CableLabs New PKI Certificate Policy
Version 1.0
8/25/2017

Table of Contents

1 Introduction

1.1 Overview

The Data-Over-Cable Service Interface Specifications (DOCSIS®) allow transparent bi-directional transfer of Internet Protocol (IP) traffic between the cable head-end and customer located cable modem (CM), over a hybrid-fiber/coax (HFC) cable network. The ability to securely provision CMs with operator subscription data over the HFC requires secure connections between the CM and the CM termination system (CMTS) at the cable head-end. This secure connection is the foundation that provides user data confidentiality and software download integrity. Paramount to the achievement of these objectives is the establishment of an efficient and effective trust infrastructure within the ecosystem. For DOCSIS 3.1 [1], Cable Television Laboratories, Inc. (CableLabs®) has established a Public Key Infrastructure (PKI) to support CM Certificate-based device authentication, remote provisioning, and secure software download features. For the PKI requirements relating to Remote PHY, which allows the CMTS to support an IP-based digital HFC plant, see the Remote PHY specification [2].

Cable Operators relying on the CableLabs PKI need to be able to determine the degree of trust which can be placed in the authenticity and integrity of the Certificates issued by the CableLabs PKI Certification Authority (CA). Information upon which such determination can be made is documented here in the CableLabs PKI Certificate Policy (CP).

This document defines the policies by which the CableLabs PKI will be governed by the CableLabs PKI Policy Authority (PKI-PA).

This CP comprises the policy framework for the CableLabs PKI and is consistent with the Internet X.509 PKI Certificate Policy and Certification Practices Framework [RFC 3647] [3]. It governs the operations of the PKI components by all individuals and entities within the infrastructure (collectively, PKI Participants). It provides the requirements that PKI Participants must meet when issuing and managing CAs, 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 must operate to issue Certificates. Where “operate” includes Certificate management (i.e., approval, issuance, and revocation) of issued 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.

In addition, this CP acts as an umbrella document establishing baseline requirements and applies consistently throughout the entire CableLabs PKI, thereby providing a uniform level of trust throughout the applicable community. It describes the overall business, legal, and technical infrastructure of the CableLabs PKI. More specifically, it describes the:

- Appropriate applications for, and the assurance levels associated with, the PKI Certificates
- Obligations of CAs
- Requirements for Compliance Audit (Audit) and related security and practices reviews
- Methods to confirm the identity of Certificate Applicants

- Operational procedures for Certificate lifecycle services: Certificate Applications, 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 (CRL) content
- Ancillary agreements, such as the Digital Certificate Authorization Agreement (DCAA) and Root CA Hosting Agreement

Throughout this CP, the words that are used to define the significance of particular requirements are:

"must"	This word, or the word "require", means that the definition is an absolute requirement of this CP.
"must not"	This phrase means that the definition is an absolute prohibition of this CP.
"should"	This word 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 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 word "optional", means that an item is truly discretionary.

1.2 References

This CP uses the following references:

Ref #	Doc Number	Reference Title
[1]	CM-SP-SECv3.1-I06-160602	Data-Over-Cable Service Interface Specifications, DOCSIS 3.1, Security Specification. CM-SP-SECv3.1-I06-160602
[2]	CM-SP-R-PHY-I06-170111	Data-Over-Cable Service Interface Specifications, DCA – MHAv2, Remote PHY Specification. CM-SP-R-PHY-I06-170111
[3]	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
[4]	X.501	ITU-T Recommendation X.501 (10/2016): Information Technology - Open Systems Interconnection - The Directory: Models.
[5]	ISO 3166-1	International Organization for Standardization (ISO) 3166-1 2013. https://www.iso.org/iso-3166-country-codes.html
[6]	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

Ref #	Doc Number	Reference Title
[7]	FIPS 140-2	Security Requirements for Cryptographic Modules, FIPS 140-2, May 25, 2001. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
[8]	RFC 6960	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, IETF (Myers, Ankney, Malpani, Galperin, Adams), June 2013.

1.3 Document Name and Identification

This document is the CableLabs PKI CP. CableLabs, acting as a Policy Authority (PA), in the future, may assign a policy object identifier value extension for the class of Certificate specified within this CP.

1.4 PKI Participants

The CableLabs PKI shown in Figure 1 is comprised of a two-tier infrastructure with an offline Root CA at tier 1, the apex of the hierarchy. The Root CA issues the tier 2 Subordinate CA (Sub-CA) Certificates. The Sub-CAs issue the end-entity device Certificates,Code Verification Certificates (CVCs) and end-entity server Certificates to authorized Subscribers (i.e., Manufacturers (MFR) and Cable Operators). MFRs embed the device Certificates into DOCSIS 3.1 compliant CMs,use the CVC to digitally sign the CM software and use the server certificates for Cable Operator owned servers. Cable Operators use the CVC to apply a digital co-signature onto the MFR signed CM software. The hosted Sub-CAs are hosted at a certified WebTrust company and can issue device Certificates to MFRs via an online Certificate Requesting Account (CRA). Low volume end-entity device certificates, CVCs, both signer and co-signer, and server certificates are issued at CableLabs in a Key Generation Ceremony.

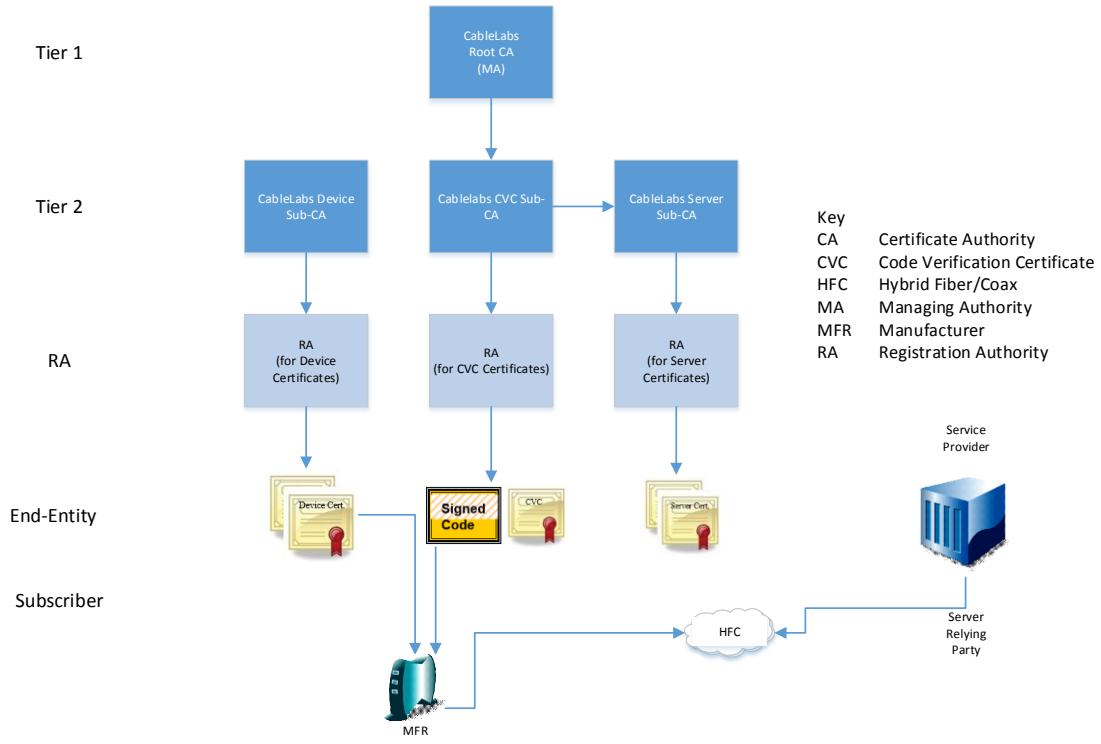

Figure 1: CableLabs PKI Architecture

1.4.1 Certification Authorities (CAs)

The CAs in the CableLabs PKI fall into four categories: (1) the Root CA, which issues the Sub-CA Certificates; (2) the device Sub-CA, which issues end-entity device Certificates via a CRA; (3) the CVC Sub-CA which issues end-entity CVCs to Subscribers; and (4) the service provider Sub-CA for issuing server certifcicates,. The CAs are authorized to issue, manage, revoke, and renew Certificates and are responsible for:

- Developing and maintaining its Certification Practice Statements (CPSs)
- Issuing compliant Certificates
- Securing delivery of Certificates to its Subscribers
- Revoking Certificates
- Generating, protecting, operating, and destroying CA private keys
- Managing all aspects of the CA services, operations, and infrastructure related to Certificates issued under this CP and ensuring that they are performed in accordance with the requirements, representations, and warranties of this CP
- Acting as a trusted party to facilitate the confirmation of the binding between a public key and the identity, and/or other attributes, of the “Subject” of the Certificate

1.4.2 Registration Authority (RA)

The RA is the entity that collects and verifies each Subscriber’s identity and the information that is to be entered into the public key Certificate. The RA interacts with the CA to enter and approve the Subscriber Certificate request information. CableLabs, within the scope of authorizing MFRs to receive a CRA, acts as a RA.

1.4.3 Subscribers

In the CableLabs PKI, the Subscriber is the entity named in the DCAA. An authorized representative of the Subscriber, as a Certificate Applicant, completes the Certificate issuance process established by the CA. In response, the CA confirms the identity of the Certificate Applicant and either approves or denies the Certificate Application. If approved, the Subscriber may request device Certificates, via a web-based CRA or directly from the Device Sub-CA, for use in DOCSIS 3.1 compliant devices, request a CVC directly from the CVC Sub-CA for use in a code signing agent to sign or, in the case of the Cable Operator, co-sign CM software, or request a server certificate directly from the Service Provider Sub-CA.

CableLabs requires that Subscribers adopt the appropriate CableLabs requirements and any additional Certificate management practices to govern the Subscriber’s practice for requesting Certificates and handling the corresponding private keys. The Subscriber agrees to be bound by its obligations through execution of the CableLabs DCAA.

CAs, technically, are also Subscribers of Certificates within a PKI, either as a Root CA issuing a self-signed Certificate to itself, or as a Sub-CA issuing a Certificate by a Root CA. References to “Subscribers” in this CP, however, apply only to the device Certificates and CVCs.

1.4.4 Relying Parties

The Relying Party may be any entity that validates the binding of a public key to the Subscriber’s name in a CableLabs PKI 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.

1.4.5 Other Participants

1.4.5.1 Management Authority (MA)

CableLabs, as the PKI-PA, may offload some of its duties to a MA to manage the design, the development, and the implementation of the PKI architecture on behalf of the PKI-PA. The MA's role is to provide trust management services to support the ecosystem in meeting its security goals using the CableLabs PKI.

The MA's primary focus is to ensure that policies for secure physical and logical access, data sharing, and communications across the cable ecosystem are realized through the execution and management of certificate policies and standards. Activities of the MA include the:

- Process for CAs to submit CPSs
- Rules/process for PKI-PA to approve CPSs
- Process for recognizing Subscribers, their authorized representatives, and their agreements for CRAs
- Process for revocation requests
- Process for Audits
- Registration of Sub-CAs
- Registration of Subscribers

The PKI-PA can perform the MA duties itself or designate a trusted third party to act as the MA on its behalf to provide operational support and maintain the CableLabs PKI in accordance with this CP.

1.4.5.2 Certificate Requesting Account (CRA)

The CRA is a web-based account portal for accounts hosted by a certified WebTrust company that is used to issue Certificates in bulk and in batch mode to Subscribers. The following applies when CableLabs uses a CRA:

In the CRA architecture, shown in Figure 2, the Subscriber uses a standard web browser to connect to the hosted Subscriber Sub-CA's web interface. Via this interface, the Subscriber will request appropriate device Certificates and pick up batched signed Certificates.

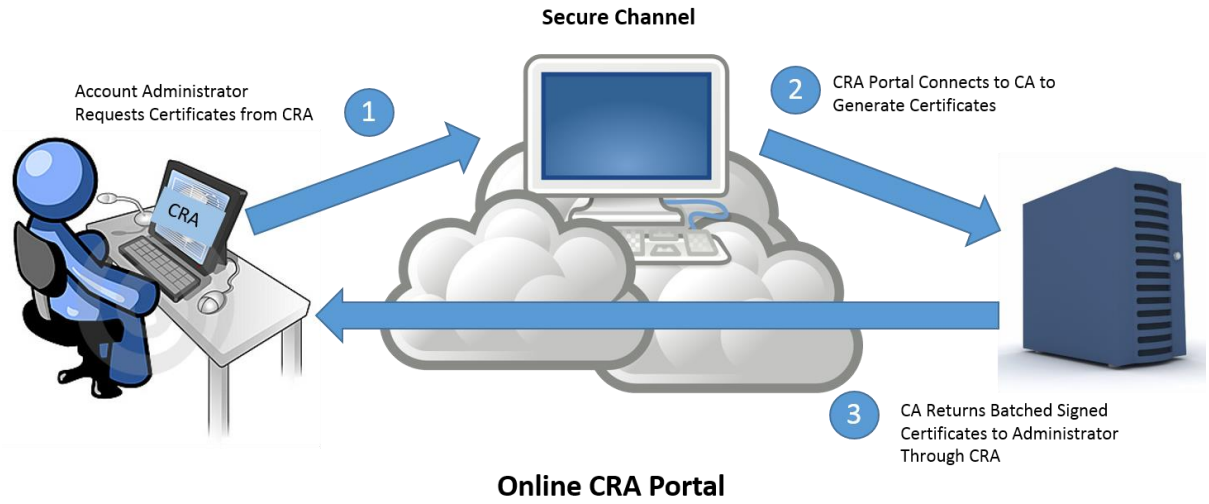

Figure 2: Certificate Requesting Account Architecture

The CRA will not require any deployment at the Subscriber's site, other than the installation of the lightweight standalone client software needed to decrypt downloaded file content. Therefore, immediate setup for a Subscriber to request and receive Certificates is fairly seamless.

1.5 Certificate Usage

This CP applies to all CableLabs PKI Participants, including Subscribers and Relying Parties. This CP sets forth policies governing the use of CableLabs PKI Certificates. Each Certificate is generally appropriate for use with the applications set forth in this CP.

1.5.1 Appropriate Certificate Uses

Certificates are suitable for device authentication of DOCSIS 3.1 and Remote PHY devices, confidentiality encryption, and code signing of CM software. The use of the Certificates permits message integrity checks, confidentiality of communications, support for non-repudiation and secure software downloads.

1.5.2 Prohibited Certificate Uses

CableLabs 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 or communication systems, air traffic control systems, or weapons control systems, where failure could lead directly to death, personal injury, or severe environmental damage.

1.6 Policy Administration

1.6.1 Organization Administering the Document

CableLabs is the PKI-PA. It owns this CP and represents the interest of its members in developing the policies that govern the CableLabs PKI. The PKI-PA is responsible for all aspects of this CP, including:

- Maintaining this CP
- Governing and operating the PKI according to this CP

- Approving the CPS for CAs that issue Certificates under this CP
- Approving the Audit for CAs operating under this CP

1.6.2 Contact Person

Inquiries regarding this CP can be directed to the PKI-PA at:

CableLabs PKI Policy Authority
CableLabs
858 Coal Creek Circle
Louisville, CO 80027
Email: pkiops@cablelabs.com
www.cablelabs.com

303-661-9100

1.6.3 Person Determining CPS Suitability for the Policy

CableLabs certificates, then the PKI-PA must approve the CPS for each CA that issues Certificates under this CP.

1.6.4 CPS Approval Procedures

CAs operating under this CP must meet all facets of the policy. The PKI-PA must determine if a CPS complies with this CP. The CA must complete a CPS on how it will meet all the CA requirements of this CP and receive approval from the PKI-PA before commencing operations. In some cases, the PKI-PA may require the additional approval of CableLabs members.

1.7 Definitions and Acronyms

1.7.1 Definitions

This CP uses the following terms and definitions:

Term	Description
Cable Operator	Provider of cable broadband and cable television system services.
Certificate	A digital representation of information which at least: • Identifies its issuing CA • Names or identifies the Subscriber of the Certificate • Contains the Subscriber's public key • Identifies its operational period • Is digitally signed by the issuing CA
Certificate Applicant	An individual representing the Subscriber 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 CableLabs for the issuance of a CRA. The request, also called a naming application (which is part of the DCAA), contains the naming information that will be included in the device Certificates.
Certificate Chain	An ordered list of Certificates containing a Subscriber Certificate and one or more CA Certificates, which terminates in a Root Certificate.

Term	Description
Certificate Policy (CP)	A document addressing all aspects associated with the generation, production, distribution, accounting, Compromise, recovery and administration of Certificates.
Certificate Requesting Account (CRA)	The online portal to assist Certificate Applicants in requesting Certificates.
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.
Certificate Status Server (CSS)	An authority that provides status information about Certificates on behalf of a CA.
Certification Authority (CA)	An entity authorized to issue, manage, revoke, and renew Certificates in the CableLabs PKI.
Certification Practice Statement (CPS)	A statement of the practices that a CA employs in issuing, suspending, revoking, and renewing Certificates and providing access to them, in accordance with the CP governing the CA.
Code Verification Certificate (CVC)	A Certificate that identifies the authenticity of the software by either the manufacturer or co-signer.
Compliance Audit (Audit)	A periodic audit that a CA system undergoes to determine its conformance with CableLabs PKI requirements that apply to it.
Compliance Auditor (Auditor)	The person, or company, performing the Compliance Audit.
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.
Confidential/Private Information	Information that is not public knowledge.
Digital Certificate Authorization Agreement (DCAA)	An agreement used by CableLabs setting forth the terms and conditions under which an organization acts as a Subscriber. The DCAA contains the Certificate Application.
Disaster Recovery Plan (DRP)	A documented process or set of procedures to recover and protect a business IT infrastructure in the event of a disaster.
Distinguished Name (DN)	Identification fields in a Certificate that are input by the CA when issuing Certificates. The information is obtained from the Subscriber's naming application.
Intellectual Property Rights	Rights under one or more of the following: copyright, patent, trade secret, trademark, trade names, 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.

Term	Description
MAC Address	A media access control (MAC) address is a hardware address that uniquely identifies each node of a network.
Management Authority (MA)	An entity whose role is to provide trust management services to support the ecosystem in meeting its security goals using the CableLabs PKI.
Online Certificate Status Protocol (OCSP)	An Internet protocol used for obtaining the revocation status of an X.509 digital certificate.
PKCS #10	Public-Key Cryptography Standard #10, developed by RSA Security Inc., which defines a structure for a CSR.
PKCS #12	Public-Key Cryptography Standard #12, developed by RSA Security Inc., which defines private key file format.
PKCS #8	Public-Key Cryptography Standard #8, developed by RSA Security Inc., which defines a secure means for the transfer of private keys.
PKI Participant	An individual or organization that is one or more of the following within the CableLabs PKI: CableLabs, a CA, a Subscriber, or a Relying Party.
Policy Authority	The entity that establishes certificate policies. Also known as the PKI policy authority (PKI-PA).
Processing Center	A secure facility created by an appropriate organization that houses, among other things, the cryptographic modules used for the issuance of Certificates.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software and workstations used for the purpose of administering Certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key Certificates.
Registration Authority (RA)	The entity that collects and verifies each Subscriber's identity and the information that is to be entered into the public key Certificate.
Relying Party	An entity that receives a Certificate with a digital signature verifiable with the public key listed in the Certificate, and is in a position to assess the trust in the authentication information provided by the Certificate depending on the CP governing the PKI and the Certificate verification.
Remote PHY	An architecture that provides conversion from digital Ethernet transport to analog RF transport.
Root CA	The top CA of a PKI.
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." A threshold number of Secret Shares (n) out of the total number of Secret Shares (m) must 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 Policy	The highest-level document describing CableLabs' security policies.
Shareholders	Holders of Secret Shares needed to operate a CA private key.

Term	Description
Sub-CA	A subordinate CA issued directly from the Root CA that allows for more specific policy implementations and protects the Root from unnecessary exposure.
Subject	The holder of a private key corresponding to a public key. The term "Subject" can, in the case of a CableLabs PKI Certificate, refer to the Subscriber requesting the Certificate.
Subscriber	The entity who requests a Certificate (e.g., a manufacturer or Cable Operator). The Subscriber is capable of using, and is authorized to use, the private key that corresponds to the public key listed in the Certificate.
Superior Entity	An entity above a certain entity within the CableLabs PKI.
Trusted Person	An employee, contractor, or consultant of an entity within the CableLabs 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 CableLabs PKI entity that must be held by a Trusted Person.
Trustworthy Systems	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 and ending with the date and time on which the Certificate expires.

1.7.2 Acronyms

This CP uses the following abbreviations and acronyms:

Term	Description
CA	Certification Authority
CM	Cable Modem
CMTS	CM Termination System
CP	Certificate Policy
CPS	Certification Practice Statement
CRA	Certificate Requesting Account
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CSS	Certificate Status Server
CVC	Code Verification Certificate
DCAA	Digital Certificate Authorization Agreement
DN	Distinguished Name
DOCSIS	Data-Over-Cable Service Interface Specifications
DRP	Disaster Recovery Plan
FIPS	Federal Information Processing Standards
FQDN	Fully Qualified Domain Name

Term	Description
HFC	Hybrid-Fiber/Coax
id-ce	Object Identifier for Version 3 Certificate extensions. (OID value: 2.5.29)
Id-kp	Extended key purpose identifiers (OID value: 1.3.6.1.5.5.7.3)
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISO	Independent System Operators
MA	Management Authority
MFR	Manufacturer
OID	Object Identifier
OU	Organizational Unit
OCSP	Online Certificate Status Protocol
PA	Policy Authority
pkcs	Public-Key Cryptosystem (OID value: 1.2.840.113549.1)
PKCS	Public-Key Cryptography Standard
PKI	Public Key Infrastructure
PKI-PA	Public Key Infrastructure Policy Authority
RA	Registration Authority
RFC	Request for Comment
RSA	Rivest, Shamir, Adelman

2 Publication and Repository Responsibilities

2.1 Repositories

In the CableLabs PKI, there is no separate entity providing repository services. Rather, each CA is responsible for its repository functions. All CAs that issue Certificates under this CP must 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

This CP, CA Certificates, and CRLs must be publicly available (e.g., on the CableLabs website, see www.cablelabs.com). The CPS for the Root CA will not be published; a redacted version of the CPS may be publicly available upon request to the CableLabs PKI-PA. There is no requirement for the publication of CPSs of Sub-CAs that issue Certificates under this CP. The CA must protect information not intended for public dissemination.

Table 1 below is a matrix of the various CableLabs PKI practice documents, showing whether or not 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. Documents not expressly made public are confidential to preserve the security of the CableLabs PKI.

Table 1: Availability of CableLabs PKI Information

Item	Classification	Available From:
CableLabs CP	Public	CableLabs
Root CA Certificate	Public	CableLabs
Sub-CA Certificates	Public	CableLabs
CRLs	Public	CableLabs
Root CA CPS	Confidential	N/A
Sub-CA CPS	Confidential	N/A

2.3 Time or Frequency of Publication

Changes to this CP must be made publicly available within thirty (30) days of approval by the PKI-PA. CA information must be published promptly after it is made available to the CA.

CA Certificates must be made publicly available within ten (10) week days after issuance.

2.4 Access Controls on Repositories

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

3 Identification and Authentication

3.1 Naming

3.1.1 Types of Names

For Certificates issued under this CP, the CA must assign X.501 Distinguished Names (DNs) [4]. The Issuer and Subject DN fields in Certificates must be populated with a non-empty DN as shown in the table below:

Table 2: Issuer and Subject DN Fields for CableLabs PKI Certificates

Certificate	Issuer DN	Subject DN	Reference
Root CA Certificate	C= US O= CableLabs OU= Root CA01 CN= CableLabs Root Certification Authority	C= US O= CableLabs OU= Root CA01 CN= CableLabs Root Certification Authority	Appendix III, Table III-1 of the DOCSIS 3.1 Security Specification [1]
Device Sub-CA Certificate	C= US O= CableLabs OU= Root CA01 CN= CableLabs Root Certification Authority	C= US O= CableLabs OU= Device CA01 CN= CableLabs Device Certification Authority	Appendix III, Table III-2 of the DOCSIS 3.1 Security Specification [1]
CM or Remote PHY Device Certificate	C= US O= CableLabs OU= Device CA01 CN= CableLabs Device Certification Authority	C= <Country> O= <Company Name> OU= <Manufacturing Location> CN= <MAC Address>	Appendix III, Table III-3 of the DOCSIS 3.1 Security Specification [1] and Annex D, Table 25 of the Remote PHY Specification [2]

CVC Sub-CA Certificate	C= US O= CableLabs OU= Root CA01 CN= CableLabs Root Certification Authority	C= US O= CableLabs OU= CVC CA01 CN= CableLabs CVC Certification Authority	Appendix III, Table III-4 of the DOCSIS 3.1 Security Specification [1]
CVC	C= US O= CableLabs OU= CVC CA01 CN= CableLabs CVC Certification Authority	C= <Country> O= <Company Name> CN= Code Verification Certificate	Appendix III, Table III-5 of the DOCSIS 3.1 Security Specification [1]
CableLabs Service Provider CA	C= US O= CableLabs OU= Root CA01 CN= CableLabs Root Certification Authority	C= US O= CableLabs OU= Service Provider CA01 CN= CableLabs Service Provider Certification Authority	Annex D, Table 26 of the Remote PHY Specification [2]
CCAP Core or AAA Server Certificate	C= US O= CableLabs OU= Service Provider CA01 CN= CableLabs Service Provider Certification Authority	C=<Country> O=<Company Name> CN=<Server FQDN>	Annex D, Table 27 of the Remote PHY Specification [2]

Values in angle brackets (<>) indicate that appropriate text as indicated below is present:

<Country>: ISO 3166-1 two-letter country code [5];
<Company Name>: name that identifies the company;
<Manufacturing Location>: name that identifies the location of manufacture;
<MAC Address>: MAC address of the CM;
<Server FQDN>: the domain name of the server.

3.1.2 Need for Names to Be Meaningful

The Certificates issued pursuant to this CP are meaningful if the names that appear in the Certificates can be understood by the Relying Parties. Names used in the Certificates must identify the object to which they are assigned in a meaningful way.

Subscriber Certificates must contain meaningful names that represent the Subscriber in a way that is easily understandable for humans. For devices, this may be a MAC address, model number or serial number.

The Subject name in CA Certificates must match the issuer name in Certificates issued by the CA, as required by RFC 5280 [6].

3.1.3 Anonymity or Pseudonymity of Subscribers

CableLabs CAs must not issue anonymous or pseudonymous Certificates.

3.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting DN forms are specified in X.501 [4].

3.1.5 Uniqueness of Names

Name uniqueness for Certificates issued by CableLabs CAs must be enforced. Each CA and RA must enforce name uniqueness within its domain. Name uniqueness is not violated when

multiple Certificates are issued to the same Subscriber. Name uniqueness is enforced for the entire Subject DN of the Certificate rather than a particular attribute (e.g., the common name). The CA and RA must identify the method for checking uniqueness of the Subject DNs within its domain.

3.1.6 Recognition, Authentication, and Role of Trademarks

Certificate Applicants must not use names in their Certificate Applications that infringe upon the Intellectual Property Rights of others. Neither CableLabs, the PKI-PA, nor any CableLabs CA/RA are 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 CableLabs, the PKI-PA, and any CableLabs CA must be entitled, without liability to any Certificate Applicant, to reject or suspend any DCAA because of such dispute. The PKI-PA must resolve disputes involving names and trademarks.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

In all cases where the party named in a Certificate generates its own keys, that party must be required to prove possession of the private key, which corresponds to the public key in the Certificate request. The CA must prove that the Subscriber possesses the private key by verifying the Subscriber's digital signature on the PKCS #10 Certificate Signing Request (CSR) with the public key in the CSR.

When the key pair is generated by the CA on behalf of a Subscriber; then in this case, proof of possession of the private key by the Subscriber is not required.

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

3.2.2 Authentication of Organization Identity

The CA's Certificate issuance process must authenticate the identity of the organization named in the DCAA by confirming that the organization:

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

3.2.3 Authentication of Individual Identity

This CP allows a Certificate to be issued only to a single entity. Certificates that contain a public key whose associated private key is shared must not be issued.

The CA/RA's Certificate issuance process must authenticate the individual identity of the following:

- That the representative submitting the DCAA 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
- That the corporate contact listed in the DCAA is an officer in the organization and can act on behalf of the organization
- That the administrator listed in the DCAA 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 Subscriber Information

Non-verifiable information may be included in CableLabs PKI Certificates, such as:

- Organizational 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 DCAA 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 DCAA and Certificate Application is authorized to act on behalf of the organization
- Administrators listed in the DCAA are authorized to act on behalf of the organization
- Contacts listed in the DCAA are authorized to act on behalf of the organization

The Root CA must obtain the PKI-PA's approval prior to issuing Sub-CA Certificates.

3.2.6 Criteria for Interoperation

No stipulation.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

Certificate re-key requests must follow the same procedures as initial Certificate issuance.

3.3.2 Identification and Authentication for Re-key After Revocation

Once a Certificate has been revoked, a re-key request must require issuance of a new Certificate. Certificate re-key requests after revocation must follow the same process as initial Certificate issuance.

3.4 Identification and Authentication for Revocation Request

Revocation requests must be signed by the entity requesting the revocation. The CA/RA must validate the identity of the requestor on the basis of credentials presented prior to the request being accepted. After a Certificate has been revoked, other than during a renewal or update action, the Subscriber must go through the initial Certificate Application process to obtain a new Certificate.

4 Certificate Lifecycle Operational Requirements

4.1 Certificate Application

A CA must include the processes, procedures, and requirements of its Certificate issuance process in its CPS.

4.1.1 Who Can Submit a Certificate Application

Only Subscribers who are authorized by CableLabs to receive CableLabs PKI Certificates may submit a Certificate Application. A Certificate Application for a CA Certificate must be submitted by an authorized representative of the Subscriber. A Certificate Applicant for a Certificate must be the Subscriber or an authorized representative of the Subscriber.

4.1.2 Enrollment Process and Responsibilities

All communications among CAs/RAs supporting the Certificate Application and issuance process must be authenticated and protected from modification; any electronic transmission of shared secrets must be protected. Communications may be electronic or out-of-band and must protect the confidentiality and integrity of the data.

The enrollment process for a Certificate Applicant must consist of:

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

4.2 Certificate Application Processing

It is the responsibility of the CA/RA to verify that the information in a Certificate Application is accurate.

4.2.1 Performing Identification and Authentication Functions

Prior to Certificate issuance, a Subscriber must sign a DCAA detailing Subscriber responsibility, which includes the requirement that the Subscriber must protect the private keys and use the Certificates and private keys for authorized purposes only.

4.2.2 Approval of Certificate Applications

A CA/RA must approve a Certificate Application if all of the following criteria are met:

- Receipt of a fully executed DCAA
- Receipt of a signed Certificate Application
- Successful identification and authentication of all required information
- Receipt of all requested supporting documentation
- Payment (if applicable) has been received
- Acceptance of the certificate application would not cause a violation of the CPS or the CP

The PKI-PA may approve or reject a Certificate Application.

4.2.3 Time to Process Certificate Applications

CAs must begin processing Certificate Applications within a reasonable time of receipt. There is no time stipulation to complete the processing of a Certificate Application unless otherwise indicated in the relevant DCAA.

4.3 Certificate Issuance

Upon receiving a request for a Certificate, the CA/RA must verify that the information in the Certificate Application is correct and accurate.

4.3.1 CA Actions During Certificate Issuance

Upon receiving the request, the CAs must:

- Verify the identity of the requester
- Verify the authority of the requester and the integrity of the information in the Certificate request
- Create and sign a Certificate if all Certificate requirements have been met
- Make the Certificate available to the Subscriber after confirming that the Subscriber has formally acknowledged its obligations

Information received from a prospective Subscriber must be verified before inclusion in a Certificate.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificates

CAs must notify Subscribers that they have created the requested Certificate(s), and provide Subscribers with access to the Certificate(s) by notifying them that their Certificate(s) are available and the means for obtaining them. Certificates must be made available to Subscribers, either via download from a website or via a message sent to the Subscriber containing the Certificates.

4.4 Certificate Acceptance

Certificates will be deemed valid immediately after issuance.

4.4.1 Conduct Constituting Certificate Acceptance

The following conduct constitutes Certificate acceptance by the Subscriber:

- Downloading a Certificate
- Failure to object 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.

This CP makes no stipulation regarding publication of Subscriber Certificates.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

The Root CA must notify the PKI-PA whenever the Root CA issues a Sub-CA Certificate.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Subscriber private key usage must be specified through Certificate extensions, including the key usage and extended key usage extensions, in the associated Certificate. Subscribers must protect their private keys from unauthorized use and must discontinue use of the private key following expiration or revocation of the Certificate. Subscribers must promptly request that a Certificate be revoked if the Subscriber has reason to believe that there has been a Compromise of the Certificate private key.

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 critical Certificate extensions, including the *basicConstraints* and *keyUsage* 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.

Relying Parties acknowledge the following:

- They are solely responsible for deciding whether or not to rely on the information in a Certificate, and agree that they have sufficient information to make an informed decision.
- To the extent permitted by applicable law, CableLabs hereby disclaims all warranties regarding the use of any Certificates, including, but not limited to,any warranty of merchantability or fitness for a particular purpose. In addition, CableLabs hereby limits its liability, and excludes all liability for indirect, special, incidental, and consequential damages.
- That reliance on Certificates is restricted to the purposes for which those Certificates were issued.

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.

4.6.1 Circumstances for Certificate Renewal

A Certificate may only be renewed if the public key has not reached the end of its Validity Period, the associated private key has not been Compromised, and the Subscriber name and attributes are unchanged. Certificates may be renewed:

- To maintain continuity of Certificate usage
- By a CA during recovery from key Compromise

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 following may request a Certificate renewal:

- The Subscriber of the Certificate or an authorized representative of the Subscriber
- The CA may request a renewal on behalf of a Subscriber
- The CA may request a renewal of its own Certificate
- The CA may renew its issued Certificates during recovery from a CA key Compromise
- The PKI-PA may request renewal of CA Certificates

4.6.3 Processing Certificate Renewal Requests

Certificate renewal requests must follow the same procedures as the initial Certificate issuance.

CA Certificate renewals must be approved by the PKI-PA.

4.6.4 Notification of New Certificate Issuance to Subscriber

CAs must notify Subscribers that they have created the requested Certificate(s), and provide Subscribers with access to the Certificate(s) by notifying them that their Certificate(s) are available and the means for obtaining them.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

The following conduct constitutes Certificate acceptance by the Subscriber:

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

4.6.6 Publication of the Renewal Certificate by the CA

CA Certificates must be published in a publicly available repository.

This CP makes no stipulation regarding publication of Subscriber Certificates.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

The Root CA must notify the PKI-PA whenever the Root CA issues a Sub-CA Certificate.

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 Subscriber of the Certificate or an authorized representative of the Subscriber
- The CA may request a re-key on behalf of a Subscriber
- 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 must validate the identity of the Subscriber in accordance with 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 Subscriber

CAs must notify Subscribers that they have created the requested Certificate(s), and provide Subscribers with access to the Certificate(s) by notifying them that their Certificate(s) are available and the means for obtaining them.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

The following conduct constitutes Certificate acceptance by the Subscriber:

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

4.7.6 Publication of the Re-keyed Certificate by the CA

CA Certificates must be published in a publicly available repository.

This CP makes no stipulation regarding publication of Subscriber Certificates.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

The Root CA must notify the PKI-PA whenever the Root CA issues a Sub-CA Certificate.

4.8 Certificate Modification

Modifying a Certificate means creating a new Certificate that has the same or a different key and a different serial number, and that differs in one or more other fields from the old Certificate. The old Certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

4.8.1 Circumstances for Certificate Modification

Certificates may be modified:

- For a Subscriber organization name change or other Subscriber characteristic change
- For Validity Period

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.

4.8.2 Who May Request Certificate Modification

The following may request a Certificate modification:

- The Subscriber of the Certificate or an authorized representative of the Subscriber
- The CA may request a Certificate modification on behalf of a Subscriber
- 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 must confirm the identity of the Subscriber in accordance with the requirements specified in this CP 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 Subscriber

CAs must notify Subscribers that they have created the requested Certificate(s), and provide Subscribers with access to the Certificate(s) by notifying them that their Certificate(s) are available and the means for obtaining them.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

The following conduct constitutes Certificate acceptance by the Subscriber:

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

4.8.6 Publication of the Modified Certificate by the CA

CA Certificates must be published in a publicly available repository.

This CP makes no stipulation regarding publication of Subscriber Certificates.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

The Root CA must notify the PKI-PA whenever the Root CA issues a Sub-CA Certificate.

4.9 Certificate Revocation and Suspension

CAs operating under this CP must make public a description of how to obtain revocation information for the Certificates they publish. This information must be given to Subscribers during Certificate request or issuance, and must be readily available to any potential Relying Party.

4.9.1 Circumstances for Revocation

A Certificate must be revoked when the binding between the Subject and the Subject's public key defined within the Certificate is no longer considered valid. Examples of circumstances that invalidate the binding are:

- The Subscriber or an authorized representative of the Subscriber asks for the Certificate to be revoked for any reason whatsoever
- The Subscriber's private key corresponding to the public key in the Certificate has been lost or Compromised:
    - Disclosed without authorization
    - Stolen
- The Subscriber can be shown to have violated the stipulations of its DCAA
- The DCAA with the Subscriber has been terminated
- There is an improper or faulty issuance of a Certificate
- A prerequisite to the issuance of the Certificate can be shown to be incorrect if:
    - Information in the Certificate is known, or reasonably believed, to be false
    - Any other circumstance that may reasonably be expected to affect the reliability, security, integrity or trustworthiness of the Certificate or the cryptographic key pair associated with the Certificate
    - The Subscriber has not submitted payment when due
- Identifying information of the Subscriber in the Certificate becomes invalid
- Attributes asserted in the Subscriber's Certificate are incorrect
- The Certificate was issued:
    - In a manner not in accordance with the procedures required by the applicable CPS
    - To an entity other than the one named as the Subject of the Certificate. Unless the entity is authorized to use that name.
    - Without the authorization of the entity named as the Subject of such Certificate
- The Subscriber's organization name changed
- The CA determines that any of the information appearing in the Certificate is inaccurate or misleading
- The continued use of that Certificate is harmful to CableLabs

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.

In addition, if it is determined subsequent to issuance of the new Certificate that a private key used to sign requests for one or more additional Certificates may have been Compromised at the time the requests for additional Certificates were made, all Certificates authorized by directly or indirectly chaining back to that Compromised key must be revoked.

4.9.2 Who Can Request Revocation

Within the CableLabs PKI, revocation requests may be made by:

- The Subscriber of the Certificate or any authorized representative of the Subscriber
- The CA for Certificates within its domain
- The PKI-PA

4.9.3 Procedure for Revocation Request

A Certificate revocation request 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 must specify the steps involved in the process of requesting a Certificate revocation in its CPS.

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

- Having the Subscriber log in to their CRA and revoking their Certificates via their account portal.
- Communication with the Subscriber providing reasonable assurances that the person or organization requesting revocation is, in fact the Subscriber. Depending on the circumstances, such communication may include one or more of the following: telephone, facsimile, e-mail, postal mail, or courier service.
- The representative is the authenticated corporate contact, administrator, legal, or technical contact.

CAs are entitled to request the revocation of Subscriber Certificates within the CA's subdomain. CAs must obtain approval from the PKI-PA prior to performing the revocation functions. The CA must send a written notice and brief explanation for the revocation to the Subscriber.

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 must 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.

4.9.5 Time Within Which CA Must Process the Revocation Request

CAs must 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.

4.9.6 Revocation Checking Requirement for Relying Parties

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

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

CAs must provide Relying Parties with information on how to find the appropriate CRL, web-based repository, or OCSP responder (if available) to check the revocation status of Certificates issued by the CA.

CA Certificate status must be posted by the PKI-PA in the CRL or OCSP responder (if available).

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. A CA must ensure that superseded Certificate status information is removed from the PKI repository upon posting of the latest Certificate status information.

CableLabs CAs must 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.

Certificate status information must be published no later than the next scheduled update. This will facilitate the local caching of Certificate status information for off-line or remote operation. PKI Participants must coordinate with the PKI repositories to which they post Certificate status information to reduce latency between creation and availability.

4.9.8 Maximum Latency for CRLs

CRLs must be published within three (3) business days of generation.

4.9.9 On-line Revocation/Status Checking Availability

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

4.9.10 On-line Revocation Checking Requirements

A Relying Party should check the status of a Certificate on which they wish to rely. 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 (where available).

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 provide authentication and integrity services commensurate with the assurance level of the Certificate being verified
- The alternative method must meet the issuance and latency requirements for CRLs stated in this CP

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 must notify CableLabs PKI Participants of a CA Certificate revocation using commercially reasonable efforts.

4.9.13 Circumstances for Suspension

The CableLabs 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

The CableLabs PKI may optionally include an authority that provides status information about Certificates on behalf of a CA through on-line transactions. In particular, it may include OCSP responders to provide on-line status information. Such an authority is termed a Certificate Status Server (CSS). Where the CSS is identified in Certificates as an authoritative source for revocation information, the operations of that authority are considered within the scope of this CP. A CSS must assert all the policy OIDs for which it is authoritative.

4.10.1 Operational Characteristics

No stipulation.

4.10.2 Service Availability

Relying Parties are bound to their obligations and the stipulations of this CP irrespective of the availability of the Certificate status service.

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

For Certificates that have expired prior to or upon end of subscription, revocation is not required. Unexpired CA Certificates must always be revoked at the end of the subscription.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

No stipulation.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5 Facility, Management, and Operational Controls

All entities performing CA functions 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 must 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 physical control requirements specified below apply equally to the CableLabs PKI 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 site location and construction, when combined with other physical security protection mechanisms such as 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. Moreover, each physical security tier encapsulates the next inner tier, such that an inner tier must be fully contained in an outside tier and cannot have a common outside wall with the outside tier, the outermost tier being the outside barrier of the building (e.g., a perimeter fence or outside wall).

5.1.2 Physical Access

Access to each tier of physical security must be auditable and controlled so that only authorized personnel can access each tier.

CAs must control access to their facilities including:

- Minimizing 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
- The use of tamper resistant locks 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 to the facility
- Video surveillance

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 plaintext information is stored in secure containers
- 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 or vent covers) are functioning properly
- The area is secured against unauthorized access

5.1.2.1 RA Equipment Physical Access

RA equipment must be protected from unauthorized access. The RA must implement physical access controls to reduce the risk of equipment tampering. These security mechanisms must be commensurate with the level of threat in the RA equipment environment.

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 must 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. The repositories (containing CA Certificates and CRLs) must be provided with uninterrupted power sufficient for a minimum of six (6) hours of operation in the absence of commercial power, to maintain availability and avoid denial of service.

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 must protect the media holding back ups of critical system data or any other sensitive information from water, fire, or other environmental hazards, and must 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 must 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 must 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. 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.

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 must 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 must be considered to be "Trusted Persons" serving in "Trusted Positions".

CAs must 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 Subscriber information or requests

Trusted Persons include, but are not limited to, customer service personnel, CA system administrators, designated engineering personnel, CA operators, Compliance Auditors (Auditors), 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 parties are required to have either physical or logical access to the CA. Access to CA cryptographic hardware must be strictly enforced by multiparty access 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 do not hold “Secret Shares” to activate the CA and vice versa.

Two or more persons are required for the following tasks:

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

Where multiparty control is required, at least one of the PKI Participants must be an administrator. Multiparty control must not be achieved using personnel that serve in the Auditor trusted role. CAs must establish, maintain, and enforce 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 two 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 authorized administrators.

5.2.3 Identification and Authentication for Each Role

CAs must 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 human resources or other personnel performing security functions and a check of well-recognized forms of identification, such as passports and driver's licenses.

5.2.4 Roles Requiring Separation of Duties

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

- 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
- Generation, issuance, or destruction of a CA Certificate
- Loading of a CA to a production environment

Individuals must not have more than one trusted role. The CA must have in place procedures to identify and authenticate its users and must ensure that no user identity can assume multiple roles.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

CAs must 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.

5.3.2 Background Check Procedures

CAs must conduct background check procedures for personnel tasked to become Trusted Persons. These procedures must align with 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 must 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:

- 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 may include, but are 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

5.3.3 Training Requirements

CAs must 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 must 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 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 CP

5.3.4 Retraining Frequency and Requirements

CAs must 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 trusted roles must be made aware of changes in the CA/RA 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/RA software or hardware upgrade, changes in automated security systems, and relocation of equipment.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

CAs must 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 may 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. Accordingly, independent contractors and consultants must be escorted and directly supervised by Trusted Persons when they are given access to the CA and its secure facility.

Contractors fulfilling trusted roles must follow all personnel requirements stipulated in this CP and must establish procedures to ensure that any subcontractors perform in accordance with this CP.

5.3.8 Documentation Supplied to Personnel

CAs must 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, RA, and CSS. 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 Audit logs, both electronic and non-electronic, must be retained in accordance with Section 5.4.3. and made available during Audits.

5.4.1 Types of Events Recorded

All auditing capabilities of the CA, RA and CSS operating systems 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.

CA/RAs must record in Audit log files all events relating to the security of the CA/RA system, including, without limitation:

- Physical Access/Site Security:
  - Personnel access to room housing CA/RA
  - Access to the CA/RA server
  - Known or suspected violations of physical security

- CA/RA Configuration:
  - CA/RA hardware configuration
  - Installation of the operating system
  - Installation of the CA/RA 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/RA 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 Subscriber information

- Certificate lifecycle events:
    - Issuance
    - Re-key
    - Renewal
    - Revocation

- Trusted Person events:
    - Logon and logoff
    - Attempts to create, remove, set passwords or change the system privileges of the privileged users
    - Unauthorized attempts to access the CA/RA 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 Subscriber
    - Account Administrator Certificates
    - Shipment of Tokens
    - Tokens driver versions

5.4.2 Frequency of Processing Log

CA/RA/CSSs must review their Audit logs in response to alerts based on irregularities and incidents within their systems. CA/RA/CSSs must review the Audit logs at least once every six (6) months and must 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 may be archived. Archive records must be retained for ten (10) years. The individual who removes

Audit logs from the CA/RA/CSS system must 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/RA/CSS 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.

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/RA/CSS system. Automated Audit processes must be invoked at system or application activation 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/RA/CSS must 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 Audit.

The Audit data should be reviewed by the Auditor for events such as repeated failed actions, requests for privileged information, attempted access of system files, and unauthenticated responses. Auditors should check for continuity of the Audit data.

5.5 Records Archival

CA/RA/CSS archive records must be sufficiently detailed to determine the proper operation of the PKI 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 Events Archived

CableLabs CA/RA/CSS records must include all relevant evidence in the recording entity's possession, including, without limitation:

- Time stamps
- CP
- CPS
- Contractual obligations and other agreements concerning operations of the CA/RA/CSS 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
- Audit reports
- Appointment of an individual to a Trusted Position
- Destruction of cryptographic modules
- All Certificate Compromise notifications

CableLabs PKI-PA records must include all relevant evidence in the recording entity's possession, including, without limitation:

- DCAAs
- All CRLs issued and/or published
- Audit 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 seven (7) years without any loss of data.

5.5.3 Protection of Archive

An entity maintaining an archive of records must 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 retention time period.

5.5.4 Archive Backup Procedures

Entities compiling electronic information must incrementally back up system archives of such information at least on a weekly basis and perform full backups at least on a monthly basis. Copies of paper-based records must be maintained in an off-site secure facility.

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 Systems (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 Persons 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 must either approve or reject the Certificate Application.

When a CA updates its private signature key and thus generates a new public key, the CA must notify all CAs and Subscribers that rely on the CA's Certificate that it has been changed.

When a CA that distributes self-signed Certificates updates its private signature key, the CA must generate key rollover Certificates, where the new public key is signed by the old private key, and vice versa. This permits acceptance of newly issued Certificates and CRLs without distribution of the new self-signed Certificate to current users. Key rollover Certificates are optional for CAs that do not distribute self-signed Certificates.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

The PKI-PA must be notified if any CA/CSSs operating under this CP experience the following:

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

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

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

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

When computing resources, software, and/or data are corrupted, CA/CSSs operating under this CP must respond as follows:

- Ensure that the system's integrity has been restored before returning to operation
- If the CA or CSS signature keys are not destroyed, CA/CSS operations must be re-established, giving priority to the ability to generate Certificate status information within the CRL issuance schedule specified in section 5.9.7
- If the CA or CSS signature keys are destroyed, CA/CSS operations must be re-established as quickly as possible, giving priority to the generation of a new CA key pair
- The PKI-PA must 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/CSS in accordance with the documented incident and Compromise reporting and handling procedures in the applicable CPS

5.7.3 Entity (CA) Private Key Compromise Procedures

In the event of a CA private key Compromise, the following operations must be performed:

- The PKI-PA must be immediately informed, as well as any entities known to be distributing the CA Certificate
- The CA must generate new keys
- The CA must initiate procedures to notify Subscribers of the Compromise
- Subscriber Certificates may be renewed automatically by the CA under the new key pair, or the CA may require Subscribers to repeat the initial Certificate Application process

If the CA distributed the public key in a Certificate, the CA must perform the following operations:

- Generate a new Certificate
- Securely distribute the new Certificate
- Initiate procedures to notify Subscribers of the Compromise

If a CSS key is compromised, all Certificates issued to the CSS must be revoked, if applicable. The CSS will generate a new key pair and request new Certificate(s), if applicable.

If RA signature keys are Compromised, lost, or suspected of Compromise:

- The RA Certificate must be revoked immediately
- A new RA key pair must be generated in accordance with procedures set forth in the applicable CPS
- A new RA Certificate must be requested in accordance with the initial Certificate Application process described in this CP
- All Certificate Application requests approved by the RA since the date of the suspected Compromise must be reviewed to determine which are legitimate
- For those Certificate requests or approvals whose legitimacy cannot be ascertained, the resultant Certificates must be revoked and their Subjects (i.e., Subscribers) must be notified of the revocation

5.7.4 Business Continuity Capabilities After a Disaster

Entities operating CAs must develop, test, and maintain a Disaster Recovery Plan (DRP) designed to mitigate the effects of any kind of natural or man-made disaster. The DRP 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.

Additionally, the DRP 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 including:

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

CAs must 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
- 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 DRP must make provisions for full recovery within one (1) week following a disaster at the primary site.

5.8 CA and RA Termination

When a CA terminates operations before all Certificates have expired, the CA signing keys must be surrendered to the PKI-PA. Prior to CA termination, the CA must provide archived data to an archive facility, as specified in the CPS (if applicable). 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.

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 CP (e.g., Audit logging and archives).

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

- Providing notice to parties affected by the termination, such as Subscribers and Relying Parties
- Who bears the cost of such notice, the terminating CA or the Superior Entity
- The revocation of the Certificate issued to the CA by the Superior Entity
- The preservation of the CA's archives and records for the time periods
- The continuation of Subscriber and customer support services

- The continuation of revocation services, such as the issuance of CRLs or the maintenance of online status checking services
- The revocation of unexpired unrevoked Certificates of Subscribers and subordinate CAs, if necessary
- Disposition of the CA's private key and the hardware token containing such private key
- Provisions needed for the transition of the CA's services to a successor CA

In addition, the RA:

- Must archive all Audit logs and other records prior to termination
- Must destroy all its private keys upon termination
- Must transfer all archive records to an appropriate authority such as the PKI-PA

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

Root key pair generation must be performed using FIPS 140-2 [7] 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.

Sub-CA key pair generation should be performed using FIPS 140-2 [7] validated cryptographic modules.

New CA keys must be generated in a Key Generation Ceremony using multi-person control for CA key pair generation.

CA key pair generation must create a verifiable Audit trail documenting 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 must 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.

6.1.1.2 Subscriber Key Pair Generation

Subscriber key pair generation may be performed by the Subscriber or CA. If the Subscribers themselves generate private keys, then private key delivery to a Subscriber is unnecessary.

When CA/RAs generate key pairs on behalf of the Subscriber, then the private key must be delivered securely to the Subscriber. Private keys may be delivered electronically or on a hardware cryptographic module. In all cases, the following requirements must be met:

- The CA must not retain any copy of the key after delivery of the private key to the Subscriber.

- CAs must use Trustworthy Systems to deliver private keys to Subscribers and must 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 must use best efforts to provide physical security of the tokens to prevent the loss, disclosure, modification, or unauthorized use of the private keys on the token. The CA must maintain a record of the Subscriber acknowledgement of receipt of the token.
- The Subscriber must 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 Subscribers.

    - For hardware modules, accountability for the location and state of the module must be maintained until the Subscriber 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.

The CA/RA must maintain a record of the Subscriber's acknowledgement of receipt of the token.

6.1.2 Private Key Delivery to Subscriber

The Subscribers themselves typically generate Subscribers' private keys, and therefore private key delivery to a Subscriber is usually unnecessary. Private keys, however, generated by the CA for the Subscriber must be delivered to Subscribers only when:

- Their Certificate Applications are approved by the PKI-PA, and
- Their key pairs are generated and are distributed to Certificate Applicants in connection with the enrollment process.

CAs must use Trustworthy Systems to deliver private keys to Subscribers and must secure such delivery through the use of a PKCS #8 package or, in CableLabs' sole discretion, any other comparably equivalent means (e.g., encryption) 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 must use best efforts to provide physical security to prevent the loss, disclosure, modification, or unauthorized use of the private keys on the tokens.

6.1.3 Public Key Delivery to Certificate Issuer

Where key pairs are generated by the Subscriber or RA, the public key must be transferred to the issuing CA to be certified; it must be delivered through a mechanism validating the identity of the Subscriber 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 must deliver the public key in a PKCS #10 CSR package 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.

6.1.4 CA Public Key Delivery to Relying Parties

CA public key Certificates must be delivered to Relying Parties in a fashion to preclude substitution attacks. Acceptable methods for Certificate delivery are:

- Distribution of CA Certificates through secure out-of-band mechanisms
- Downloading the CA Certificates from trusted websites (CA or PKI-PA website)

6.1.5 Key Sizes

Key pairs must be of sufficient length to prevent others from determining the key pair's private key using cryptanalysis during the period of expected utilization of such key pairs. CableLabs PKI Certificates must meet the following requirements for key size:

Table 3: Key Size

Certificate	Key Size	Reference
Root CA Certificate	4096-bit RSA	Appendix III, Table III-1 of the DOCSIS 3.1 Security Specification [1]
Device Sub-CA Certificate	3072-bit RSA	Appendix III, Table III-2 of the DOCSIS 3.1 Security Specification [1]
CM Device Certificate	2048-bit RSA	Appendix III, Table III-3 of the DOCSIS 3.1 Security Specification [1]
CVC Sub-CA Certificate	3072-bit RSA	Appendix III, Table III-4 of the DOCSIS 3.1 Security Specification [1]
CVC	2048-bit RSA	Appendix III, Table III-5 of the DOCSIS 3.1 Security Specification [1]
Service Provider Sub-CA Certificate	3072-bit RSA	Annex D, Figure 47 of the Remote PHY Specification[2]
CCAP Core Certificate	2048-bit RSA	Annex D, Figure 47 of the Remote PHY Specification[2]
AAA Server Certificate	2048-bit RSA	Annex D, Figure 47 of the Remote PHY Specification[2]

6.1.6 Public Key Parameters Generation and Quality Checking

CSRs will be reviewed to confirm that the public key meets the key sizes defined in CP section 6.1.5.

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

Appendix III, Tables III-1, III-2, and III-4 of the DOCSIS 3.1 Security Specification [1] as well as Annex D of the Remote PHY Specification [2] specify that CA Certificates:

- Must include a *keyUsage* extension
- Must set the criticality of the *keyUsage* extension to TRUE
- Must assert the *keyCertSign* and *cRLSign* bits in the *keyUsage* extension

The table below shows the specific *keyUsage* extension settings for CableLabs PKI CA Certificates (i.e., Root CAs and Sub-CAs).

Table 4: keyUsage Extension for CA Certificates

Field	Format	Criticality	Value	Comment
keyUsage	BIT STRING	TRUE	{ id-ce 15 }	Included in all CA Certificates
digitalSignature	(0)		0	Not Set
nonRepudiation	(1)		0	Not Set
keyEncipherment	(2)		0	Not Set
dataEncipherment	(3)		0	Not Set
keyAgreement	(4)		0	Not Set
keyCertSign	(5)		1	Set
cRLSign	(6)		1	Set
encipherOnly	(7)		0	Not Set
decipherOnly	(8)		0	Not Set

Appendix III, Tables III-3, of the DOCSIS 3.1 Security Specification [1] as well as Annex D of the Remote PHY Specifiction [2] specifies that device Certificates:

- Must include a *keyUsage* extension
- Must set the criticality of the *keyUsage* extension to TRUE
- Must assert the *digitalSignature* bit
- Must assert the *keyEncipherment* bit

The table below shows the specific *keyUsage* extension settings for CM device Certificates.

Table 5: keyUsage Extension for Device Certificates

Field	Format	Criticality	Value	Comment
keyUsage	BIT STRING	TRUE	{ id-ce 15 }	Included in all Subscriber Certificates
digitalSignature	(0)		1	Set
nonRepudiation	(1)		0	Not Set
keyEncipherment	(2)		1	Set
dataEncipherment	(3)		0	Not Set
keyAgreement	(4)		0	Not Set
keyCertSign	(5)		0	Not Set
cRLSign	(6)		0	Not Set

encipherOnly	(7)		0	Not Set
decipherOnly	(8)		0	Not Set

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

Private keys within the CableLabs PKI must be protected using Trustworthy Systems. Private key holders must take necessary precautions to prevent the loss, disclosure, modification, or unauthorized use of such private keys in accordance with this CP and contractual obligations specified in the appropriate DCAA.

The relevant standard for cryptographic modules is Security Requirements for Cryptographic Modules [FIPS 140-2] [7].

- Root CAs must perform all CA cryptographic operations on cryptographic modules rated at a minimum of FIPS 140-2 Level 3 [7] or higher.
- Sub-CAs, RAs, and CSSs must use a FIPS 140-2 Level 2 [7] or higher validated hardware cryptographic module.
- Subscribers should use a FIPS 140-2 Level 1 [7] or higher validated cryptographic module for their cryptographic operations.

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

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

CA signature keys may 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 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 three (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 three (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 signature keys and Subscriber private signature keys must not be escrowed.

If the CA retains Subscriber private encryption keys for business continuity purposes, the CA must escrow such Subscriber private keys to protect them from unauthorized modification or disclosure through physical and cryptographic means.

6.2.4 Private Key Backup

CAs must 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 Subscriber or other authorized administrator. Private keys that are backed up, must not be stored in plaintext form and storage must ensure security controls consistent with the CableLabs security specifications with which the device is compliant. Subscribers may have the option of using enhanced private key protection mechanisms available today including the use of smart cards, biometric access devices, and other hardware tokens to store private keys.

CSS private keys may be backed up. If backed up, all copies must be accounted for and protected in the same manner as the original.

6.2.5 Private Key Archival

CA private signature keys and Subscriber private signature keys must not be archived. If the CA retains Subscriber private encryption keys for business continuity purposes, the CA must archive such Subscriber private keys, in accordance with CP section 5.5.

Upon expiration of a CA Certificate, the key pair associated with the Certificate will be securely retained for a period of at least five (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.

6.2.6 Private Key Transfer into or from a Cryptographic Module

CA and CSS private keys may be exported from the cryptographic module only to perform CA/CSS key backup procedures, as described in CP section 6.2.4. At no time must the 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 private keys on one hardware cryptographic module and transferring them into another, must 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 must 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 Subscriber private keys into a smart card, must 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 [7].

6.2.8 Method of Activating Private Keys

All CA/RA/CSSs must protect the activation data for their private keys against loss, theft, modification, disclosure, or unauthorized use.

CA administrators must 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 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.

6.2.8.1 CA Administrator Activation

Method of activating the CA system by a CA administrator must require:

- Use of a smart card, biometric access device, password 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, a Microsoft Windows logon or screen saver password, or a network logon password
- 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

6.2.8.2 Offline CA Private Keys

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. Once the private key is activated, it must be active until termination of the session.

6.2.8.3 Online CA Private Keys

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

6.2.8.4 Subscriber Private Keys

The CableLabs standards for protecting activation data for Subscribers' private keys must be in accordance with the specific obligations appearing in the applicable agreement executed between CableLabs and the Subscriber.

6.2.9 Method of Deactivating Private Keys

Cryptographic modules that have been activated must not be available to unauthorized access. After use, the cryptographic module must be deactivated 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 must remove the token containing the private key from the reader in order to deactivate it.

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 must remove the token containing the private keys from the reader in order to deactivate them. Once removed from the reader, tokens must be securely stored.

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

6.2.10 Method of Destroying Private Keys

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 must decommission the CA private signature key 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 residual remains of the key that could lead to the reconstruction of the key. For Root CAs, PKI-PA security personnel must witness this process.

Subscribers 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 section 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

CAs may archive their public keys by archiving their public key Certificate.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The Certificate Validity Period (i.e., Certificate operational period and key pair usage period) must be set to the time limits set forth as follows:

Table 6: Validity Period

Certificate	Validity Period	Reference
Root CA Certificate	50 years	Appendix III, Table III-1 of the DOCSIS 3.1 Security Specification [1]
Device Sub-CA Certificate	35 years	Appendix III, Table III-2 of the DOCSIS 3.1 Security Specification [1]
CM Device Certificate	20 years	Appendix III, Table III-3 of the DOCSIS 3.1 Security Specification [1]
CVC Sub-CA Certificate	35 years	Appendix III, Table III-4 of the DOCSIS 3.1 Security Specification [1]
Code Verification Certificate	Up to 10 years	Appendix III, Table III-5 of the DOCSIS 3.1 Security Specification [1]
Service Provider Sub-CA Certificate	35 years	Annex D Figure 47 of the Remote PHY Specification [2]
CCAP Core Certificate	Up to 5 years	Annex D Figure 47 of the Remote PHY Specification [2]
AAA Server Certificate	Up to 5 years	Annex D Figure 47 of the Remote PHY Specification [2]

As necessary to ensure the continuity and security of the CableLabs PKI, CableLabs must commission new CAs.

CableLabs PKI Participants must 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

The activation data (e.g., PINs, passwords, or manually-held key shares) used to unlock private keys, in conjunction with any other access control procedure, must have an appropriate level of strength for the keys or data to be protected and must meet the applicable Security Policy requirements of the cryptographic module used to store the keys. CAs must generate and install activation data for their private keys and must 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.

When a CA uses passwords as activation data for the CA signing key, at a minimum the activation data must be changed upon CA re-key.

Subscriber activation data may be user selected.

6.4.2 Activation Data Protection

Data used to unlock private keys must be protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data should be either biometric in nature or memorized. If written down, it must be secured at the level of the data that the associated cryptographic module is used to protect, and must not be stored with the cryptographic module. In all cases, the protection mechanism must include a facility to temporarily lock the account, or terminate the application, after a predetermined number of failed login attempts as set forth in the respective CPS.

CAs must 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 must use multi-party control and 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 must 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 must constitute Confidential/Private Information.

CAs must include in their DRPs 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 must maintain an Audit trail of Secret Shares, and Shareholders must participate in the maintenance of an Audit trail.

6.4.3 Other Aspects of Activation Data

CAs, RAs, and CSSs must change the activation data whenever the token is re-keyed or returned from maintenance.

6.4.3.1 Activation Data Transmission

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

6.4.3.2 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 period lapses, CAs must decommission activation data by overwriting and/or physical destruction.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

CA/RA/CSSs must ensure that the systems maintaining software and data files are Trustworthy Systems secure from unauthorized access. In addition, CA/RA/CSSs must limit access to production servers to those individuals with a valid business reason for access. General application users must not have accounts on the production servers.

CA/RA/CSSs must have production networks logically separated from other components. This separation prevents network access except through defined application processes. CA/RA/CSSs must 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, CA/RA/CSSs must require the use of passwords with a minimum character length and a combination of alphanumeric and special characters, and must 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 securely. 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 CP, 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 must 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
- Enforce domain integrity boundaries for security critical processes
- Support recovery from key or system failure

CSSs, operating under this CP, must follow the computer security functions listed:

- 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

Remote workstations used to administer the CAs must follow the computer security functions listed below:

- 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
- 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 Lifecycle Technical Controls

6.6.1 System Development Controls

The system development controls for the CA and CSS are as follows:

- Use software that has been designed and developed under a formal, documented development methodology.
- Hardware and software procured must be purchased in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the MFR cannot identify the PKI component that will be installed on a particular device).
- Hardware and software developed specifically for the CA and CSS 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 hardware and software must be dedicated to performing PKI activities. There must be no other applications, hardware devices, network connections, or component software installed that are not part of the PKI 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 equipment. All applications required to perform the PKI operation must be obtained from documented sources. CA, RA, and CSS hardware and software must be scanned for malicious code on first use and periodically thereafter.
- Hardware and software updates must be purchased or developed in the same manner as 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 and CSS 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 and CSS software, when first loaded, must be verified as being that supplied from the MFR, with no modifications, and be the version intended for use.

In addition, only applications required to perform the organization's mission must be loaded onto the RA workstation, and all such software must be obtained from sources authorized by local policy.

6.6.3 Lifecycle Security Controls

No stipulation.

6.7 Network Security Controls

CAs, CSSs, and RAs must employ appropriate security measures to ensure they are guarded against denial of service and intrusion attacks. Such measures must include the use of network guards, firewalls, or filtering routers. The network guard, firewall, or filtering router must limit services allowed to and from the PKI equipment to those required to perform PKI functions.

Protection of PKI equipment must be provided against known network attacks. All unused network ports and services must be turned off. Any network software present on the PKI equipment must be necessary to the functioning of the PKI 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 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 must 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 (3) minutes. Electronic or manual procedures may be used to maintain system time. Clock adjustments are auditable events.

7 Certificate, CRL AND OCSP Profiles

7.1 Certificate Profile

CableLabs Certificates must conform to RFC 5280 [6].

CableLabs PKI Certificates must contain the identity and attribute data of a Subject using the base Certificate with applicable extensions. The base Certificate must contain the version number of the Certificate, the Certificate's identifying serial number, the signature algorithm used to sign the Certificate, the issuer's DN, the Validity Period of the Certificate, the Subject's DN, information about the Subject's public key, and extensions.

Table 7: Certificate Profile Basic Fields

Field	RFC 5280 Section	Comments
tbsCertificate	4.1.1.1	Follows RFC 5280 [6] guidance
Version	4.1.2.1	See CP section 7.1.1
serialNumber	4.1.2.2	Unique positive integer (20 octets) assigned by the CA
Signature	4.1.2.3	See CP section 7.1.3
Issuer	4.1.2.4	See CP section 7.1.4
validity	4.1.2.5	See CP section 6.3.2
subject	4.1.2.6	See CP section 7.1.4
subjectPublicKeyInfo	4.1.2.7	See CP section 7.1.3
extensions	4.1.2.9	See CP section 7.1.2
signatureAlgorithm	4.1.1.2	Follows RFC 5280 [6] guidance
algorithmIdentifier	4.1.1.2	
algorithm	4.1.1.2	See CP section 7.1.3
parameters	4.1.1.2	See CP section 7.1.3
signatureValue	4.1.1.3	Follows RFC 5280 [6] guidance

7.1.1 Version Number(s)

CableLabs Certificates must be X.509 v3 Certificates. The Certificate version number must be set to the integer value of "2" for Version 3 Certificates.

7.1.2 Certificate Extensions

CableLabs PKI Certificate extensions provide methods for associating additional attributes with public keys and for managing relationships between CAs. CableLabs PKI Certificates must follow the guidance in RFC 5280 [6] and must contain the standard extensions shown in the tables below, unless they are denoted as optional.

The table below shows the standard Certificate extensions for the CableLabs PKI Root CA Certificate defined in Appendix III, Table III-1, of the DOCSIS 3.1 Security Specification [1].

Table 8: Root CA Certificate Standard Extensions

Field	OID	Include	Criticality
keyUsage	{id-ce 15}	Yes	TRUE
basicConstraints	{id-ce 19}	Yes	TRUE
subjectKeyIdentifier	{id-ce 14}	Yes	FALSE
subjectAltName	{id-ce 17}	Optional	FALSE

The table below shows the standard Certificate extensions for the CableLabs PKI Sub-CA Certificates defined in Appendix III, Table III-2 and Table III-4 of the DOCSIS 3.1 Security Specification [1] and Annex D of the Remote PHY Specification [2].

Table 9: Sub-CA Certificate Standard Extensions

Field	OID	Include	Criticality
keyUsage	{id-ce 15}	Yes	TRUE
basicConstraints	{id-ce 19}	Yes	TRUE
subjectKeyIdentifier	{id-ce 14}	Yes	FALSE
authorityKeyIdentifier	{id-ce 35}	Yes	FALSE
subjectAltName	{id-ce 17}	Optional	FALSE

The table below shows the standard Certificate extensions for the CM Device Certificate defined in Appendix III, Table III-3, of the DOCSIS 3.1 Security Specification [1].

Table 10: CM Certificate Standard Extensions

Field	OID	Include	Criticality
keyUsage	{id-ce 15}	Yes	TRUE
authorityKeyIdentifier	{id-ce 35}	Yes	FALSE

The table below shows the standard Certificate extensions for the Code Verification Certificate defined in Appendix III, Table III-5, of the DOCSIS 3.1 Security Specification [1].

Table 11: Code Verification Certificate Standard Extensions

Field	OID	Include	Criticality
extKeyUsage	{id-ce 37}	Yes	TRUE
authorityKeyIdentifier	{id-ce 35}	Yes	FALSE

Table 12: CCAP Core Certificate Standard Extensions

Field	OID	Include	Criticality
keyUsage	{id-ce 15}	Yes	TRUE
authorityKeyIdentifier	{id-ce 35}	Yes	FALSE
subjectAltName	{id-ce 17}	Yes	FALSE

Table 13: AAA Server Certificate Standard Extensions

Field	OID	Include	Criticality
keyUsage	{id-ce 15}	Yes	TRUE
authorityKeyIdentifier	{id-ce 35}	Yes	FALSE
subjectAltName	{id-ce 17}	Yes	FALSE

7.1.2.1 Subject Key Identifier Extension

Appendix III, Tables III-1, III-2, and III-4 of the DOCSIS 3.1 Security Specification [1] as well as the Remote PHY Specification Annex D [2] specify that CA Certificates:

- Must include the *subjectKeyIdentifier* extension
- Must set the criticality of the *subjectKeyIdentifier* extension to FALSE
- Must calculate the *keyIdentifier* of the *subjectKeyIdentifier* per Method 1

The table below shows the specific *subjectKeyIdentifier* extension settings for CableLabs PKI CA Certificates (i.e., Root CAs, Sub-CAs).

Table 14: subjectKeyIdentifier Extension for CA Certificates

Field	Format	Criticality	Value	Comment
subjectKeyIdentifier		FALSE	{ id-ce 14 }	Included in all CA Certificates
keyIdentifier	OCTET STRING		<key identifier>	Calculated per Method 1

7.1.2.2 Basic Constraints Extension

Appendix III, Table III-1 of the DOCSIS 3.1 Security Specification [1] specifies that the Root CA Certificate:

- Must include the *basicConstraints* extension
- Must set the criticality of the *basicConstraints* extension to TRUE
- Must set the *cA* field of the *basicConstraints* extension to TRUE

The table below shows the specific *basicConstraints* extension settings for CableLabs PKI Root CA Certificate.

Table 15: basicConstraints Extension for Root CA Certificate

Field	Format	Criticality	Value	Comment
basicConstraints		TRUE	{ id-ce 19 }	Included in Root Certificate
cA	BOOLEAN		TRUE	Set
pathLenConstraint	INTEGER			Not Set

Appendix III, Tables III-2 and III-4 of the DOCSIS 3.1 Security Specification [1] as well as the Remote PHY Specification Annex D [2] specify that Sub-CA Certificates:

- Must include the *basicConstraints* extension
- Must set the criticality of the *basicConstraints* extension to TRUE
- Must set the *cA* field of the *basicConstraints* extension to TRUE
- Must set the *pathLenConstraint* field of the *basicConstraints* to "0" (zero)

The table below shows the specific *basicConstraints* extension settings for CableLabs PKI Sub-CA Certificates.

Table 16: basicConstraints Extension for CableLabs Sub-CA Certificates

Field	Format	Criticality	Value	Comment
basicConstraints		TRUE	{ id-ce 19 }	Included in all sub-CA Certificates
cA	BOOLEAN		TRUE	Set
pathLenConstraint	INTEGER		0	Set to "0" (Zero)

7.1.2.3 Extended Key Usage

Appendix III, Tables III-2 and III-4 of the DOCSIS 3.1 Security Specification [1] as well as the Remote PHY Specification Annex D [2] specify that Sub-CA Certificates:

- Must include the *extKeyUsage* extension
- Must set the criticality of the *extKeyUsage* extension to TRUE
- Must set the *codeSigning* field of the *extKeyUsage*

The table below shows the specific *extKeyUsage* extension settings for CableLabs PKI CVCs.

Table 17: extKeyUsage Extension for Code Verification Certificates

Field	Format	Criticality	Value	Comment
extKeyUsage		FALSE	{ id-ce 37 }	Included in Code Verification Certificates
codeSigning	OID		{ id-kp 3 }	Set

7.1.3 Algorithm Object Identifiers (OIDs)

Certificates issued under this CP must use the following OID for its *signature* algorithm:

Table 18: Signature OIDS for Certificates

Field	Format	Criticality	Value	Comment
signature				
algorithmIdentifier				
algorithm	OID		{ pkcs 1.11 }	Sha256WithRSAEncryption
parameters	ANY		NULL	

Certificates issued under this CP must use the following OID for its *subjectPublicKeyInfo* algorithm:

Table 19: subjectPublicKeyInfo for Certificate

Field	Format	Criticality	Value	Comment
subjectPublicKeyInfo				
algorithm				
algorithmIdentifier				
algorithm	OID		{ pkcs 1.1}	rsaEncryption
parameters	ANY		NULL	
subjectPublicKey	BIT STRING		<subject public key>	Modulus length

7.1.4 Name Forms

See CP section 3.1.1.

7.1.5 Name Constraints

The CAs must not assert name constraints in CableLabs PKI Certificates.

7.1.6 Certificate Policy Object Identifier

No stipulation.

7.1.7 Usage of Policy Constraints Extension

The CAs must not assert policy constraints in CA Certificates.

7.1.8 Policy Qualifiers Syntax and Semantics

Certificates issued under this CP must not contain policy qualifiers.

7.1.9 Processing Semantics for the Critical *certificatePolicies* Extension

Certificates issued under this CP must not contain a critical *certificatePolicies* extension.

7.2 CRL Profile

CRLs, as defined in section 13.4.1.1 of the DOCSIS 3.1 Security Specification [1] as well as the Remote PHY Specification section 8.4 [2], must conform to RFC 5280 [6] and contain the basic fields and contents specified in the table below:

Table 20: CRL Profile Basic Fields

Field	Referenced Standard	Section	Comments
version	[RFC 5280]	5.1.2.1	See Section 7.2.1.
signature	[RFC 5280]		Algorithm used to sign the CRL.
issuer	[RFC 5280]	5.1.2.3	Entity that has signed and issued the CRL.
thisUpdate	[RFC 5280]	5.1.2.4	Indicates the issue date of the CRL. CRLs are effective upon issuance.
nextUpdate	[RFC 5280]	5.1.2.5	Indicates the date by which the next CRL will be issued.
revokedCertificates	[RFC 5280]	5.1.2.6	Listing of revoked Certificates, including the Serial Number of the revoked Certificate and the Revocation Date.
authorityKeyIdentifier	[RFC 5280]	5.2.1	Follows the guidance in RFC 5280 [6]. Criticality is FALSE.
cRLNumber	[RFC 5280]	5.2.3	A monotonically increasing sequence number for a given CRL scope and issuer. Criticality is FALSE.
signatureAlgorithm	[RFC 5280]	5.1.1.2	Follows the guidance in RFC 5280 [6].
signatureValue	[RFC 5280]	5.1.1.3	Follows the guidance in RFC 5280 [6].

7.2.1 Version Number(s)

The CAs must support the issuance of X.509 Version 2 CRLs. The CRL version number must be set to the integer value of "1" for Version 2.

7.2.2 CRL and CRL Entry Extensions

Critical CRL extensions must not be used.

7.3 OCSP Profile

OCSP is a way to obtain timely information about the revocation status of a particular Certificate. OCSP responses, as defined in section 13.4.2 of the DOCSIS 3.1 Security Specification [1] as well as the Remote PHY Specification section 13.4.2 [2], must conform to RFC 6960 [8] 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.

7.3.1 Version Number(s)

OCSP responses must support use of OCSP version 1.

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 CP must undergo a periodic Audit as defined by CableLabs.

8.2 Identity/Qualifications of Assessor

Auditors performing the Audit must be either 1) from an independent Audit firm that is approved to Audit according to AICPA/CICA WebTrust for Certification Authorities principles and criteria, or 2) an IT security specialist and PKI subject matter expert who can offer input regarding acceptable risks, mitigation strategies, and industry best practices.

8.3 Assessor's Relationship to Assessed Entity

The Auditor either must be a private firm that is independent from the entity being audited, or it must be sufficiently organizationally separated from those entities to provide an unbiased, independent evaluation. Auditors must not have a conflict of interest that hinders their ability to perform auditing services.

8.4 Topics Covered by Assessment

The purpose of an Audit must be to verify that a PKI component complies with all the requirements of the current versions of this CP.

The Audit must be a WebTrust for Certification Authorities or an equivalent Audit standard approved by PKI-PA which includes: A Report of Policies and Procedures in Operation and Test of Operational Effectiveness.

All aspects of the CA operation must undergo inspection and should:

- 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

8.5 Actions Taken as a Result of Deficiency

When the Auditor finds a discrepancy between the requirements of this CP and the design, operation, or maintenance of the PKI-PA, the following actions must be performed:

- The Auditor must note the discrepancy
- The Auditor must notify the responsible parties promptly
- The party responsible for correcting the discrepancy will propose a remedy, including expected time for completion, to the PKI-PA

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 pose an immediate threat to the security or integrity of the CableLabs PKI, then the PKI-PA:

- Must determine whether revocation and Compromise reporting are necessary
- Must be entitled to suspend services to the audited entity
- If necessary, may terminate such services related to this CP and the terms of the audited entity's contract

8.6 Communication of Results

Audit results must be communicated to the PKI-PA and may be communicated to others as deemed appropriate.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

Subscribers may be charged a fee for the issuance, management, and renewal of Certificates.

9.1.2 Certificate Access Fees

CAs must 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 must 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 (i.e., DCAA).

9.2 Financial Responsibility

9.2.1 Insurance Coverage

CableLabs 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 must have sufficient financial resources to maintain their operations and perform their duties, and they must be reasonably able to bear the risk of liability to Subscribers 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 Subscriber information must be kept confidential and private:

- CA application records
- Certificate Application records
- Personal or non-public information about Subscribers
- Transactional records (both full records and the Audit trail of transactions)
- Security measures controlling the operations of CA hardware and software

9.3.2 Information Not Within the Scope of Confidential Information

Certificates, Certificate revocation, and other status information, CableLabs repositories, and information contained within them, must not be considered Confidential/Private Information.

9.3.3 Responsibility to Protect Confidential Information

CableLabs PKI Participants receiving private information must secure it from Compromise and disclosure to third parties.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

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

9.4.2 Information Treated as Private

CAs must protect all Subscribers' personally identifying information from unauthorized disclosure. Records of individual transactions may be released upon request of any Subscribers involved in the transaction or their legally recognized agents. The contents of the archives maintained by CAs operating under this CP must not be released except as required by law.

9.4.3 Information Not Deemed Private

Information included in the Certificates is deemed public information and is not afforded protections.

9.4.4 Responsibility to Protect Private Information

Sensitive information must be stored securely and may be released only as required by law.

9.4.5 Notice and Consent to Use Private Information

The PKI-PA or CableLabs CAs are not required to provide any notice or obtain the consent of the Subscriber in order to release private information.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

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

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property Rights

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 DN within any Certificate issued to such Certificate Applicant.

Private keys corresponding to Certificates of CAs and Subscribers are the property of the CAs and Subscribers 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 Rights in and to such Secret Shares.

Without limiting the generality of the foregoing, CableLabs' Root public keys and Certificates containing them, including all CA and Subscriber public keys and Certificates containing them, are the property of CableLabs. CableLabs licenses software and hardware MFRs to reproduce such public key Certificates to place copies in CableLabs compliant hardware devices or software.

9.6 Representations and Warranties

The PKI-PA must:

- Approve the CPS for each CA that issues Certificates under this CP
- Review periodic Audits to ensure that CAs are operating in compliance with their approved CPSs
- Review name space control procedures to ensure that DNs are uniquely assigned for all Certificates issued under this CP
- Revise this CP to maintain the level of assurance and operational practicality
- 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 must warrant that:

- The CA procedures are implemented in accordance with this CP

- The CA will provide its 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
- Its Certificates meet all material requirements of this CP and the applicable CPS
- The revocation of Certificates is 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

To the extent permitted by applicable law, CableLabs disclaims any warranties, including any warranty of merchantability or fitness for a particular purpose.

9.6.3 Subscriber Representations and Warranties

Subscribers must sign an agreement containing the requirements the Subscriber must meet, including protection of their private keys and use of the Certificates before being issued the Certificates. In addition, Subscribers must warrant that:

- The Subscriber must 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 Subscriber and the Certificate has been accepted and is operational (not expired or revoked) at the time the digital signature is created.
- Subscriber's private keys are protected from unauthorized use or disclosure.
- All representations made by the Subscriber in the Certificate Application the Subscriber submitted are true.
- All information supplied by the Subscriber 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 Subscriber will promptly notify the appropriate CA upon suspicion of loss or Compromise of their private key(s).
- The Subscriber is an end-user Subscriber 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.

DCAAs may include additional representations and warranties.

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 must 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 stipulation.

9.7 Disclaimers of Warranties

To the extent permitted by applicable law, DCAAs must disclaim CableLabs' and the applicable Subscriber'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 Subscribers must be as set forth in the applicable DCAAs.

9.9 Indemnities

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

- Falsehood or misrepresentation of fact by the Subscriber on the Certificate Application
- Failure by the Subscriber 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 Subscriber's failure to take the precautions necessary to prevent the Compromise, loss, disclosure, modification, or unauthorized use of the Subscriber's private key(s) or a digital certificate. In the event of the imbedding of a digital certificate in an device not manufactured to the appropriate CableLabs specification Subscriber is to pay to CableLabs the gross revenue from the sale/use of such unauthorized devices.
- The Subscriber'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

This 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, CableLabs 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 PKI Participants

Unless otherwise specified by agreement between the parties, CableLabs PKI Participants must 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 must review this CP at least once every year. Corrections, updates, or changes to this CP must be made publicly available. Suggested changes to this CP must be communicated to the PKI-PA; 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 this CP without notification for amendments that are not material, including without limitation corrections of typographical errors, changes to web links, and changes to contact information. The PKI-PA's decision to designate amendments as material or non-material must be within the PKI-PA's sole discretion.

Change notices to this CP must be distributed electronically to CableLabs PKI Participants and observers in accordance with the PKI-PA document change procedures.

9.12.3 Circumstances Under Which OID Must be Changed

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 must not require a change in certificate policy object identifier.

9.13 Dispute Resolution Provisions

The PKI-PA must facilitate the resolution between entities when conflicts arise as a result of the use of Certificates issued under this CP.

9.14 Governing Law

Subject to any limitation appearing in applicable law, the laws of the State of Colorado, should govern the enforceability, construction, interpretation, and validity of this CP. This choice of law is made to ensure uniform procedures and interpretation for all CableLabs PKI Participants, no matter where they are located.

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 CP must 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 must remain in effect until this CP is updated.

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 this CP must 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, CableLabs PKI agreements (e.g., DCAAs) must include a force majeure clause protecting CableLabs and the applicable Subscriber.

9.17 Other Provisions

No stipulation.