



California Independent System Operator  
Certification Practice Statement  
for  
Windows Certification Authority

---

Version 1.0

July 2015

## Table of Contents

<b>1.0 INTRODUCTION.....</b>	<b>8</b>
1.1 OVERVIEW .....	8
1.2 DOCUMENT NAME AND IDENTIFICATION.....	9
1.3 PKI PARTICIPANTS .....	9
1.3.1 Certification Authorities (CAs).....	9
1.3.2 Registration authorities.....	10
1.3.3 End Entities .....	10
1.3.4 Relying parties.....	10
1.3.5 Other participants.....	10
1.4 CERTIFICATE USAGE.....	10
1.4.1 Appropriate certificate uses.....	10
1.5 POLICY ADMINISTRATION.....	10
1.5.1 Organization administering the document .....	10
1.5.2 Contact person.....	11
1.5.3 Person determining CPS suitability for the policy .....	11
1.5.4 CPS approval procedures.....	11
1.6 DEFINITIONS AND ACRONYMS .....	11
1.6.1 General definitions .....	11
1.6.2 Acronyms .....	14
<b>2.0 PUBLICATION AND REPOSITORY RESPONSIBILITIES.....</b>	<b>14</b>
2.1 REPOSITORIES .....	14
2.2 PUBLICATION OF CERTIFICATION INFORMATION .....	15
2.3 TIME AND FREQUENCY OF PUBLICATION .....	15
2.4 ACCESS CONTROLS ON REPOSITORIES .....	15
<b>3.0 IDENTIFICATION AND AUTHENTICATION .....</b>	<b>15</b>
3.1 NAMING .....	15
3.1.1 Types of names.....	15
3.1.2 Need for names to be meaningful .....	15
3.1.3 Anonymity or pseudonymity of subscribers .....	15
3.1.4 Rules for interpreting various name forms .....	16
3.1.5 Uniqueness of names .....	16
3.1.6 Recognition, authentication, and role of trademarks .....	16
3.2 INITIAL IDENTITY VALIDATION.....	16
3.2.1 Method to prove possession of private key.....	16
3.2.2 Authentication of organization identity.....	16
3.2.3 Authentication of individual attributes.....	16
3.2.4 Non-verified attribute information.....	16
3.2.5 Validation of authority.....	16
3.2.6 Criteria for interoperation.....	16
3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS.....	17
3.3.1 Identification and authentication for routine re-key.....	17
3.3.2 Identification and authentication for re-key after revocation.....	17
3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST.....	17
<b>4.0 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS.....</b>	<b>17</b>
4.1 CERTIFICATE APPLICATION .....	17
4.1.1 Who can submit a certificate application .....	17
4.1.2 Enrollment process and responsibilities.....	17
4.2 CERTIFICATE APPLICATION PROCESSING.....	17
4.2.1 Performing identification and authentication functions.....	17

4.2.2.	<i>Approval or rejection of certificate applications</i> .....	17
4.2.3.	<i>Time to process certificate applications</i> .....	17
4.3	CERTIFICATE ISSUANCE.....	18
4.3.1.	<i>CA actions during certificate issuance</i> .....	18
4.3.2.	<i>Notification by the CA of issuance of certificate</i> .....	18
4.4	CERTIFICATE ACCEPTANCE.....	18
4.4.1.	<i>Conduct constituting certificate acceptance</i> .....	18
4.4.2.	<i>Publication of the certificate by the CA</i> .....	18
4.4.3.	<i>Notification of certificate issuance by the CA to other entities</i> .....	18
4.5	KEY PAIR AND CERTIFICATE USAGE.....	18
4.5.1.	<i>Private key and certificate usage</i> .....	18
4.5.2.	<i>Relying party public key and certificate usage</i> .....	18
4.6	CERTIFICATE RENEWAL.....	19
4.6.1.	<i>Circumstance for certificate renewal</i> .....	19
4.6.2.	<i>Who may request renewal</i> .....	19
4.6.3.	<i>Processing certificate renewal requests</i> .....	19
4.6.4.	<i>Notification of new certificate issuance to subscriber</i> .....	19
4.6.5.	<i>Conduct constituting acceptance of a renewal certificate</i> .....	19
4.6.6.	<i>Publication of the renewal certificate by the CA</i> .....	19
4.6.7.	<i>Notification of certificate issuance by the CA to other entities</i> .....	19
4.7	CERTIFICATE RE-KEY.....	19
4.7.1.	<i>Circumstance for certificate re-key</i> .....	19
4.7.2.	<i>Who may request certification of a new public key</i> .....	19
4.7.3.	<i>Processing certificate re-keying requests</i> .....	19
4.7.4.	<i>Notification of new certificate issuance</i> .....	19
4.7.5.	<i>Conduct constituting acceptance of a re-keyed certificate</i> .....	19
4.7.6.	<i>Publication of the re-keyed certificate by the CA</i> .....	20
4.7.7.	<i>Notification of certificate issuance by the CA to other entities</i> .....	20
4.8	CERTIFICATE MODIFICATION.....	20
4.8.1.	<i>Circumstance for certificate modification</i> .....	20
4.8.2.	<i>Who may request certificate modification</i> .....	20
4.8.3.	<i>Processing certificate modification requests</i> .....	20
4.8.4.	<i>Notification of new certificate issuance to subscriber</i> .....	20
4.8.5.	<i>Conduct constituting acceptance of modified certificate</i> .....	20
4.8.6.	<i>Publication of the modified certificate by the CA</i> .....	20
4.8.7.	<i>Notification of certificate issuance by the CA to other entities</i> .....	20
4.9	CERTIFICATE REVOCATION AND SUSPENSION.....	20
4.9.1.	<i>Circumstances for revocation</i> .....	20
4.9.2.	<i>Who can request revocation</i> .....	21
4.9.3.	<i>Procedure for revocation request</i> .....	21
4.9.4.	<i>Revocation request grace period</i> .....	21
4.9.5.	<i>Time within which CA must process the revocation request</i> .....	21
4.9.6.	<i>Revocation checking requirement for relying parties</i> .....	21
4.9.7.	<i>CRL issuance frequency</i> .....	21
4.9.8.	<i>Maximum latency for CRLs</i> .....	21
4.9.9.	<i>On-line revocation/status checking availability</i> .....	22
4.9.10.	<i>On-line revocation checking requirements</i> .....	22
4.9.11.	<i>Other forms of revocation advertisements available</i> .....	22
4.9.12.	<i>Special requirements in reference to key compromise</i> .....	22
4.9.13.	<i>Circumstances for suspension</i> .....	22
4.9.14.	<i>Who can request suspension</i> .....	22
4.9.15.	<i>Procedure for suspension request</i> .....	22
4.9.16.	<i>Limits on suspension period</i> .....	22
4.10	CERTIFICATE STATUS SERVICES.....	22
4.10.1.	<i>Operational characteristics</i> .....	22

4.10.2.	<i>Service availability</i> .....	22
4.10.3.	<i>Optional features</i> .....	22
4.11	<b>KEY ESCROW AND RECOVERY</b> .....	22
4.11.1.	<i>Key escrow and recovery policy and practices</i> .....	22
4.11.2.	<i>Session key encapsulation and recovery policy and practices</i> .....	22
<b>5.0</b>	<b>FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS</b> .....	<b>23</b>
5.1	<b>PHYSICAL CONTROLS</b> .....	23
5.1.1.	<i>Site location and construction</i> .....	23
5.1.2.	<i>Physical access</i> .....	23
5.1.3.	<i>Power and air conditioning</i> .....	24
5.1.4.	<i>Water exposures</i> .....	25
5.1.5.	<i>Fire prevention and protection</i> .....	25
5.1.6.	<i>Media storage</i> .....	25
5.1.7.	<i>Waste disposal</i> .....	25
5.1.8.	<i>Off-site backup</i> .....	25
5.2	<b>PROCEDURAL CONTROLS</b> .....	25
5.2.1.	<i>Trusted roles</i> .....	25
5.2.2.	<i>Number of persons required per task</i> .....	26
5.2.3.	<i>Identification and authentication for each role</i> .....	26
5.2.4.	<i>Roles requiring separation of duties</i> .....	27
5.3	<b>PERSONNEL CONTROLS</b> .....	27
5.3.1.	<i>Qualifications, experience, and clearance requirements</i> .....	27
5.3.2.	<i>Background check procedures</i> .....	27
5.3.3.	<i>Training requirements</i> .....	28
5.3.4.	<i>Retraining frequency and requirements</i> .....	28
5.3.5.	<i>Job rotation frequency and sequence</i> .....	28
5.3.6.	<i>Sanctions for unauthorized actions</i> .....	28
5.3.7.	<i>Independent contractor requirements</i> .....	28
5.3.8.	<i>Documentation supplied to personnel</i> .....	28
5.4	<b>AUDIT LOGGING PROCEDURES</b> .....	28
5.4.1.	<i>Types of events recorded</i> .....	28
5.4.2.	<i>Frequency of audit log processing</i> .....	29
5.4.3.	<i>Retention period for audit log</i> .....	29
5.4.4.	<i>Protection of audit log</i> .....	29
5.4.5.	<i>Audit log backup procedures</i> .....	29
5.4.6.	<i>Audit collection system (internal vs. external)</i> .....	29
5.4.7.	<i>Notification to event-causing subject</i> .....	29
5.4.8.	<i>Vulnerability assessments</i> .....	29
5.5	<b>RECORDS ARCHIVAL</b> .....	29
5.5.1.	<i>Types of records archived</i> .....	29
5.5.2.	<i>Retention period for archive</i> .....	30
5.5.3.	<i>Protection of archive</i> .....	30
5.5.4.	<i>Archive backup procedures</i> .....	30
5.5.5.	<i>Requirements for time-stamping of records</i> .....	30
5.5.6.	<i>Archive collection system</i> .....	30
5.5.7.	<i>Procedures to obtain and verify archive information</i> .....	30
5.6	<b>KEY CHANGEOVER</b> .....	30
5.7	<b>COMPROMISE AND DISASTER RECOVERY</b> .....	30
5.7.1.	<i>Incident and compromise handling procedures</i> .....	30
5.7.2.	<i>Computing resources, software, and/or data are corrupted</i> .....	30
5.7.3.	<i>Entity private key compromise procedures</i> .....	31
5.7.4.	<i>Business continuity capabilities after a disaster</i> .....	31
5.8	<b>CA OR RA TERMINATION</b> .....	31

<b>6.0</b>	<b>TECHNICAL SECURITY CONTROLS</b>	<b>31</b>
6.1	KEY PAIR GENERATION AND INSTALLATION	31
6.1.1.	Key pair generation	31
6.1.2.	Private key delivery	31
6.1.3.	Public key	31
6.1.4.	CA public key delivery to relying parties	31
6.1.5.	Key sizes	32
6.1.6.	Public key parameters generation and quality checking	32
6.1.7.	Key usage purposes (as per X.509 v3 key usage field)	32
6.2	PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS	32
6.2.1.	Cryptographic module standards and controls	32
6.2.2.	Private key (n out of m) multi-person control	32
6.2.3.	Private key escrow	32
6.2.4.	Private key backup	32
6.2.5.	Private key archival	33
6.2.6.	Private key transfer into or from a cryptographic module	33
6.2.7.	Private key storage on cryptographic module	33
6.2.8.	Method of activating private key	33
6.2.9.	Method of deactivating private key	33
6.2.10.	Method of destroying private key	33
6.2.11.	Cryptographic Module Rating	33
6.3	OTHER ASPECTS OF KEY PAIR MANAGEMENT	33
6.3.1.	Public key archival	33
6.3.2.	Certificate operational periods and key pair usage periods	33
6.4	ACTIVATION DATA	33
6.4.1.	Activation data generation and installation	33
6.4.2.	Activation data protection	34
6.4.3.	Other aspects of activation data	34
6.5	COMPUTER SECURITY CONTROLS	34
6.5.1.	Specific computer security technical requirements	34
6.5.2.	Computer security rating	34
6.6	LIFE CYCLE TECHNICAL CONTROLS	34
6.6.1.	System development controls	34
6.6.2.	Security management controls	34
6.6.3.	Life cycle security controls	34
6.7	NETWORK SECURITY CONTROLS	34
6.8	TIME-STAMPING	35
<b>7.0</b>	<b>CERTIFICATE, CRL, AND OCSP PROFILES</b>	<b>35</b>
7.1	CERTIFICATE PROFILE	35
7.1.1.	Version number(s)	35
7.1.2.	Certificate extensions	35
7.1.3.	Algorithm object identifiers	36
7.1.4.	Name forms	36
7.1.5.	Name constraints	36
7.1.6.	Certificate policy object identifier	36
7.1.7.	Usage of Policy Constraints extension	36
7.1.8.	Policy qualifiers syntax and semantics	36
7.1.9.	Processing semantics for the critical Certificate Policies extension	36
7.2	CRL PROFILE	36
7.3	OCSP PROFILE	37
7.3.1.	Version number(s)	37
7.3.2.	OCSP extensions	37
<b>8.0</b>	<b>COMPLIANCE AUDIT AND OTHER ASSESSMENTS</b>	<b>37</b>

8.1	FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT.....	37
8.2	IDENTITY/QUALIFICATIONS OF ASSESSOR .....	37
8.3	ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY .....	37
8.4	TOPICS COVERED BY ASSESSMENT .....	38
8.5	ACTIONS TAKEN AS A RESULT OF DEFICIENCY .....	38
8.6	COMMUNICATION OF RESULTS .....	38
<b>9.0</b>	<b>OTHER BUSINESS AND LEGAL MATTERS.....</b>	<b>38</b>
9.1	FEES.....	38
9.1.1.	<i>Certificate issuance or renewal fees.....</i>	39
9.1.2.	<i>Certificate access fees.....</i>	39
9.1.3.	<i>Revocation or status information access fees.....</i>	39
9.1.4.	<i>Fees for other services.....</i>	39
9.1.5.	<i>Refund policy.....</i>	39
9.2	FINANCIAL RESPONSIBILITY.....	39
9.2.1.	<i>Insurance coverage.....</i>	39
9.2.2.	<i>Other assets.....</i>	39
9.2.3.	<i>Insurance or warranty coverage for End-Entities.....</i>	39
9.3	CONFIDENTIALITY OF BUSINESS INFORMATION.....	39
9.3.1.	<i>Scope of confidential information.....</i>	39
9.3.2.	<i>Information not within the scope of confidential information.....</i>	39
9.3.3.	<i>Responsibility to protect confidential information.....</i>	40
9.4	PRIVACY OF PERSONAL INFORMATION.....	40
9.4.1.	<i>Privacy plan.....</i>	40
9.4.2.	<i>Information treated as private.....</i>	40
9.4.3.	<i>Information not deemed private.....</i>	40
9.4.4.	<i>Responsibility to protect private information.....</i>	40
9.4.5.	<i>Notice and consent to use private information.....</i>	40
9.4.6.	<i>Disclosure pursuant to judicial or administrative process.....</i>	40
9.4.7.	<i>Other information disclosure circumstances.....</i>	40
9.5	INTELLECTUAL PROPERTY RIGHTS.....	40
9.6	REPRESENTATIONS AND WARRANTIES.....	40
9.6.1.	<i>CA representations and warranties.....</i>	40
9.6.2.	<i>RA representations and warranties.....</i>	41
9.6.3.	<i>Relying party representations and warranties.....</i>	41
9.6.4.	<i>Representations and warranties of other participants.....</i>	41
9.7	DISCLAIMERS OF WARRANTIES.....	41
9.8	LIMITATIONS OF LIABILITY .....	41
9.9	INDEMNITIES .....	42
9.10	TERM AND TERMINATION .....	42
9.10.1.	<i>Term.....</i>	42
9.10.2.	<i>Termination.....</i>	42
9.10.3.	<i>Effect of termination and survival.....</i>	42
9.11	INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS .....	42
9.12	AMENDMENTS.....	42
9.12.1.	<i>Procedure for amendment.....</i>	42
9.12.2.	<i>Notification mechanism and period.....</i>	43
9.12.3.	<i>Circumstances under which OID must be changed.....</i>	43
9.13	DISPUTE RESOLUTION PROVISIONS .....	43
9.14	GOVERNING LAW.....	43
9.15	COMPLIANCE WITH APPLICABLE LAW .....	43
9.16	MISCELLANEOUS PROVISIONS.....	43
9.16.1.	<i>Entire agreement.....</i>	43
9.16.2.	<i>Assignment.....</i>	43
9.16.3.	<i>Severability.....</i>	44

9.16.4. *Enforcement (attorneys' fees and waiver of rights)*.....44  
9.16.5. *Force Majeure* .....44  
9.17 OTHER PROVISIONS .....44

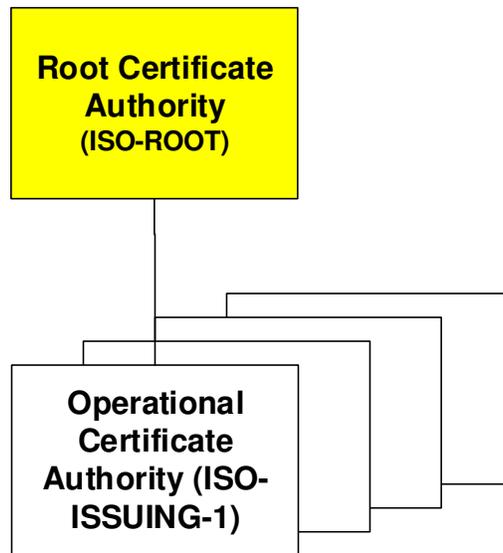
## 1.0 INTRODUCTION

### 1.1 Overview

This document is the Certification Practice Statement (CPS) for the California Independent System Operator (ISO) Windows Certification Authority.

The *Certificate Policies for the California Independent System Operator Windows Enterprise Public Key Infrastructure* (hereafter called *the Windows CP*) defines policy for use in the Windows PKI. These policies are used for issuing certificates for the purposes of Authentication, Message Origin Authentication and Key Agreement. The Windows CA operates according to the Policy defined in the Windows CP document.

The California ISO operates a two-level certification authority hierarchy as depicted in Figure 1. The Root CA is a self-signed certification authority named *ISO-ROOT*. 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 End Entities.



**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 ISO maintains many servers and applications in support of its enterprise applications and systems. These servers exchange information internally through interfaces and communications within the ISO's network. Additionally, the ISO employs system administrators and other staff who administer these server systems and their server applications.

This Certification Practice Statement covers the practices employed in issuing Windows digital certificates for use by these internal systems, California ISO employees, California ISO contractors, and California ISO systems and applications.

The Windows CA will operate in accordance with this CPS, the Windows CP, the laws of the state of California, and other applicable federal regulations. The CA will ensure that all RAs operating on its behalf will comply with the relevant provisions of the Windows CP concerning the operation of RAs. The CA will take all reasonable measures to ensure that California ISO employees and contractors that use the Windows CA are aware of their 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 laws of the state of California and other applicable federal laws concerning the enforceability, construction, interpretation and validity will govern this CPS.

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

The operation of a Certification Authority requires the assignment of certain roles with corresponding responsibilities. This CPS states who has been assigned specific roles and lists their respective responsibilities. The table under Section 5.2.1.1 shows the roles and responsibilities of the entities in the Windows CA.

## **1.2 Document name and identification**

This document is identified by name as *California Independent System Operator Certification Practice Statement for Windows Certification Authority*.

## **1.3 PKI participants**

This section describes the attributes or types of entities that fill the roles of participants of the Windows CA.

### **1.3.1. Certification Authorities (CAs)**

The California ISO is the Certification Authority for the Windows CA operating under this practice statement and is responsible for:

- Creating and signing of certificates binding End Entities with their public encryption keys.
- Publishing certificates and revocation lists to a repository.

- Ensuring adherence to the CP document.

### **1.3.2. Registration authorities**

Authorized ISO employees can act as the Registration Authorities for the Windows CA.

### **1.3.3. End Entities**

The End Entities include internal applications and devices that require certificates for the purpose of authenticating attributes, authenticating message origin or establishing secure sessions with appropriate ISO applications and/or the ISO networks.

End Entities are devices or applications for which certificates are issued provided that responsibility for the certificate and accountability for it is attributable to an individual or a group within the ISO's Information Technology department. The End Entity, identified within the certificate, is a device or application maintained by the ISO.

Windows certificates will only be issued after request or authorization for issuance from one or more Registration Authorities. The California ISO may administer any number of End Entity certificates.

### **1.3.4. Relying parties**

A Relying Party may be an ISO Employee, Contractor, Vendor or group that interacts with the Registration Authority.

### **1.3.5. Other participants**

The Windows CA requires at least one certificate and CRL repository. This repository is in the form of one or more directories that comply with the LDAP Version 3 standard.

## **1.4 Certificate usage**

### **1.4.1. Appropriate certificate uses**

This CPS and the digital certificates created under it pertain only to approved End Entity systems and applications on the ISO network. Any application of the certificates described in this CPS other than described above is prohibited.

## **1.5 Policy administration**

This section includes the name and mailing addresses of the organization and individuals responsible for creating and maintaining this Certification Practice Statement document.

### **1.5.1. Organization administering the document**

The California ISO is responsible for administering this document. The mailing address for the California ISO 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 of 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 Windows CP document is:

Manager, Information Security

California ISO

250 Outcropping Way

Folsom, CA 95630

### **1.5.4. CPS approval procedures**

A CA's accreditation into the Windows PKI is in accordance with procedures specified by the PMA.

## **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 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 issued and 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.

**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 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 device or application.

**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 the Windows PKI, the CA that is named ISO-ROOT.

**Registration Authority (RA)**

An ISO Employee or Contractor that is responsible for the identification and authentication of certificate End Entities before certificate issuance. An RA is delegated certain tasks on behalf of a CA.

**Object Identifier (OID)**

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

**Operational Authority**

Personnel who are responsible for the overall operations for the Windows 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, the California ISO in this case, responsible for setting, implementing, and administering policy decisions regarding CPs and CPSs throughout the Windows 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 an ISO Windows CA to authenticate an attribute or for key agreement to establish a secure session.

**Repository**

A location where CRLs and certificates are stored.

**Secure Hash Algorithm 2 (SHA-2)**

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 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.

**1.6.2. Acronyms**

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

**2.0 PUBLICATION AND REPOSITORY RESPONSIBILITIES****2.1 Repositories**

The California ISO operates all the repositories to which certificates and Certificate Revocation Lists (CRLs) are published. The repository is part of ISO IT infrastructure and is available for a significant proportion of every 24-hour period.

## 2.2 Publication of certification information

The Windows CA:

- Publishes its CPS signed by the PMA that is made available online or via an e-mail request to the point of contact listed in Section 1.5.2.
- Ensures 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
- Provides 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.

The Windows CA will use a central repository for publishing digital certificates and CRLs.

## 2.3 Time and frequency of publication

The Windows CA promptly publishes certificates upon issuance and issues an up-to-date CRL at least every twenty-four hours. When a certificate is revoked the updated CRL is issued within 60 minutes after certificate revocation.

## 2.4 Access controls on repositories

Access controls may be instituted at the discretion of the Windows CA with respect to certificates.

## 3.0 IDENTIFICATION AND AUTHENTICATION

This section describes the procedures used to authenticate the attributes of an End Entity certificate for the Windows CA or RA prior to certificate issuance.

### 3.1 Naming

#### 3.1.1. Types of names

Each Entity will 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.

#### 3.1.2. Need for names to be meaningful

The Windows digital certificates will use the CAISO naming conventions for naming its subjects. The root of the naming tree is: C=US, O=CAISO. The Issuer Common Name is **ISO-ISSUING-1**. The content of Subject names will be associated with the authenticated attributes of the End Entity.

#### 3.1.3. Anonymity or pseudonymity of subscribers

No stipulation.

### **3.1.4. Rules for interpreting various name forms**

No stipulation.

### **3.1.5. Uniqueness of names**

The Windows digital certificates will use the ISO naming conventions for naming its subjects. The root of the naming tree is: C=US, O=CAISO. The Issuer Common Name is **ISO-ISSUING-1**. The content of Subject names will be associated with the authenticated attributes of the End Entity. In cases where multiple certificates are issued to the same End Entity, the certificates will be differentiated using the certificates' serial numbers.

### **3.1.6. 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.

## **3.2 Initial identity validation**

### **3.2.1. Method to prove possession of private key**

A signed certificate request will constitute possession of private key.

### **3.2.2. Authentication of organization identity**

Depending on the Relying Party, an approved internal point of contact or ISO Information Security will validate an organization's identity.

### **3.2.3. Authentication of individual attributes**

The requesting ISO Employee, Contractor, Vendor or group will establish the identity of the individual who is asking for a certificate. The RA keeps a record of identification details.

### **3.2.4. Non-verified attribute information**

The system or application attributes in the digital certificate is not verified. The attributes may be empty, may have an incorrect device name and/or an incorrect domain name.

### **3.2.5. Validation of authority**

The approved internal point of contact, or ISO Information Security, will validate the identity according to the procedures in Sections 3.2.2. and 3.2.3.

### **3.2.6. Criteria for interoperation**

Not applicable.

### **3.3 Identification and authentication for re-key requests**

#### **3.3.1. Identification and authentication for routine re-key**

Not applicable.

#### **3.3.2. Identification and authentication for re-key after revocation**

Not applicable.

### **3.4 Identification and authentication for revocation request**

Not applicable.

## **4.0 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS**

The Windows CA will operate in accordance with the Windows CP when managing the keys provided to RAs and End Entities.

### **4.1 Certificate Application**

#### **4.1.1. Who can submit a certificate application**

Any organization with appropriate business dealings with the California ISO or its employees or contractors can request a certificate.

#### **4.1.2. Enrollment process and responsibilities**

Requests for a certificate may be submitted for the individual who is submitting the application or for a device, system, or software application under the control of that individual.

### **4.2 Certificate application processing**

The application processing will eventually deliver the request to the RA. For example, the Relying Party may forward the request to the Help Desk for the Windows CA. The RA will verify the authenticity of the request and ask the CA to prepare the certificate. The California ISO publishes its CP and this CPS on a web site that is accessible to all ISO Employees and Contractors.

#### **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 the Windows CA to issue a certificate. The issuance and publication of the digital certificate by the Windows CA indicates a complete and final approval of the digital certificate application by the CA.

#### **4.2.3. Time to process certificate applications**

The Windows RA shall process a digital certificate request within **ten** (10) working days of receipt of the request.

## **4.3 Certificate issuance**

### **4.3.1. CA actions during certificate issuance**

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

### **4.3.2. Notification by the CA of issuance of certificate**

Notification of digital certificate issuance is via receipt of the digital certificate.

## **4.4 Certificate acceptance**

### **4.4.1. Conduct constituting certificate acceptance**

Any of the following methods constitutes acceptance of certificate:

1. Use of the certificate.

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

The Windows CA publishes its certificates to its LDAP repository.

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

Notification of digital certificate issuance is by publication to the LDAP repository.

## **4.5 Key pair and certificate usage**

### **4.5.1. Private key and certificate usage**

Utilization of the delivered certificate constitutes an agreement of having read, understood, and abiding by the terms and conditions as defined in the either this CPS.

The digital certificate may be only be used for:

- Authentication: establish the identity of a communicating party,
- Key Encipherment: establish symmetric encryption key for integrity and confidentiality protection.
- Message origin authentication: establish the origin of a message from a communicating party.

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

After the digital certificate is issued, the Relying Party will determine its usage. Relying Parties are obligated to use certificates for the purpose for which they are issued and must use the certificates only in accordance with the certification path validation procedure specified in X.509v3 standards. The digital certificate may be only be used for:

- Authentication: establish the identity of a communicating party,
- Key Encipherment: establish symmetric encryption key for integrity and confidentiality protection.
- Message Origin Authentication: establish the origin of a message from a communicating party.

## **4.6 Certificate renewal**

Expiration of a Windows digital certificate is an expected event. Existing certificates are not renewed. Requests for a new digital certificate follow the procedures outlined in Section 4.3.

### **4.6.1. Circumstance for certificate renewal**

Expiration of a Windows digital certificate is an expected event. The request for a certificate renewal follows the same procedure as requesting a new certificate.

### **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**

The Windows CA does not re-key certificates.

### **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**

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**

The Windows CA does not modify certificates.

**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**

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

**4.9.1. Circumstances for revocation**

A digital certificate must be revoked:

- When any of the information in the digital certificate changes;
- When the system or application is decommissioned;
- When the system of application no longer requires the use of the digital certificate issued;
- 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 Windows CA in its discretion may revoke a digital certificate.

#### **4.9.2. Who can request revocation**

The revocation of a digital certificate may only be requested by:

- An authorized individual within the organization;
- The individual or organization which made the application for the certificate on behalf of a system, device or software application;
- Policy Management Authority;
- The Operational Authority;
- The RAs of the Windows CA.

#### **4.9.3. Procedure for revocation request**

The request to revoke a digital certificate is manually or electronically communicated to an RA of the Windows CA. The RA will authenticate the origin and the validity of the request. The RA will maintain a log of all revocation requests and the resulting action. Any action taken as a result of a revocation request will be initiated within **twenty-four** (24) hours of receipt. The processing of the request may or may not result in the revocation of the digital certificate.

#### **4.9.4. Revocation request grace period**

In the event of the compromise, or suspected compromise, of any Entity's private key, an Entity must notify the Windows CA immediately. When a digital certificate is revoked the revocation will be published immediately in an appropriate CRL. The CRL, or equivalent means, will be the means to provide notice of key compromise or suspected key compromise.

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

Any action taken as a result of a revocation request will be initiated within **twenty-four** (24) hours of receipt.

#### **4.9.6. Revocation checking requirement for relying parties**

Prior to using a certificate, a Relying Party must check the status of all certificates in the certificate validation chain against the appropriate and current CRL. If a CRL is not being used, then a certificate must be validated against an authoritative, trusted directory, OCSP, or some equivalent measure, to ensure a certificate has not been revoked prior to establishing a connection.

#### **4.9.7. CRL issuance frequency**

A new CRL is issued minimally every twenty-four hours and is valid for at least thirty hours. A new CRL is also issued within 60 minutes after a certificate is revoked.

#### **4.9.8. Maximum latency for CRLs**

When a digital certificate is revoked the revocation will be published immediately in an appropriate CRL repository.

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

Not applicable.

**4.9.10. On-line revocation checking requirements**

Not applicable.

**4.9.11. Other forms of revocation advertisements available**

Not applicable.

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

Not applicable.

**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**

Not applicable.

**4.10.1. Operational characteristics**

Not applicable.

**4.10.2. Service availability**

Not applicable.

**4.10.3. Optional features**

Not applicable.

**4.11 Key escrow and recovery****4.11.1. Key escrow and recovery policy and practices**

Not applicable.

**4.11.2. Session key encapsulation and recovery policy and practices**

Not applicable.

## **5.0 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS**

### **5.1 Physical controls**

#### **5.1.1. Site location and construction**

The site location of the Windows CA has been designed and implemented to meet the requirements for a Security Zone as specified in the CP Document and is both manually and electronically monitored for unauthorized intrusion. Cryptographic and operational functions are housed in the CAISO secure data center facilities.

CA equipment is protected from unauthorized access while the cryptographic module is installed and activated. Physical access controls have been established to reduce the risk of equipment tampering when the cryptographic module is not installed and activated. Cryptographic tokens are protected against theft, loss, and unauthorized use at all times.

#### **5.1.2. Physical access**

The RA has implemented policies and procedures to ensure that the physical environment in which the Windows CA systems are installed maintain a high level of security: (i) the system is installed in a secure facility that is isolated from outside networks, with all access controlled; (ii) the entrances and exits from the secure areas are under constant video surveillance and all systems that provide authentication, as well as those that record entry, exit and network activity, are in secured areas; and (iii) the software components are built in an environment designed to minimize security risks. The security techniques employed are designed to resist a large number and combination of different forms of attack. The specific mechanisms include:

- Proximity card readers
- Perimeter alarms
- Closed circuit television
- Mantraps (individual and multi-person)
- Human Guards

Physical access to the systems is controlled; (i) only operative personnel and essential personnel with a valid business reason (e.g., resources to conduct statutory independent audits) are provided such access; (ii) the access control system is always functional and requires unique login credentials; (iii) those admitted physical access are only granted access to business and proprietary information based on their "need to know" and; (iv) facility access is logged and such logs are reviewed by the Security Officer or designee.

To prevent tampering, cryptographic hardware is stored in a secure site, with access limited to authorized personnel, having the following characteristics:

- inventory control processes and procedures to manage the origination, arrival, condition, departure and destination of each device;
- access control processes and procedures to limit physical access to authorized personnel;
- all successful or failed physical access attempts are recorded in an event journal;
- incident processes and procedures to handle abnormal events, security breaches, and investigation and reports;
- audit processes and procedures to verify the effectiveness of the controls;

When storing the cryptographic module containing the CA's private key, the cryptographic module is deactivated upon removal from the CA hardware. If the device is being permanently removed from service, then any key contained within the device that has been used for any cryptographic purpose is erased from the device by initializing the device.

The California ISO provides for physical access controls to ensure that:

- All removable media and paper containing sensitive plain-text information is stored in secure containers.
- An access log is maintained and inspected periodically.
- Activation data is either memorized or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and is not stored with the cryptographic module.

The California ISO uses human guards to continually monitor the perimeter of the facility housing the CA equipment on a 24 hour, 365 day basis. In addition there are guards who monitor the building. The California ISO also uses CCTV and IDS to monitor the Data Center.

### **5.1.3. Power and air conditioning**

The California ISO has backup generators and sufficient UPS capability to lock out input, finish any pending actions, and record the state of the equipment automatically before lack of power or air conditioning causes a shutdown. The directories are provided with uninterrupted power. Additionally, generators will be on line and available to maintain availability of services.

#### **5.1.4. Water exposures**

The California ISO has taken reasonable precautions to minimize the impact of water exposure. CA equipment is installed in computer racks which are not in danger of exposure to water (e.g. on tables or elevated floors). Potential water damage from fire prevention and protection measures (e.g. sprinkler systems) are excluded from this requirement.

#### **5.1.5. Fire prevention and protection**

The California ISO follows best industry standard practices for fire prevention and protection.

#### **5.1.6. Media storage**

Media storage is subject to multiple-layer security storage requirements. These procedures include full back-up of data, offsite storage in two physically separate locations with security similar to that of the facility in which the CA activities are performed. Media is stored so as to protect them from accidental damage (e.g., water, fire, or electromagnetic). Media that contain audit, archive, or backup information is duplicated and stored in locations separate from the CAs.

#### **5.1.7. Waste disposal**

The California ISO provides that sensitive media and documentation, no longer needed for operations, is destroyed in the appropriate disposal process. For example, sensitive paper documentation is shredded, burned, or otherwise rendered unrecoverable.

#### **5.1.8. Off-site backup**

The California ISO makes full system backups once a week with daily incremental back-ups that are sufficient to enable recovery from a system failure. At a minimum, backups are performed and stored offsite daily. A full backup copy is stored at an offsite location which is separate from the CA equipment. The backup is stored at a site with physical and procedural controls commensurate to that of the operational CA. Procedures for CA private key backup are specified in Section 6.2.4 of this CPS.

### **5.2 Procedural controls**

#### **5.2.1. Trusted roles**

##### **5.2.1.1 CA trusted roles**

All employees, contractors and consultants of CAISO who have access to or control over cryptographic operations that may materially affect the Issuing Authority's issuance, use, or revocation of certificates, including access to restricted operations, shall, for the purposes of this CPS, be considered as serving in a trusted position. Such personnel include, but are not limited to, customer service personnel, system administration personnel, designated engineering personnel and executives who are designated to oversee the Issuing Authority's trustworthy system infrastructure.

All activities concerning the ISO-ROOT will be under strict dual custody procedures.

The functions of the Windows CA are not required to be under dual custody. However, the following table summarizes how the Windows CA ensures separation of duties.

Titles & Roles	Responsibilities
Manager, Information Security, Policy Management Authority (PMA)	<ul style="list-style-type: none"> <li>• Sets, implements and administers policy for the PKI</li> </ul>
Systems Engineer, Support Services	<ul style="list-style-type: none"> <li>• Operator of the PKI service (CA, RA)</li> <li>• Initial creation of accounts for PKI officers</li> <li>• Managing PKI Administrators, Local Registration Authority Administrators (account creation, modification and removal)</li> <li>• Super Registration Officer</li> <li>• Requests certificates for registration officers</li> <li>• Verification of Certificate Policy and CPS compliance</li> </ul>
Information Security Analyst, Operational Authority	<ul style="list-style-type: none"> <li>• Sets policy for the operation of the Windows PKI (CP, CPS).</li> <li>• Contact Person for CP or CPS.</li> </ul>
Information Security Analyst, PKI Administrator	<ul style="list-style-type: none"> <li>• Audit of operational logs</li> </ul>

### 5.2.1.2 RA trusted roles

The Windows CA ensures that RA personnel understand their responsibility for the identification and authentication of prospective End Entities and perform the following functions:

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

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

### 5.2.2. Number of persons required per task

The Windows CA requires multi-user control for CA key generation. All other duties associated with CA roles may be performed by an individual operating alone.

### 5.2.3. Identification and authentication for each role

The Windows CA personnel are employees or contractors of ISO that 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) is:

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

#### **5.2.4. Roles requiring separation of duties**

See Section 5.2.2.

### **5.3 Personnel controls**

The PMA ensures that all personnel performing duties with respect to the operation of the Windows CA or RA:

- Have received comprehensive training with respect to the duties they are to perform, and
- Are not assigned duties that may cause a conflict of interest with their duties.

#### **5.3.1. Qualifications, experience, and clearance requirements**

Background, qualifications, experience and clearance requirements are:

- College degree in related fields or five years experience in security.
- Experience in one or more of the following:
  - Data Entry
  - System Administration
  - Windows NT
  - UNIX
  - Networking
  - Certification Authority
  - Digital Certificates
  - PKI
  - Information or physical security
- Internet security
- Be able to work autonomously, under short time frames, and be able to multi-task.
- Certification desired but not mandatory
- Security clearance requirements are not applicable

#### **5.3.2. Background check procedures**

The CA performs background checks in accordance with CAISO policy and procedures.

### 5.3.3. Training requirements

All personnel performing duties with respect to the operation of a CA or RA must receive comprehensive training in:

- The CA 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.**

### 5.3.4. Retraining frequency and requirements

Personnel performing CA duties will review all relevant documents, including the CP, CPS, and relevant documentation as required.

### 5.3.5. Job rotation frequency and sequence

No stipulation.

### 5.3.6. Sanctions for unauthorized actions

For any deliberate violation of trust for persons in a trusted position as defined in this CPS, the person must be removed from that position of trust. Further actions of organizations for a violation of trust lies outside of this CPS.

### 5.3.7. Independent contractor requirements

Contracting personnel must follow the same employment requirements as ISO employees.

### 5.3.8. Documentation supplied to personnel

Documentation is stored in a designated secure area and is available to authorized personnel.

## 5.4 Audit logging procedures

The Windows CA will follow the security audit procedures outlined in the Windows CP.

### 5.4.1. Types of events recorded

The Windows CA records 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 End Entities, and update and recover their keys;
- Failed read-and-write operations on the certificate and CRL directory.

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 system information.

#### **5.4.2. Frequency of audit log processing**

CA personnel review audit logs when issues arise and all significant events are explained. Actions taken following these reviews are documented. In case there are no issues that warrant review of the audit log, the CA personnel must review the audit log at least annually.

#### **5.4.3. Retention period for audit log**

The Windows CA retains its audit logs onsite for at least one year and subsequently retains them in the manner described in Section 5.5 of this CPS.

#### **5.4.4. Protection of audit log**

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

#### **5.4.5. Audit log backup procedures**

Audit logs and audit summaries are backed up or copied if in manual form.

#### **5.4.6. Audit collection system (internal vs. external)**

System logs are collected for OS related activity, and application text logs are captured for application events. Application logs are maintained on the CA system with least privilege access granted only to authorized users.

#### **5.4.7. Notification to event-causing subject**

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.

#### **5.4.8. Vulnerability assessments**

No stipulation.

### **5.5 Records archival**

#### **5.5.1. 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 attributes and authentication information.

### **5.5.2. 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.

### **5.5.3. Protection of archive**

Archive records are protected against accidental and malicious tampering.

### **5.5.4. 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.

### **5.5.5. Requirements for time-stamping of records**

No stipulation.

### **5.5.6. Archive collection system**

No stipulation.

### **5.5.7. Procedures to obtain and verify archive information**

The Windows CA verifies the integrity of the back-ups once every six months. Material stored off-site will be periodically verified for data integrity.

## **5.6 Key changeover**

The CAISO PKI does not support key changeover. Upon or prior to expiration of an existing certificate an application for a new End Entity certificate is initiated.

## **5.7 Compromise and disaster recovery**

### **5.7.1. Incident and compromise handling procedures**

Incidents are handled according to the CAISO's standard incident handling procedures.

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

Business continuity plans are documented regarding the PKI environment.

### **5.7.3. Entity private key compromise procedures**

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

- Revoke all certificates issued using that key;
- Immediately notify:
  - The PMA;
  - All of its RAs;
  - 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 ensures 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 Windows CA immediately.

### **5.7.4. Business continuity capabilities after a disaster**

Business continuity plans are documented regarding the PKI environment.

## **5.8 CA or RA termination**

The Windows CA will publish a notification of termination 30 days prior to terminating its service.

## **6.0 TECHNICAL SECURITY CONTROLS**

### **6.1 Key pair generation and installation**

#### **6.1.1. Key pair generation**

An authorized RA will generate the key pair.

#### **6.1.2. Private key delivery**

In cases where an authorized RA generates keys for a Relying Party, the key will be delivered in a secure manner.

#### **6.1.3. Public key**

The public key contained in a Certificate Signing Request (standard PKCS10 file) and delivered to the RA. The RA delivers the public key to the CA for certification.

#### **6.1.4. CA public key delivery to relying parties**

The Windows CA's public key will be delivered in a certificate signed by the Root. The Root's public key will be delivered in a self-signed certificate. This self-signed certificate, and the Windows CA's certificate will be published on an ISO internal

website. Additionally, the Root's self-signed certificate and the Windows CA's certificate may be delivered along with the End Entity certificate.

#### **6.1.5. Key sizes**

The length of the RA RSA key must be a minimum of 4096 bits. The length of the CA's RSA key is a minimum of 4096 bits.

The length of the End Entity RSA key must be a minimum of 2048 bits.

#### **6.1.6. Public key parameters generation and quality checking**

Not Applicable. Operational public keys in the Windows CA use the RSA algorithm.

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

End Entity's keys may only be used for Digital Signature (for purposes other than non-repudiation), Key Encipherment and Key Agreement. Extended Key Usage may include Client Authentication, Server Authentication, Encrypted File System and Email Protection.

### **6.2 Private Key Protection and Cryptographic Module Engineering Controls**

The private key must be protected from disclosure at all times.

#### **6.2.1. Cryptographic module standards and controls**

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

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

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

Two or more employees are required for the Windows CA key generation and certification.

#### **6.2.3. Private key escrow**

Not applicable.

#### **6.2.4. Private key backup**

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.

**6.2.5. Private key archival**

The Windows PKI does not archive private keys.

**6.2.6. Private key transfer into or from a cryptographic module**

The Windows CA uses the RSA#Microsoft Software Key Storage Provider, which supports the SHA2 family and 4096 bit keys.

**6.2.7. Private key storage on cryptographic module**

No stipulation.

**6.2.8. Method of activating private key**

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.

**6.2.9. Method of deactivating private key**

No stipulation.

**6.2.10. Method of destroying private key**

Upon termination of use of a private key, all copies of the private key in computer memory and shared disk space must be securely destroyed by over-writing.

**6.2.11. Cryptographic Module Rating**

See Section 6.2.1.

**6.3 Other aspects of key pair management****6.3.1. Public key archival**

The public keys will be archived by the Windows CA in the course of normal archival procedures.

**6.3.2. Certificate operational periods and key pair usage periods**

The root certificate will have a cryptoperiod of 20 years. The issuing certificates will have a cryptoperiod of 10 years. End entity certificates issued by the Windows CA have a maximum life of five (5) years. Private Key Usage period is not set within the certificates. Its validity period is the same as the certificate.

**6.4 Activation data****6.4.1. Activation data generation and installation**

Activation data may be in the form of a password, which follows the ISO's standard policies and procedures for passwords. An Entity will have the capability to change its password at any time.

#### **6.4.2. Activation data protection**

Data used for Entity initialization must be protected from unauthorized access. This protection mechanism must follow CAISO's standard policies and procedures for protecting passwords.

#### **6.4.3. Other aspects of activation data**

No stipulation.

### **6.5 Computer security controls**

#### **6.5.1. Specific computer security technical requirements**

The Windows CA follows computer security control procedures outlined in the Windows CP.

#### **6.5.2. Computer security rating**

No stipulation.

### **6.6 Life cycle technical controls**

#### **6.6.1. System development controls**

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

#### **6.6.2. Security management controls**

The CA system must not be installed on a domain controller and the root CA must not be domain-joined.

The Local Administrator account on the CA server must be renamed and use a 30 character, complex password. The Enterprise and Domain Administrator groups must be removed on the CA server.

The configuration of the CA system as well as any modifications and upgrades is documented and controlled. There is a method of detecting unauthorized modification to the CA software or configuration. When there are significant changes, the CA provides notice to the PMA by email.

#### **6.6.3. Life cycle security controls**

No stipulation.

### **6.7 Network security controls**

The CA server is protected from attack through any open or general-purpose network with which it is connected. This Windows CA is not accessible by external entities. A firewall separates the network of the CA system from other internal and external

networks. Communication with the repository uses the *push* model, with the CA being the initiator of the connection. Additionally, the Windows CA publishes to a directory a list of usable certificates.

## 6.8 Time-stamping

No stipulation.

## 7.0 CERTIFICATE, CRL, AND OCSP PROFILES

### 7.1 Certificate profile

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

#### 7.1.1. 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:	End Entity's distinguished name
Subject Public Key:	End Entity's public key
Signature:	CA signature to authenticate certificate

as well as the certificate extensions defined in Section 7.1.2. of this document.

#### 7.1.2. 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
CertificatePolicies:	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:	subject 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

### 7.1.3. Algorithm object identifiers

End entities must support the RSA algorithm with key sizes of 4096 bits, or greater. The digest algorithm must be SHA-2.

The Windows CA uses, and End Entities must support for signing and verification, the following algorithms:

- RSA with 4096 bit keys
- The digest algorithm must be SHA-2.

### 7.1.4. Name forms

Every DN is in the form of an X.500 printableString.

### 7.1.5. Name constraints

Subject and issuer DNs comply with the x.500 standard.

### 7.1.6. Certificate policy object identifier

The Windows CA includes the Policy OID within the certificates it issues under the extension CERTIFICATEPOLICIES.

### 7.1.7. Usage of Policy Constraints extension

No stipulation.

### 7.1.8. Policy qualifiers syntax and semantics

No stipulation.

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

No stipulation.

## 7.2 CRL profile

### 7.2.1. Version number(s)

The Windows CA issues CRLs according to the X.509 Version 2 standard.

### 7.2.2. CRL and CRL entry extensions

The CRL of the Windows CA contains the following fields:

Version: version of X.509 CRL, which is 2  
 SignatureAlgorithm: algorithm ID for signing the certificate  
 Issuer: name of the issuing CA

Effective date:	the date starting which the CRL is valid
Next update date:	the date before which the CA expects to issue another CRL
Revocation list:	the serial number and revocation date for each revoked certificate
Signature:	CA signature to authenticate the CRL

### **7.3 OCSP profile**

The Windows CA supports OCSP.

#### **7.3.1. Version number(s)**

The Windows CA supports OCSP.

#### **7.3.2. OCSP extensions**

The Windows CA supports OCSP.

## **8.0 COMPLIANCE AUDIT AND OTHER ASSESSMENTS**

This CPS and the CA are subject to both internal and third party reviews.

### **8.1 Frequency or circumstances of assessment**

The Windows CA must establish that the environment in which it is operating complies with the requirements of the CP and this CPS. This must occur:

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

The Windows 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 the CP or this CP and state any periods of non-compliance.

### **8.2 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. An independent auditor selected by the PMA will conduct the third party review.

### **8.3 Assessor's relationship to assessed entity**

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

Where an inspector is external to the California ISO, the inspector must be independent of the CA and must comply with the provisions of the Non-Disclosure Agreement and

Confidentiality requirements of the ISO. 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 the California 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.

#### **8.4 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;
- an RA implements and complies with those technical, procedural and personnel practices and policies set out by the CA.

#### **8.5 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. Necessary corrective action on identified deficiencies will be taken immediately.

#### **8.6 Communication of results**

These results will not be made public unless required by law. In cases of revocation of the CA certificate, notification and communication will follow policies stated in the ISO CP.

### **9.0 OTHER BUSINESS AND LEGAL MATTERS**

#### **9.1 Fees**

The Windows CA will not charge for services at this time.

**9.1.1. Certificate issuance or renewal fees**

The Windows CA will not charge for services at this time.

**9.1.2. Certificate access fees**

The Windows CA will not charge for services at this time.

**9.1.3. Revocation or status information access fees**

The Windows CA will not charge for services at this time.

**9.1.4. Fees for other services**

The Windows CA will not charge for services at this time.

**9.1.5. Refund policy**

Not applicable.

**9.2 Financial responsibility**

Not applicable.

**9.2.1. Insurance coverage**

Not applicable.

**9.2.2. Other assets**

Not applicable.

**9.2.3. Insurance or warranty coverage for End-Entities**

Not applicable.

**9.3 Confidentiality of business information****9.3.1. Scope of confidential information**

Certificates and CRLs, and personal or corporate information appearing on them and in public directories are not considered confidential or private. All other personal or corporate information held by the Windows CA or one of its RAs is considered confidential and will not be disclosed, unless required by applicable law or regulation.

Information pertaining to the CA's management of a certificate may only be disclosed to where required by law.

Any request for the disclosure of information must be signed by the requester and delivered to the CA Operational Authority.

**9.3.2. 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.

### **9.3.3. 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.

## **9.4 Privacy of personal information**

See section 9.3.1.

### **9.4.1. Privacy plan**

No stipulation.

### **9.4.2. Information treated as private**

See section 9.3.1.

### **9.4.3. Information not deemed private**

See section 9.3.2.

### **9.4.4. Responsibility to protect private information**

See section 9.3.3.

### **9.4.5. Notice and consent to use private information**

No stipulation.

### **9.4.6. Disclosure pursuant to judicial or administrative process**

No stipulation.

### **9.4.7. Other information disclosure circumstances**

No stipulation.

## **9.5 Intellectual property rights**

No stipulation.

## **9.6 Representations and warranties**

### **9.6.1. CA representations and warranties**

The Windows CA will take reasonable efforts to ensure that all RAs will follow the requirements of this CPS when dealing with any certificates.

In cases where the Windows CA generates the key pair for a Relying Party, the Windows CA will use industry standards and accepted practices to generate the key pair.

The Windows CA uses industry standards and accepted methods to transmit a key pair to the Relying Party. In all cases the private key is protected using a PIN or a password.

The Windows CA will use a central repository for publishing certificates. The delivery of a certificate constitutes notice of issuance.

The CA will use one of the following means to inform the Relying Party of his or her certificate revocation:

1. Email, or
2. In writing.

The Windows CA will promptly revoke certificates on a valid request from authorized entities. The Windows CA will publish the CRL to a directory, minimally once every 24 hours.

### **9.6.2. RA representations and warranties**

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

The Windows CA uses a Registration Authority (RA) who submits End Entity information to the CA. The RA certifies that it has authenticated the attributes of the End Entity in accordance with the provisions of this CPS.

### **9.6.3. Relying party representations and warranties**

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

### **9.6.4. Representations and warranties of other participants**

No stipulation.

## **9.7 Disclaimers of warranties**

The ISO assumes no liability whatsoever in relation to the use of Windows PKI certificates or associated public/private key pairs for any use other than in accordance with the CP and this CPS.

ISO, its governors, officers, directors, employees or agents makes no representations, warranties or conditions, express or implied other than as expressly stated in the CP and this CPS 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 Windows PKI.

## **9.8 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, a ISO PKI certificate or its associated public/private key pair.

The disclaimers and limitations of liability in this section and Section 9.7 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.

## **9.9 Indemnities**

No stipulations.

## **9.10 Term and termination**

### **9.10.1. Term**

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

### **9.10.2. Termination**

ISO shall have the exclusive right to terminate this CPS.

### **9.10.3. Effect of termination and survival**

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

## **9.11 Individual notices and communications with participants**

All items in this CPS are subject to the notification requirement.

The CA ensures that any agreements 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.

## **9.12 Amendments**

### **9.12.1. Procedure for amendment**

Modifications such as additions, deletions, changes, upgrades and updates must be reviewed by the Policy Management Authority, the Operational Authority, the ISO Corporate Counsel, or outside legal firm specializing in CPS and PKI technologies.

The Policy Management Authority and the Operational Authority must jointly approve any changes to this CPS.

Prior to making significant changes to this CPS, the Policy Management Authority (PMA) will notify the CA and RAs.

### **9.12.2. Notification mechanism and period**

The PMA will notify all affected parties of any major proposed changes to this CPS. The notification must contain a statement of major proposed changes, the final date for receipt of comments, and the proposed effective date of change.

Written and signed comments on major 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.

### **9.12.3. 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.

## **9.13 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 Windows CA.

## **9.14 Governing law**

The PMA ensures that any agreements by the Windows 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. This will be accomplished by conducting a legal review of the CP and CPS documents as needed, but minimally once every two years.

## **9.15 Compliance with applicable law**

See Section 9.14.

## **9.16 Miscellaneous provisions**

### **9.16.1. Entire agreement**

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

### **9.16.2. Assignment**

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

**9.16.3. Severability**

The PMA ensures that any agreements by the Windows 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.

**9.16.4. Enforcement (attorneys' fees and waiver of rights)**

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

**9.16.5. Force Majeure**

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

**9.17 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 CPS and shall govern with regard to interpretation of this CPS.