OCF Certificate Policy

VERSION 2.0 | January 2020

OPEN CONNECTIVITY FOUNDATION®

CONTACT admin@openconnectivity.org

Legal Disclaimer

NOTHING CONTAINED IN THIS DOCUMENT SHALL BE DEEMED AS GRANTING YOU ANY KIND OF LICENSE IN ITS CONTENT, EITHER EXPRESSLY OR IMPLIEDLY, OR TO ANY INTELLECTUAL PROPERTY OWNED OR CONTROLLED BY ANY OF THE AUTHORS OR DEVELOPERS OF THIS DOCUMENT. THE INFORMATION CONTAINED HEREIN IS PROVIDED ON AN "AS IS" BASIS, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE AUTHORS AND DEVELOPERS OF THIS SPECIFICATION HEREBY DISCLAIM ALL OTHER WARRANTIES AND CONDITIONS, EITHER EXPRESS OR IMPLIED, STATUTORY OR AT COMMON LAW, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. OPEN CONNECTIVITY FOUNDATION, INC. FURTHER DISCLAIMS ANY AND ALL WARRANTIES OF NON-INFRINGEMENT, ACCURACY OR LACK OF VIRUSES.

Change History

Release	Date	Description
01	Sep 11, 2018	Baseline - Bug 1671 - Certificate Policy for OCF PKI (Also Bug 1673 is included as part of it)
02	Sep 11, 2018	Bug 2436 - Certificate Policy correction of mutually exclusive language
03	Sep 11, 2018	Bug 2510 - Change Dispute Legal Venue to Delaware in CP Fix some formatting issue
04	Nov 09, 2018	Bug 2631 - CP Updates for RAs MAs and CAs as well as OID update in the Security Spec
05	Jan 21, 2020	Bug 3122 - CP Updates for Revocation Policy, clarified revocation conditions and responsible actors

Contents

1 Introduction 11
1.1 OVERVIEW 11
1.1.1 Certificate Policy (CP) 11
1.1.2 Key Words for Requirements 11
1.1.3 Role of the CP and Other Practice Documents 12
1.1.4 Assurance Level 13
1.2 DOCUMENT NAME AND IDENTIFICATION 13
1.3 PKI PARTICIPANTS 14
1.4 CERTIFICATE USAGE 17
1.4.1 Appropriate Certificate Uses 17
1.4.2 Prohibited Certificate Uses 17
1.5 POLICY ADMINISTRATION 17
1.5.1 Organization Administering the Document 17
1.5.2 Contact Person 17
1.5.3 Person Determining CPS Suitability for the Policy 17
1.5.4 CPS Approval Procedures 17
1.6 DEFINITIONS AND ACRONYMS 18

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES 19

2.1 REPOSITORIES 19
2.2 PUBLICATION OF CERTIFICATION INFORMATION 19
2.3 TIME OR FREQUENCY OF PUBLICATION 19
2.4 ACCESS CONTROLS ON REPOSITORIES 19

3 IDENTIFICATION AND AUTHENTICATION 20

3.1 NAMING 20
3.1.1 Types of Names 20
3.1.2 Need for Names to be Meaningful 20
3.1.3 Anonymity or Pseudonymity of Members 20
3.1.4 Rules for Interpreting Various Name Forms 20
3.1.5 Uniqueness of Names 20
3.1.6 Recognition, Authentication, and Role of Trademarks 20
3.2 INITIAL IDENTITY VALIDATION 21
3.2.1 Method to Prove Possession of Private Key 21
3.2.2 Authentication of Organization Identity 21
3.2.3 Conduct a trademark search of the logo in the U.S. Patent and Trademark Office or equivalent international trademark office. Authentication of Individual Identity 21
3.2.4 Non-verified Member Information 22
3.2.5 Validation of Authority 22
3.2.6 Criteria for Interoperation 22
3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS 22
3.3.1 Identification and Authentication for Routine re-key 22
3.3.2 Identification and Authentication for Re-key After Revocation 22
3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST 23

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS....24
4.1 CERTIFICATE APPLICATION....24
4.1.1 Who Can Submit a Certificate Application....24
4.1.2 Enrollment Process and Responsibilities....24
4.2 CERTIFICATE APPLICATION PROCESSING....24
4.2.1 Performing Identification and Authentication Functions....24
4.2.2 Approval or Rejection of Certificate Applications....24
4.2.3 Time to Process Certificate Applications....25
4.3 CERTIFICATE ISSUANCE....25
4.3.1 RA Actions During Certificate Issuance....25
4.3.2 Notification to Member by the CA of Issuance of Certificate....25
4.4 CERTIFICATE ACCEPTANCE....25
4.4.1 Conduct Constituting Certificate Acceptance....25
4.4.2 Publication of the Certificate by the CA....26
4.4.3 Notification of Certificate Issuance by the CA to Other Entities....26
4.5 KEY PAIR AND CERTIFICATE USAGE....26
4.5.1 Member Private Key and Certificate Usage....26
4.5.2 Relying Party Public Key and Certificate Usage....26
4.6 CERTIFICATE RENEWAL....26
4.6.1 Circumstance for Certificate Renewal....26
4.6.2 Who May Request Renewal....27
4.6.3 Processing Certificate Renewal Requests....27
4.6.4 Notification of New Certificate Issuance to Member....27
4.6.5 Conduct Constituting Acceptance of a Renewal Certificate....27
4.6.6 Publication of the Renewal Certificate by the CA....27
4.6.7 Notification of Certificate Issuance by the CA to Other Entities....27
4.7 CERTIFICATE RE-KEY....27
4.7.1 Circumstance for Certificate Re-key....27
4.7.2 Who May Request Certification of a New Public Key....27
4.7.3 Processing Certificate Re-keying Requests....28
4.7.4 Notification of New Certificate Issuance to Member....28
4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate....28
4.7.6 Publication of the Re-keyed Certificate by the CA....28
4.7.7 Notification of Certificate Issuance by the CA to Other Entities....28
4.8 CERTIFICATE MODIFICATION....28
4.8.1 Circumstance for Certificate Modification....28
4.8.2 Who May Request Certificate Modification....28
4.8.3 Processing Certificate Modification Requests....29
4.8.4 Notification of New Certificate Issuance to Member....29
4.8.5 Conduct Constituting Acceptance of Modified Certificate....29
4.8.6 Publication of the Modified Certificate by the CA....29
4.8.7 Notification of Certificate Issuance by the CA to Other Entities....29
4.9 MEMBER CERTIFICATE REVOCATION AND SUSPENSION....29
4.9.1 Circumstances for Revocation....29
4.9.2 Who Can Request Revocation....30
4.9.3 Procedure for Revocation Request....30

4.9.4 Revocation Request Grace Period....31
4.9.5 Time Within Which CA Must Process the Revocation Request....31
4.9.6 Revocation Checking Requirement for Relying Parties....31
4.9.7 CRL Issuance Frequency....31
4.9.8 Maximum Latency for CRLs....31
4.9.9 On-line Revocation/Status Checking Availability....31
4.9.10 On-line Revocation Checking Requirements....31
4.9.11 Other Forms of Revocation Advertisements Available....32
4.9.12 Special Requirements Regarding Key Compromise....32
4.9.13 Circumstances for Suspension....32
4.9.14 Who Can Request Suspension....32
4.9.15 Procedure for Suspension Request....32
4.9.16 Limits on Suspension Period....32
4.10 CERTIFICATE STATUS SERVICES....32
4.10.1 Operational Characteristics....32
4.10.2 Service Availability....32
4.10.3 Optional Features....32
4.11 END OF SUBSCRIPTION....32
4.12 KEY ESCROW AND RECOVERY....33
4.12.1 Key Escrow and Recovery Policy and Practices....33
4.12.2 Session Key Encapsulation and Recovery Policy and Practices....33

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS....34

5.1 PHYSICAL CONTROLS....34
5.1.1 Site Location and Construction....34
5.1.2 Physical Access....34
5.1.3 Power and Air Conditioning....35
5.1.4 Water Exposures....36
5.1.5 Fire Prevention and Protection....36
5.1.6 Media Storage....36
5.1.7 Waste Disposal....36
5.1.8 Off-site Backup....36
5.2 PROCEDURAL CONTROLS....36
5.2.1 Trusted Roles....37
5.2.2 Number of Persons Required per Task....37
5.2.3 Identification and Authentication for Each Role....38
5.2.4 Roles Requiring Separation of Duties....38
5.3 PERSONNEL CONTROLS....38
5.3.1 Qualifications, Experience, and Clearance Requirements....38
5.3.2 Background Check Procedures....39
5.3.3 Training Requirements....39
5.3.4 Retraining Frequency and Requirements....40
5.3.5 Job Rotation Frequency and Sequence....40
5.3.6 Sanctions for Unauthorized Actions....40
5.3.7 Independent Contractor Requirements....40
5.3.8 Documentation Supplied to Personnel....40
5.4 AUDIT LOGGING PROCEDURES....40

5.4.1 Types of Events Recorded 41
5.4.2 Frequency of Processing Log 42
5.4.3 Retention Period for Audit Log 42
5.4.4 Protection of Audit Log 42
5.4.5 Audit Log Backup Procedures 42
5.4.6 Audit Collection System (Internal vs. External) 42
5.4.7 Notification to Event-Causing Subject 43
5.4.8 Vulnerability Assessments 43
5.5 RECORDS ARCHIVAL 43
5.5.1 Types of Records Archived 43
5.5.2 Retention Period for Archive 44
5.5.3 Protection of Archive 44
5.5.4 Archive Backup Procedures 44
5.5.5 Requirements for Time-Stamping of Records 44
5.5.6 Archive Collection System (Internal or External) 44
5.5.7 Procedures to Obtain and Verify Archive Information 44
5.6 KEY CHANGEOVER 44
5.7 COMPROMISE AND DISASTER RECOVERY 45
5.7.1 Incident and Compromise Handling Procedures 45
5.7.2 Computing Resources, Software, and/or Data are Corrupted 45
5.7.3 Entity Private Key Compromise Procedures 45
5.7.4 Business Continuity Capabilities after a Disaster 46
5.8 CA OR RA TERMINATION 46

6 TECHNICAL SECURITY CONTROLS 48

6.1 KEY PAIR GENERATION AND INSTALLATION 48
6.1.1 Key Pair Generation 48
6.1.2 Private Key Delivery to Member 48
6.1.3 Public Key Delivery to Certificate Issuer 49
6.1.4 CA Public Key Delivery to Relying Parties 49
6.1.5 Key Sizes 49
6.1.6 Public Key Parameters Generation and Quality Checking 49
6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field) 49
6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS 49
6.2.1 Cryptographic Module Standards and Controls 49
6.2.2 Private Key (m out of n) Multi-Person Control 50
6.2.3 Private Key Escrow 50
6.2.4 Private Key Backup 50
6.2.5 Private Key Archival 51
6.2.6 Private Key Transfer into or from a Cryptographic Module 51
6.2.7 Private Key Storage on Cryptographic Module 51
6.2.8 Method of Activating Private Key 52
6.2.9 Method of Deactivating Private Key 52
6.2.10 Method of Destroying Private Key 53
6.2.11 Cryptographic Module Rating 53
6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT 53

6.3.1 Public Key Archival 53
6.3.2 Certificate Operational Periods and Key Pair Usage Periods 53
6.4 ACTIVATION DATA 54
6.4.1 Activation Data Generation and Installation 54
6.4.2 Activation Data Protection...54
6.4.3 Other Aspects of Activation Data 54
6.5 COMPUTER SECURITY CONTROLS..55
6.5.1 Specific Computer Security Technical Requirements 55
6.5.2 Computer Security Rating...56
6.6 LIFE CYCLE TECHNICAL CONTROLS 56
6.6.1 System Development Controls...56
6.6.2 Security Management Controls..57
6.6.3 Life Cycle Security Controls...57
6.7 NETWORK SECURITY CONTROLS 57
6.8 TIME-STAMPING 57

7 CERTIFICATE, CRL, AND OCSP PROFILES 58

7.1 CERTIFICATE PROFILE 58
7.2 CRL PROFILE 58
7.3 OCSP PROFILE 58
7.3.1 Version Number(s)..58
7.3.2 OCSP Extensions 58

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS...................59

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT 59
8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR 59
8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY................................59
8.4 TOPICS COVERED BY ASSESSMENT 59
8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY 60
8.6 COMMUNICATION OF RESULTS..61

9 OTHER BUSINESS AND LEGAL MATTERS.................................62

9.1 FEES 62
9.1.1 Certificate Issuance or Renewal Fees..62
9.1.2 Certificate Access Fees 62
9.1.3 Revocation or Status Information Access Fees 62
9.1.4 Fees for Other Services 62
9.1.5 Refund Policy..62
9.2 FINANCIAL RESPONSIBILITY 62
9.2.1 Insurance Coverage..62
9.2.2 Other Assets 62
9.2.3 Insurance or Warranty Coverage for End-Entities............................62
9.3 CONFIDENTIALITY OF BUSINESS INFORMATION 62
9.3.1 Scope of Confidential Information 62
9.3.2 Information not Within the Scope of Confidential Information 63
9.3.3 Responsibility to Protect Confidential Information............................63
9.4 PRIVACY OF PERSONAL INFORMATION..63

9.4.1 Privacy Plan ... 63
9.4.2 Information Treated as Private ... 63
9.4.3 Information not Deemed Private ... 63
9.4.4 Responsibility to Protect Private Information ... 63
9.4.5 Notice and Consent to Use Private Information ... 63
9.4.6 Disclosure Pursuant to Judicial or Administrative Process ... 63
9.4.7 Other Information Disclosure Circumstances ... 64
9.5 INTELLECTUAL PROPERTY RIGHTS ... 64
9.6 REPRESENTATIONS AND WARRANTIES ... 64
9.6.1 CA Representations and Warranties ... 64
9.6.2 RA Representations and Warranties ... 65
9.6.3 Member Representations and Warranties ... 65
9.6.4 Relying Party Representations and Warranties ... 66
9.6.5 Representations and Warranties of Other Participants ... 66
9.7 DISCLAIMERS OF WARRANTIES ... 66
9.8 LIMITATIONS OF LIABILITY ... 66
9.9 INDEMNITIES ... 66
9.10 TERM AND TERMINATION ... 66
9.10.1 Term ... 66
9.10.2 Termination ... 67
9.10.3 Effect of Termination and Survival ... 67
9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS ... 67
9.12 AMENDMENTS ... 67
9.12.1 Procedure for Amendment ... 67
9.12.2 Notification Mechanism and Period ... 67
9.12.3 Circumstances Under Which OID Must be Changed ... 67
9.13 DISPUTE RESOLUTION PROVISIONS ... 67
9.14 GOVERNING LAW ... 67
9.15 COMPLIANCE WITH APPLICABLE LAW ... 68
9.16 MISCELLANEOUS PROVISIONS ... 68
9.16.1 Entire Agreement ... 68
9.16.2 Assignment ... 68
9.16.3 Severability ... 68
9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights) ... 68
9.16.5 Force Majeure ... 68
9.17 OTHER PROVISIONS ... 68

10 REFERENCES ... 69

11 GLOSSARY ... 70

12 ABBREVIATIONS AND ACRONYMS ... 73

Figures

Figure 1 OCF Certificate Hierarchy 14

1 INTRODUCTION

1.1 Overview

The Open Connectivity Foundation (OCF) is connecting billions of connected devices (phones, computers, sensors, and others) allowing them to communicate with one another regardless of manufacturer, operating system, chipset or physical transport. The Open Connectivity Foundation (OCF) is creating a specification and sponsoring an open source project to make this possible. OCF will unlock the massive opportunity in the IoT market, accelerate industry innovation and help developers and companies create solutions that map to a single open specification. OCF will help ensure secure interoperability for consumers, business, and industry.

The Security Working Group (SWG) of the Technology Steering Committee (TSC) of the OCF is focused on providing a framework for the security of the devices, data on these devices and communications between devices. It is the belief of the SWG that this can be best accomplished using the most secure tools and cryptologic capabilities available in the state of the science; to this end the use of a Public Key Infrastructure (PKI) is being recommended within this document along with the policy governing the creation of certificates and the organizational framework for creating, managing, revoking and distributing those certificates.

.

1.1.1 Certificate Policy (CP)

This Certificate Policy comprises the policy framework for the PKI and is consistent with the *Internet X.509 PKI Certificate Policy and Certification Practices Framework* [RFC 3647]. It governs the operations of the PKI components by all individuals and entities within the PKI (collectively, “PKI Participants”). It provides the minimum requirements that PKI Participants are required to meet when issuing and managing Certification Authorities (CAs), digital certificates, and private keys. In addition, it informs potential Relying Parties about what they need to know prior to relying on issued certificates.

This CP also defines the terms and conditions under which the CAs SHALL operate to issue certificates. Where “operate” includes certificate management (i.e., approve, issue, and revoke) of certificates and "issue" in this context refers to the process of digitally signing with the private key associated with its authority certificate a structured digital object conforming to the X.509, version 3 certificate format.

The CP acts as an umbrella document establishing baseline requirements and applies consistently throughout the entire PKI, thereby providing a uniform level of trust throughout the applicable community.

1.1.2 Key Words for Requirements

Throughout this document, capitalized key words are used to define the significance of particular requirements. The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described here [RFC 2119]:

“MUST” This word or the adjectives “REQUIRED” or “SHALL” means that the item is an absolute requirement of this CP. “SHALL” will be used when an entity or organization needs to take action. “MUST” will be used otherwise.

“MUST NOT” This phrase, or the phrase “SHALL NOT” means that the item is an absolute prohibition of this CP.

“SHOULD” This word or the adjective “RECOMMENDED” means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood and the case carefully weighed before choosing a different course.

“SHOULD NOT” This phrase, or the phrase “NOT RECOMMENDED” means that there may exist valid reasons in particular circumstances when the listed behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.

“MAY” This word or the adjective “OPTIONAL” means that this item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because it enhances the product, for example; another vendor may omit the same item.

1.1.3 Role of the CP and Other Practice Documents

The CP describes the overall business, legal, and technical infrastructure of the PKI. More specifically, it describes, among other things:

- Appropriate applications for the PKI certificates
- Obligations of CAs
- Minimum requirements for audit and related security and practices reviews
- Methods to confirm the identity of Certificate Applicants
- Operational procedures for certificate lifecycle services: certificate application, issuance, acceptance, revocation, and renewal
- Operational security procedures for audit logging, records retention, and disaster recovery
- Physical, personnel, key management, and logical security
- Certificate Profile and Certificate Revocation List content

Other documents include:

- **Security Policies**, which describe additional requirements concerning personnel, physical, telecommunications, logical, and cryptographic key management security
- **Security Robustness/Hardening Rules,** which describes key holders’ responsibilities, defines/lists sensitive data, defines minimum hardening/security requirements, etc.

- **Audit Policy**, which describes requirements under which audits will refer to
- **Compromise Key and Recovery Plan**, which provides procedures for handling a compromised key and the methods of recovery
- **Disaster Recovery Plan**, which provides procedures for handling a natural disaster or man-made disaster and procedures to retrieve off-site components to get the CA back-on-line
- Ancillary agreements, such as an Ecosystem Member Compliance Agreement, Root CA Hosting Agreement, and interoperation agreements

In many instances, the CP refers to these other documents for specific, detailed requirements where including the specifics in the CP would compromise the security of the PKI. the CP is an integral part of the OCF PKI document architecture and sets the minimum standards for governing, administrating and operating the PKI. Ancillary security and operational documents supplement the CP in setting more detailed requirements. Additionally, each OCF PKI CA is governed by a Certification Practice Statement(s) (CPS), which describes how the applicable CP requirements are met by that particular CA. CAs operating in the OCF PKI SHALL draft, implement, and maintain a CPS. Table 1 is a matrix of the various OCF PKI practice documents, whether they are publicly available, and their locations. The list is not intended to be exhaustive, nor will each document listed be applicable to every CA. Note that documents not expressly made public are confidential to preserve the security of the OCF PKI.

Table 1: Availability of Practice Documents

Documents	Availability	Available From:
OCF Certificate Policy (CP)	Public	OCF
Root CA CPS	Confidential	N/A
Sub CA CPS	Confidential	N/A
Ancillary Agreements	Public	TBD
Revocation Policy	Confidential	N/A
Audit Policy	Confidential	N/A
Compromised Key and Recovery Plan	Confidential	N/A
Disaster Recovery Plan	Confidential	N/A

1.1.4 Assurance Level

Digital certificates provide assurances that the Ecosystem Member’s distinguished name is unique and unambiguous within a CA’s domain, and the identity of the Member’s organization is based on a comparison of information submitted by the Member against information in business records or databases for the ecosystem PKI the Member belongs to.

1.2 Document Name and Identification

This document is the Certificate Policy for PKI participants within the Open Connectivity Foundation PKI hierarchy operating under this CP. This document is named for the OCF, the Technical Steering Committee, the Security Working Group, the document abbreviation (CP for Certificate Policy) and the document number followed by the date in *yymmdd* format (e.g. OCF-TSC-SWG-CP-D03-171101.docx). A reference to the CP may be contained within the device or server certificate itself.

1.3 PKI Participants

The PKI will consist of a two-tier infrastructure with offline Root CAs at tier 1 that issue intermediate CA certificates (sub-CAs). The sub-CAs issue compliant end-entity device certificates. The Security Working Group can support one or more Root CAs. Each Root CA will have at least one sub-CA. The CAs will issue certificates to Members. Members will embed the certificates in compliant devices. The OCF will make the list of approved Root CAs available to Members.

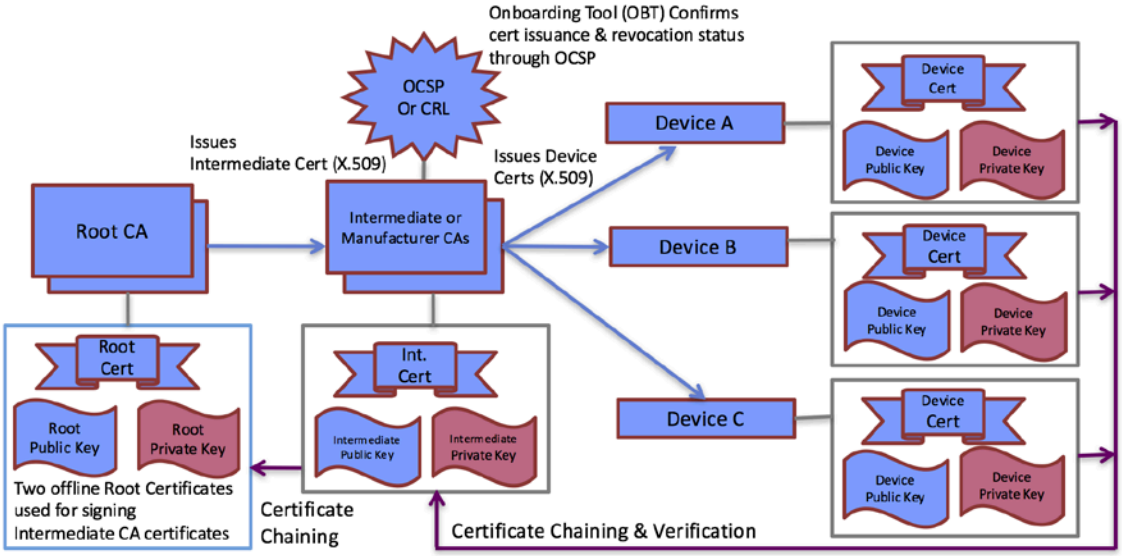

Figure 1 OCF Certificate Hierarchy

The following describes the relevant participant roles in the PKI.

1.3.1 Open Connectivity Foundation

The OCF has established the framework for the OCF PKI including this CP which was established with the approval of the OCF, the Technology Steering Committee and the Security Working Group.

1.3.2 PKI Policy Authority

The PKI Policy Authority (PKI-PA) owns this policy and represents the interest of the OCF.

An internal or external entity selected by OCF will act as the PKI-PA for the OCF PKI Root CA domains operating under this CP. The PKI-PA is responsible for:

- Governing and operating the PKI according to this and future revisions of this CP including but not limited to:
  - Migration planning for any revisions to the CP
  - Manage member certificate, contract, and key contact records
  - Revocation and security breach response planning

- Approving the Certificate Practice Statement (CPS) for each CA that issues certificates under this CP. In this model, CAs may be independent approved external CAs, or manufacturers wishing to operate and underwrite their own CA with the accordant fiscal and legal liability.
- Approving the compliance audit report for each CA operating under this policy and the continued conformance of each CA that issues certificates under this policy with applicable requirements as a condition for allowing continued participation

1.3.3 Certification Authorities

At the heart of the PKI are entities called "Certification Authorities" or "CAs." CA is an umbrella term that refers to the collection of hardware, software, and operating personnel that create, sign, and issue public key certificates to Members or other CAs. The CAs are responsible for:

- Develop and maintain a CPS showing compliance with the CP.
- Verifying their physical site security through periodic audits requested by the PA
- Issue compliant certificates
- Deliver certificates to Members in accordance with the CP, and other applicable documents such as the Member's Member Agreement
- Revocation of CA Certificates
- Generate, protect, operate, and destroy CA private keys
- CA Certificate lifecycle management ensuring that all aspects of the CA services, operations, and infrastructure related to certificates issued under this CP are performed in accordance with the requirements, representations, and warranties of this CP
- Act as trusted parties to facilitate the confirmation of the binding between a public key and the identity, and/or other attributes, of the "Subject" of the Certificate. In the PKI, the Subject of a CA certificate is the Member (i.e., OCF) requesting the CA certificate and the Subject of a device certificate is the Member (i.e., OCF Member) requesting the device certificate.

CAs fall into two categories: (1) Root CAs, which are operated by a PKI-PA designated Root CA service providers and issue sub-CA certificates; and (2) the sub-CAs which are operated by the PKI-PA designated CA service providers and issue certificates.

1.3.4 Registration Authorities

Registration Authorities (RAs) are entities that enter into an agreement with a Certification Authority to collect and verify each Member's identity and information to be entered into the Member's certificate. The RA performs its function in accordance with this CP and its approved CPS and will perform front-end functions of confirming the identity of the certificate applicant, approving or denying Certificate Applications, requesting revocation of certificates, and approving or denying Certificate Requesting Account (CRA) and account renewals.

1.3.5 Members

In the PKI, the Member is the organization named in the Ecosystem Member Agreement (EMA). An authorized representative of the Member, acting as a Certificate Applicant, SHALL complete the certificate application process established by the RA. The RA verifies the identity of the Certificate Applicant and either approves or denies the application. If approved, the RA communicates to the CA, and the Member can then request certificates, via a web-based CRA.

The Member agrees to be bound by its obligations through execution of the EMA between Member and the RA, and any other applicable agreements.

CAs, technically, are also Members within a PKI, either as a Root CA issuing a self-signed Certificate to itself, or as a sub-CA issued by a Root CA. References to “Members” in this CP, however, apply only to the organizations requesting device certificates.

1.3.6 Relying Parties

The Relying Party is any entity that validates the binding of a public key to the Member’s name in a certificate. The Relying Party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. The Relying Party can use the certificate to verify the integrity of a digitally signed message, to identify the initiator of a communication, or to establish confidential communications with the holder of the certificate.

1.3.7 Other Participants

Certificate Requesting Account

The Certificate Requesting Account is a web-based account portal that has the capability of issuing certificates with very low attendant cost to Members throughout the certificate management lifecycle. The Member company assigns an account administrator and 1-2 alternates who are registered at the CA. The Member’s account administrator uses a standard web browser and optional hardware token (e.g., USB token) to connect to their CRA account. Via this interface, the Member can request certificates and pick up batched signed certificates.

Certificates delivered from a CRA shall be in encrypted format and the member will be required to have the means to decrypt the contents of the file. Decryption may be accomplished with software or hardware tools.

Secure Element Providers

Device certificates may be provisioned within secure storage/cryptographic semiconductors during production. In this case, production testers securely generate and program device certificates into the semiconductor chips and the testers are sub-CA’s of the associated Ecosystem. As such, the production testers are also Members of the Ecosystem.

Tester sub-CA’s must provide a secure environment to prevent unauthorized access to private keys, certificates and other credentials that devices must use to authenticate themselves to gain access to the Ecosystem.

Device makers may implement secure semiconductors into their device designs to outsource the security logistics for provisioning PKI credentials to the semiconductor vendor.

Auditors

The PKI participants operating under this CP MAY require the services of other security authorities, such as compliance auditors. The CA's CPS will identify the parties responsible for providing such services, and the mechanisms used to support these services.

1.4 Certificate Usage

Certificates can be used for multiple purposes: signing, encryption, and for validating and setting up communications channels with authorized devices. For certificates created under this CP certificates are used primarily for identification and the authentication of OCF devices.

1.4.1 Appropriate Certificate Uses

Certificates are suitable for authentication of devices.

1.4.2 Prohibited Certificate Uses

PKI Certificates are not designed, intended, or authorized for use or resale as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation systems, aircraft communication systems, air traffic control systems, self-driving/navigating automobiles, weapons control systems, or other devices where failure could lead directly to death, personal injury, or severe environmental damage.

1.5 Policy Administration

1.5.1 Organization Administering the Document

The PKI-PA is responsible for all aspects of this CP.

1.5.2 Contact Person

Inquiries regarding this CP MUST be directed to the PKI-PA.

1.5.3 Person Determining CPS Suitability for the Policy

The PKI-PA SHALL approve the CPS for each CA that issues certificates under this policy, such approval not to be unreasonably withheld for any CA that complies with the approval procedures and security requirements, including security audits, of this policy.

1.5.4 CPS Approval Procedures

CAs and RAs operating under this CP are required to meet all facets of the policy. The PKI-PA SHALL make the determination that a CPS complies with this policy. The CA and RA SHALL meet all requirements of an approved CPS before commencing operations. In some cases, the PKI-PA MAY require the additional approval of the Open Connectivity Foundation. The PKI-PA will make this determination based on the nature of the system function, the type of communications, or the operating environment. In each case, the determination of suitability MUST be based on a compliance auditor's results and recommendations.

1.6 Definitions and Acronyms

See CP §§ 11 and 12.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

In the PKI, there is no separate entity providing repository services. Rather, each CA is responsible for their repository functions. All CAs that issue certificates under this policy SHALL post all CA certificates and CRLs issued by the CA in a repository that is publicly accessible on the Internet.

2.2 Publication of Certification Information

The CP, CA certificates, and CRLs MUST be made publicly available. The CPS for the Root CA will not be published; a redacted version of the CPS will be publicly available upon request to the PKI-PA. There is no requirement for the publication of CPSs of sub-CAs that issue certificates under this policy. The CA SHALL protect information not intended for public dissemination.

2.3 Time or Frequency of Publication

Changes to this CP MUST be made publicly available within thirty (30) business days of approval by the PKI-PA.

CA certificates MUST be made publicly available within three (3) business days after issuance.

Publication requirements for CRLs are provided in CP § 4.9.7.

2.4 Access Controls on Repositories

The CAs SHALL implement controls to prevent unauthorized addition, deletion, or modification of repository entries.

The CPS MUST detail what information in the repository MUST be exempt from automatic availability and to whom, and under which conditions the restricted information MAY be made available.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

For certificates issued under this policy the CA SHALL assign X.501 distinguished names. The subject field in certificates MUST be populated with a non-empty X.500 distinguished name as specified in CP §3.1.4. The issuer field of certificates MUST be populated with a non-empty X.500 Distinguished Name as specified in CP § 3.1.4.

3.1.2 Need for Names to be Meaningful

Member Certificates MUST contain meaningful names with commonly understood semantics permitting the determination of the identity of the organization that is the Subject of the Certificate.

The subject name in CA certificates MUST match the issuer name in certificates issued by the CA, as required by [RFC 5280].

3.1.3 Anonymity or Pseudonymity of Members

CAs SHALL NOT issue anonymous or pseudonymous certificates.

3.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting Distinguished Name forms are specified in X.501.

3.1.5 Uniqueness of Names

Name uniqueness for certificates issued by CAs MUST be enforced. Each CA SHALL enforce name uniqueness within the X.500 name space within its domain. Name uniqueness is not violated when multiple certificates are issued to the same Member. Name uniqueness is enforced for the entire Subject Distinguished Name of the certificate rather than a particular attribute (e.g., the common name). The CA SHALL identify the method for checking uniqueness of Subject Distinguished Names within its domain.

3.1.6 Recognition, Authentication, and Role of Trademarks

CAs operating under this policy SHALL not issue a certificate knowing that it infringes the trademark of another. Certificate Applicants SHALL not use names in their Certificate Applications that infringe upon the Intellectual Property Rights of others. Neither the PKI-PA, nor any CA SHALL be required to determine whether a Certificate Applicant has Intellectual Property Rights in the name appearing in a Certificate Application or to arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any intellectual property rights, including, without limitation, rights in a domain name, trade name, trademark, or service mark, and the PKI-PA, and any CA SHALL be entitled, without liability to any Certificate Applicant, to reject or suspend any Certificate Application because of such dispute. The PKI-PA SHALL resolve disputes involving names and trademarks.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

If the Member generates the certificate key pair, then the CA SHALL prove that the Member possesses the private key by verifying the Member's digital signature on the PKCS #10 Certificate Signing Request (CSR) with the public key in the CSR. The Member will submit the CSR via their online Certificate Requesting Account, which will employ two-factor authentication, e.g., a USB token with the account administrator's certificate and a PIN.

If a key pair is generated by the CA or sub-CA on behalf of a Member; then in this case proof of possession of the private key by the Member is not required.

The PKI-PA MAY approve other methods to prove possession of a private key by a Member.

3.2.2 Authentication of Organization Identity

The CA's certificate issuance process MUST authenticate the identity of the organization named in the Ecosystem Member Agreement by confirming that the organization:

- Exists in a business database (e.g., Dun and Bradstreet), or alternatively, has organizational documentation issued by or filed with the applicable government (e.g., government issued business credentials) that confirms the existence of the organization, such as articles of incorporation, Certificate of Formation, Charter Documents, or a business license that allow it to conduct business
- Conducts business at the address listed in the agreement
- Is not listed on any of the following U.S. Government denied lists: US Department of Commerce' Bureau of Industry and Security Embargoed Countries List, and the US Department of Commerce' Bureau of Industry and Security Denied Entities List

Second, the CA's certificate issuance process validates the information in the Certificate Application including the Icon and Friendly Name to be inserted into the certificate.

- Authentication of the contacts listed in the customer profile
- The information listed in the certificate application is verified for accuracy and validity for the given organization
- Verify the Friendly name is associated with the organization requesting the certificate by obtaining positive confirmation from the registered domain holder that the applicant has the exclusive right to use the Friendly name.

3.2.3 Conduct a trademark search of the logo in the U.S. Patent and Trademark Office or equivalent international trademark office. Authentication of Individual Identity

The CA's certificate issuance process MUST authenticate that the:

- Representative submitting the Ecosystem Member Agreement and Certificate Application, is a duly authorized representative of the organization as an employee, partner, member, agent, etc., and is authorized to act on behalf of the organization

- Corporate Contact listed in the Ecosystem Member Agreement is an officer in the organization and can act on behalf of the organization
- Administrator listed in the Ecosystem Member Agreement and Certificate Application, is a duly authorized representative of the organization as an employee, partner, member, agent, etc. and is authorized to act on behalf of the organization.

3.2.4 Non-verified Member Information

Non-verifiable information MAY be included in PKI certificates, such as:

- Organization Unit (OU)
- Any other information designated as non-verified in the certificate

3.2.5 Validation of Authority

The CA's certificate issuance process MUST confirm that the:

- Corporate Contact listed in the Ecosystem Member Agreement is an officer in the organization who can sign on behalf of the organization and bind the organization to the terms and conditions of the agreement
- Representative submitting the Ecosystem Member Agreement Administrators listed on the Ecosystem Member Agreement and certificate application are authorized to act on behalf of the organization
- Contacts listed on the Ecosystem Member Agreement are authorized to act on behalf of the organization

3.2.6 Criteria for Interoperation

The PKI-PA SHALL determine the criteria for interoperation with the PKI. See CP § 1.3.7.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine re-key

CA and Member certificate re-key shall follow the same procedures as initial certificate issuance.

For each certificate, the type of the certificate (e.g. Bridge v. Device) MUST be specified and validated during onboarding and subsequent verifications as an X509.v3 Extension.

3.3.2 Identification and Authentication for Re-key After Revocation

Once a certificate has been revoked issuance of a new certificate is required, and the Member SHALL go through the initial identity validation process per CP § 3.2.

3.4 Identification and Authentication for Revocation Request

After a certificate has been revoked other than during a renewal or update action, the Member is required to go through the initial registration process described per CP § 3.2 to obtain a new certificate.

Revocation requests MUST be authenticated and MAY be authenticated using that certificate's public key, regardless of whether or not the associated private key has been compromised.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

The Certificate Application is a package consisting of the following:

- The Ecosystem Member Agreement
- The Member profile containing contact information
- The Naming Document, which specifies the content to be bound in the certificate
- Any associated fees

A CA and RA SHALL include the processes, procedures, and requirements of their certificate application process in their CPS.

4.1.1 Who Can Submit a Certificate Application

An application for a CA certificate MUST be submitted by an authorized representative of the applicant CA.

An application for a Member certificates MUST be submitted by the Member or an authorized representative of the Member.

4.1.2 Enrollment Process and Responsibilities

The enrollment process, for a Certificate Applicant, MUST include the following:

- Completing the Certificate Application package
- Providing the requested information
- Responding to authentication requests in a timely manner
- Submitting required payment

Communication of information MAY be electronic or out-of-band.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

The identification and authentication functions MUST meet the requirements described in CP §§ 3.2 and 3.3.

4.2.2 Approval or Rejection of Certificate Applications

A RA will approve a certificate application if all of the following criteria are met:

- A fully executed Ecosystem Member Agreement
- A completed and signed Naming Document
- Successful identification and authentication of all required contact information in the Member profile
- Receipt of all requested supporting documentation
- Payment (if applicable) has been received

A RA will reject a certificate application for any of the following:

- The Member fails to execute the required agreement
- An authorized representative fails to sign the certificate application

- Identification and authentication of all required information cannot be completed
- The Member fails to furnish requested supporting documentation
- The Member fails to respond to notices within a specified time
- Payment (if applicable) has not been received

The PKI-PA MAY approve or reject a certificate application.

4.2.3 Time to Process Certificate Applications

CAs SHALL begin processing certificate applications within a reasonable time of receipt. There is no time stipulation to complete the processing of an application unless otherwise indicated in the relevant Ecosystem Member Agreement or CPS.

4.3 Certificate Issuance

4.3.1 RA Actions During Certificate Issuance

Upon receipt of a certificate application package, the RA's certificate application process MUST:

- Provide the Ecosystem Member Agreement with the applicable terms and conditions governing the use of the certificate
- Provide the applicant with the certificate application form
- Provide the identity and record of the applicant. (per CP § 3.2.3)
- Provide the applicant's authorization (by the organization named in the certificate application) to act on behalf of the organization. (per CP § 3.2.3)
- If applicable, provide the Member's public key and verification that the Member is in possession of the private key for each certificate required. (per CP § 3.2.1)
- Provide a list of contacts for the roles requested (e.g., legal, technical, etc.)

These steps MAY be performed in any order that is convenient for the RA and applicant that does not defeat security, but all MUST be completed before certificate issuance.

4.3.2 Notification to Member by the CA of Issuance of Certificate

CAs SHALL notify Members that they have created the requested Certificates, and provide Members with access to the Certificates by notifying them that their Certificates are available and the means for obtaining them. Certificates MUST be made available to Members, via download from the CA web site or via the Member's CRA.

4.4 Certificate Acceptance

Before a Member can make effective use of its private key, a PKI-PA SHALL explain to the Member its responsibilities as defined in CP § 9.6.3.

4.4.1 Conduct Constituting Certificate Acceptance

The following conduct constitutes certificate acceptance by the Member:

- Downloading a Certificate
- Failure to object timely to the certificate or its content

4.4.2 Publication of the Certificate by the CA

CA certificates MUST be published in a publicly available repository as specified in CP § 2.1.

This policy makes no stipulation regarding publication of Member certificates.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

The PKI-PA SHALL be notified whenever a CA operating under this policy issues a CA certificate.

RAs MAY receive notification of the issuance of certificates they approve.

4.5 Key Pair and Certificate Usage

4.5.1 Member Private Key and Certificate Usage

Member private key usage MUST be specified through certificate extensions, including the key usage and extended key usage extensions, in the associated certificate. Per the Ecosystem Member Agreement, Members SHALL protect their private keys from unauthorized use and SHALL discontinue use of the private key following expiration or revocation of the certificate.

Certificate use MUST be consistent with the keyUsage field extensions included in the certificate.

4.5.2 Relying Party Public Key and Certificate Usage

Relying Parties SHOULD assess:

- The restrictions on key and certificate usage specified in this CP and which are specified in critical certificate extensions, including the basic constraints and key usage extensions.
- The status of the certificate and all the CA certificates in the certificate chain. If any of the Certificates in the Certificate Chain have been revoked, the Relying Party is solely responsible to determine whether reliance on a Certificate prior to revocation of a Certificate in the Certificate chain is reasonable. Any such reliance is made solely at the risk of the Relying party.

4.6 Certificate Renewal

Certificate renewal is the issuance of a new certificate for an existing key pair without changing any information in the certificate except the validity period and serial number.

CAs issuing certificates SHALL support renewal of certificates.

4.6.1 Circumstance for Certificate Renewal

Certificate renewal is supported for certificates where the private key associated with the certificate has not been compromised. Certificates MAY be renewed to maintain continuity of certificate usage

A certificate MAY be renewed after expiration. The original certificate MAY or MAY NOT be revoked, but MUST NOT be further re-keyed, renewed, or modified.

4.6.2 Who May Request Renewal

The Member of the certificate or an authorized representative of the Member MAY request a certificate renewal.

4.6.3 Processing Certificate Renewal Requests

For a certificate renewal request, the CA SHALL confirm the identity of the Member in accordance with the requirements specified in CP § 3.2.

4.6.4 Notification of New Certificate Issuance to Member

Notification of issuance of certificate renewal to the Member MUST be in accordance with CP § 4.3.2.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Conduct constituting Acceptance of a renewed certificate MUST be in accordance with CP § 4.4.1.

4.6.6 Publication of the Renewal Certificate by the CA

Publication of a renewed certificate MUST be in accordance with CP § 4.4.2.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

Notification of the issuance of certificates MUST be in accordance with CP § 4.4.3.

4.7 Certificate Re-key

Certificate re-key consists of creating a new certificate for a different key pair (and serial number) but can retain the contents of the original certificate’s subjectName. Certificate re-key does not violate the requirement for name uniqueness. The new certificate MAY be assigned a different validity period, key identifiers, and/or be signed with a different key.

4.7.1 Circumstance for Certificate Re-key

Certificates MAY be re-keyed:

- To maintain continuity of Certificate usage
- For loss or compromise of original certificate’s private key
- By a CA during recovery from key compromise

A certificate MAY be re-keyed after expiration. The original certificate MAY or MAY NOT be revoked, but MUST NOT be further re-keyed, renewed, or modified.

4.7.2 Who May Request Certification of a New Public Key

The following may request a certificate re-key:

- The Member of the certificate or an authorized representative of the Member
- The CA MAY request a re-key of its own certificate
- The CA MAY re-key its issued certificates during recovery from a CA key compromise
- The PKI-PA MAY request re-key of CA certificates

4.7.3 Processing Certificate Re-keying Requests

For certificate re-key, the CA SHALL confirm the identity of the Member in accordance with the requirements specified in this CP § 3.2 for the authentication of an original Certificate Application.

CA certificate re-key MUST be approved by the PKI-PA.

4.7.4 Notification of New Certificate Issuance to Member

Notification of issuance of a re-keyed certificate to the Member MUST be in accordance with CP § 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

Conduct constituting Acceptance of a re-keyed certificate MUST be in accordance with CP § 4.4.1.

4.7.6 Publication of the Re-keyed Certificate by the CA

Publication of a re-keyed certificate MUST be in accordance with CP § 4.4.2.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

Notification of the issuance of certificates MUST be in accordance with CP § 4.4.3.

4.8 Certificate Modification

Modifying a certificate means creating a new certificate that contains a different serial number and that differs in one or more other fields from the original certificate.

4.8.1 Circumstance for Certificate Modification

Certificates MAY be modified:

- For a Member organization name change or other Member characteristic change
- To extend the validity period to maintain continuity of Certificate usage
- For loss or compromise of original certificate’s private key
- By a CA during recovery from key compromise

A certificate MAY be modified after expiration.

The original certificate MAY or MAY NOT be revoked, but MUST NOT be further re-keyed, renewed, or modified. If not revoked, the CA will flag the certificate as inactive in its database but will not publish the certificate on a CRL.

4.8.2 Who May Request Certificate Modification

The following may request a certificate modification:

- The Member of the certificate or an authorized representative of the Member
- The CA MAY request a certificate modification of its own certificate
- The CA MAY modify its issued certificates during recovery from a CA key compromise
- The PKI-PA MAY request modification of CA certificates

4.8.3 Processing Certificate Modification Requests

For certificate modification requests, the CA SHALL confirm the identity of the Member in accordance with the requirements specified in this CP § 3.2 for the authentication of an initial Certificate Application.

CA certificate modification MUST be approved by the PKI-PA.

4.8.4 Notification of New Certificate Issuance to Member

Notification of issuance of a new certificate to the Member MUST be in accordance with CP § 4.3.2.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Conduct constituting Acceptance of a modified certificate MUST be in accordance with CP § 4.4.1.

4.8.6 Publication of the Modified Certificate by the CA

Publication of a modified certificate MUST be in accordance with CP § 4.4.2.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Notification of the issuance of certificates MUST be in accordance with CP § 4.4.3.

4.9 Member Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

CAs MUST revoke Member End-Entity or Member Intermediate CA certificates under the following circumstances by the Member's request:

- The Member or an authorized representative of the Member asks for the certificate to be revoked for any reason whatsoever

CAs MUST request confirmation from OCF PKI-PA and revoke Member End-Entity or Member Intermediate CA certificate if confirmed under the following circumstances:

- The Member’s private key corresponding to the public key in the certificate has been lost or compromised:
  - Disclosed without authorization
  - Stolen
- There is an improper or faulty issuance of a certificate, e.g. a prerequisite to the issuance of the certificate can be shown to be incorrect;
- The CA determines that any of the information appearing in the Certificate is inaccurate or misleading

CAs MUST discontinue issuing new Member End-Entity certificates or revoke Member Intermediate CA certificate (whichever is applicable) under the following circumstances identified by the OCF PKI-PA's request for such action:

- The Member can be shown to have violated the stipulations of its Member agreement

- The Ecosystem Member Agreement with the Member has been terminated
- The Member has not submitted OCF Membership payment when due
- The continued use of that certificate is deemed harmful to the OCF by the OCF PKI-PA and Member, and the OCF Incident Response Plan has been completed

Whenever any of the above circumstances occur, the associated certificate MUST be revoked and placed on the CRL. Revoked certificates MUST be included on all new publications of the certificate status information until the certificates expire.

4.9.2 Who Can Request Revocation

Within the PKI, revocation requests MAY be made by:

- The Member of the certificate or any authorized representative of the Member
- The CA, or affiliated RA, for certificates within its domain
- The PKI-PA

4.9.3 Procedure for Revocation Request

A request to revoke a certificate MUST identify the date of the request, the certificate to be revoked, the reason for revocation, and allow the requestor to be authenticated. The CA SHALL specify the steps involved in the process of requesting a certificate revocation in their CPS.

Prior to the revocation of a Member Certificate, the CA SHALL authenticate the request. Acceptable procedures for authenticating revocation requests include:

- Have Member log in to their Certificate Requesting Account and revoking their Certificates via their account portal. The Member will submit their request via their online Certificate Requesting Account, which will employ two-factor authentication, e.g., a USB token with the account administrator’s certificate and a PIN.
- Communication with the Member providing reasonable assurances that the person or organization requesting revocation is, in fact the Member. Such communication MUST include two or more of the following: telephone confirmation, signed facsimile, signed e-mail, postal mail, or courier service.
- The representative is the Corporate Contact, Administrator, Legal, or Technical contact authenticated in CP § 3.2.5.

CAs are entitled to request the revocation of Member Certificates within the CA’s Subdomain. The CA SHALL send a written notice and brief explanation for the revocation to the Member. Notwithstanding anything to the contrary in this CP, CAs are authorized to take any action they deem necessary, under the circumstances and without liability to any party, to protect the security and integrity of the CA and/or the PKI.

The requests from CAs to revoke a CA Certificate MUST be authenticated by the PKI-PA.

Upon revocation of a certificate, the CA that issued the Certificate SHALL publish notice of such revocation in the CA’s repository or issue it upon request from the PKI-PA.

4.9.4 Revocation Request Grace Period

Revocation requests SHOULD be submitted as promptly as possible within a reasonable time of becoming aware of a revocation circumstance listed in CP § 4.9.1.

4.9.5 Time Within Which CA Must Process the Revocation Request

CAs SHALL begin investigation of a Certificate revocation request within five (5) business days of receipt to decide whether revocation or other appropriate action is warranted based upon the circumstances of the request in CP § 4.9.1.

4.9.6 Revocation Checking Requirement for Relying Parties

Relying Parties SHOULD check the status of Certificates on which they wish to rely by checking:

- The most recent CRL from the CA that issued the Certificate
- The applicable web-based repository
- By using an OCSP (Online Certificate Status Protocol) responder

CAs SHALL provide Relying Parties with information within the certificate CRL Distribution Point extension on how to find the appropriate CRL, web-based repository, or OCSP responder to check the revocation status of certificates issued by the CA.

CA certificate status MUST be posted by the PKI-PA in CRL, web-based repository, or OCSP responder.

4.9.7 CRL Issuance Frequency

CRLs MUST be issued periodically, even if there are no changes to be made, to ensure timeliness of information. Certificate status information MAY be issued more frequently than the issuance frequency described below.

CAs SHALL update and reissue CRLs at least (i) once every twelve (12) months and (ii) within 24 hours after revoking a Certificate, with the value of the *nextUpdate* field not more than twelve (12) months beyond the value of the *thisUpdate* field.

4.9.8 Maximum Latency for CRLs

CRLs SHOULD be published immediately and MUST be published within 24 hours of generation.

4.9.9 On-line Revocation/Status Checking Availability

CAs SHALL have a web-based repository that permits Relying Parties to make online inquiries regarding revocation and other Certificate status information. CAs SHALL provide Relying Parties with information on how to find the appropriate repository to check Certificate status and how to find the correct OCSP responder.

4.9.10 On-line Revocation Checking Requirements

A Relying Party SHOULD check the status of a certificate on which they wish to rely on. If a Relying Party does not check the status of a Certificate by consulting the most recent CRL, the Relying Party SHOULD check the Certificate status by consulting the applicable on-line repository or by requesting Certificate status using the applicable

OCSP responder. If the Relying Party does not check the status of the certificates as described in this paragraph or the CPS, the Relying Party is estopped from asserting any claim against the CA related to or arising out of the Relying Party's reliance on the certificate.

4.9.11 Other Forms of Revocation Advertisements Available

A CA may also use other methods to publicize the certificates it has revoked. Any alternative method MUST meet the following requirements:

- The alternative method MUST be described in the CA's CPS
- The alternative method MUST meet the issuance and latency requirements for CRLs stated in CP §§ 4.9.7 and 4.9.8

4.9.12 Special Requirements Regarding Key Compromise

When a CA certificate is revoked a CRL MUST be issued within 24 hours of notification. The PKI-PA SHALL notify PKI Participants of a CA certificate revocation using commercially reasonable efforts.

4.9.13 Circumstances for Suspension

The PKI does not offer suspension services for its Certificates.

4.9.14 Who Can Request Suspension

No stipulation.

4.9.15 Procedure for Suspension Request

No stipulation.

4.9.16 Limits on Suspension Period

No stipulation.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

Certificate status MUST be available via CRL through a URL specified in a CA's CPS, and MAY be available via LDAP directory or OCSP responder.

4.10.2 Service Availability

Certificate Status Services MUST be available 24 x 7. CRL and OCSP capability SHOULD provide a response time of ten (10) seconds or less under normal operating conditions.

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

End of subscription MUST be stipulated in the Ecosystem Member Agreement.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

No stipulation.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

All entities performing CA functions SHALL implement and enforce the following physical, procedural, logical, and personnel security controls for a CA.

5.1 Physical Controls

CA equipment MUST be protected from unauthorized access while the cryptographic module is installed and activated. The CA SHALL implement physical access controls to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. CA cryptographic tokens MUST be protected against theft, loss, and unauthorized use.

All the physical control requirements specified below apply equally to the Common Policy Root CA and subordinate CAs, and any remote workstations used to administer the CAs except where specifically noted.

5.1.1 Site Location and Construction

All CA operations MUST be conducted within a physically protected environment that deters, prevents, and detects unauthorized use of, access to, or disclosure of sensitive information and systems. The location and construction of the facility housing the CA equipment, as well as sites housing remote workstations used to administer the CAs, MUST be consistent with facilities used to house high-value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards, high security locks, and intrusion sensors, MUST provide robust protection against unauthorized access to the CA equipment and records.

Such requirements are based in part on the establishment of physical security tiers. A tier is a barrier such as a locked door or closed gate that provides mandatory access control for individuals and requires a positive response (e.g., door unlocks or gate opens) for each individual to proceed to the next area. Each successive tier provides more restricted access and greater physical security against intrusion or unauthorized access.

CAs SHALL construct the facilities housing their CA functions with at least three physical security tiers, Tiers 1 through 3. CAs SHALL perform all validation operations within Tier 2 or higher. CAs SHALL place Information Services systems necessary to support CA functions in Tier 3 or higher. Online and offline cryptographic modules MUST be placed in Tier 3 or higher. CAs SHALL further protect offline cryptographic modules by placing them within Tier 3 or higher.

CAs SHALL describe their Site Location and Construction in more detail in their CPS.

5.1.2 Physical Access

Access to each tier of physical security, constructed in accordance with CP § 5.1.1, MUST be auditable and controlled so that only authorized personnel can access each tier.

CAs SHALL control access to their CA facilities including:

- Minimal exposure of privileged functions through definition of function-specific roles or authorization groups

- Access control enforcement of these roles or groups
- Use of proximity card identification badges
- Logging of access into and out of the facility
- Use of tamper resistant physical intrusion alarm systems to detect break-ins or unauthorized access to physical security tiers within the facility
- Automated notification to outside alarm monitoring agency of a potential security breach when facility-based guards are not present

At a minimum, the physical access controls for CA equipment, as well as remote workstations used to administer the CAs, MUST:

- Ensure that no unauthorized access to the hardware is permitted
- Ensure that all removable media and paper containing sensitive plain-text information is stored in secure containers
- Be manually or electronically monitored for unauthorized intrusion at all times
- Ensure an access log is maintained and inspected periodically
- Require two-person physical access control to both the cryptographic module and computer systems

When not in use, removable cryptographic modules, activation information used to access or enable cryptographic modules, and CA equipment MUST be placed in secure containers. Activation data MUST be either memorized or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and MUST NOT be stored with the cryptographic module or removable hardware associated with remote workstations used to administer the CA.

A security check of the facility housing the CA equipment or remote workstations used to administer the CAs MUST occur if the facility is to be left unattended. At a minimum, the check MUST verify the following:

- The equipment is in a state appropriate to the current mode of operation (e.g., that cryptographic modules are in place when ―open, and secured when ―closed, and for the CA, that all equipment other than the repository is shut down)
- Any security containers are properly secured
- Physical security systems (e.g., door locks, vent covers) are functioning properly
- The area is secured against unauthorized access

A person or group of persons SHALL be made explicitly responsible for making such checks. When a group of persons is responsible, a log identifying the person performing a check at each instance MUST be maintained. If the facility is not continuously attended, the last person to depart SHALL initial a sign-out sheet that indicates the date and time and asserts that all necessary physical protection mechanisms are in place and activated.

5.1.3 Power and Air Conditioning

CA facilities MUST be equipped with primary and backup power systems to ensure continuous, uninterrupted access to electric power. Also, these facilities MUST be equipped with primary and backup heating/ventilation/air conditioning systems to control temperature and relative humidity.

The CA SHALL have backup capability sufficient to lock out input, finish any pending actions, and record the state of the equipment automatically before lack of power or air conditioning causes a shutdown.

5.1.4 Water Exposures

CA facilities MUST be constructed, equipped and installed, and procedures MUST be implemented, to prevent floods or other damaging exposure to water. Potential water damage from fire prevention and protection measures (e.g., sprinkler systems) are excluded from this requirement.

5.1.5 Fire Prevention and Protection

CA facilities MUST be constructed and equipped, and procedures MUST be implemented, to prevent and extinguish fires or other damaging exposure to flame or smoke. These measures MUST meet all local applicable safety regulations.

5.1.6 Media Storage

CAs SHALL protect the media holding back ups of critical system data or any other sensitive information from water, fire, or other environmental hazards, and SHALL use protective measures to deter, detect, and prevent the unauthorized use of, access to, or disclosure of such media.

5.1.7 Waste Disposal

CAs SHALL implement procedures for the disposal of waste (paper, media, or any other waste) to prevent the unauthorized use of, access to, or disclosure of waste containing confidential/private information.

CA media and documentation that are no longer needed for operations MUST be destroyed in a secure manner. For example, paper documentation MUST be shredded, burned, or otherwise rendered unrecoverable.

5.1.8 Off-site Backup

CAs SHALL maintain backups of critical system data or any other sensitive information, including audit data, in a secure off-site facility. Full system backups sufficient to recover from system failure MUST be made on a periodic schedule, and described in a CA's CPS. Backups are to be performed and stored off-site not less than once per week. At least one full backup copy MUST be stored at an off-site location (separate from CA equipment). Only the latest full backup need be retained. The backup MUST be stored at a site with physical and procedural controls commensurate to that of the operational CA. An active/active infrastructure, whereby data are synchronized between two sites and one site alone is capable of hosting the PKI in the event of a disaster at the other site, will meet the requirements of off-site backup.

Requirements for CA private key backup are specified in CP § 6.2.44.

5.2 Procedural Controls

Procedural controls are requirements on roles that perform functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles SHALL be extraordinarily responsible, or the integrity of the CA will be weakened. The functions performed in these roles form the basis of trust for the entire PKI. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion.

5.2.1 Trusted Roles

Employees, contractors, and consultants that are designated to manage the CA's trustworthiness SHALL be considered to be "Trusted Persons" serving in "Trusted Positions." Persons seeking to become Trusted Persons-SHALL meet the screening requirements of CP § 5.3.

CAs SHALL consider the categories of their personnel identified in this section as Trusted Persons having a Trusted Position. Trusted Persons include all employees, contractors, and consultants that have access to or control authentication or cryptographic operations that may materially affect:

- The validation of information in Certificate Applications
- The acceptance, rejection, or other processing of Certificate Applications, revocation requests, or renewal requests, or enrollment information
- The issuance, or revocation of Certificates, including (in the case of Processing Centers) personnel having access to restricted portions of its repository
- The handling of Member information or requests

Trusted Persons include, but are not limited to, customer service personnel, CA system administrators, designated engineering personnel, CA operators, auditor, and executives that are designated to manage infrastructural trustworthiness.

5.2.2 Number of Persons Required per Task

Multiparty control procedures are designed to ensure that at a minimum, two trusted personnel are required to have either physical or logical access to the CA at a time. Access to CA cryptographic hardware MUST be strictly enforced by multiple Trusted Persons throughout its lifecycle, from incoming receipt and inspection to final logical and/or physical destruction. Once a CA device is activated with operational keys, further access controls MUST be invoked to maintain split control over both physical and logical access to the device. Persons with physical access to CA modules must not be able to activate the CA, nor vice versa.

Two or more persons are required for the following tasks:

- Access to CA hardware
- Management of CA cryptographic hardware
- CA key generation
- CA signing key activation
- CA private key backup

Where multiparty control is required, at least one of the participants SHALL be an Administrator. All participants SHALL serve in a trusted role as defined in CP § 5.2.1.

Multiparty control MUST not be achieved using personnel that serve in the Auditor trusted role. CAs SHALL establish, maintain, and enforce rigorous control procedures to ensure the segregation of duties based on job responsibility and to ensure that multiple Trusted Persons are required to perform sensitive tasks.

Other manual operations such as the validation and issuance of Certificates, not issued by an automated validation and issuance system, require the participation of at least 2 Trusted Persons, or a combination of at least one trusted person and an automated validation and issuance process. Manual operations for Key Recovery MAY optionally require the validation of two (2) authorized Administrators.

5.2.3 Identification and Authentication for Each Role

CAs SHALL confirm the identity and authorization of all personnel seeking to become Trusted Persons before such personnel are:

- Issued access devices and granted access to the required facilities
- Given electronic credentials to access and perform specific functions on CA systems

Authentication of identity MUST include the personal (physical) presence of such personnel before Trusted Persons performing HR or security functions within an entity and a check of well-recognized forms of identification, such as passports and driver's licenses. Identity MUST be further confirmed through background checking procedures in CP § 5.3.

5.2.4 Roles Requiring Separation of Duties

Roles requiring Separation of duties include (but are not limited to) the:

- Validation of information in Certificate Applications
- Acceptance, rejection, or other processing of Certificate Applications, revocation requests, key recovery requests or renewal requests, or enrollment information
- Issuance, or revocation of Certificates, including personnel having access to restricted portions of the repository
- Handling of Member information or requests
- Generation, issuing or destruction of a CA certificate
- Loading of a CA to a Production environment

No individual SHALL have more than one trusted role. CA SHALL have in place procedure to identify and authenticate its users and SHALL ensure that no user identity can assume multiple roles.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

CAs SHALL require that personnel assigned to Trusted roles have the requisite background, qualifications, and experience or be provided the training needed to perform their prospective job responsibilities competently and satisfactorily. The requirements governing the qualifications, selection and oversight of individuals who operate, manage, oversee, and audit the CA MUST be set forth in the CPS.

5.3.2 Background Check Procedures

CAs SHALL conduct background check procedures for personnel tasked become Trusted Persons. These procedures MUST be subject to any limitations on background checks imposed by local law. To the extent one of the requirements imposed by this section cannot be met due to a prohibition or limitation in local law, the investigating entity SHALL utilize a substitute investigative technique permitted by law that provides substantially similar information, including but not limited to obtaining a background check performed by an applicable agency. Background investigations MAY include a:

- Confirmation of previous employment
- Check of one or more professional references
- Confirmation of the highest or most relevant educational degree obtained
- Search of criminal records (local, state or provincial, and national)
- Check of credit/financial records
- Search of driver’s license records

Factors revealed in a background check that MAY be considered grounds for rejecting candidates for Trusted Positions or for taking action against an existing Trusted Person (all subject to and in accordance with applicable law) MAY include but is not limited to the following:

- Misrepresentations made by the candidate or Trusted Person
- Highly unfavorable or unreliable personal references
- Certain criminal convictions
- Indications of a lack of financial responsibility

Background checks MUST be repeated for personnel holding Trusted Positions at least every five (5) years.

5.3.3 Training Requirements

CAs SHALL provide their personnel with the requisite on-the-job training needed for their personnel to perform their job responsibilities relating to CA operations competently and satisfactorily. They SHALL also periodically review their training programs, and their training MUST address the elements relevant to functions performed by their personnel.

Training programs MUST address the elements relevant to the particular environment of the person being trained, including, without limitation:

- Security principles and mechanisms of the CA and the its environment
- Hardware and software versions in use
- All duties the person is expected to perform
- Incident and Compromise reporting and handling
- Disaster recovery and business continuity procedures
- The stipulations of this policy

5.3.4 Retraining Frequency and Requirements

CAs SHALL provide refresher training and updates to their personnel to the extent and frequency required to ensure that such personnel maintain the required level of proficiency to perform their job responsibilities competently and satisfactorily.

All individuals responsible for PKI roles SHALL be made aware of changes in the CA operation. Any significant change to the operations MUST have a training (awareness) plan, and the execution of such plan MUST be documented. Examples of such changes are CA software or hardware upgrade, changes in automated security systems, and relocation of equipment.

Documentation MUST be maintained identifying all personnel who received training and the level of training completed.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

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

5.3.7 Independent Contractor Requirements

CAs SHALL permit independent contractors or consultants to become Trusted Persons only to the extent necessary to accommodate clearly defined outsourcing relationships. CAs SHOULD only use contractors or consultants as Trusted Persons if the CA does not have suitable employees available to fill the roles of Trusted Persons. Otherwise, independent contractors and consultants SHALL be escorted and directly supervised by Trusted Persons when they are given access to the CA and its secure facility.

Contractors fulfilling trusted roles are subject to all personnel requirements stipulated in this policy and SHALL establish procedures to ensure that any subcontractors perform in accordance with this policy.

5.3.8 Documentation Supplied to Personnel

CAs SHALL give their personnel the requisite training and documentation needed to perform their job responsibilities competently and satisfactorily.

5.4 Audit Logging Procedures

Audit log files MUST be generated for all events relating to the security of the CA. Where possible, the audit logs MUST be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism MUST be used. All CA audit logs, both electronic and non-electronic, MUST be retained and made available during compliance audits.

5.4.1 Types of Events Recorded

All auditing capabilities of the CA operating system and applications MUST be enabled during installation. All audit logs, whether recorded automatically or manually, MUST contain the date and time, the type of event, and the identity of the entity that caused the event.

CAs SHALL record in audit log files all events relating to the security of the CA system, including, without limitation:

- Physical Access / Site Security:
  - Personnel access to room housing CA
  - Access to the CA server
  - Known or suspected violations of physical security
- CA Configuration:
  - CA hardware configuration
  - Installation of the operating system
  - Installation of the CA software
  - System configuration changes and maintenance
  - Installation of hardware cryptographic modules
  - Cryptographic module lifecycle management-related events (e.g., receipt, use, de-installation, and retirement)
- Account Administration:
  - System Administrator accounts
  - Roles and users added or deleted to the CA system
  - Access control privileges of user accounts
  - Attempts to create, remove, set passwords or change the system privileges of the privileged users (trusted roles)
  - Attempts to delete or modify audit logs
  - Changes to the value of maximum authentication attempts
  - Resetting operating system clock
  - Electrical power outages
- CA Operational events:
  - Key generation
  - Start-up and shutdown of CA systems and applications
  - Changes to CA details or keys
  - Records of the destruction of media containing key material, activation data, or personal Member information)
- Certificate lifecycle events:
  - Issuance
  - Re-key
  - Renew
  - Revocation
- Trusted employee events:
  - Logon and logoff

  - Attempts to create, remove, set passwords or change the system privileges of the privileged users
  - Unauthorized attempts to the CA system,
  - Unauthorized attempts to access system files,
  - Failed read and write operations on the Certificate,
  - Personnel changes

- Token events:
  - Serial number of tokens shipped to Member
  - Account Administrator Certificates
  - Shipment of tokens
  - Tokens driver versions

5.4.2 Frequency of Processing Log

CAs SHALL review their audit logs in response to alerts based on irregularities and incidents within their CA systems. Review of the audit log MUST be required at least once every three months. CAs SHALL compare their audit logs with supporting manual and electronic logs when any action is deemed suspicious.

Audit log processing MUST consist of a review of the audit logs and documenting the reason for all significant events in an audit log summary. Audit log reviews MUST include a verification that the log has not been tampered with, a brief inspection of all log entries, and a more thorough investigation of any alerts or irregularities in the logs. Actions taken based on audit log reviews MUST be documented.

5.4.3 Retention Period for Audit Log

Audit logs MUST be retained onsite at least two (2) months after processing and thereafter archived in accordance with CP § 5.5. The individual who removes audit logs from the CA system SHALL be different from the individuals who, in combination, command the CA signature key.

5.4.4 Protection of Audit Log

Audit logs MUST be protected from unauthorized viewing, modification, deletion, or other tampering. CA system configuration and procedures MUST be implemented together to ensure that only authorized people archive or delete security audit data. Procedures MUST be implemented to protect archived data from deletion or destruction before the end of the security audit data retention period (note that deletion requires modification access).

5.4.5 Audit Log Backup Procedures

Incremental backups of audit logs MUST be created frequently, at least monthly.

5.4.6 Audit Collection System (Internal vs. External)

The audit log collection system MAY or MAY NOT be external to the CA system. Automated audit processes MUST be invoked at system or application startup and cease only at system or application shutdown. Audit collection systems MUST be configured such that security audit data is protected against loss (e.g., overwriting or overflow of automated log files). Should it become apparent that an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, operations MUST be suspended until the problem has been remedied.

5.4.7 Notification to Event-Causing Subject

Where an event is logged by the audit collection system, no notice is required to be given to the individual, organization, device, or application that caused the event.

5.4.8 Vulnerability Assessments

The CA SHALL perform routine self-assessments of security controls for vulnerabilities. Events in the audit process are logged, in part, to monitor system vulnerabilities. The assessments MUST be performed following an examination of these monitored events. The assessments MUST be based on real-time automated logging data and MUST be performed at least on an annual basis as input into an entity's annual Compliance Audit.

The audit data SHOULD be reviewed by the security auditor for events such as repeated failed actions, requests for privileged information, attempted access of system files, and unauthenticated responses. Security auditors SHOULD check for continuity of the audit data.

5.5 Records Archival

CA archive records MUST be sufficiently detailed to determine the proper operation of the CA and the validity of any certificate (including those revoked or expired) issued by the CA. Records MAY be kept in the form of either computer-based messages or paper-based documents, provided their indexing, storage, preservation, and reproduction are accurate, reliable, and complete.

5.5.1 Types of Records Archived

CA records MUST include all relevant evidence in the recording entity's possession, including, without limitation:

- Time stamps
- Certificate Policy
- Certification Practice Statement
- Contractual obligations and other agreements concerning operations of the CA System and equipment configuration
- Modifications and updates to system or configuration
- Certificate request documentation
- Records of all actions taken on certificates issued and/or published
- Record of re-key
- Revocation request information
- Records of all CRLs issued and/or published
- Compliance Auditor reports
- Appointment of an individual to a Trusted Role
- Destruction of cryptographic modules

- All certificate compromise notifications

The PKI-PA and RA records MUST include all relevant evidence in the recording entity's possession, including, without limitation:

- Ecosystem Member Agreements
- Token lifetime (issuance, recovery, destruction, etc.) documentation
- All CRLs issued and/or published
- Compliance Auditor reports
- Destruction of cryptographic modules
- All certificate compromise notifications

5.5.2 Retention Period for Archive

Archive records MUST be kept for a minimum of 10 years without any loss of data.

5.5.3 Protection of Archive

An entity maintaining an archive of records SHALL protect the archive so that only the entity's authorized Trusted Persons are able to obtain access to the archive. The archive MUST be protected against unauthorized viewing, modification, deletion, or other tampering. The archive media and the applications required to process the archive data MUST be maintained to ensure that the archive data can be accessed for the time period set forth in CP § 5.5.2.

5.5.4 Archive Backup Procedures

Entities compiling electronic information SHALL incrementally back up system archives of such information on a daily basis and perform full backups on a weekly basis. Copies of paper-based records MUST be maintained in an off-site secure facility; those paper record backups MUST be performed with a period of no longer than every four (4) weeks.

5.5.5 Requirements for Time-Stamping of Records

CA archive records MUST be automatically time-stamped as they are created. System clocks used for time-stamping MUST be maintained in synchrony with an authoritative time standard.

5.5.6 Archive Collection System (Internal or External)

Archive data may be collected in any expedient manner.

5.5.7 Procedures to Obtain and Verify Archive Information

Only authorized Trusted Personnel are able to obtain access to the archive. The integrity of the information is verified as usable when it is restored.

5.6 Key Changeover

To minimize risk from compromise of a CA's private signing key, that key may be changed often. From that time on, the CA will only use the new key to sign certificates. If the old private key is used to sign OCSP responder certificates or CRLs that cover certificates signed with that key, the old key MUST be retained and protected.

A CA Certificate may be renewed if the CA’s Superior Entity reconfirms the identity of the CA. Following such reconfirmation, the Superior Entity SHALL either approve or reject the renewal application.

When a CA updates its private signature key and thus generates a new public key, the CA SHALL notify all CAs, RAs, and Members that rely on the CA’s certificate that it has been changed.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

The PKI-PA SHALL be notified if any CAs operating under this policy experience the following:

- Suspected or detected compromise of the CA systems
- Physical penetration of the site housing the CA systems
- Successful denial of service attacks on CA components

The PKI-PA will take appropriate steps to protect the integrity of the PKI.

The CA’s Management Authority SHALL reestablish operational capabilities as quickly as possible in accordance with procedures set forth in the CA's CPS.

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

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

- Before returning to operation, ensure that the system’s integrity has been restored.
- The PKI-PA SHALL be notified as soon as possible.
- A report of the incident and a response to the event MUST be promptly made by the affected CA or RA in accordance with the documented incident and Compromise reporting and handling procedures in the applicable CPS.

5.7.3 Entity Private Key Compromise Procedures

In the event of a CA private key compromise, the following operations MUST be performed.

- The PKI-PA SHALL be immediately informed.
- If the CA signature keys are not destroyed, CA operation MUST be reestablished, giving priority to the ability to generate certificate status information.
- If the CA signature keys are destroyed, CA operation MUST be reestablished as quickly as possible, giving priority to the generation of a new CA key pair.
- The CA SHALL generate new keys in accordance with CP § 6.1.1.
- Initiate procedures to notify Members of the compromise.
- Member certificates MAY be renewed automatically by the CA under the new key pair (see CP § 4.6), or the CA MAY require Members to repeat the initial certificate application process.

5.7.4 Business Continuity Capabilities after a Disaster

Entities operating CAs SHALL develop, test, and maintain a Disaster Recovery Plan (DRP) designed to mitigate the effects of any kind of natural or man-made disaster. The Plan MUST identify conditions for activating the recovery and what constitutes an acceptable system outage and recovery time for the restoration of information systems services and key business functions within a defined recovery time objective (RTO).

Additionally, the Plan MUST include:

- Frequency for taking backup copies of essential business information and software
- Requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location
- Separation distance of the Disaster recovery site to the CA's main site
- Procedures for securing the Disaster facility during the period of time following a disaster and prior to restoring a secure environment either at the original or a remote site

The DRP MUST include administrative requirements:

- Maintenance schedule for the plan
- Awareness and education requirements
- Responsibilities of the individuals
- Regular testing of contingency plans

CAs SHALL have the capability of restoring or recovering essential operations within twenty-four (24) hours following a disaster with, at a minimum, support for the following functions: Certificate issuance, Certificate revocation, and publication of revocation information. The disaster recovery equipment MUST have physical security protections comparable to the production CA system, which includes the enforcement of physical security tiers.

A CA's disaster recovery plan MUST make provisions for full recovery within one week following a disaster at the primary site.

5.8 CA or RA Termination

When a CA operating under this policy terminates operations before all certificates have expired, the CA signing keys MUST be surrendered to the PKI-PA. Prior to CA termination, the CA SHALL provide archived data to an archive facility as specified in the CPS. As soon as possible, the CA will advise all other organizations to which it has issued certificates of its termination, using an agreed-upon method of communication specified in the CPS.

CAs that have ceased issuing new certificates but are continuing to issue CRLs until all certificates have expired are required to continue to conform with all relevant aspects of this policy (e.g., audit logging and archives).

The termination of a CA MUST be subject to the contract between the terminating CA and its Superior Entity. A terminating CA and its Superior Entity SHALL, in good faith, use commercially reasonable effort to agree on a termination plan that minimizes disruption to Members and Relying Parties. The termination plan MAY cover issues such as:

- Providing notice to parties affected by the termination, such as Members and Relying Parties
- Identifying who bears the cost of such notice, the terminating CA or the Superior Entity
- Revoking the Certificate issued to the CA by the Superior Entity
- Preserving the CA’s archives and records for the time periods required in CP § 5.4.6,
- Continuing Member and customer support services
- Continuing revocation services, such as the issuance of CRLs or the maintenance of online status checking services
- Revoking unexpired unrevoked Certificates of Members and subordinate CAs, if necessary,
- Paying compensation (if necessary) to Members whose unexpired unrevoked Certificates are revoked under the termination plan or provision, for the issuance of substitute Certificates by a successor CA
- Disposing the CA’s private key and the hardware token containing such private key, and
- Providing provisions needed for the transition of the CA’s services to a successor CA

6 TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Key pair generation MUST be performed using FIPS 140 validated cryptographic modules and processes that provide the required cryptographic strength of the generated keys and prevent the loss, disclosure, modification, or unauthorized use of private keys. Any pseudo-random numbers use and parameters for key generation material MUST be generated by a FIPS-approved method.

CA keys MUST be generated in a Key Generation Ceremony using multi-person control for CA key pair generation, as specified in CP § 6.2.2.

CA key pair generation MUST create a verifiable audit trail that the security requirements for procedures were followed. The documentation of the procedure MUST be detailed enough to show that appropriate role separation was used. An independent third party SHALL validate the execution of the key generation procedures either by witnessing the key generation or by examining the signed and documented record of the key generation.

6.1.2 Private Key Delivery to Member

Member key pair generation MUST be performed by the Member, CA or sub-CA. If the Members themselves generate private keys, then private key delivery to a Member is unnecessary.

When CAs generate key pairs on behalf of the Member, the private key MUST be delivered securely to the Member. Private keys MUST be delivered electronically or on a hardware cryptographic module or secure semiconductor chip. In all cases, the following requirements MUST be met:

- The CA SHALL not retain any copy of the key for more than two weeks after delivery of the private key to the Member
- CAs SHALL use FIPS 140-2 Level 3 systems and deliver private keys to Members via SSL/TLS and SHALL secure such delivery through the use of a PKCS#8 package or, at the CAs sole discretion, any other comparably equivalent means (e.g., PKCS#12 package) in order to prevent the loss, disclosure, modification, or unauthorized use of such private keys
- Where key pairs are pre-generated on hardware tokens, the entities distributing such tokens SHALL use best efforts to provide physical security of the tokens to prevent the loss, disclosure, modification, or unauthorized use of the private keys on them; the RA SHALL maintain a record of the Member acknowledgment of receipt of the token
- The Member SHALL acknowledge receipt of the private key(s)
- Delivery MUST be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct Members
  - For hardware modules, accountability for the location and state of the module MUST be maintained until the Member accepts possession of it

- For electronic delivery of private keys, the key material MUST be encrypted using a cryptographic algorithm and key size at least as strong as the private key activation data MUST be delivered using a separate secure channel

6.1.3 Public Key Delivery to Certificate Issuer

When a public key is transferred to the issuing CA to be certified, it MUST be delivered through a mechanism validating the identity of the Member and ensuring that the public key has not been altered during transit and that the Certificate Applicant possesses the private key corresponding to the transferred public key. The Certificate Applicant SHALL deliver the public key in a PKCS#10 CSR or an equivalent method ensuring that the public key has not been altered during transit; and the Certificate Applicant possesses the private key corresponding to the transferred public key. The Certificate Applicant will submit the CSR via their online Certificate Requesting Account, which employs two-factor authentication, e.g., a USB token with the account administrator's certificate and a PIN.

6.1.4 CA Public Key Delivery to Relying Parties

The Root CA public key certificate MUST be delivered to Relying Parties in a secure fashion to preclude substitution attacks. Acceptable methods for certificate delivery are:

- The Root CA Certificate is delivered as part of a Member's certificate request
- Secure distribution of Root CA certificates through secure out-of-band mechanisms
- Downloading the Root CA certificates from trusted web sites (e.g., PKI-PA web site); The Root CA SHALL calculate the hash of the certificate before posting it on a website so that it can be made available via out-of-band to Relying Parties to validate the posted Root CA certificate

6.1.5 Key Sizes

Key sizes for CA and Member certificates are defined in the OCF Security Specification.

6.1.6 Public Key Parameters Generation and Quality Checking

No stipulation.

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

Key usage for CA and Member certificates are defined in the OCF Security Specification.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

CA private keys within the PKI MUST be protected using FIPS 140-2 Level 3 systems. Private key holders SHALL take necessary precautions to prevent the loss, disclosure, modification, or unauthorized use of such Private Keys in accordance with this CP.

The relevant standard for cryptographic modules is Security Requirements for Cryptographic Modules [FIPS 140-2].

- Root CAs SHALL perform all CA cryptographic operations on cryptographic modules rated at a minimum of FIPS 140-2 level 3 or higher
- Sub-CAs SHALL use a FIPS 140-2 Level 3 or higher validated hardware cryptographic module
- Members SHOULD use a FIPS 140-2 Level 1 or higher validated cryptographic module for their cryptographic operations

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

Multi-person control is enforced to protect the activation data needed to activate CA private keys so that a single person SHALL NOT be permitted to activate or access any cryptographic module that contains the complete CA private signing key.

CA signature keys MUST be backed up only under multi-person control. Access to CA signing keys backed up for disaster recovery MUST be under multi-person control. The names of the parties used for multi-person control MUST be maintained on a list that MUST be made available for inspection during compliance audits.

CAs MAY use “Secret Sharing” to split the private key or activation data needed to operate the private key into separate parts called “Secret Shares” held by individuals called “Shareholders.” Some threshold number of Secret Shares (m) out of the total number of Secret Shares (n) MUST be required to operate the private key. The minimum threshold number of shares (m) needed to sign a CA certificate MUST be 3. The total number of shares (n) used MUST be greater than the minimum threshold number of shares (m).

CAs MAY also use Secret Sharing to protect the activation data needed to activate private keys located at their respective disaster recovery sites. The minimum threshold number of shares (m) needed to sign a CA certificate at a disaster recovery site MUST be 3. The total number of shares (n) used MUST be greater than the minimum threshold number of shares (m).

6.2.3 Private Key Escrow

CA private keys and Member private keys MUST NOT be escrowed.

6.2.4 Private Key Backup

CAs SHALL back up their private keys, under the same multi-person control as the original signature key. The backups allow the CA to be able to recover from disasters and equipment malfunction. At least one copy of the private signature key MUST be stored off-site. Private keys that are backed up MUST be protected from unauthorized modification or disclosure through physical or cryptographic means. Backups, including all activation data needed to activate the cryptographic token containing the private key, MUST be protected with a level of physical and cryptographic protection equal to or exceeding that for cryptographic modules within the CA site, such as at a disaster recovery site or at another secure off-site facility, such as a bank safe. All copies of the CA private signature key MUST be accounted for and protected in the same manner as the original.

Device private keys MAY be backed up or copied, but MUST be held under the control of the Member or other authorized administrator. Backed up device private keys MUST not be stored in plaintext form and storage MUST ensure security controls consistent with the OCF Security Specification the device is compliant with. Members MAY have the option of using enhanced private key protection mechanisms available today including the use of smart cards, secure elements, biometric access devices, and other hardware tokens to store private keys.

6.2.5 Private Key Archival

CA private keys and Member private keys MUST not be archived. Upon expiration of a CA Certificate, the key pair associated with the certificate will be securely retained for a period of at least 5 years using hardware cryptographic modules that meet the requirements of this CP. These CA key pairs MUST not be used for any signing events after the expiration date of the corresponding CA Certificate, unless the CA Certificate has been renewed in terms of this CP.

6.2.6 Private Key Transfer into or from a Cryptographic Module

CA private keys MAY be exported from the cryptographic module only to perform CA key backup procedures as described in CP § 6.2.4. At no time shall the CA private key exist in plaintext outside the cryptographic module.

All other keys MUST be generated by and in a cryptographic module. In the event that a private key is to be transported from one cryptographic module to another, the private key MUST be encrypted during transport; private keys MUST never exist in plaintext form outside the cryptographic module boundary.

Private or symmetric keys used to encrypt other private keys for transport MUST be protected from disclosure.

Entry of a private key into a cryptographic module MUST use mechanisms to prevent loss, theft, modification, unauthorized disclosure, or unauthorized use of such private key.

Processing Centers generating CA or RA private keys on one hardware cryptographic module and transferring them into another shall securely transfer such private keys into the second cryptographic module to the extent necessary to prevent loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys. Such transfers shall be limited to making backup copies of the private keys on tokens.

CAs pre-generating private keys and transferring them into a hardware token, for example transferring generated end-user Member private keys into a smart card, SHALL securely transfer such private keys into the token to the extent necessary to prevent loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys.

6.2.7 Private Key Storage on Cryptographic Module

No stipulation beyond that specified in FIPS 140-2.

6.2.8 Method of Activating Private Key

All CAs SHALL protect the activation data for their private keys against loss, theft, modification, disclosure, or unauthorized use.

CA administrators SHALL be authenticated to the cryptographic token before the activation of the associated private key(s). Acceptable means of authentication include but are not limited to passphrases, PINs or biometrics. Entry of activation data MUST be protected from disclosure (i.e., the data should not be displayed while it is entered).

For device certificates, the device MAY be configured to activate its private key, provided that appropriate physical and logical access controls are implemented for the device. The strength of the security controls MUST be commensurate with the level of threat in the device's environment, and MUST protect the device's hardware, software, private keys and its activation data from compromise.

CA Administrator Activation

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

- Use a smart card, biometric access device, password in accordance with CP § 6.4.1, or security of equivalent strength to authenticate the Administrator before the activation of the private key, which includes, for instance, a password to operate the private key, an operating system logon or screen saver password, or a network logon password; and
- Take commercially reasonable measures for the physical protection of the Administrator's workstation to prevent use of the workstation and its associated private key without the Administrator's authorization

Offline Root CAs Private Key

Once the CA system has been activated, a threshold number of Shareholders MUST be required to supply their activation data in order to activate an offline CA's private key, as defined in CP § 6.2.2. Once the private key is activated, it MUST be active until termination of the session.

Online Subordinate CAs Private Keys

An online CA's private key MUST be activated by a threshold number of Shareholders, as defined in CP § 6.2.2, supplying their activation data (stored on secure media). Once the private key is activated, the private key may be active for an indefinite period until it is deactivated when the CA goes offline.

Member Private Keys

The standards for protecting activation data for Members' private keys MUST be in accordance with the specific obligations appearing in the applicable agreement executed between the OCF and the Member.

6.2.9 Method of Deactivating Private Key

Cryptographic modules that have been activated MUST not be available to unauthorized access. After use, the cryptographic module MUST be deactivated, e.g., via a manual logout procedure or automatically after a period of inactivity. CA cryptographic modules MUST be stored securely when not in use.

When an online CA is taken offline, the CA SHALL remove the token containing the private key from the reader in order to deactivate it, or take similar action based upon the type of hardware used to store the private key.

With respect to the private keys of offline CAs, after the completion of a Key Generation Ceremony, in which such private keys are used for private key operations, the CA SHALL remove the token containing the private keys from the reader in order to deactivate them, or take similar action based upon the type of hardware used to store the private key. Once removed from the reader, tokens MUST be securely stored.

When an online CA is taken offline, the CA SHALL remove the token containing such CA’s private key from the reader in order to deactivate it.

When deactivated, private keys MUST be kept in encrypted form only.

6.2.10 Method of Destroying Private Key

Private keys MUST be destroyed in a way that prevents their theft, disclosure, or unauthorized use.

Upon termination of the operations of a CA, individuals in trusted roles SHALL decommission the CA private signature keys by deleting it using functionality of the token containing such CA’s private key so as to prevent its recovery following deletion, or the loss, theft, modification, disclosure, or unauthorized use of such private key. CA private keys MUST be destroyed in a manner that reasonably ensures that there are no residuals remains of the key that could lead to the reconstruction of the key.

For Root CAs, PKI-PA security personnel SHALL witness this process.

Members MAY destroy their private signature keys when they are no longer needed or when the certificates to which they correspond expire or are revoked. Physical destruction of hardware is not required.

6.2.11 Cryptographic Module Rating

See CP § 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

CAs MAY archive their public keys in accordance with CP § 5.5.1.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

CA and Member Certificate validity periods are define in the OCF Security Specification.

Validity periods MUST be nested such that the validity periods of issued certificates MUST be contained within the validity period of the issuing CA.

As necessary to ensure the continuity and security of the PKI, OCF SHALL commission new CAs.

PKI Participants SHALL cease all use of their key pairs after their usage periods have expired.

6.4 Activation data

6.4.1 Activation Data Generation and Installation

CAs SHALL generate and install activation data for their private keys and SHALL use methods that protect the activation data to the extent necessary to prevent the loss, theft, modification, disclosure, or unauthorized use of such activation data.

To the extent passwords are used as activation data, CAs activation participants SHALL generate passwords that cannot easily be guessed or cracked by dictionary attacks. Participants may not need to generate activation data, for example if they use biometric access devices.

6.4.2 Activation Data Protection

CAs SHALL protect the activation data for their private keys using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys.

CAs SHALL use multi-party control in accordance with CP § 6.2.2. CAs SHALL provide the procedures and means to enable Shareholders to take the precautions necessary to prevent the loss, theft, modification, disclosure, or unauthorized use of the Secret Shares that they possess. Shareholders SHALL not:

- Copy, disclose, or make the Secret Share available to a third party, or make any unauthorized use of it whatsoever
- Disclose their or any other person’s status as a Shareholder to any third party

The Secret Shares and any information disclosed to the Shareholder in connection with their duties as a Shareholder SHALL constitute confidential/private information.

CAs SHALL include in their disaster recovery plans provisions for making Secret Shares available at a disaster recovery site after a disaster (Note, the important aspect of disaster recovery vis-à-vis shares is that a process exists for making the necessary number of shares available, even if the requisite shareholders are not available). CAs SHALL maintain an audit trail of Secret Shares, and Shareholders SHALL participate in the maintenance of an audit trail.

6.4.3 Other Aspects of Activation Data

Activation Data Transmission

To the extent activation data for their private keys are transmitted, Activation Data Participants SHALL protect the transmission using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys. To the extent desktop computer or network logon user name/password combination is used as activation data for an end-user Member, the passwords transferred across a network MUST be protected against access by unauthorized users.

Activation Data Destruction

Activation data for CA private keys MUST be decommissioned using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of the private keys protected by such activation data. After the record retention periods in CP § 5.5.2 lapses, CAs SHALL decommission activation data by overwriting and/or physical destruction.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

CAs SHALL ensure that the systems maintaining CA software and data files are Trustworthy Systems secure from unauthorized access, which can be demonstrated by compliance with audit criteria applicable under CP § 5.4.1. In addition, CAs SHALL limit access to production servers to those individuals with a valid business reason for access. General application users SHALL not have accounts on the production servers.

CAs SHALL have production networks logically separated from other components. This separation prevents network access except through defined application processes. CAs SHALL use firewalls to protect the production network from internal and external intrusion and limit the nature and source of network activities that may access production systems.

To the extent that passwords are used, CAs SHALL require the use of passwords with a minimum character length and a combination of alphanumeric and special characters, and SHALL require that passwords be changed on a periodic basis and whenever necessary. Direct access to a CA’s database maintaining the CA’s repository MUST be limited to Trusted Persons having a valid business reason for such access.

Computer security controls are required to ensure CA operations are performed as specified in this policy. The following computer security functions MAY be provided by the operating system, or through a combination of operating system, software, and physical safeguards:

- Require authenticated logins
- Provide discretionary access control
- Provide a security audit capability
- Enforce access control for CA services and PKI roles
- Enforce separation of duties for PKI roles
- Require identification and authentication of PKI roles and associated identities
- Prohibit object reuse or require separation for CA random access memory
- Require use of cryptography for session communication and database security
- Archive CA history and audit data
- Require self-test security-related CA services
- Require a trusted path for identification of PKI roles and associated identities
- Require a recovery mechanism for keys and the CA system
- Enforce domain integrity boundaries for security-critical processes.

For other CAs operating under this policy, the computer security functions listed below are required. These functions MAY be provided by the operating system, or through a combination of operating system, software, and physical safeguards. The CA and its ancillary parts SHALL include the following functionality:

- Authenticate the identity of users before permitting access to the system or applications
- Manage privileges of users to limit users to their assigned roles
- Generate and archive audit records for all transactions (see CP § 5.4)
- Enforce domain integrity boundaries for security critical processes
- Support recovery from key or system failure

For certificate status servers operating under this policy, the computer security functions listed below are required:

- Authenticate the identity of users before permitting access to the system or applications
- Manage privileges of users to limit users to their assigned roles
- Enforce domain integrity boundaries for security critical processes
- Support recovery from key or system failure

For remote workstations used to administer the CAs, the computer security functions listed below are required:

- Authenticate the identity of users before permitting access to the system or applications
- Manage privileges of users to limit users to their assigned roles
- Generate and archive audit records for all transactions (see CP § 5.4)
- Enforce domain integrity boundaries for security critical processes
- Support recovery from key or system failure

All communications between any PKI trusted role and the CA MUST be authenticated and protected from modification.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The system development controls for the CA are as follows:

- The CA SHALL use software that has been designed and developed under a formal, documented development methodology.
- Hardware and software procured to operate the CA MUST be purchased in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the vendor cannot identify the PKI component that will be installed on a particular device).
- Hardware and software developed specifically for the CA MUST be developed in a controlled environment, and the development process MUST be defined and documented. This requirement does not apply to commercial off-the-shelf hardware or software.

- The CA hardware and software MUST be dedicated to performing one task: the CA. There shall be no other applications, hardware devices, network connections, or component software installed that are not parts of the CA operation. Where the CA operation supports multiple CAs, the hardware platform MAY support multiple CAs.
- Proper care MUST be taken to prevent malicious software from being loaded onto the CA equipment. All applications required to perform the operation of the CA MUST be obtained from documented sources.
- Hardware and software updates MUST be purchased or developed in the same manner as the corresponding original equipment, and MUST be installed by trusted and trained personnel in a defined manner.

6.6.2 Security Management Controls

The configuration of the CA system, in addition to any modifications and upgrades, MUST be documented and controlled. There MUST be a mechanism for detecting unauthorized modification to the software or configuration. The CA software, when first loaded, MUST be verified as being that supplied from the vendor, with no modifications, and be the version intended for use.

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 Network Security Controls

A network guard, firewall, or filtering router MUST protect network access to CA equipment. The network guard, firewall, or filtering router MUST limit services allowed to and from the CA equipment to those required to perform CA functions.

Protection of CA equipment MUST be provided against known network attacks. All unused network ports and services MUST be turned off. Any network software present on the CA equipment MUST be necessary to the functioning of the CA application.

Any boundary control devices used to protect the network on which PKI equipment is hosted MUST deny all but the necessary services to the PKI equipment.

Repositories, certificate status servers, and remote workstations used to administer the CAs MUST employ appropriate network security controls. Networking equipment MUST turn off unused network ports and services. Any network software present MUST be necessary to the functioning of the equipment.

The CA SHALL establish connection with a remote workstation used to administer the CA only after successful authentication of the remote workstation at a level of assurance commensurate with that of the CA.

6.8 Time-Stamping

Certificates, CRLs, and other revocation database entries MUST contain time and date information. Such time information need not be cryptographic-based. Asserted times MUST be accurate to within three minutes. Electronic or manual procedures MAY be used to maintain system time. Clock adjustments are auditable events (see CP § 5.4.1).

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate Profile

All OCF certificates MUST conform to profile requirements defined in the OCF Security Specification.

7.2 CRL Profile

No stipulation.

7.3 OCSP Profile

OCSP is used to check the revocation status of certificates. OCSP Responses MUST conform to [RFC5019] and MUST either be:

- Signed by the CA that issued the Certificates whose revocation status is being checked, or
- Signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked. Such OCSP Responder signing Certificate MUST contain the extension id-pkix-ocsp-nocheck as defined by [RFC2560].

7.3.1 Version Number(s)

OCSP responses MUST support use of OCSP version 1 as defined by [RFC2560] and [RFC5019].

7.3.2 OCSP Extensions

Critical OCSP extensions MUST NOT be used.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or Circumstances of Assessment

CAs operating under this policy SHALL be subject to a periodic compliance audit at least once per year. Compliance Audits are conducted at the sole expense of the audited entity. The PKI-PA MAY require a periodic compliance audit of CAs operating under this policy as stated in CP § 8.4.

8.2 Identity/Qualifications of Assessor

The CA MAY select an auditor, subject to the qualifications described herein. The auditor SHALL demonstrate competence in the field of compliance audits, and SHALL be thoroughly familiar with the CA's CPS and this CP. The auditor SHALL be a Certified Information System Auditor (CISA), or IT security specialist, and a PKI subject matter specialist who can offer input regarding acceptable risks, mitigation strategies, and industry best practices.

Audits performed by an independent third party audit firm MUST be performed by a certified public accounting firm with demonstrated expertise in computer security or by accredited computer security professionals employed by a competent security consultancy. Such firm SHALL also have demonstrated expertise in the performance of IT security and PKI compliance audits and the selected Audit Scheme.

The qualified audit firm SHALL be bound by law, government regulation, or professional code of ethics and SHALL maintain Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage.

8.3 Assessor's Relationship to Assessed Entity

The compliance auditor either SHALL be a private firm that is independent from the CA being audited, or it SHALL be sufficiently organizationally separated from those entities to provide an unbiased, independent evaluation. Compliance auditors SHALL not have a conflict of interest that hinders their ability to perform auditing services. To insure independence and objectivity, the compliance auditor may not have served the entity in developing or maintaining the entity's CA Facility or CPS. The PKI-PA SHALL determine whether a compliance auditor meets these requirements.

8.4 Topics Covered by Assessment

CA's SHALL perform an annual compliance audit that MUST be a WebTrust for Certification Authorities or an equivalent audit standard approved by the PKI-PA which includes: A Report of Policies and Procedures in Operation and Test of Operational Effectiveness. The purpose of the annual compliance audit shall be to verify that a CA complies with all the requirements of the current versions of this CP and the CA's CPS.

All aspects of the CA operation MUST be subject to the compliance audit and SHOULD address the items listed below. A WebTrust for Certification Authorities or equivalent will satisfy this requirement.

- Identify foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes
- Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes
- Assess the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats

In addition to compliance audits, if the PKI-PA has a reasonable belief that a CA is not operating in conformance with this CP, the PKI-PA SHALL be entitled, to perform other reviews and investigations, which include, but are not limited to:

- A “Security and Practices Review,” which consists of a review of a CA’s secure facility, security documentation, CPS, and any other appropriate material to ensure that the CA meets the CP.
- An “Exigent Audit/Investigation” on CAs, including, for example, in the event the PKI-PA has reason to believe that the audited entity has failed to meet the CP Standards, has experienced an incident or Compromise, or has acted or failed to act, such that the audited entity’s failure, the incident or Compromise, or the act or failure to act poses an actual or potential threat to the security or integrity of the PKI.
- A “Supplemental Risk Management Reviews” on CAs following incomplete or exceptional findings in a Compliance Audit.

The PKI-PA SHALL be entitled to delegate the performance of these audits, reviews, and investigations to (a) the Superior Entity of the entity being audited, reviewed, or investigated or (b) a third-party audit firm. Entities that are subject to an audit, review, or investigation SHALL provide cooperation with the PKI-PA and the personnel performing the audit, review, or investigation.

8.5 Actions Taken as a Result of Deficiency

When the compliance auditor finds a discrepancy between the requirements of this CP or the stipulations in the CPS and the design, operation, or maintenance of the PKI Authorities, the following actions MUST be performed:

- The compliance auditor SHALL note the discrepancy;
- The compliance auditor SHALL notify the parties identified in CP § 8.6 of the discrepancy; and
- The party responsible for correcting the discrepancy will propose a remedy, including expected time for completion, to the parties identified in CP § 8.6.

In the event the audited entity fails to develop a corrective action plan or implement it, or if the report reveals exceptions or deficiencies that the PKI-PA reasonably believes poses an immediate threat to the security or integrity of the PKI, then PKI-PA:

- SHALL determine whether revocation and compromise reporting are necessary
- SHALL be entitled to suspend services to the audited entity

- If necessary, MAY terminate such services subject to this CP and the terms of the audited entity’s contract

8.6 Communication of Results

Following any Compliance Audit, the audited entity SHALL provide the PKI-PA with the Audit Compliance Report and identification of corrective measures within 30 days of completion. A special compliance audit MAY be required to confirm the implementation and effectiveness of the remedy.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

Members MAY be charged a fee for the issuance, management, and renewal of certificates.

9.1.2 Certificate Access Fees

CAs SHALL not charge a fee as a condition of making a Certificate available in a repository or otherwise making Certificates available to Relying Parties.

9.1.3 Revocation or Status Information Access Fees

CAs SHALL not charge a fee as a condition of making CRLs available in a repository or otherwise available to Relying Parties.

9.1.4 Fees for Other Services

No stipulation.

9.1.5 Refund Policy

Refund policies SHOULD be stipulated in the appropriate agreement (e.g., Member Agreement).

9.2 Financial Responsibility

9.2.1 Insurance Coverage

PKI Participants SHOULD maintain a commercially reasonable level of insurance coverage for errors and omissions, either through an errors and omissions insurance program with an insurance carrier or a self-insured retention.

9.2.2 Other Assets

CAs SHALL have sufficient financial resources to maintain their operations and perform their duties, and they SHALL be reasonably able to bear the risk of liability to Members and Relying Parties.

9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The following Member information MUST be kept confidential and private:

- Certificate Application records
- CA application status, whether approved or disapproved
- Transactional records (both full records and the audit trail of transactions)

- Audit trail records
- Audit reports
- Contingency planning and disaster recovery plans
- Security measures controlling the operations of CA hardware and software

9.3.2 Information not Within the Scope of Confidential Information

PKI Participants acknowledge that Certificates, Certificate revocation and other status information, repositories, and information contained within them are not considered confidential/private information. Information not expressly deemed confidential/private information under CP § 9.3.1 MUST be considered neither confidential nor private.

9.3.3 Responsibility to Protect Confidential Information

The PKI Participants receiving private information SHALL secure it from compromise and disclosure to third parties.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

CAs SHALL have a Privacy Plan to protect personally identifying information from unauthorized disclosure.

9.4.2 Information Treated as Private

CAs acquiring services under this policy SHALL protect all Members' personally identifiable information from unauthorized disclosure. Records of individual transactions MAY be released upon request of any Members involved in the transaction or their legally recognized agents. The contents of the archives maintained by CAs operating under this policy SHALL not be released except as required by law.

9.4.3 Information not Deemed Private

Information included in certificates is deemed pubic information and is not subject to protections outlined in § 9.4.2.

9.4.4 Responsibility to Protect Private Information

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

9.4.5 Notice and Consent to Use Private Information

The PKI-PA or CAs are not required to provide any notice or obtain the consent of the Member in order to release private information in accordance with other stipulations in § 9.4.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

The PKI-PA or CAs SHALL not disclose private information to any third party unless authorized by this policy, required by law, government rule or regulation, or order of a court of competent jurisdiction.

9.4.7 Other Information Disclosure Circumstances

No stipulations.

9.5 Intellectual Property Rights

The PKI-PA retains all Intellectual Property Rights in and to this CP.

CAs retain all Intellectual Property Rights in and to the Certificates and revocation information that they issue.

A Certificate Applicant retains all rights it has (if any) in any trademark, service mark, or trade name contained in any Certificate Application and distinguished name within any Certificate issued to such Certificate Applicant.

Private keys corresponding to Certificates of CAs and Members are the property of the CAs and Members that are the respective Subjects of these Certificates. Secret Shares of a CA's private key are the property of the CA, and the CA retains all Intellectual Property Right in and to such Secret Shares.

Without limiting the generality of the foregoing, the root public keys and Certificates containing them, including all CA and Member public keys and certificates containing them, are the property of the PKI-PA. The PKI-PA licenses software and hardware manufacturers to reproduce such public key Certificates to place copies in compliant hardware devices or software.

9.6 Representations and Warranties

The PKI-PA SHALL:

- Approve the CPS for each CA that issues certificates under this policy
- Review periodic compliance audits to ensure that CAs are operating in compliance with their approved CPSs
- Review name space control procedures to ensure that distinguished names are uniquely assigned for all certificates issued under this CP
- Publicly distribute this CP
- Coordinate modifications to this CP to ensure continued compliance by CAs operating under approved CPSs

9.6.1 CA Representations and Warranties

CAs operating under this CP SHALL warrant that:

- The CA procedures are implemented in accordance with this CP
- The CA will provide their CPS to the PKI-PA, as well as any subsequent changes, for conformance assessment
- The CA operations are maintained in conformance to the stipulations of the approved CPS
- Any certificate issued is in accordance with the stipulations of this CP
- There are no material misrepresentations of fact in the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate

- There are no errors in the information in the Certificate that were introduced by the entities approving the Certificate Application as a result of a failure to exercise reasonable care in managing the Certificate Application
- Their Certificates meet all material requirements of this CP and the applicable CPS
- The revocation of certificates in accordance with the stipulations in this CP
- Revocation services (when applicable) and use of a repository conform to all material requirements of this CP and the applicable CPS in all material aspects.

9.6.2 RA Representations and Warranties

RAs that perform registration functions under this CP SHALL warrant that:

- The RA complies with the stipulations of this CP
- The RA complies with and maintains its operations in conformance to the stipulations of the approved CPS
- There are no material misrepresentations of fact in the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate
- There are no errors in the information in the Certificate that were introduced by the entities approving the Certificate Application as a result of a failure to exercise reasonable care in managing the Certificate Application
- Their Certificates meet all material requirements of this CP and the applicable CPS
- Revocation services (when applicable) and use of a repository conform to all material requirements of this CP and the applicable CPS in all material aspects

9.6.3 Member Representations and Warranties

Members SHALL sign an agreement containing the requirements the Member shall meet including protection of their private keys and use of the certificates before being issued the certificates. In addition, Members SHALL warrant that:

- The Member SHALL abide by all the terms, conditions, and restrictions levied on the use of their private keys and certificates
- Each digital signature created using the private key corresponding to the public key listed in the Certificate is the digital signature of the Member and the Certificate has been accepted and is operational (not expired or revoked) at the time the digital signature is created
- Member’s private keys are protected from unauthorized use or disclosure
- All representations made by the Member in the Certificate Application the Member submitted are true
- All information supplied by the Member and contained in the Certificate is true
- The Certificate is being used exclusively for authorized and legal purposes, consistent with all material requirements of this CP
- The Member will promptly notify the appropriate CA upon suspicion of loss or compromise of their private key(s)
- The Member is an end-user Member and not a CA, and is not using the private key corresponding to any public key listed in the Certificate for purposes of

digitally signing any Certificate (or any other format of certified public key) or CRL, as a CA or otherwise

9.6.4 Relying Party Representations and Warranties

This CP does not specify the steps a Relying Party SHOULD take to determine whether to rely upon a certificate. The Relying Party decides, pursuant to its own policies, what steps to take. The CA merely provides the tools (i.e., certificates and CRLs) needed to perform the trust path creation, validation, and CP mappings that the Relying Party may wish to employ in its determination. Relying Parties acknowledge that they have sufficient information to make an informed decision as to the extent to which they choose to rely on the information in a Certificate, that they are solely responsible for deciding whether or not to rely on such information, and that they SHALL bear the legal consequences of their failure to perform the Relying Party obligations in terms of this CP.

9.6.5 Representations and Warranties of Other Participants

No stipulations.

9.7 Disclaimers of Warranties

To the extent permitted by applicable law, Member Agreements MUST disclaim OCF's and the applicable Affiliate's possible warranties, including any warranty of merchantability or fitness for a particular purpose.

9.8 Limitations of Liability

The liability (and/or limitation thereof) of Members MUST be as set forth in the applicable Member Agreements.

9.9 Indemnities

To the extent permitted by applicable law, Members are required to indemnify CAs for:

- Falsehood or misrepresentation of fact by the Member on its Certificate Application
- Failure by the Member to disclose a material fact on the Certificate Application, if the misrepresentation or omission was made negligently or with intent to deceive any party
- The Member's failure to take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the Member's private key(s)
- The Member's use of a name (including that which infringes upon the Intellectual Property Rights of a third party)

9.10 Term and Termination

9.10.1 Term

The CP becomes effective when approved by the PKI-PA. Amendments to this CP become effective upon publication. This CP has no specified term.

9.10.2 Termination

This CP as amended from time to time MUST remain in force until it is replaced by a new version. Termination of this CP is at the discretion of the PKI-PA.

9.10.3 Effect of Termination and Survival

Upon termination of this CP, PKI Participants are nevertheless bound by its terms for all certificates issued for the remainder of the validity periods of such certificates.

9.11 Individual Notices and Communications with Participants

Unless otherwise specified by agreement between the parties, PKI participants SHALL use commercially reasonable methods to communicate with each other, taking into account the criticality and subject matter of the communication.

9.12 Amendments

9.12.1 Procedure for Amendment

The PKI-PA SHALL review this CP at least once every year. Corrections, updates, or changes to this CP MUST be made available as per CP § 9.12.2. Suggested changes to this CP MUST be communicated to the contact in CP § 1.5.2; such communication MUST include a description of the change, a change justification, and contact information for the person requesting the change.

9.12.2 Notification Mechanism and Period

The PKI-PA reserves the right to amend the CP without notification for amendments that are not material, including without limitation corrections of typographical errors, changes to URLs, and changes to contact information. The PKI-PA's decision to designate amendments as material or non-material SHALL be within the PKI-PA's sole discretion.

9.12.3 Circumstances Under Which OID Must be Changed

Object Identifiers (OIDs) will be changed if the PKI-PA determines that a change in the CP reduces the level of assurance provided. If the PKI-PA determines that a change is necessary in the OID corresponding to a Certificate Policy, the amendment MUST contain new object identifiers for the Certificate policies corresponding to each Class of Certificate. Otherwise, amendments shall not require a change in Certificate policy object identifier.

9.13 Dispute Resolution Provisions

The PKI-PA SHALL facilitate the resolution between entities when conflicts arise as a result of the use of certificates issued under this policy.

9.14 Governing Law

Subject to any limits appearing in applicable law, the laws of the State of Colorado, U.S.A., SHALL govern the enforceability, construction, interpretation, and validity of this CP, irrespective of contract or other choice of law provisions and without the requirement to establish a commercial nexus in Colorado, USA. This choice of law is made to ensure uniform procedures and interpretation for all Participants, no matter where they are located.

This governing law provision applies only to this CP. Agreements incorporating the CP by reference MAY have their own governing law provisions, provided that this CP § 9.14 governs the enforceability, construction, interpretation, and validity of the terms of the CP separate and apart from the remaining provisions of any such agreements, subject to any limitations appearing in applicable law.

9.15 Compliance with Applicable Law

This CP is subject to applicable national, state, local, and foreign laws, rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information. All CAs operating under this policy are required to comply with applicable law.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation

9.16.2 Assignment

No stipulation

9.16.3 Severability

Should it be determined that one section of this CP is incorrect or invalid, the other sections of this CP shall remain in effect until the CP is updated. The process for updating this CP is described in CP § 9.12.

In the event that a clause or provision of this CP is held to be unenforceable by a court of law or other tribunal having authority, the remainder of the CP shall remain valid.

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

No stipulation

9.16.5 Force Majeure

To the extent permitted by applicable law, OCF PKI agreement (e.g., Ecosystem Member Agreements) shall include a force majeure clause protecting OCF and the applicable Affiliate.

9.17 Other Provisions

No stipulation.

10 REFERENCES

[RFC 2119] Key Words for use in RFCs to Indicate Requirement Level, IETF (Bradner), March 1997. http://www.ietf.org/rfc/rfc2119.txt

[RFC 2560] X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, IETF (Myers, Ankney, Malpani, Galperin, Adams), June 1999. http://www.ietf.org/rfc/rfc2560.txt

[RFC 3647] Internet X.509 PKI Certificate Policy and Certification Practices Framework, IETF (Chokhani, Ford, Sabett, Merrill, and Wu), November 2003. http://www.ietf.org/rfc/rfc3647.txt

[RFC 5019] The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments, IETF (Deacon, Hurst), September 2007. http://www.ietf.org/rfc/rfc5019.txt

[RFC 5280] Internet X.509 PKI Certificate and Certification Revocation List (CRL) Profile, IETF (Cooper, Santesson, Farrell, Boeyen, Housley, and Polk), May 2008. http://www.ietf.org/rfc/rfc5280.txt

[FIPS 140-2] Security Requirements for Cryptographic Modules, FIPS 140-2, May 25, 2001. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

11 GLOSSARY

This document uses the following terms:

Audit Requirements Guide A document that sets forth the security and audit requirements and practices for CAs.

Certificate A message that, at least, states a name or identifies the CA, identifies the Member, contains the Member's public key, identifies the Certificate's Validity Period, contains a Certificate serial number, and is digitally signed by the CA that issued the certificate.

Certificate Applicant An individual or organization that requests the issuance of a Certificate by a CA.

Certificate Application A request from a Certificate Applicant (or authorized agent of the Certificate Applicant) to a CA for the issuance of a Certificate.

Certificate Chain An ordered list of Certificates containing a Member Certificate and one or more CA Certificates, which terminates in a root Certificate.

Control Objectives Criteria that an entity SHALL meet in order to satisfy a Compliance Audit.

Certificate Polikcy (CP) The principal statement of policy governing the PKI.

Certificate Revocation List (CRL) A periodically (or exigently) issued list, digitally signed by a CA, of identified Certificates that have been revoked prior to their expiration dates. The list generally indicates the CRL issuer's name, the date of issue, the date of the next scheduled CRL issue, the revoked Certificates' serial numbers, and the specific times and reasons for revocation.

Certificate Signing Request (CSR) A message conveying a request to have a Certificate issued.

Certification Authority (CA) An entity authorized to issue, manage, revoke, and renew Certificates in the PKI.

Certification Practice Statement (CPS) A statement of the practices that a CA employs in approving or rejecting Certificate Applications and issuing, managing, and revoking Certificates.

Certificate Requesting Account (CRA) The online portal to assist Certificate Applicants in requesting Certificates.

Compliance Audit A periodic audit that a CA system undergoes to determine its conformance with PKI requirements that apply to it.

Compromise A violation of a security policy, in which an unauthorized disclosure of, or loss of control over, sensitive information has occurred. With respect to private keys, a Compromise is a loss, theft, disclosure, modification, unauthorized use, or other compromise of the security of such private key.

CRL Usage Agreement An agreement setting forth the terms and conditions under which a CRL or the information in it can be used.

Ecosystem Member Agreement An agreement used by a CA setting forth the terms and conditions under which an individual or organization acts as a Member.

Exigent Audit/Investigation An audit or investigation by the OCF where the OCF has reason to believe that an entity's failure to meet PKI Standards, an incident or Compromise relating to the entity, or an actual or potential threat to the security of the PKI posed by the entity has occurred.

Intellectual Property Rights Rights under one or more of the following: copyright, patent, trade secret, trademark, or any other intellectual property rights.

Key Generation Ceremony A procedure whereby a CA's key pair is generated, its private key is backed up, and/or its public key is certified.

Member The entity who requests a Certificate (e.g., a manufacturer). The Member is capable of using, and is authorized to use, the private key that corresponds to the public key listed in the Certificate.

PKI Participant An individual or organization that is one or more of the following the OCF, a CA, a Member, or a Relying Party.

PKCS #10 Public-Key Cryptography Standard #10, developed by RSA Security Inc., which defines a structure for a Certificate Signing Request.

PKCS #8 Public-Key Cryptography Standard #8, developed by RSA Security Inc., which defines a secure means for the transfer of private keys.

Processing Center A secure facility created by an appropriate organization (e.g., Symantec) that houses, among other things, the cryptographic modules used for the issuance of Certificates.

Public Key Infrastructure (PKI) The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a Certificate-based public key cryptographic system.

Relying Party An individual or organization that acts in reliance on a certificate and/or a digital signature.

RSA (Algorithm) A public key cryptographic system invented by Rivest, Shamir, and Adelman.

Secret Share A portion of the activation data needed to operate the private key, held by individuals called “Shareholders.” Some threshold number of Secret Shares (n) out of the total number of Secret Shares (m) shall be required to operate the private key.

Secret Sharing The practice of splitting a CA private key or the activation data to operate a CA private key in order to enforce multi-person control over CA private key operations.

Security Repository OCF’s database of relevant security information accessible on-line.

Sub domain The portion of the PKI under control of an entity and all entities subordinate to it within the hierarchy.

Sub domain Participants An individual or organization that is one or more of the following within the Subdomain: the OCF, a Member, or a Relying Party.

Subject The holder of a private key corresponding to a public key. The term “Subject” can, in the case of a Device Certificate, refer to the Member requesting the device certificate.

Superior Entity An entity above a certain entity within the PKI.

Trusted Person An employee, contractor, or consultant of an entity within the PKI responsible for managing infrastructural trustworthiness of the entity, its products, its services, its facilities, and/or its practices.

Trusted Position The positions within the PKI that MUST be held by a Trusted Person.

Trustworthy System Computer hardware, software, and procedures that are reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy.

Validity Period The period starting with the date and time a Certificate is issued (or on a later date and time certain if stated in the Certificate) and ending with the date and time on which the Certificate expires or is earlier revoked.

12 ABBREVIATIONS AND ACRONYMS

This document uses the following abbreviations:

CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRA	Certificate Requesting Account
CRL	Certificate Revocation List
CSR	Certificate Signing Request
FIPS	Federal Information Processing Standards
IETF	Internet Engineering Task Force
ISO	Independent System Operators
LSVA	Logical Security Vulnerability Assessment
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OSU	Online Sign-up
PA	Policy Authority
PKCS	Public-Key Cryptography Standard
PKI	Public Key Infrastructure
RFC	Request for comment
RA	Registration Authority
RSA	Rivest, Shamir, Adelman