CableLabs PKI Certification Practice Statement

Version 3 Issued

9/11/2019

Copyright Notice

Table of Contents

1 Introduction

1.1 Overview

This Certification Practice Statement (CPS) of the Cable Television Laboratories, Inc. (CableLabs®) PKI Certification Authority (CableLabs CA) applies to the services associated with the issuance and management of CableLabs digital certificates This CPS addresses the technical, procedural, and personnel policies and practices of the CA in all services and during the complete lifecycle of Certificates as issued by the CableLabs CA. This CPS may be updated from time to time.

The purpose of this CPS is to:

- Define the practices used by CableLabs CA to issue certificates.
- Determine if the Subscriber (i.e., Manufacturer or Cable Operator) is fulfilling the requirements of the CableLabs PKI Certificate Policy (CP).
- Assist the Auditors to be sure they are evaluating all aspects of the CableLabs PKI CP
- Ensure consistent Audits by qualified third parties.

This CPS identifies the roles, responsibilities, and practices of all entities involved in the lifecycle, use, reliance upon and management of CableLabs digital certificates. The provisions of this CPS, with regard to practices, level of services, responsibilities and liability, bind all parties involved, including the CA, Registration Authority (RA), Subscribers and Relying Parties. Certain provisions might also apply to other entities such as the Certificate service provider. It is essential to establish the trustworthiness of the entire Certificate Chain of the CableLabs PKI Certificate hierarchy, including the Root CA. A Subscriber or Relying Party of a CableLabs digital certificate may refer to this CPS in order to establish trust.. The CPS is consistent with the Internet X.509 PKI Certificate Policy and Certification Practices Framework [RFC 3647] [3].

1.2 References

This CPS 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

Ref #	Doc Number	Reference Title
[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
[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.
[9]	RFC 2560	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, IETF (Myers, Ankney, Malpani, Galperin, Adams), June 1999.
[10]	https://www.cablelabs.com/resources/digital-certificate-issuance-service/	CableLabs New PKI Certificate Policy Version 1.2

1.3 Document Name and Identification

This document is the CableLabs PKI CPS.

1.4 PKI Participants

This CPS supports the PKI participants as defined in the CableLabs new PKI CP[10] Management Authority (MA)

CableLabs, as the PKI Policy Authority (PKI-PA), may offload some of its duties to a Management Authority (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 Certificate Requesting Accounts (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 the CableLabs PKI CP.

1.4.1 Certification Authorities (CAs)

Refer to the CableLabs New PKI CP [10]

1.4.1.1 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.

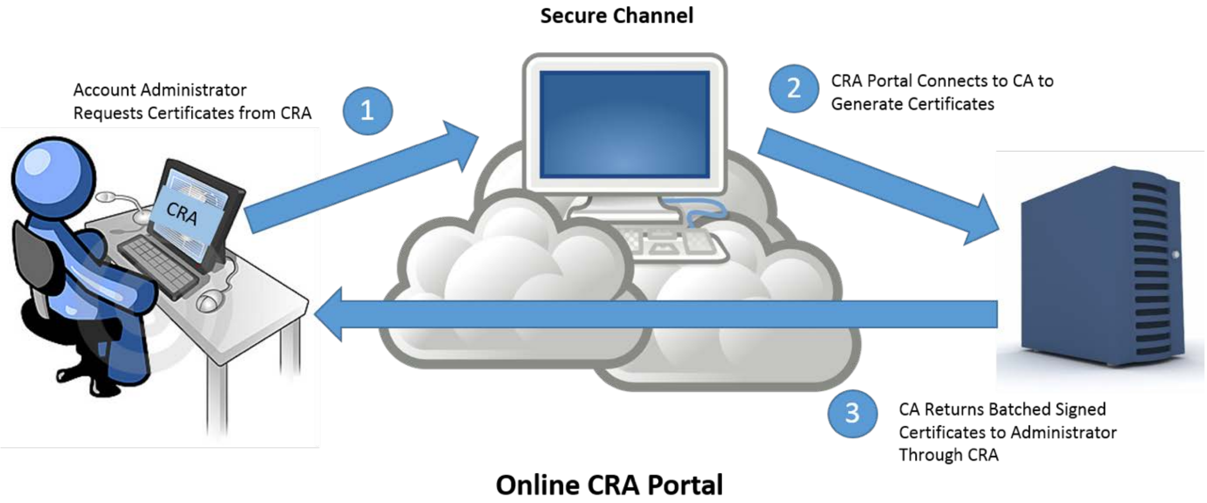
Secure Channel
Account Administrator Requests Certificates from CRA
1
CRA
2
CRA Portal Connects to CA to Generate Certificates
3
CA Returns Batched Signed Certificates to Administrator Through CRA
Online CRA Portal

Figure 1: 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.

1.4.2 Registration Authority (RA)

Refer to the CableLabs New PKI CP [10]

1.4.3 Subscribers

Refer to the CableLabs New PKI CP [10]

1.4.4 Relying Parties

Refer to the CableLabs New PKI CP [10]

1.4.5 Other Participants

Refer to the CableLabs New PKI CP [10]

1.5 Certificate Usage

This CPS supports certificate usage as defined in the CableLabs New PKI CP [10]

Subscribers requesting certificates sign a digital certificate services agreement (DCSA) stating they will only use certificates in devices compliant to specifications and related CPs.

1.5.1 Appropriate Certificate Uses

Refer to the CableLabs New PKI CP [10]

1.5.2 Prohibited Certificate Uses

Refer to the CableLabs New PKI CP [10]

1.6 Policy Administration

1.6.1 Organization Administering the Document

CableLabs is the PKI-PA. It owns the CableLabs PKI CPS and represents the interest of its members in maintaining it for the CableLabs PKI. The PKI-PA is responsible for all aspects of the CPS, including:

- Maintaining the CPS
- Governing and operating the PKI according to the CPS
- Approving the CPS for CAs that issue Certificates under a given CP

1.6.2 Contact Person

Inquiries regarding this CPS can be directed to CableLabs at:

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

303-661-9100

1.6.3 Person Determining CPS Suitability for the Policy

CableLabs CAs submit their completed CPS to the PKI-PA, which evaluates the CPS and determines the suitability and applicability of the CPS to the CableLabs PKI CP.

1.6.4 CPS Approval Procedures

Before commencing operations, CAs in the CableLabs PKI submit their CPS to the PKI-PA for approval. Once approved, CAs may commence operations.

1.7 Definitions and Acronyms

1.7.1 Definitions

This CPS 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.
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.

Term	Description
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.
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.

Term	Description
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.
Root CA Operator	CableLabs or a 3rd party that issues and distributes CAs.
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.
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 (i.e., 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.

Term	Description
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 CPS 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
HFC	Hybrid-Fiber/Coax
HSM	Hardware Security Module
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
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

Term	Description
RA	Registration Authority
RFC	Request for Comment
RSA	Rivest, Shamir, Adelman

2 Publication and Repository Responsibilities

2.1 Repositories

CableLabs makes its Root Certificate, CA Certificates, Sub-CA Certificates, and revocation data for issued digital Certificates available in its online repository located at http://www.cablelabs.com/resources/digital-certificate-issuance-service/.

2.2 Publication of Certification Information

The CableLabs Root Certificate, CA Certificates, Sub-CA Certificates, and revocation data for issued digital Certificates is available through several means of communications:

- *On the web: www.cablelabs.com*
- *By email to:* PKIOps@CableLabs.com
- *By Telephone: 303-661-9100*
- *By Fax: 303-664-9199*

Information not intended for public dissemination is protected by CableLabs IT access controls.

2.3 Time or Frequency of Publication

CableLabs publishes changes to the CableLabs PKI CP within thirty (30) week days after their approval by the PKI–PA.

A CableLabs selected Root CA operator provides the CA Certificates issued by the Root CA to CableLabs as soon as possible after issuance.

CableLabs publishes its CA Certificates in its repository within ten (10) week days after issuance.

(N/A for Sub-CAs)

2.4 Access Controls on Repositories

CableLabs applies read-only access to the repository for unrestricted public viewing. Logical and physical access controls prevent unauthorized addition, deletion, or modification to the repository entries.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of Names

The CableLabs CA assigns X.501 Distinguished Names (DNs) [4] with the issuer and Subject DN fields in Certificates populated with a non-empty DN as shown in the Table 2.

3.1.2 Need for Names to Be Meaningful

CableLabs uses DNs that identify the entity (i.e., organization and device MAC address) that is the Subject of the Certificate.

The CableLabs Certificate Application process uses DNs that identify the entity (i.e., organization and device MAC address) that is the Subject of the Certificate and the entity that is the issuer of the Certificate.

3.1.3 Anonymity or Pseudonymity of Subscribers

The CableLabs Certificate Application process does not allow the issuance of anonymous or pseudonymous Certificates. It validates that the organization name in the Subject DN appears in a business database and is in good standing.

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

CableLabs CAs maintain a database of all issued Certificates within its domain to enforce unique Subject DNs for all issued Certificates.

3.1.6 Recognition, Authentication, and Role of Trademarks

CableLabs does not verify an Applicant's right to use a trademark and does not resolve trademark disputes. CableLabs may reject any application or require revocation of any Certificate that is part of a trademark dispute.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

CableLabs CAs establish that the Applicant holds the private key corresponding to the public key by performing signature verification on the CSR file submitted by the Applicant.

3.2.2 Authentication of Organization Identity

CableLabs CAs validate the identity of the organization 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

CableLabs CAs verify that the organization requesting a Certificate appears on the authorized organization list issued by the PKI-PA and that only duly authorized representatives of the organization, which can act on behalf of the organization, can request Certificates.

CableLabs CAs verify, with an authorized organization, that the requester of a Certificate is a duly authorized representative of the organization and can act on behalf of the organization.

3.2.4 Non-verified Subscriber Information

Non-verifiable information may be included in CableLabs PKI Certificates if allowed by the CP such as:

- *Organizational Unit (OU)*
- *Any other information designated as non-verified in the Certificate*

3.2.5 Validation of Authority

CableLabs CAs verify, with an authorized organization, that the individuals listed on their DCAA are duly authorized representatives of the organization and can act on behalf of the organization.

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

CableLabs CAs' identification and authentication of Certificate re-key requests follow the same requirements as for an initial Certificate issuance request (see section 3.2), but may also rely on information previously provided or obtained during the initial Certificate request.

3.3.2 Identification and Authentication for Re-key After Revocation

For revoked Certificates, CableLabs CAs apply the initial Certificate issuance requirements (see section 3.2) prior to rekeying the Certificate.

3.4 Identification and Authentication for Revocation Request

CableLabs CAs authenticate that all revocation requests are received from a duly authorized representative of the organization listed on the Subject DN of the Certificate to be revoked, or a representative of the PKI-PA.

For revoked Certificates, CableLabs CAs apply the initial Certificate issuance requirements (see section 3.2) prior to issuance of a new Certificate.

4 Certificate Lifecycle Operational Requirements

4.1 Certificate Application

The CableLabs Certificate issuance process is described in sections 4.1, 4.2, 4.3 and 4.4.

4.1.1 Who Can Submit a Certificate Application

Individuals authorized to request Certificates on behalf of the Applicant may submit Certificate requests. Applicants are responsible for any data supplied in a Certificate request. CableLabs CAs do not knowingly issue Certificates to entities on a government denied list maintained by the United States or that is located in a country with which the laws of the United States prohibit doing business.

4.1.2 Enrollment Process and Responsibilities

Communications between the CA and RA are authenticated and secured by secure electronic communications, such as secure email, or by out-of-band methods such as hand delivery of the information.

- *For CableLabs CAs, the enrollment process includes:Submitting an executed DCAA*
- *Submitting a Certificate Application*
- *Paying any applicable fees*
- *Delivering the public key Certificate to the Applicant*

4.2 Certificate Application Processing

CableLabs CAs verify that the information in a Certificate Application is accurate as described in the following sections.

4.2.1 Performing Identification and Authentication Functions

After receiving a Certificate Application, the CableLabs CAs verify the fully executed DCAA and the Certificate Application information. The CAs check that the Subject DN organization name is authorized to request Certificates and its name appears in a business database.

4.2.2 Approval of Certificate Applications

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

- *Receipt of a fully executed DCAA*
- *Receipt of a validly 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

CableLabs CAs begin processing a Certificate Application once they have received a fully executed DCAA.

4.3 Certificate Issuance

CableLabs CAs/RAs confirm the source of the Certificate request before issuance and review that the Certificate Application information is compliant with the Certificate profile specified in the DOCSIS 3.1 Security Specification [1].

4.3.1 CA Actions During Certificate Issuance

Upon receiving the request, the CableLabs CAs will:

- 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

4.3.2 Notification to Subscriber by the CA of Issuance of Certificates

CableLabs CAs deliver Certificates in a secure manner to Subscribers within a reasonable time after issuance. Generally, CableLabs CAs deliver Certificates via email to the email address designated by the Subscriber in the DCAA.

4.4 Certificate Acceptance

Certificates are 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

CableLabs publishes its CA Certificates in its repository within ten (10) business days after issuance.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

The CableLabs PKI Root CA provides notification of a Certificate issuance to the PKI-PA via email to the email address agreed to between the Root CA and PKI-PA.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

CableLabs CAs set the Certificate extensions according to the Certificate profiles specified in the DOCSIS 3.1 Security Specification [1].

Subscribers are contractually obligated to protect their private keys from unauthorized use or disclosure and to discontinue using a private key after expiration or revocation of the associated Certificate.

4.5.2 Relying Party Public Key and Certificate Usage

Refer to the CableLabs New PKI CP [10]

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

The CableLabs CA will not further re-key, renew, or modify the original Certificate once it has been renewed.

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

CableLabs CAs process renewal applications in the same manner as those used during the Certificate's original issuance.

The Root CA will request approval from the PKI-PA before performing a CA Certificate renewal.

4.6.4 Notification of New Certificate Issuance to Subscriber

CableLabs CAs deliver Certificates in a secure manner to Subscribers within a reasonable time after issuance. Generally, CableLabs CAs deliver Certificates via email to the email address designated by the Subscriber in the DCAA or via the CableLabs CA website..

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

CableLabs publishes its CA Certificates in its repository within ten (10) business days after issuance.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

The Root CA will request approval from the PKI-PA before issuing 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

CableLabs CAs process Certificate re-key applications in the same manner as those used during the Certificate's original issuance.

The Root CA will request approval from the PKI-PA before re-keying a CA Certificate.

4.7.4 Notification of New Certificate Issuance to Subscriber

CableLabs CAs deliver Certificates to Subscribers within a reasonable time after issuance. Generally, CableLabs CAs deliver Certificates via email to the email address designated by the Subscriber in the DCAA or via the CableLabs CA website.

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

CableLabs publishes its CA Certificates in its repository within ten (10) business days after issuance.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

The Root CA will request approval from the PKI-PA before issuing a Sub-CA Certificate.

4.8 Certificate Modification

The CableLabs CA will not further re-key, renew, or modify the original Certificate once it has been 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

CableLabs CAs process Certificate modification applications in the same manner as those used during the Certificate's original issuance.

The Root CA will request approval from the PKI-PA before modification of a CA Certificate.

4.8.4 Notification of New Certificate Issuance to Subscriber

CableLabs CAs deliver Certificates in a secure manner to Subscribers within a reasonable time after issuance. Generally, CableLabs CAs deliver Certificates via email to the email address designated by the Subscriber in the DCAA.

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

CableLabs publishes its CA Certificates in its repository within ten (10) business days after issuance.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

The Root CA will request approval from the PKI-PA before issuing a Sub-CA Certificate.

4.9 Certificate Revocation and Suspension

Relying Parties may obtain CableLabs CA Certificate revocation information from the CableLabs website or by email.

4.9.1 Circumstances for Revocation

CableLabs CAs may revoke any Certificate in their sole discretion, including if they believe that:

- 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:
- 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
    - 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 the Certificate is harmful to the Ecosystem

CableLabs CAs place all revoked Certificates in the appropriate CRL until the revoked Certificate expires.

4.9.2 Who Can Request Revocation

Within the CableLabs PKI, revocation requests may include the following:

- 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

CableLabs CAs process a revocation request as follows:

1. *They log the identity of the entity making the request and the reason for requesting revocation*

2. *They may request confirmation of the revocation from a known administrator, where applicable, via out-of-band communication (e.g., telephone, fax, etc.)*
3. *If the request is authenticated as originating from the Subscriber, they revoke the Certificate*
4. *For requests from third parties, CableLabs CAs begin investigating the request within 5 business days after receipt and decide whether revocation is appropriate based on the following criteria:*
   a. *the nature of the alleged problem*
   b. *the number of reports received about a particular Certificate*
   c. *the identity of the complainants (for example, complaints from a law enforcement official*
5. *If it is determined that revocation is appropriate, the Certificate is revoked and placed on the CRL*

CableLabs CAs authenticate the request. Acceptable procedures for authenticating revocation requests include:

- *Having the Subscriber log into 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*

CableLabs CAs obtain approval from the PKI-PA prior to performing a revocation. The CA sends a written notice and brief explanation for the revocation to the Subscriber.

The requests from CAs to revoke a CA Certificate are authenticated by 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

CableLabs CAs will begin investigation of a Certificate revocation request within five (5) business days of receipt of a revocation request.

4.9.6 Revocation Checking Requirement for Relying Parties

CableLabs CAs will provide Relying Parties with information on how to find the appropriate CRL or OCSP responder (if available) on their web-based repository.

The PKI-PA posts CA Certificates in a CRL or OCSP responder (if available).

4.9.7 CRL Issuance Frequency

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

4.9.8 Maximum Latency for CRLs

CRLs are published within 24 hours of generation.

4.9.9 On-line Revocation/Status Checking Availability

CableLabs CAs will provide Relying Parties with information on how to find the appropriate CRL or OCSP responder (if available) on their web-based repository.

4.9.10 On-line Revocation Checking Requirements

Refer to the CableLabs New PKI CP [10]

4.9.11 Other Forms of Revocation Advertisements Available

CableLabs CAs employing an alternative method to publicize revoked Certificates will describe the method in this CPS.

4.9.12 Special Requirements Regarding Key Compromise

CableLabs CAs will issue a new CRL within 24 hours after confirmation of a CA Certificate compromise.CableLabs CAs use commercially reasonable efforts to notify potential Relying Parties if it discovers or suspects the compromise of a Private Key.

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

A CSS will assert all the policy OIDs for which it is authoritative.

4.10.1 Operational Characteristics

No stipulation.

4.10.2 Service Availability

Refer to the CableLabs New PKI CP [10]

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

A Subscriber's subscription service ends if its Certificate expires or is revoked, or if the applicable Subscriber Agreement expires without renewal.

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

CableLabs CAs protect their equipment from unauthorized access and implement physical controls to reduce the risk of equipment tampering. The secure parts of CA hosting facilities are protected using physical access controls making them accessible only to appropriately authorized individuals.CableLabs CAs securely store all removable media and paper containing sensitive plaintext information related to their CA operations in secure containers in accordance with its data classification policy.

5.1.1 Site Location and Construction

The CableLabs PKI facility is equipped with logical and physical controls that make CableLabs CA operations inaccessible to non-trusted personnel.

5.1.2 Physical Access

Building access control system minimizes exposure of privileged functions through definition of function-specific roles or authorization groups and enforcement. Uses proximity card identification badges ,maintains logs of access to the building and maintains video survelliance of the perimeter of the building. When a potential or actual breach is detected an outside alarm monitoring agency is notified.

Access to the room housing the CA requires two-factor authentication—the individual must have an authorized access card and pin.

CableLabs deactivates and securely stores its CA equipment when not in use. Activation data must either be memorized or recorded and stored in a manner commensurate with the security afforded the cryptographic module. Activation data is never stored with the cryptographic module or removable hardware associated with equipment used to administer private keys.

If CableLabs ever becomes aware that the CA is to be left unattended or has been left unattended for an extended period of time, CableLabs personnel will perform a security check of the data center to verify that:

1. *Equipment is in a state appropriate to the current mode of operation*
2. *Any security containers are properly secured*
3. *Physical security systems (e.g., door locks) are functioning properly*
4. *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.

> *Access to the RA computers require username and password authentication—the individual must have authorized access. RA documentation is securely stored on password and permission controlled server. RA computers' hard drives are encrypted to protect data when the computer is turned off should the hard drive be removed from the computer.*

5.1.3 Power and Air Conditioning

The CableLabs CA facility has primary and secondary power supplies that ensure continuous and uninterrupted access to electric power. Uninterrupted Power Supplies (UPS) and diesel generators provide redundant backup power.The CableLabs CA facility uses multiple load-balanced HVAC systems for heating, cooling, and air ventilation to prevent overheating and to maintain a suitable humidity level.

5.1.4 Water Exposures

The CableLabs CA facility is located on the second floor of the CableLabs building and is situated so that it is isolated from excess moisture.

5.1.5 Fire Prevention and Protection

The CableLabs CA facility is equipped with fire suppression mechanisms.

5.1.6 Media Storage

CableLabs CAs protect their media from accidental damage and unauthorized physical access. Backup files are created on a periodic basis and are maintained at locations separate from the primary CA operations facility.

5.1.7 Waste Disposal

All unnecessary copies of printed sensitive information are shredded on-site before disposal. All electronic media are zeroized (all data is overwritten with binary zeros so as to prevent the recovery of the data).

5.1.8 Off-site Backup

CableLabs CAs maintain at least one full backup and make regular backup copies of any information necessary to recover from a system failure. Backup copies of CA private keys and activation data are stored for disaster recovery purposes off-site in safe deposit boxes at a local bank and are accessible only by trusted personnel.

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

Personnel acting in trusted roles include CA and RA system administration personnel, and personnel involved with identity vetting and the issuance and revocation of Certificates. The functions and duties performed by persons in trusted roles are distributed so that one person alone cannot circumvent security measures or subvert the security and trustworthiness of the PKI operations. All personnel in trusted roles must be free from conflicts of interest that might prejudice the impartiality of the PKI's operations. Trusted roles are appointed by senior management. A list of personnel appointed to trusted roles is maintained and reviewed annually.

5.2.2 Number of Persons Required per Task

CableLabs CAs require that at least two people acting in a trusted role take action requiring a trusted role, such as activating CA private keys, generating a CA key pair, or backing up a CA private key.

5.2.3 Identification and Authentication for Each Role

All personnel are required to authenticate themselves to CA and RA systems before they are allowed access to systems necessary to perform their trusted roles.

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

Trusted roles are appointed by senior management. A list of personnel appointed to trusted roles is maintained and reviewed annually.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

CableLabs CAs ensure that all individuals assigned to trusted roles have the experience, qualifications, and trustworthiness required to perform their duties under this CPS.

5.3.2 Background Check Procedures

CableLabs CAs verify the identity of each employee appointed to a trusted role and perform a background check prior to allowing such person to act in a trusted role. This requires each individual to appear in-person before a human resources employee whose responsibility it is to verify identity. The human resources employee verifies the individual's identity using government-issued photo identification (e.g., passports and/or driver's licenses reviewed pursuant to U.S. Citizenship and Immigration Services Form I-9, Employment Eligibility Verification, or comparable procedures for the jurisdiction in which the individual's identity is being verified). Background checks include employment history, education, character references, social security number, previous residences, driving records and criminal background. Checks of previous residences are over the past three years. All other checks are for the previous five years. The highest education degree obtained is verified regardless of the date awarded. Based upon the information obtained during the background check, the human resources department makes an adjudication decision, with the assistance of legal counsel when necessary, as to whether the individual is suitable for the position to which he/she will be assigned.

5.3.3 Training Requirements

CableLabs CAs provide skills training to all employees involved in PKI operations. The training relates to the person's job functions and covers:

- *Basic PKI knowledge*
- *Authentication and verification policies and procedures*
- *Disaster recovery and business continuity procedures*
- *Applicable industry and government guidelines*

5.3.4 Retraining Frequency and Requirements

CableLabs CA personnel must maintain skill levels that are consistent with industry-relevant training and performance programs in order to continue acting in trusted roles. CableLabs CAs make all personnel acting in trusted roles aware of any changes to its PKI operations. If the PKI operations change, the CableLabs CAs will provide documented training, in accordance with an executed training plan, to all personnel acting in trusted roles.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

CableLabs CA personnel failing to comply with this CPS, whether through negligence or malicious intent, are subject to administrative or disciplinary actions, including termination of employment. If a person in a trusted role is cited by management for unauthorized or inappropriate actions, the person will be immediately removed from the trusted role pending *management review. After management has reviewed and discussed the incident with the employee involved, management may reassign that employee to a non-trusted role or dismiss the individual from employment as appropriate.*

5.3.7 Independent Contractor Requirements

Independent contractors, who are assigned to perform trusted roles, are subject to the duties and requirements specified for such roles in this CPS.

5.3.8 Documentation Supplied to Personnel

Personnel in trusted roles are provided with the documentation necessary to perform their duties, including a copy of the CP, this CPS, and other technical and operational documentation needed to maintain the integrity of CA operations. Personnel are also given access to information on internal systems and security documentation, identity vetting policies and procedures, and other information.

5.4 Audit Logging Procedures

.

CableLabs CA systems require identification and authentication at system logon with a unique user name and password. Important system actions are logged to establish the accountability of the operators who initiate such actions.

5.4.1 Types of Events Recorded

The CableLabs CA system requires identification and authentication at system logon with a unique user name and password. Important system actions are logged to establish the accountability of the operators who initiate such actions.The CableLabs CA system enables all essential event auditing capabilities of its CA applications in order to record the events listed below. If the applications cannot automatically record an event, the CableLabs CA administrators implement manual procedures to satisfy the requirements. Each event records the relevant (i) date and time, (ii) type of event, (iii) success or failure, and (iv) user or system that caused the event or initiated the action.

- 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)
  - Anytime cryptographic keys are accessed

- 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

- 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
  - Backup to store off site material

- 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 system
  - Unauthorized attempts to access system files
  - Failed read and write operations on the Certificate
  - Personnel changes

5.4.2 Frequency of Processing Log

The CableLabs CA administrator reviews the logs generated by the CA system once every three (3) months, makes system and file integrity checks, and conducts a vulnerability assessment. During these checks, the administrator (i) checks whether anyone has tampered with the log, (ii) scans for anomalies or specific conditions, including any evidence of malicious activity, and (iii) prepares a written summary of the review. Any anomalies or irregularities found in the logs are investigated. The summaries include recommendations to CA operations management and any actions taken as a result of a review.

5.4.3 Retention Period for Audit Log

The CableLabs CA retains Audit logs on-site at least for two (2) months or until after they are reviewed. Archive records are retained for ten (10) years. The individuals who remove Audit logs from the CA systems are different than the individuals who control the CA signature keys.

5.4.4 Protection of Audit Log

CA Audit log information is retained on equipment until after it is copied by a system administrator. The CA system is configured to ensure that (i) only authorized people have read access to logs, (ii) only authorized people may archive Audit logs, and (iii) Audit logs are not modified. Audit logs are protected from destruction prior to the end of the Audit log retention period and are retained securely on-site until transferred to a backup site. The CableLabs CA off-site storage location is a safe and secure location that is separate from the location where the data was generated.

5.4.5 Audit Log Backup Procedures

The CableLabs CA makes regular backup copies of Audit logs and Audit log summaries and sends a copy of the Audit log off-site on a monthly basis.

5.4.6 Audit Collection System (Internal vs. External)

Automatic Audit processes begin on system startup and end at system shutdown. If an automated Audit system fails and the integrity of the system or confidentiality of the information protected by the system is at risk, the administrators will consider suspending the CA's operations until the problem is 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 CableLabs CA performs annual risk assessments that identify and assess reasonably foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate data or Certificate issuance process. It also routinely assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to control such risks. Internal Auditors review the Audit data checks for continuity. The CableLabs CA Audit log monitoring tools alert the appropriate personnel of any events, such as repeated failed actions, requests for privileged information, attempted access of system files, and unauthenticated responses.

5.5 Records Archival

The CableLabs CA complies with all record retention policies that apply by law. It includes sufficient detail in all archived records to show that a Certificate or time-stamp token was issued in accordance with this CPS.

5.5.1 Types of Events Archived

The CableLabs CA retains the following information in its archives

- DCAAs
- All CRLs issued and/or published
- Audit reports

- Destruction of cryptographic modules
- All Certificate Compromise notifications

5.5.2 Retention Period for Archive

The CableLabs CA retains archived data associated with CA system, or the supporting issuance, archives data for certificate types for at least ten (10) years.

5.5.3 Protection of Archive

Archive records are stored in a secure off-site server cloud location and are maintained in a manner that prevents unauthorized modification, substitution, or destruction. Archives are not released except as allowed by the PKI-PA or as required by law. The CableLabs CA maintains any software application required to process the archive data until the data is either destroyed or transferred to a newer medium.If the CableLabs CA needs to transfer any media to a different archive site or equipment, it will maintain both archived locations and/or pieces of equipment until the transfer is complete. All transfers to new archives will occur in a secure manner.

5.5.4 Archive Backup Procedures

On at least a monthly basis, the CableLabs CA creates an archive disk of the Audit data by grouping the data types together by source into separate, compressed archive files. Each archive file is hashed to produce checksums that are stored separately for integrity verification at a later date. The CableLabs CA stores the archive disk in a secure off-site location for the duration of the set retention period.

5.5.5 Requirements for Time-Stamping of Records

The CableLabs CA automatically time-stamps archived records with system time as they are created and are checked with an authoritative time standard.

5.5.6 Archive Collection Systems (Internal or External)

Archive information is collected internally by the CableLabs CA.

5.5.7 Procedures to Obtain and Verify Archive Information

The CableLabs CA may elect to retrieve the information from archival after receiving a request made for a proper purpose by a customer, its agent, or a party involved in a dispute over a transaction involving the CableLabs PKI. The integrity of archive information is verified by comparing a hash of the compressed archive file with the file checksum originally stored for that file. The CableLabs CA may elect to transmit the relevant information via a secure electronic method or courier, or it may also refuse to provide the information in its discretion and may require prior payment of all costs associated with the data.

5.6 Key Changeover

Toward the end of a CA private key's lifetime, CableLabs ceases using the expiring CA private key to sign Certificates and uses the old private key only to sign CRLs and OCSP responder Certificates. A new CA signing key pair is commissioned and all subsequently issued

Certificates and CRLs are signed with the new private signing key. Both the old and the new key pairs may be concurrently active. This key changeover process helps minimize any adverse effects from CA certificate expiration. The corresponding new CA public key Certificate is provided to Subscribers and relying parties through the delivery methods detailed in this CPS.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

The CableLabs CA maintains incident response procedures to guide personnel in response to security incidents, natural disasters, and similar events that may give rise to system compromise. It reviews, tests, and updates its incident response plans and procedures on at least an annual basis.

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

The CableLabs CA makes regular system backups on at least a monthly basis and maintains backup copies of its private keys, which are stored in a secure, off-site location. If it discovers that any of its computing resources, software, or data operations have been compromised, the CableLabs CA assesses the threats and risks that the compromise presents to the integrity or security of its operations or those of affected parties. If it determines that a continued operation could pose a significant risk to Relying Parties or Subscribers, the CableLabs CA suspends such operation until it determines that the risk is mitigated.

5.7.3 Entity (CA) Private Key Compromise Procedures

If the CableLabs CA suspects that one of its private keys has been Compromised or lost then an emergency response team will convene and assess the situation to determine the degree and scope of the incident and take appropriate action. Specifically, the CableLabs CA will perform the actions listed:

- 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 the CableLabs PKI 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

The CableLabs CA may generate a new key pair and sign a new Certificate. If a disaster physically damages its equipment and destroys all copies of the CA signature keys then the CableLabs CA will provide notice to affected parties at the earliest feasible time.

5.7.4 Business Continuity Capabilities After a Disaster

To maintain the integrity of its services, the CableLabs CA implements data backup and recovery procedures as part of its Business Continuity Management Plan (BCMP). Stated goals of the BCMP are to ensure that CSS be only minimally affected by any disaster involving the CableLabs CA facility and that the CableLabs CA be capable of maintaining other services or resuming them as quickly as possible following a disaster. The CableLabs CA reviews, tests, and updates the BCMP and supporting procedures at least annually.The CableLabs CA systems are redundantly configured at its facility and can be mirrored at a separate, geographically diverse location for failover in the event of a disaster. If a disaster causes the primary CA operations to become inoperative, the CableLabs CA will re-initiate its operations at its secondary location giving priority to the provision of certificate status information and time stamping capabilities, if affected.

5.8 CA and RA Termination

The CableLabs CA system will perform the following:

- 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

The CableLabs CA key pairs are generated by individuals acting in trusted roles and using a cryptographic hardware device as part of scripted Key Generation Ceremony. The cryptographic hardware is evaluated to FIPS 140-2 [7]. Activation of the hardware requires the *use of two-factor authentication tokens. The CableLabs CA creates auditable evidence during the key generation process to prove that the CPS was followed and role separation was enforced during the key generation process. The CableLabs CA requires that an internal Auditor, external Auditor, or independent third party attend the ceremony, or an external Auditor examines the signed and documented record of the Key Generation Ceremony, as allowed by applicable policy.*

6.1.1.2 Subscriber Key Pair Generation

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

When the CableLabs CA generates key pairs on behalf of the Subscriber, the keys will be delivered electronically (such as through secure email or stored in a cloud-based system) or on a hardware cryptographic module. In all cases, it will follow the requirement listed below:

- The CA must not retain any copy of the key for more than 2 weeks 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.

When assisting the Subscriber with key generation, the CableLabs CA shall maintain a record of the Subscriber's acknowledgement of receipt of the Subscriber's key pair.

6.1.2 Private Key Delivery to Subscriber

When the CableLabs CA generates key pairs on behalf of the Subscriber, the keys will be encrypted and delivered electronically (such as through secure email or stored in a cloud-based system) or on a hardware cryptographic module.

6.1.3 Public Key Delivery to Certificate Issuer

Subscribers generate key pairs and submit the public key to the CableLabs CA in a PKCS #10 CSR as part of the Certificate request process. The Subscriber's signature on the request is authenticated prior to issuing the Certificate.

6.1.4 CA Public Key Delivery to Relying Parties

Relying Parties may obtain CableLabs CA Certificates from the CableLabs website (www.cablelabs.com)or by email.

6.1.5 Key Sizes

The CableLabs CA follows the key size requirements in the CP document.

6.1.6 Public Key Parameters Generation and Quality Checking

The CableLabs CA reviews key size settings on all Certificate requests to confirm that they meet the key size requirements as defined in the CP.

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

The CableLabs CA reviews keyUsage settings on all Certificate requests to confirm that they meet the keyUsage requirements as specified in the DOCSIS 3.1 Security Specification [1].

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

The CableLabs CA ensures that the private key of a Certificate is properly generated, used, and stored in a crypto module that meets or exceeds the requirements of the FIPS 140 [7] level listed below for the specific type of Certificate being issued.

- 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

The CableLabs CA authentication mechanism is protected securely when not in use and may only be accessed by actions of multiple trusted persons.Backups of CA private keys are securely stored off-site and require two-person access. Re-activation of a backed-up CA private key requires the same security and multi-person control as when performing other sensitive CA private key operations.

6.2.3 Private Key Escrow

The CableLabs CA does not escrow its signature keys. The CableLabs CA may provide escrow services for other types of Certificates in order to provide key recovery services.

6.2.4 Private Key Backup

CA key pairs are backed up by multiple trusted individuals using a cryptographic hardware device as part of scripted key backup process. The CA private keys are generated and stored inside a cryptographic module, which has been evaluated to at least FIPS 140-2 [7]. When keys are transferred to other media for backup and disaster recovery purposes, the keys are transferred and stored in an encrypted form.

6.2.5 Private Key Archival

The CableLabs CA does not archive private keys.

6.2.6 Private Key Transfer into or from a Cryptographic Module

All keys must be generated by and in a cryptographic module. Private keys are exported from the cryptographic module into backup tokens only for Hardware Security Module (HSM) transfer, offline storage, and backup purposes. The private keys are encrypted when transferred out of the module and never exist in plaintext form. When transported between cryptographic modules, the CableLabs CA encrypts the private key and protects the keys used for encryption from disclosure. Private keys used to encrypt backups are securely stored and require two-person access.

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

CA private keys are activated according to the specifications of the cryptographic module manufacturer. Activation data entry is protected from disclosure.

6.2.8.1 CA Administrator Activation

The CA administrator is activated according to the activation requirements below. Activation data entry is protected from disclosure.

- 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

Offline CA private keys are activated according to the specifications of the cryptographic module manufacturer. Activation data entry is protected from disclosure.

6.2.8.3 Online CA Private Keys

Online CA private keys are activated according to the specifications of the cryptographic module manufacturer. Activation data entry is protected from disclosure.

6.2.8.4 Subscriber Private Keys

Subscribers are solely responsible for protecting their private keys. Subscribers should use a strong password or equivalent authentication method to prevent unauthorized access or use of the Subscriber's private key.

6.2.9 Method of Deactivating Private Keys

CA private keys are deactivated via logout procedures on the applicable HSM when not in use are securely stored. Root private keys are further deactivated by removing them entirely from the storage partition on the HSM.

6.2.10 Method of Destroying Private Keys

CableLabs CA personnel, acting in trusted roles, destroy CA, RA, and CSS private keys when no longer needed. Subscribers shall destroy their private keys when the corresponding Certificate is revoked or expired or if the private key is no longer needed.

The CableLabs CA may destroy a private key by deleting it from all known storage partitions. It also zeroizes the HSM and associated backup tokens according to the specifications of the hardware manufacturer. This reinitializes the device and overwrites the data with binary zeros. If the zeroization or re-initialization procedure fails, the device will be crushed, shredded, and/or incinerated in a manner that destroys the ability to extract any private key.

6.2.11 Cryptographic Module Rating

See CableLabs PKI CP section 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

The CableLabs CA archives copies of public keys in accordance with Section 5.5.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The CableLabs CA follows the validity period requirements as defined in the CP.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The CableLabs CA activates the cryptographic module containing its CA private keys according to the specifications of the hardware manufacturer. This method has been evaluated as meeting the requirements of FIPS 140-2 Level 3 [7]. The cryptographic hardware is held under two-person control. The CableLabs CA will only transmit activation data via an appropriately protected channel and at a time and place that is distinct from the delivery of the associated cryptographic module.All CableLabs CA personnel and Subscribers are instructed to use strong passwords and to protect PINs and passwords. CableLabs CA employees are *required to create non-dictionary, alphanumeric passwords with a minimum length and to change their passwords on a regular basis. If the CableLabs CA uses passwords as activation data for a signing key, it will change the activation data change upon rekey of the CA Certificate.*

6.4.2 Activation Data Protection

The CableLabs CA protects data used to unlock private keys from disclosure using a combination of cryptographic and physical access control mechanisms. Protection mechanisms include keeping activation mechanisms secure using role-based physical control. All CableLabs CA personnel are instructed not to share their password with another individual. The CableLabs CA locks accounts used to access secure CA processes if a certain number of failed password attempts occur.

6.4.3 Other Aspects of Activation Data

The CableLabs CA, RA, and CSS reset their activation data whenever the token is re-keyed or returned from maintenance.

6.4.3.1 Activation Data Transmission

The CableLabs CA protects the transmission of activation data using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys.

6.4.3.2 Activation Data Destruction

The CableLabs CA may destroy activation for a private key by deleting it from all known storage partitions. It also zeroizes the HSM and associated backup tokens according to the specifications of the hardware manufacturer. This reinitializes the device and overwrites the data with binary zeros. If the zeroization or re-initialization procedure fails, the device will be crushed, shredded, and/or incinerated in a manner that destroys the ability to extract any private key activation data.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The CableLabs CA secures its CA systems and authenticates and protects communications between its systems and trusted roles. The CA workstations run on trustworthy systems that are configured and hardened using industry best practices. All CA systems are scanned for malicious code and protected against spyware and viruses.

6.5.2 Computer Security Rating

No stipulation.

6.6 Lifecycle Technical Controls

6.6.1 System Development Controls

The CableLabs CA follows the system development controls listed. It monitors the acquisition and development of its CA systems. Change requests require the approval of at least one *administrator who is different from the person submitting the request. The CableLabs CA only installs software on CA systems if the software is part of the CA's operation. CA hardware and software are dedicated to performing operations of the CA.*

Non-PKI hardware and software is purchased without identifying the purpose for which the component will be used. All hardware and software are shipped under standard conditions to ensure delivery of the component directly to a trusted employee who ensures that the equipment is installed without opportunity for tampering.

Some of the PKI software components used are developed in-house or by consultants using standard software development methodologies. All such software is designed and developed in a controlled environment and subjected to quality assurance review. Other software is purchased commercial off the shelf (COTS). Quality assurance is maintained throughout the process through testing and documentation or by purchasing from trusted vendors.

Updates of equipment and software are purchased or developed in the same manner as the original equipment or software and are installed and tested by trusted and trained personnel. All hardware and software essential to CA's operations is scanned for malicious code on first use.

6.6.2 Security Management Controls

The CableLabs CA monitors the security-related configurations of its CA systems. When loading software onto a CA system, it verifies that the software is the correct version and is supplied by the vendor free of any modifications. The CableLabs CA verifies the integrity of software used with its CA processes on first use.

6.6.3 Lifecycle Security Controls

No stipulation.

6.7 Network Security Controls

The CableLabs CA documents and controls the configuration of its systems, including any upgrades or modifications made. The CA system is not connected to any network. CA Keys are kept offline and brought online only when necessary to for Certificate issuance.

6.8 Time-Stamping

The CableLabs CA electronically or manually time-stamps Certificate management records with system time as they are created.

7 Certificate, CRL AND OCSP Profiles

7.1 Certificate Profile

The CableLabs CA follows the Certificate profile basic fields in Table 7 as specified in the RFC 5280 [6].

7.1.1 Version Number(s)

All Certificates issued by the CableLabs CAs are X.509 version 3 Certificates.

7.1.2 Certificate Extensions

The CableLabs CA follows the standard Certificate extensions in Table 8 through Table 11 as specified in the DOCSIS 3.1 Security Specification [1].

7.1.2.1 Subject Key Identifier Extension

The CableLabs CA follows the subjectKeyIdentifier extension in Table 12 as specified in the DOCSIS 3.1 Security Specification [1].

7.1.2.2 Basic Constraints Extension

The CableLabs CA follows the basicConstraints extension in Table 13 and Table 14 as specified in the DOCSIS 3.1 Security Specification [1].

7.1.2.3 Extended Key Usage

The CableLabs CA follows the extKeyUsage extension in Table 15 as specified in the DOCSIS 3.1 Security Specification [1].

7.1.3 Algorithm Object Identifiers (OIDs)

The CableLabs CA follows the signature OIDs for Certificates in Table 16 as specified in the DOCSIS 3.1 Security Specification [1].

The CableLabs CA follows the subjectPublicKeyInfo for Certificates in Table 17 as specified in the DOCSIS 3.1 Security Specification [1].

7.1.4 Name Forms

See CP section 3.1.1.

7.1.5 Name Constraints

The CableLabs CA does not assert name constraints for Certificates it issues.

7.1.6 Certificate Policy Object Identifier

No stipulation.

7.1.7 Usage of Policy Constraints Extension

The CableLabs CA does not assert policy constraints for Certificates it issues.

7.1.8 Policy Qualifiers Syntax and Semantics

The CableLabs CA does not contain a policy qualifier for Certificates it issues.

7.1.9 Processing Semantics for the Critical *certificatePolicies* Extension

The CableLabs CA does not contain a critical certificatePolicies extension in Certificates it issues.

7.2 CRL Profile

The CableLabs CA follows the CRL profile basic fields in Table 18 as specified in the RFC 5280 [6].

7.2.1 Version Number(s)

The CableLabs CA sets the CRL version number to Version 2.

7.2.2 CRL and CRL Entry Extensions

The CableLabs CA does not use any critical CRL extensions.

7.3 OCSP Profile

The CableLabs CA OCSP responders profile conforms to the requirements as defined in section 13.4.2 of the DOCSIS 3.1 Security Specification [1].

7.3.1 Version Number(s)

CableLabs CA OCSP responders conform to version 1 of RFC 2560 [9].

7.3.2 OCSP Extensions

The CableLabs CA does not use any critical OCSP extensions.

8 Compliance Audit and Other Assessments

8.1 Frequency or Circumstances of Assessment

The CableLabs CA receives an annual Audit by an independent external Auditor to assess its compliance with this CPS and the applicable CP. which shall be equivalent to requirements as set out by a WebTrust Audit. Should a CA have undergone WebTrust then that WebTrust Audit is an acceptable."

8.2 Identity/Qualifications of Assessor

WebTrust Auditors must meet the following requirements:

1. *Qualifications and experience: Auditing must be the Auditor's primary business function. The individual, or at least one member of the Audit group, must be qualified as a Certified Information Systems Auditor (CISA), an AICPA Certified Information Technology Professional (CPA.CITP), a Certified Internal Auditor (CIA), or have another recognized information security auditing credential. Auditors must be subject to disciplinary action by its licensing body.*
2. *Expertise: The individual or group must be trained and skilled in the auditing of secure information systems and be familiar with PKI, certification systems, and Internet security issues.*
3. *Rules and standards: The Auditor must conform to applicable standards, rules, and best practices promulgated by the American Institute of Certified Public Accountants (AICPA), CPA Canada, the Institute of Chartered Accountants of England & Wales (ICAEW), the International Accounting Standards adopted by the European*

Commission (IAS), Information Systems Audit and Control Association (ISACA), the Institute of Internal Auditors (IIA), or another qualified auditing standards body.

4. *Reputation: The firm must have a reputation for conducting its auditing business competently and correctly.*
5. *Insurance: Auditors must maintain Professional Liability/Errors and Omissions Insurance, with policy limits of at least $1 million in coverage.*

8.3 Assessor's Relationship to Assessed Entity

The CableLabs CA will select WebTrust Auditors that do not have a financial interest, business relationship, or course of dealing that could foreseeably create a significant bias for or against the CableLabs CA.

8.4 Topics Covered by Assessment

The Audit covers the CableLabs CA business practices disclosure, the integrity of its PKI operations, and compliance with this CPS and the applicable CP.

8.5 Actions Taken as a Result of Deficiency

If an Audit reports a material noncompliance with this CPS or the applicable CP, then (1) the Auditor will document the discrepancy, (2) the Auditor will promptly notify the CableLabs CA, and (3) the CableLabs CA will develop a plan to cure the noncompliance. CableLabs will submit the plan to the PKI-PA for approval.

8.6 Communication of Results

The results of each Audit are reported to the PKI-PA and to any third party entities which are entitled by law, regulation, or agreement to receive a copy of the Audit results.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

The CableLabs CA charges fees for Certificate issuance and renewal. It may change its fees at any time in accordance with the applicable Subscriber agreement.

9.1.2 Certificate Access Fees

The CableLabs CA does not charge a fee for access to Certificates on its website, it does, however, reserve the right to charge a reasonable fee for access to its Certificate databases in the future.

9.1.3 Revocation or Status Information Access Fees

The CableLabs CA does not charge a Certificate revocation fee or a fee for checking the validity status of an issued Certificate using a CRL. It may charge a fee for providing Certificate status information via OCSP.

9.1.4 Fees for Other Services

No stipulation.

9.1.5 Refund Policy

The CableLabs CA refund policy is stipulated in the Subscriber agreement.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

The CableLabs CA maintains Commercial General Liability insurance with a policy limit of at least $2 million in coverage and Professional Liability/Errors & Omissions insurance with a policy limit of at least $5 million in coverage.

9.2.2 Other Assets

The CableLabs CA is supported and funded by CableLabs and thus maintains sufficient financial resources to maintain its CA operations.

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 CableLabs CA considers the following information as confidential and protects it against disclosure using a reasonable degree of care:

- 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

The CableLabs CA considers any information not listed as confidential as public information. Published Certificate and revocation data is considered public information.

9.3.3 Responsibility to Protect Confidential Information

CableLabs CA employees, agents, and contractors are responsible for protecting confidential information and are contractually obligated to do so.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

The CableLabs CA follows the privacy policy where personal information is only disclosed when the disclosure is required by law or when requested by the subject of the personal information.

9.4.2 Information Treated as Private

The CableLabs CA treats all personal information about an individual that is not publicly available in the contents of a Certificate or CRL as private information. It protects private information using appropriate safeguards and a reasonable degree of care.

9.4.3 Information Not Deemed Private

For the CableLabs CA, private information does not include Certificates, CRLs, or their contents.

9.4.4 Responsibility to Protect Private Information

CableLabs CA employees and contractors are expected to handle personal information in strict confidence and meet the CA's requirements concerning the protection of personal data. All sensitive information is securely stored and protected against accidental disclosure.

9.4.5 Notice and Consent to Use Private Information

Personal information obtained from an applicant during the application or identity verification process is considered private information if the information is not included in a Certificate. The CableLabs CA will only use private information after obtaining the subject's consent or as required by applicable law or regulation. All Subscribers must consent to the global transfer and publication of any personal data contained in a Certificate or CRL.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

The CableLabs CA may disclose private information, without notice, if it believes the disclosure is required by law or regulation.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property Rights

The CableLabs CA owns the intellectual property rights in its CA services, including the Certificates, trademarks used in providing the services, and this CPS. Certificate and revocation information are the property of the CableLabs CA and it grants permission to reproduce and distribute Certificates on a non-exclusive and royalty-free basis, provided that they are reproduced and distributed in full. Private and public keys remain the property of the Subscribers who rightfully hold them. All activation data of the CA private keys are the property of the CableLabs CA.

9.6 Representations and Warranties

The PKI-PA warrants the following items:

- Approve the CPS for each CA that issues Certificates under the CableLabs PKI 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 the CP
- Revise the CP to maintain the level of assurance and operational practicality
- Publicly distribute the CP
- Coordinate modifications to the CP to ensure continued compliance by CAs operating under approved CPSs

9.6.1 CA Representations and Warranties

Except as expressly stated in this CPS or in a separate agreement with a Subscriber, the CableLabs CA does not make any representations regarding its products or services. It reresents, to the extent specified in this CPS, that it warrants the following listed items:

- The CA procedures are implemented in accordance with the 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 the 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 the CP and the applicable CPS
- The revocation of Certificates is in accordance with the stipulations in the CP
- Revocation services (when applicable) and use of a repository conform to all material requirements of the CP and the applicable CPS in all material aspects

9.6.2 RA Representations and Warranties

RAs represent that:

1. *The RA's Certificate issuance and management services conform to this CPS and applicable CP*
2. *Information provided by the RA does not contain any false or misleading information*
3. *Translations performed by the RA are an accurate translation of the original information*
4. *All Certificates requested by the RA meet the requirements of this CPS*

9.6.3 Subscriber Representations and Warranties

Prior to being issued and receiving a Certificate, Subscribers are solely responsible for any misrepresentations they make to third parties and for all transactions that use Subscriber's *private key, regardless of whether such use was authorized. Subscribers are required to notify the CableLabs CA and any applicable RA if a change occurs that could affect the status of the Certificate. Subscribers represent to the CableLabs CA and Relying Parties that, for each Certificate, the Subscriber will warrant the following items listed in the Subscriber agreement (i.e., the DCAA):*

- 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 the CableLabs PKI 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.

9.6.4 Relying Party Representations and Warranties

Each Relying Party represents that, prior to relying on a CableLabs PKI Certificate, it has determined whether to rely upon the Certificate as issued by the CableLabs CA.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

The CableLabs CA stipulates the disclaimers of warranties in its Subscriber agreement (i.e., the DCAA).

9.8 Limitations of Liability

The CableLabs CA stipulates the limitations of liability in its Subscriber agreement (i.e., the DCAA)..

9.9 Indemnities

The CableLabs CA stipulates the requirements to indemnify the CA in its Subscriber agreement (i.e., the DCAA).

9.10 Term and Termination

9.10.1 Term

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

9.10.2 Termination

The CableLabs CA stipulates the termination requirements of the CP in its Subscriber agreement (i.e., the DCAA).

9.10.3 Effect of Termination and Survival

The CableLabs CA stipulates the effect of termination and survival requirements of the CP in its Subscriber agreement (i.e., the DCAA).

9.11 Individual Notices and Communications with PKI Participants

The CableLabs CA stipulates the notice and communication requirements with participants of changes to the CP in its Subscriber agreement (i.e., the DCAA).

9.12 Amendments

9.12.1 Procedure for Amendment

This CPS is reviewed annually. Amendments are made by posting an updated version of the CPS to the online repository. Controls are in place to reasonably ensure that this CPS is not amended and published without the prior authorization of the PKI-PA.

9.12.2 Notification Mechanism and Period

The CableLabs CA posts CPS revisions to its website (www.cablelabs.com). It does not guarantee or set a notice-and-comment period and may make changes to this CPS without notice and without changing the version number. The PKI-PA is responsible for determining what constitutes a material change of the CP.

9.12.3 Circumstances Under Which OID Must be Changed

The PKI-PA is solely responsible for determining whether an amendment to the CPS requires an OID change.

9.13 Dispute Resolution Provisions

Parties are required to notify the CableLabs CA and attempt to resolve disputes directly with the CA before resorting to any dispute resolution mechanism, including adjudication or any type of alternative dispute resolution as stipulated in the Subscriber agreement (i.e., the DCAA).

9.14 Governing Law

The CableLabs CA stipulates in the Subscriber agreement (i.e., the DCAA), that the laws of the State of Colorado should govern the enforceability, construction, interpretation, and validity of this CPS and applicable CP unless otherwise negotiated in writing.

9.15 Compliance with Applicable Law

The CableLabs CA stipulates in the Subscriber agreement (i.e., the DCAA), that the CA complies 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 the CableLabs PKI CPS is incorrect or invalid, the other sections of the CPS remain in effect until the CPS is updated.

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

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

No stipulation.

9.16.5 Force Majeure

The CableLabs CA stipulates a force majeure clause in the Subscriber agreement (i.e., the DCAA).

9.17 Other Provisions

No stipulation.