Certificate Policy
for the
California Independent System Operator
Windows Enterprise Public Key Infrastructure

Version 1.0

July 2015

Table of Contents

1.0 INTRODUCTION

1.1 Overview

This document defines certificate policy for use in the California Independent System Operator Windows Enterprise Public Key Infrastructure (Windows PKI) 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 *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 ISO PKI Subscribers.

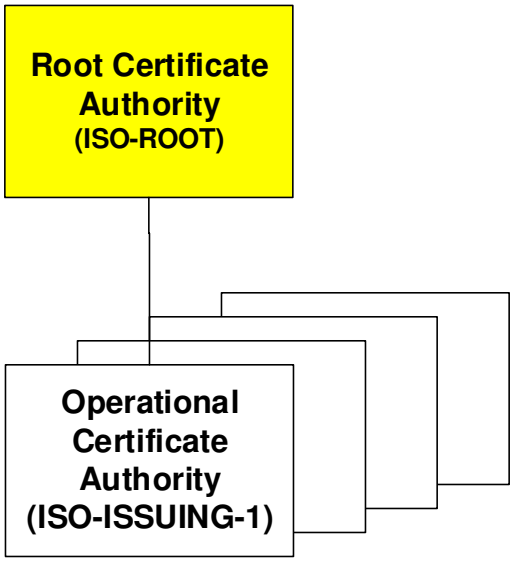

Figure 1 California ISO Certification Authority Hierarchy

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 Windows PKI and its Subscribers and Relying Parties. Users of this document are to consult the issuing Certification Authority and the *California Independent System Operator Certification Practice Statement for Windows Certification Authority* (Windows CPS) to obtain further details of the implementation of this Certificate Policy. This policy is associated with Windows 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.

This policy is for the management and use of Windows 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 this policy 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.

All CAs created must be associated with at least one Certificate and one CRL repository for the type of certificate. Digital certificates must be made available to the respective Subscribers. The repository may be used by other CAs.

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.

1.2 Document name and identification

This document is identified by name as *Certificate Policy for the California Independent System Operator Windows Enterprise Public Key Infrastructure*.

1.3 PKI participants

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

1.3.1. CERTIFICATION AUTHORITIES (CAs)

A CA operating under these policies is responsible for:

- creation and signing of certificates binding End Entities and PKI personnel with their attribute authentication and key agreement keys for use with appropriate 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

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.

An RA 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. End Entities

End Entities include devices, systems, and applications for which certificates are issued provided that responsibility and accountability for the certificates are attributable to an individual or an organization within the California ISO.

Windows PKI certificates will only be issued after request or authorization for issuance. They may be issued to employees, contractors, vendors or organization within the California ISO.

Eligibility for a certificate is at the sole discretion of the ISO. A CA may administer any number of certificates.

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.

1.4 Certificate usage

1.4.1. Appropriate certificate uses

A CA must advise appropriate use of certificates, as described in the Windows CPS.

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:
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 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.

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.

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 ISO-ROOT. The Root CA's certificate is self-signed.

Registration Authority (RA)

A person or organization that is responsible for the attributes and authentication of certificate End Entities before certificate issuance, but does not actually sign or issue the certificates. 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 ISO Windows PKI they are used to uniquely identify the policies and 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, 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 an ISO PKI CA to authenticate an identity 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.

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.

1.6.2. Acronyms

Acronym	Term
CA	Certification Authority
CAISO	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

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.

2.1 Repositories

The ISO operates all the repositories to which certificates and Certificate Revocation Lists (CRLs) are published.

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 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.

3.1.2. 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

A CA must validate identity, as described in the Windows CPS.

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

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:

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.

4.1 Certificate Application

A CA must process certificate applications, as described in the Windows CPS.

4.2 Certificate application processing

A CA must process certificate applications, as described in the Windows CPS.

4.3 Certificate acceptance

A CA must process certificate applications, as described in the Windows CPS.

4.4 Key pair and certificate usage

A CA must process certificate applications, as described in the Windows CPS.

4.5 Certificate renewal

A CA must process certificate applications, as described in the Windows CPS.

4.5.1. Circumstance for certificate renewal

Not applicable.

4.5.2. Who may request renewal

Not applicable.

4.5.3. Processing certificate renewal requests

Not applicable.

4.5.4. Notification of new certificate issuance to subscriber

Not applicable.

4.5.5. Conduct constituting acceptance of a renewal certificate

Not applicable.

4.5.6. Publication of the renewal certificate by the CA

Not applicable.

4.5.7. Notification of certificate issuance by the CA to other entities

Not applicable.

4.6 Certificate re-key

Not applicable.

4.6.1. Circumstance for certificate re-key

Not applicable.

4.6.2. Who may request certification of a new public key

Not applicable.

4.6.3. Processing certificate re-keying requests

Not applicable.

4.6.4. Notification of new certificate issuance to subscriber

Not applicable.

4.6.5. Conduct constituting acceptance of a re-keyed certificate

Not applicable.

4.6.6. Publication of the re-keyed certificate by the CA

Not applicable.

4.6.7. Notification of certificate issuance by the CA to other entities

Not applicable.

4.7 Certificate modification

Not applicable.

4.7.1. Circumstance for certificate modification

Not applicable.

4.7.2. Who may request certificate modification

Not applicable.

4.7.3. Processing certificate modification requests
Not applicable.

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

4.7.5. Conduct constituting acceptance of modified certificate
Not applicable.

4.7.6. Publication of the modified certificate by the CA
Not applicable.

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

4.8 Certificate revocation and suspension
A CA must revoke and/or suspend certificates, as described in the Windows CPS.

4.9 Certificate status services
Not applicable.

4.10 End of subscription
Not applicable.

4.11 Key escrow and recovery

4.11.1. Key escrow and recovery policy and practices
No stipulation.

4.11.2. Session key encapsulation and recovery policy and practices
No stipulation.

5.0 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls
A CA must implement physical controls, as described in the Windows CPS.

5.2 Procedural controls
A CA must implement procedures controls, as described in the Windows CPS.

5.3 Personnel controls
A CA must implement personnel controls, as described in the Windows CPS.

5.4 Audit logging procedures
A CA must implement audit logging procedures, as described in the Windows CPS.

5.5 Records archival

A CA must archive records, as described in the Windows CPS.

5.6 Key changeover

A CA must process key changeover, as described in the Windows CPS.

5.7 Compromise and disaster recovery

A CA must account for compromise and disaster recovery, as described in the Windows CPS.

5.8 CA or RA termination

A CA must process terminations, as described in the Windows CPS.

6.0 TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

A CA must generate and install keys, as described in the Windows CPS.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

A CA must protect keys implement controls over cryptographic modules, as described in the Windows CPS.

6.3 Activation data

6.3.1. Activation data generation and installation

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.

6.3.2. Activation data protection

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.

6.3.3. Other aspects of activation data

No stipulation.

6.4 Computer security controls

A CA must implement computer security controls, as described in the Windows CPS.

6.5 Life cycle technical controls

A CA must implement life cycle technical controls, as described in the Windows CPS.

6.6 Network security controls

A CA must implement network security controls, as described in the Windows CPS.

6.7 Time-stamping

No stipulation.

7.0 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

All ISO 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:	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.

7.1.2. 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
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

7.1.3. Algorithm object identifiers

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

CAs must use, 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 must be in the form of an X.500 printableString.

7.1.5. Name constraints

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

7.1.6. Certificate policy object identifier

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

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)

CRLs for these policies are based on the X.509 Version 2 standard.

7.2.2. CRL and CRL entry extensions

The CA must issue its CRLs in accordance with X.509 Version 2 CRLs.

7.3 OCSP profile

The California ISO does support OCSP.

7.3.1. Version number(s)

The California ISO does support OCSP.

7.3.2. OCSP extensions

The California ISO does support OCSP.

8.0 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.

8.1 Frequency or circumstances of assessment

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.

8.2 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.

8.3 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. 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.

8.4 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; 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.

8.5 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.

8.6 Communication of results

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 **Error! Reference source not found.**of this policy.

9.0 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

No stipulation.

9.1.1. Certificate issuance or renewal fees

No stipulation.

9.1.2. Certificate access fees

No stipulation.

9.1.3. Revocation or status information access fees

No stipulation.

9.1.4. Fees for other services

No stipulation.

9.1.5. Refund policy

No stipulation.

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 will ensure that their authentication and validation procedures are implemented as set forth in Section 0.

9.6.3. 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 **Error! Reference source not found.**and **Error! Reference source not found.**

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 CP shall remain in effect unless otherwise terminated by ISO.

9.10.2. Termination

ISO shall have the exclusive right to terminate this CP.

9.10.3. 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.

9.11 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.

9.12 Amendments

9.12.1. Procedure for amendment

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

9.12.2. Notification mechanism and period

The PMA will notify all CAs of any proposed major changes to this Certificate Policy.

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

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.

9.15 Compliance with applicable law

See Section 9.14.

9.16 Miscellaneous provisions

9.16.1. 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.

9.16.2. Assignment

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

9.16.3. 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.

9.16.4. 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.

9.16.5. Force Majeure

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

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 CP and shall govern with regard to interpretation of this CP.