personnel, devices and applications.

A CA must ensure that private keys issued to its personnel to access and operate CA applications are used only for such purposes. If required, its personnel would be issued sets of Subscriber keys and certificates to be used for purposes other than CA use.

There is no stipulation for protection of RA private keys

**Basic, Medium, and High Assurance**

A CA must ensure that its certificate signing private key is used only to sign certificates and CRLs. A CA may issue certificates to Subscribers, CA and RA personnel, devices and applications.

A CA must ensure that private keys issued to its personnel to access and operate CA applications are used only for such purposes. If required, its personnel would be issued sets of Subscriber keys and certificates to be used for purposes other than CA use.

A CA must ensure that the private keys that it holds or stores, and activation data are protected in accordance with this policy.

Each person performing RA duties on-line through a remote administration application with the CA must ensure that his or her private keys are protected in accordance with this policy. Private keys used by an RA administrator to access and operate RA Applications on-line with the CA must not be used for any other purpose.

All other Entities must ensure that their private keys and activation data are protected in accordance with this policy.

### 6.3.1. Cryptographic module standards and controls

**Rudimentary (Test) Assurance**

All CA Digital Signature key generation, CA Digital Signature key storage and certificate signing operations must be performed in a hardware cryptographic module rated to at least FIPS 140-1 Level 2 or otherwise verified to an equivalent level of functionality and assurance.

The RA Administrator Digital Signature key generation and signing operations must be performed in a hardware cryptographic module rated to at least FIPS 140-1 Level 2 or otherwise verified to an equivalent level of functionality and assurance.

End Entities are not required to use a hardware cryptographic module.

**Basic Assurance**

All CA Digital Signature key generation, CA Digital Signature key storage and certificate signing operations must be performed in a hardware cryptographic module rated to at least FIPS 140-1 Level 2 or otherwise verified to an equivalent level of functionality and assurance.

The RA Administrator Digital Signature key generation and signing operations must be performed in a hardware cryptographic module rated to at least FIPS 140-1 Level 2 or otherwise verified to an equivalent level of functionality and assurance.

End Entities are not required to use a hardware cryptographic module.

**Medium Assurance**

All CA Digital Signature key generation, CA Digital Signature key storage and certificate signing operations must be performed in a hardware cryptographic module rated to at least FIPS 140-1 Level 2 or otherwise verified to an equivalent level of functionality and assurance.

The RA Administrator Digital Signature key generation and signing operations must be performed in a hardware cryptographic module rated to at least FIPS 140-1 Level 2 or otherwise verified to an equivalent level of functionality and assurance.

End Entities must use a cryptographic module validated to at least FIPS 140-1 Level 1 or otherwise verified to an equivalent level of functionality and assurance.

**High Assurance**

All CA Digital Signature key generation, CA Digital Signature key storage and certificate signing operations must be performed in a hardware cryptographic module rated to at least FIPS 140-1 Level 2 or otherwise verified to an equivalent level of functionality and assurance.

The RA Administrator Digital Signature key generation and signing operations must be performed in a hardware cryptographic module rated to at least FIPS 140-1 Level 2 or otherwise verified to an equivalent level of functionality and assurance.

End Entities must use a hardware cryptographic module validated to at least FIPS 140-1 Level 2 or otherwise verified to an equivalent level of functionality and assurance.

### 6.3.2. Private key (n out of m) multi-person control

There must be multiple person control for root CA private key. Two or more employees of CAISO or its Managed PKI Service Provider are required for sub CA key generation and certification.

### 6.3.3. Private key escrow

Not applicable

### 6.3.4. Private key backup

**Rudimentary (Test) Assurance**
No stipulation

**Basic and Medium Assurance**
An Entity may optionally back-up its own private key. If so, the keys must be copied and stored in encrypted form and protected at a level no lower than stipulated for the primary version of the key.

**High Assurance**
A Subscriber cannot back-up its own private key. In the event the subscriber requires a back-up function, the CA may issue another certificate to the subscriber, which will be distinguished from the primary certificate by using a DN qualifier. A CA will back up its private keys.

### 6.3.5. Private key archival

The CAISO system does not archive private keys.

### 6.3.6. Private key transfer into or from a cryptographic module

**Rudimentary (Test) Assurance**
No stipulation.

**Basic Assurance**
Not applicable.

**Medium and High Assurance**
The private key is generated on the cryptographic module itself.

### 6.3.7. Private key storage on cryptographic module

**Rudimentary (Test) Assurance**
No stipulation.

**Basic Assurance**
Not applicable.

**Medium and High Assurance**

The private key is stored on the cryptographic module.

### 6.3.8. Method of activating private key

**Rudimentary (Test) Assurance**

No stipulation.

**Basic, Medium, and High Assurance**

The Entity must be authenticated to the hardware or software cryptographic module before the activation of the private key. This authentication may be in the form of a password. When deactivated, private keys must be kept in encrypted form only.

### 6.3.9. Method of deactivating private key

No stipulation.

### 6.3.10. Method of destroying private key

**Rudimentary (Test) Assurance**

No stipulation.

**Basic, Medium, and High Assurance**

Upon termination of use of a private key, all copies of the private key in computer memory and shared disk space must be destroyed. The method of over-writing must be approved by the PMA. Private key destruction procedures must be described in the CPS or other publicly available document.

### 6.3.11. Cryptographic Module Rating

See Section 6.2.1.

## 6.4 Other aspects of key pair management

### 6.4.1. Public key archival

**Rudimentary (Test) Assurance**

No stipulation.

**Basic, Medium, and High Assurance**

The Issuing CA must retain all public keys.

### 6.4.2. Certificate operational periods and key pair usage periods

The usage period for End-entities is no more than fifteen (15) months. For Root CA's the usage period is no more than twenty years. For Issuing/Operational CAs the usage period is no more than ten years. For RA's the usage period is no more than one year.

## 6.5 Activation data

### 6.5.1. Activation data generation and installation

**Rudimentary (Test) Assurance**
No stipulation.

**Basic, Medium, and High Assurance**
Any activation data must be unique and unpredictable. The activation data, in conjunction with any other access control, must have an appropriate level of strength for the keys or data to be protected.

### 6.5.2. Activation data protection

**Rudimentary (Test) Assurance**
No stipulation.

**Basic, Medium, and High Assurance**
Data used for Entity initialization must be protected from unauthorized use by a combination of cryptographic and physical access control mechanisms.

The private keys of Entities must be protected from unauthorized use by a combination of cryptographic and physical access control mechanisms.

### 6.5.3. Other aspects of activation data

No stipulation

## 6.6 Computer security controls

### 6.6.1. Specific computer security technical requirements

**Rudimentary (Test) Assurance**
No stipulation.

**Basic, Medium, and High Assurance**
Each CA server must include the following functionality:

- Access control to CA services and PKI roles;
- Enforced separation of duties for PKI roles;
- Identification and authentication of PKI roles and associated identities;
- Object re-use or separation for CA random access memory;
- Use of cryptography for session communication;
- Archival of CA and End-Entity history and audit data;
- Audit of security related events;
- Trusted path for identification of PKI roles and associated identities;
- Recovery mechanisms for keys and the CA system.

This functionality may be provided by the operating system, or through a combination of operating system, PKI CA software, and physical safeguards.

### 6.6.2. Computer security rating

No stipulation.

## 6.7 Life cycle technical controls

### 6.7.1. System development controls

The CA must use software that has been designed and developed by a formal methodology and supported by and Configuration Management tools.

### 6.7.2. Security management controls

The configuration of the CA system as well as any modifications and upgrades must be documented and controlled. There must be a method of detecting unauthorized modification to the CA software or configuration.

The CA must ensure that it has a configuration management process in place to support the evolution of the CA system.

Notice must be given to PMA about significant changes.

### 6.7.3. Life cycle security controls

No stipulation.

## 6.8 Network security controls

The CA server must be protected from attack through any open or general-purpose network with which it is connected. Such protection must be provided through the installation of a device configured to allow only the protocols and commands required for the operation of the CA.

A CA must ensure that its CPS defines those protocols and commands required for the operation of the CA.

## 6.9 Time-stamping

No stipulation.

# 7.1 CERTIFICATE, CRL, AND OCSP PROFILES

## 7.2 Certificate profile

All ISO certificates will follow the X.509 Version 3 standard.

### 7.2.1. Version number(s)

The CA must issue X.509 Version 3 certificates, in accordance with the PKIX Certificate

The PKI End-Entity software must support all the basic (non-extension) X.509 fields including:

`Version`: version of X.509 certificate, version 3

| | |
|---|---|
| Serial Number: | unique serial number for certificate |
| SignatureAlgorithm: | algorithm ID for signing the certificate |
| Issuer: | name of the issuing CA |
| Validity: | start and expiration dates for certificate |
| Subject: | subscriber's distinguished name |
| Subject Public Key: | subscriber's public key |
| Signature: | CA signature to authenticate certificate |

Other certificate extensions are defined in Section 7.1.2. of this policy.

### 7.2.2. Certificate extensions

All certificates may contain one or more of the following extensions:

| | |
|---|---|
| SubjectKeyIdentifier: | a unique identifier for the subject's public key |
| AuthorityKeyIdentifier: | a unique identifier for the issuer's public key |
| CertificatePolcies: | the policy identifier according to which the CA issues the certificate along with a policy qualifier, which may include a URL to the CA's CPS. |
| SubjectAlternativeName: | subscriber's alternative name |
| KeyUsage: | allowed usages of private key |
| ExtendedKeyUsage: | additional application-specific usages for the private key |
| BasicConstraints: | an indication of whether the certificate owner is a CA or and End Entity |
| CRLDP: | CRL Distribution Points |
| AIA (Authority Information Access): | location of the issuing CA's certificate |

### 7.2.3. Algorithm object identifiers

**Rudimentary (Test) Assurance**

End entities must support the RSA algorithm with key sizes of 2048 bits, or greater. The digest algorithm must be SHA-2.

CAs must use, and end entities must support for signing and verification, the following algorithms:

- RSA with 2048 bit keys
- The digest algorithm must be SHA-2 or greater.

**Basic, Medium, and High Assurance**

End entities must support the RSA algorithm with key sizes of 2048, or greater, bits. The digest algorithm must be must be SHA-2 or greater.

CA must use, and end entities must support for signing and verification, the following algorithms:

- RSA with 2048 bit keys
- The digest algorithm must be SHA-2 or greater.

#### 7.2.4. Name forms

Every DN must be in the form of an X.500 printableString.

#### 7.2.5. Name constraints

Subject and issuer DNs must comply with the X.500 standard.

#### 7.2.6. Certificate policy object identifier

A CA must ensure that the Policy OID is contained within the certificates it issues.

#### 7.2.7. Usage of Policy Constraints extension

No stipulation.

#### 7.2.8. Policy qualifiers syntax and semantics

No stipulation.

#### 7.2.9. Processing semantics for the critical Certificate Policies extension

No stipulation.

### 7.3 CRL profile

#### 7.3.1. Version number(s)

**Rudimentary (Test) Assurance**
No stipulation.

**Basic, Medium, and High Assurance**
CRLs for these policies are based on the X.509 Version 2 standard.

#### 7.3.2. CRL and CRL entry extensions

**Rudimentary (Test) Assurance**
No stipulation.

**Basic, Medium, and High Assurance**
The CA must issue its CRLs in accordance with X.509 Version 2 CRLs.

### 7.4 OCSP profile

CAISO and its Managed PKI Service Provider do not support OCSP.

#### 7.4.1. Version number(s)

ISO and its Managed PKI Service Provider do not support OCSP.

### 7.4.2. OCSP extensions

ISO and its Managed PKI Service Provider do not support OCSP.

## 8.1 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

A compliance inspection determines whether a CA is operating in an environment that meets the standards established in its CPS and satisfies the requirements of the this CP.

### 8.2 Frequency or circumstances of assessment

**Rudimentary (Test) Assurance**

No stipulation

**Basic, Medium, and High Assurance**

A CA issuing certificates pursuant to this CP must establish that the environment in which it is operating complies with the requirements of this policy. This must occur:

- prior to initial issuance of operational certificates; and
- at a minimum, every two years thereafter.

The CA must certify annually to the PMA that its operating environment at all times during the period in question complied with the requirements of this policy. The CA must also provide to the PMA reasons for which the CA has not complied with this CP and its CPS and state any periods of non-compliance.

### 8.3 Identity/qualifications of assessor

Any person or entity, external to CAISO, seeking to perform a compliance inspection must possess significant experience with PKI and cryptographic technologies as well as the operation of relevant PKI software.

### 8.4 Assessor's relationship to assessed entity

Where an inspector is within ISO, the inspector must be independent of the CA.

Where an inspector is external to ISO, the inspector must be independent of the CA and must comply with the provisions of the Non-Disclosure Agreement and Confidentiality requirements of ISO or its Managed Service Provider. No person may be appointed an inspector or perform as an inspector who is, whose partner is, or a member of whose firm is:

(i) A member of the relevant Officer , Director or CA personnel's family;
(ii) A member of the family of another Officer or Director of ISO; or
(iii) Employed by, or a member of the immediate family of, a person referred to above where such family members are employed in a senior position of authority in an inspecting organization.

## 8.5 Topics covered by assessment

The compliance inspection must follow the inspection guidelines instituted by PMA. This will include whether:

- The CPS outlines, in sufficient detail, the technical, procedural and personnel policies and practices of the CA, which meet the requirements of all the certificate policies supported by the CA;
- The CA operates in an environment that implements and complies with those technical, procedural and personnel practices and policies; and
- An RA, if used, implements and complies with those technical, procedural and personnel practices and policies set out by the CA
- An LRA, if used, implements and complies with those technical, procedural and personnel practices and policies set out by the CA.

## 8.6 Actions taken as a result of deficiency

The inspection results must be submitted to the accreditation authority and the Policy Management Authority (PMA). If irregularities are found, the CA must submit a report to the PMA as to any action the CA will take in response to the inspection report. Where a CA fails to take appropriate action in response to the inspection report, the PMA may:

- Indicate the irregularities, but allow the CA to continue operations until the next programmed inspection; or
- Allow the CA to continue operations for a maximum of thirty days pending correction of any problems prior to revocation; or
- Revoke the CA's certificate.

Any decision regarding which of these actions to take will be based on the severity of the irregularities.

## 8.7 Communication of results

**Rudimentary (Test) Assurance**

No stipulation

**Basic, Medium, and High Assurance**

These results will not be made public unless required by law. In cases of revocation of the CA certificate, the Issuing CA will also ensure that notice of revocation of a certificate will be posted to the CRL within the time limits stated in Section 4.9.7. of this policy.

# 9.1 OTHER BUSINESS AND LEGAL MATTERS

## 9.2 Fees

No stipulation.

### 9.2.1. Certificate issuance or renewal fees

No stipulation.

### 9.2.2. Certificate access fees
No stipulation.

### 9.2.3. Revocation or status information access fees
No stipulation.

### 9.2.4. Fees for other services
No stipulation.

### 9.2.5. Refund policy
No stipulation.

## 9.3 Financial responsibility
Not applicable

### 9.3.1. Insurance coverage
Not applicable

### 9.3.2. Other assets
Not applicable

### 9.3.3. Insurance or warranty coverage for end-entities
Not applicable

## 9.4 Confidentiality of business information

### 9.4.1. Scope of confidential information
Certificates and CRLs, and personal or corporate information appearing on them and in public directories, are not considered sensitive. All other personal or corporate information held by a CA or an RA (e.g., registration and revocation information, logged events, correspondence between the Subscriber and the CA or RA, etc.) is considered sensitive and must not be disclosed without the prior consent of the Subscriber, unless required by applicable law or regulation.

Inspection information is considered sensitive and must not be disclosed to anyone for any purpose other than inspection purposes or where required by law.
Information pertaining to the CA's management of a Subscriber's certificate may only be disclosed to the Subscriber, the Sponsor or where required by law.

### 9.4.2. Information not within the scope of confidential information

Certificates and CRLs, and personal or corporate information appearing on them and in public directories, are not considered sensitive.

### 9.4.3. Responsibility to protect confidential information

Any requests for the disclosure of information must be signed and delivered to the CA.

Any disclosure of information is subject to the requirements of the Federal and State of California legislation and any applicable ISO policy.

## 9.5 Privacy of personal information

See section 9.3.1.

### 9.5.1. Privacy plan

No stipulation.

### 9.5.2. Information treated as private

See section 9.3.1.

### 9.5.3. Information not deemed private

See section 9.3.2.

### 9.5.4. Responsibility to protect private information

See section 9.3.3.

### 9.5.5. Notice and consent to use private information

No stipulation.

### 9.5.6. Disclosure pursuant to judicial or administrative process

No stipulation.

### 9.5.7. Other information disclosure circumstances

No stipulation.

## 9.6 Intellectual property rights

No stipulation.

## 9.7 Representations and warranties

### 9.7.1. CA representations and warranties

**All policies**

An Issuing CA will ensure that its certification and repository services, issuance and revocation of certificates and issuance of CRLs are in accordance this CP. It will also take reasonable efforts to ensure that all RAs and Subscribers will follow the

requirements of this policy when dealing with any certificates containing this policy's OID or the associated keys.

**Basic, Medium, and High Assurance**
CAs will ensure that their authentication and validation procedures are implemented as set forth in Section 3.0

### 9.7.2. RA representations and warranties

RAs will ensure that their authentication and validation procedures are implemented as set forth in Section 3.0

### 9.7.3. Subscriber representations and warranties

A Subscriber must agree to abide by an acceptable use policy which outlines the terms and conditions of use, including permitted applications and purposes as required by the CA. Any information required to be submitted to a CA or RA in connection with a certificate must be complete and accurate. **By utilizing the delivered certificate, the Subscriber is agreeing that they have read, understood, and will abide by the terms and conditions as defined in the CPS.**
Any information required to be submitted to a CA or RA in connection with a certificate must be complete and accurate.

The Subscriber will use the keys and certificates only for the purposes identified in this Certificate Policy and the Certification Practice Statement of the issuing CA. Only the organization, user, application or device identified in the Subscriber's certificate DN is entitled to utilize the certificate for identity authentication and for establishing a session key for secure communication as described in the Certification Practice Statement.

The following additional requirements apply:

## Protection of private keys

**Rudimentary (Test) Assurance**
No stipulation

**Basic, Medium, and High Assurance**

Subscribers are required to protect their private keys and key tokens (if applicable) in accordance with Sections 6.2 of this policy, and to take all reasonable measures to prevent their loss, disclosure, modification, or unauthorized use.

**Notification upon key compromise**
**Rudimentary (Test) Assurance**
No stipulation

**Basic, Medium, and High Assurance**

Where a Subscriber suspects private key compromise, he or she must immediately notify the Issuing CA in a manner specified by that CA.

Where any other entity suspects private key compromise, they should immediately notify the Issuing CA.

### 9.7.4. Relying party representations and warranties

The rights and obligations of a Relying Party who is a member of the ISO PKI are covered in this policy. See sections 4.5.2. and 4.9.6.

### 9.7.5. Representations and warranties of other participants

No stipulation.

## 9.8 Disclaimers of warranties

The Subscriber identified within the certificate is liable for all transactions occurring with their respective certificate(s). ISO assumes no liability whatsoever in relation to the use of ISO PKI certificates or associated public/private key pairs for any use other than in accordance with this CP.

ISO, its governors, officers, directors, employees or agents makes no representations, warranties or conditions, express or implied other than as expressly stated in this CP or in any other document.

No joint venture, partnership, trust, agency or fiduciary relationship is established or deemed to be established between ISO, its partners, market participants or others using the ISO PKI.

## 9.9 Limitations of liability

ISO disclaims any liability of any kind whatsoever for any award, damages or other claim or obligation of any kind arising from tort, contract or any other reason with respect to any service associated with the issuance, use of, or reliance upon, an ISO PKI certificate or its associated public/private key pair.

The disclaimers and limitations of liability in this section and Section 9.7 of this policy are subject to any signed contract agreement that may be entered into by the ISO that provides otherwise. Any such disclaimers or limitations of liability must be consistent with this Certificate Policy.

## 9.10 Indemnities

Subscribers will indemnify ISO and hold ISO harmless from any liability with respect to any service associated with the issuance, use of, or reliance upon, a ISO PKI certificate or its associated public/private key pair.

## 9.11 Term and termination

### 9.11.1. Term

This CP shall remain in effect unless otherwise terminated by ISO.

### 9.11.2. Termination

ISO shall have the exclusive right to terminate this CP.

### 9.11.3. Effect of termination and survival

All provisions of this CP essential to the resolution of any claim arising under this CP shall survive termination of this CP for as long as necessary to resolve such dispute.

## 9.12 Individual notices and communications with participants

All items in this Certificate Policy are subject to the notification requirement.
A CA must ensure that any agreements by that CA will be governed by the laws of California and the California ISO Tariff and state and federal law concerning the enforceability, construction, interpretation and validity of this Certificate Policy.

## 9.13 Amendments

### 9.13.1. Procedure for amendment

Prior to making significant changes to this Certificate Policy, the Policy Management Authority (PMA) will notify the subscribers.

### 9.13.2. Notification mechanism and period

The PMA will notify all CAs of any proposed major changes to this Certificate Policy. The notification must contain a statement of proposed changes, the final date for receipt of comments, and the proposed effective date of change. The PMA may request CAs to notify their Subscribers of the proposed changes. The PMA will also post a notice of the proposal on the ISO World Wide Web site for major revisions.

The comment period will be 30 days unless otherwise specified. The comment period will be defined in the notification.

Written and signed comments on proposed changes must be directed to the PMA.
Decisions with respect to the proposed changes are at the sole discretion of the PMA.

The PMA will determine the period for final change notice.

### 9.13.3. Circumstances under which OID must be changed

If a policy change is determined by the PMA to warrant the issuance of a new policy, the PMA may assign a new Object Identifier (OID) for the modified policy.

## 9.14 Dispute resolution provisions

Any dispute related to key and certificate management between the ISO and an organization or individual outside of ISO will be resolved using the appropriate dispute settlement mechanism established by the California ISO Tariff.

A dispute related to key and certificate management between departments should be resolved by negotiation if possible. A dispute not settled by negotiation should be resolved by the Policy Management Authority (PMA) or, where appropriate, through a mediator or arbitrator(s) appointed by the PMA.

A dispute related to key and certificate management within a department is to be resolved by the appropriate departmental authority in conjunction with the Issuing CA.

## 9.15 Governing law

A CA must ensure that any agreements by that CA will be governed by the laws of California and the California ISO Tariff and state and federal law concerning the enforceability, construction, interpretation and validity of this Certificate Policy.

## 9.16 Compliance with applicable law

See Section 9.14

## 9.17 Miscellaneous provisions

### 9.17.1. Entire agreement

This CP and any other provision incorporated into this CP by reference shall constitute the entire understanding with regard to the matters addressed herein.

### 9.17.2. Assignment

The ISO Tariff provisions regarding assignment shall apply to this CP.

### 9.17.3. Severability

A CA must ensure that any agreements by that CA will be governed by the laws of California and the California ISO Tariff and state and federal law concerning the enforceability, construction, interpretation and validity of this Certificate Policy.

### 9.17.4. Enforcement (attorneys' fees and waiver of rights)

The ISO Tariff provisions regarding dispute resolution shall apply to any dispute arising under this CP, including the question of whether attorneys' fees are available.

### 9.17.5. Force Majeure

The ISO Tariff provisions regarding *force majeure* shall apply to this CP.

## 9.18 Other provisions

The ISO Tariff as it may be amended from time to time is hereby incorporated by reference to the extent referenced in this CP and shall govern with regard to interpretation of this CP.