Certificate Management Practices
For
Digital Certificates Used in DFAST Devices

Contents

1 TERMS AND DEFINITIONS 5
2 ABBREVIATIONS AND ACRONYMS 6
3 REFERENCES 7
4 REQUIREMENTS 7
5 INTRODUCTION 7
6 PKI HIERARCHY 8
7 NAMING 8
7.1 Types of Names 8
7.2 Uniqueness of Names 8
7.3 Name Claim Dispute Resolution Procedure 8
8 AUTHENTICATION 8
9 LOGISTICS 9
9.1 Certificate Applications for End-Entity Certificates 9
9.2 Request and Issuance of End-Entity Certificates 10
9.3 Certificate Delivery and Acceptance 10
9.4 Key Pair Generation and Installation 10
9.4.1 Key Pair Generation 10
9.4.2 Private Key Delivery to Entity 10
9.4.3 Public Key Delivery to CA 10
9.4.4 Public Key Delivery to Manufacturer 11
9.4.5 Key Sizes 11
9.4.6 Key Usage Purposes 11
9.5 Private Key Protection 11
9.5.1 Private Key Entry into Cryptographic Module 11
9.5.2 Method of Destroying Private Key 11
9.6 Validity Periods for the Public and Private Keys 11
10 REKEY, RENEWAL, AND REVOCATION 11
10.1 Routine Rekey and Renewal for End-Entity Certificates 11
10.2 Rekey After Revocation 12
10.3 Certificate Revocation 12
11 AUDIT LOGING AND RECORDS 12

11.1 Audit Logging 12
11.1.1 Types of Events Logged 12
11.1.2 Frequency of Processing Log 13
11.1.3 Retention Period for Audit Log 13
11.1.4 Protection of Audit Log 13
11.1.5 Audit Log Backup Procedures 13
11.1.6 Audit Collection System 13
11.2 Records Archival 13
11.2.1 Types of Events Recorded 13
11.2.2 Retention Period for Archive 13
11.2.3 Protection of Archive 14
11.2.4 Requirements for Time-Stamping of Records 14
12 KEY COMPROMISE AND DISASTER RECOVERY 14
12.1 Key Compromise 14
12.2 Corruption of Computing Resources, Software, and/or Data 15
13 SECURITY CONTROLS 15
13.1 Physical Controls 15
13.1.1 Media Storage 15
13.1.2 Waste Disposal 15
13.1.3 Off-Site Backup 15
13.2 Procedural Controls 15
13.2.1 Trusted Roles 15
13.2.2 Number of Persons Required Per Task 16
13.2.3 Identification and Authentication for Each Role 16
13.3 Personnel Controls 16
13.3.1 Background, Qualifications, Experience, and Clearance Requirements . 16
13.3.2 Training Requirements 16
13.3.3 Limited Roles of Non-Trusted Personnel 16
13.3.4 Documentation Supplied to Personnel 16
13.4 Computer Security Controls 16
14 PRIVACY AND CONFIDENTIALITY 17
14.1 Types of Information to be Kept Confidential and Private 17
14.2 Types of Information Not Considered Confidential 17
14.3 Release to Law Enforcement Officials, Court Order, or Request 17
15 INTELLECTUAL PROPERTY RIGHTS 17
15.1 Property Rights in Certificates and Revocation Information 17
15.2 Property Rights in Names 17
15.3 Property Rights in Keys and Key Material 17
16 COMPLIANCE AUDITS 18
16.1 Topics Covered by Audit 18
16.2 Actions Taken as a Result of Deficiency 18
17 ADMINISTRATION 18
17.1 Change Procedures 18

17.2 Contact Person 18
18 SUPPLEMENTAL MANUFACTURER SECURITY POLICIES AND PROCEDURES 18
18.1 Security Policies and Procedures 19
18.2 Personnel Security Practices 19
18.3 Key Pair Generation Policies and Practices 19
18.4 Private Key Protection Plan 19
18.5 Audit Logging and Procedures 19
18.6 Compromise Key and Recovery Plan 19
18.7 Rekey and Renewal Procedures 19

Figures

Figure 2. Manufacturer Authentication 9
Figure 5. Compromise Key Response Process 14

Tables

Table 1. Requirements for Certificate Replacement After Revocation 12

1 Terms and Definitions

This document uses the following terms:

CableLabs Device CA	One or more Certification Authority (CAs) owned or operated by or for CableLabs that issue Certificates to Manufacturers. As used in this term of art, "Certification" does not imply product certification by CableLabs.
CableLabs PKI Repository	CableLabs' database of relevant PKI information accessible on-line.
Participants	An individual or organization that is one or more of the following within the CableLabs PKI: CableLabs, a Manufacturer, or a Relying Party.
Certificate	A message that, at least, states a name or identifies the CA, identifies the Manufacturer, contains the Manufacturer's public key, identifies the Certificate's Validity Period, contains a Certificate serial number, contains some identification of the product, product type or product model and is digitally signed by a CA.
Certificate Chain	An ordered list of Certificates containing an end-user Manufacturer Certificate and CA Certificates, which terminates in a root Certificate.
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	A message conveying a request to have a Certificate issued.
Certification Authority (CA)	An entity identified by CableLabs as authorized to issue, manage, revoke, and renew Certificates and to manage various aspects of the CableLabs PKI.
Class	A specified level of assurances as defined within the applicable certificate policy.
Compromise	A violation (or suspected violation) of a security policy, in which an unauthorized disclosure of, or loss of control over, sensitive information may have 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.
Contact Person	Contact Person is the CableLabs Security Contact Person listed in Section 5.13.1.3 of this enclosure.
End-Entity	A Manufacturer who uses a Certificate in an end entity device.
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.
Manufacturer	In the case of an individual Certificate, a person who is the Subject of, and has been issued, a Certificate. In the case of an organizational Certificate, an organization that owns the equipment or device that is the Subject of, and that has been issued, a Certificate. A Manufacturer is capable of using, and is authorized to use, the private key that corresponds to the public key listed in the Certificate.
PKCS #10	Public-Key Cryptography Standard #10, developed by RSA Security Inc., which defines a structure for a Certificate Signing Request.
PKCS #12	Public-Key Cryptography Standard #12, developed by RSA Security Inc., which defines a secure means for the transfer of private keys.
Public Key Infrastructure (PKI)	The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a Certificate-based public key cryptographic system.

Registration Authority (RA)	A mechanism to allow Manufacturers to obtain Certificates in bulk in an automated, safe, and secure fashion. The RA assists the Manufacturer in applying for Certificates, placing Certificate Applications, revoking Certificates, and/or renewing Certificates in an automated fashion.
Relying Party	An individual or organization that acts in reliance on a Certificate and/or a digital signature.
RSA	A public key cryptographic system invented by Rivest, Shamir, and Adelman.
Secret Share	A portion of a CA private key or a portion of the activation data needed to operate a CA private key under a Secret Sharing arrangement.
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 Group	A group of security experts in the cable industry comprising CableLabs and Cable Operator members.
Subject	The holder of a private key corresponding to a public key. The term "Subject" can, in the case of an organizational Certificate, refer to the equipment or device that holds a private key. A Subject is assigned an unambiguous name, which is bound to the public key contained in the Subject's Certificate.
Trusted Person	An employee, contractor, or consultant of an entity responsible for managing infrastructural trustworthiness of the entity, its products, its services, its facilities, and/or its practices.
Trusted Position	The positions within an entity that must be held by a Trusted Person.
Trustworthy System	Computer hardware, software, and procedures that are reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy.
Validity Period	The period starting with the date and time a Certificate is issued (or on a later date and time certain if stated in the Certificate) and ending with the date and time on which the Certificate expires or is earlier revoked.

2 Abbreviations and Acronyms

This document uses the following acronyms:

CP	Certificate Policy
CA	Certification Authority
CRL	Certificate Revocation List
FIPS	United States Federal Information Processing Standards
LSVA	Logical security vulnerability assessment
PKCS	Public-Key Cryptography Standard
PKI	Public Key Infrastructure
RFC	Request for comment
SAS	Statement on Auditing Standards (promulgated by the American Institute of Certified Public Accountants).

3 References

References refer to companion standards and specificationsand background material.

[1] *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*, IETF (S. Chokhani, W. Ford), RFC 2527, March 1999.

[2] *ITU-T Recommendation X.509 (1997 E): Information Technology – Open Systems Interconnection – The Directory: Authentication Framework*, June 1997.

[3] *OpenCable System Security Specification.*

4 Requirements

Throughout this document, the words that are used to define the significance of particular requirements are capitalized. These words are:

"MUST"	This word or the adjective "REQUIRED" means that the item is an absolute requirement of this specification.
"MUST NOT"	This phrase means that the item is an absolute prohibition of this specification.
"SHOULD"	This word or the adjective "RECOMMENDED" means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood and the case carefully weighed before choosing a different course.
"SHOULD NOT"	This phrase means that there may exist valid reasons in particular circumstances when the listed behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
"MAY"	This word or the adjective "OPTIONAL" means that this item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because it enhances the product, for example; another vendor may omit the same item.

5 Introduction

Digital Certificates provide a secure mechanism to identify and authenticate an entity via the verification of a digital signature within a public key infrastructure (PKI). Such authentication is based on mechanisms that validate that the Certificate, and the associated private key are, in fact, trusted and follow the specified set of requirements. This issue is commonly known as Certificate validation. The integrity of the overall PKI is necessarily based upon the integrity of each component of the PKI.

This Enclosure details the logistics for the uniform handling of private keys, secrets, and Certificates issued to users of the cable industry PKI. It provides information about the practices Manufacturers follow in requesting, receiving, and managing Certificates used in digital cable products. This Enclosure forms the basis for establishing the CableLabs PKI as a Trustworthy System. Cable Service Providers, and other Manufacturers, will rely on device Certificates to authenticate devices that receive a wide variety of cable services.

The following assumptions are made with respect to this document:

- The reader should be familiar with PKI since this document does not attempt to teach PKI;
- The reader should be familiar with the applicable specifications for devices requiring Certificates;
- The reader should be familiar with System Security Specification that specifies the technical format, definition, and use Certificates;
- Manufacturers will establish and maintain their own internal security processes and procedures as outlined in this document; and
- This document is a living document and will be updated from time to time.

This Enclosure covers practices and procedures concerning the management and issuance of Class 2 Certificates from the CableLabs Device CA. These requirements protect the security and integrity of the overall PKI and apply to all Manufacturers in order to provide assurances of uniform trust throughout the PKI hierarchy. The term "issue" in this context refers to the process of digitally signing with the private key associated with its authority Certificate conforming to the ISO X.509, version 3 certificate format [1] [2].

6 PKI Hierarchy

The CableLabs PKI hierarchy includes three levels of certificates. The CableLabs Manufacturer Root Certification Authority serves as the root CA. The root CA issues certificates to one or more device CAs maintained by or on behalf of CableLabs (by the Certification Authority), which is (are) called the CableLabs Device CA(s). The CableLabs Device CA issues end entity device Certificates to Manufacturers for use in cable devices. Note that CableLabs may maintain multiple CableLabs Device CAs to issue Certificates to Manufacturers, and that multiple CableLabs Device CAs may issue Certificates to a single Manufacturer. See System Security Specification [6] for more detailed information on the CableLabs PKI hierarchy.

7 Naming

7.1 Types of Names

CableLabs Device CA Certificates consist of the components specified in System Security Specification Section 5.4

End-Entity Certificates consist of the components specified in System Security Specification Section 5.5

7.2 Uniqueness of Names

The CableLabs Device CA ensures that Subject Distinguished Names are unique within the domain of the CableLabs Device CA through the Manufacturer enrollment process.

7.3 Name Claim Dispute Resolution Procedure

Manufacturers are prohibited from using names in their Certificate Applications that infringe upon the Intellectual Property Rights of others. The CableLabs Device CA, however, does not verify whether a Manufacturer has Intellectual Property Rights in the name appearing in a Certificate Application or arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any domain name, trade name, trademark, or service mark. The Cablelabs Device CA is entitled, without liability to any Manufacturer, to reject or suspend any Certificate Application because of such dispute.

8 Authentication

The MFG Root CA or Cablelabs Device CA authenticate the identity of the Manufacturer requesting a Certificate before final approval of its status by performing the following steps:

- A determination that the Manufacturer exists by using business records, database, or alternatively, documentation that confirms the existence of the organization;
- A confirmation by telephone, confirmatory postal mail, and/or comparable procedure to the Manufacturer to confirm certain information about the Manufacturer, confirm that the Manufacturer has authorized the Certificate Application, confirm the employment of the representative submitting the Certificate Application on behalf of the Manufacturer, and confirm the authority of the representative to act on behalf of the Manufacturer;
- A confirmation by telephone, confirmatory postal mail, and/or comparable procedure to the Manufacturer's representative to confirm that the person named as representative has submitted the Certificate Application;
- The Manufacturer rightfully holds the private key corresponding to the public key to be listed in the Certificate;

- The information to be included in the Certificate is accurate; and
- A check to ensure that the Subject distinguished name is a unique and unambiguous Subject name within the MFG Root CA Sub domain.

The MFG Root CA or Cablelabs Device CA may subcontract such services provided that the subcontractor meets these requirements, security requirements, and all other requirements imposed on the MFG Root CA when performing these services under this Enclosure. Please see Figure 1 below.

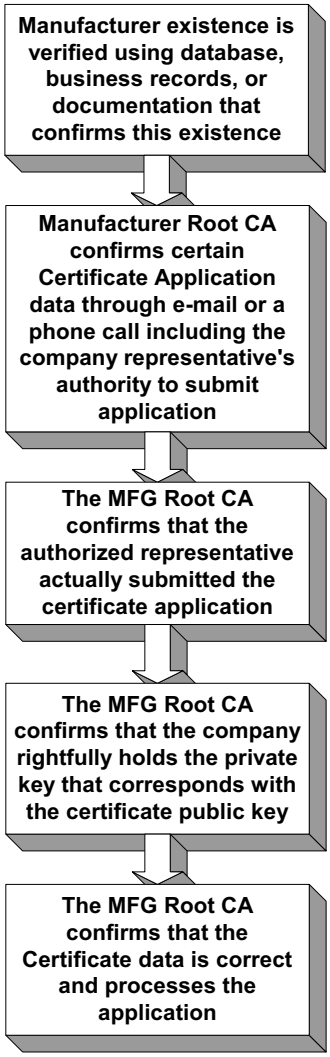

Figure 1. Manufacturer Authentication

9 Logistics

9.1 Certificate Applications for End-Entity Certificates

In order to obtain End-Entity Certificates from the CableLabs Device CA, the Manufacturer shall submit a Ceritificate Application and undergo an enrollment process consisting of:

- Generating, or arranging to have generated (at the CableLabs Device CA), a key pair in accordance with 9.4;
- The Manufacturer delivering its public key, directly to the CableLabs Device CA in accordance with Section § 9.4; and

- Demonstrating to the CableLabs Device CA that the Manufacturer has possession of the private key corresponding to the public key delivered to the CableLabs Device CA.

All information provided by the Manufacturer in the Certificate Application MUST be true, accurate, and complete.

After a Manufacturer submits a Certificate Application, the CableLabs Device CA attempts to confirm the information in the Certificate Application pursuant to this Enclosure (see above section on Authentication). Upon successful performance of all required authentication procedures , the CableLabs Device CA approves the Certificate Application. If authentication is unsuccessful, the CableLabs Device CA denies the Certificate Application.

Following the approval of a Certificate Application, an account corresponding to the Manufacturer is established within the CableLabs Device CA domain. *The process of establishing an account, and an automated system for delivering Certificates in bulk to the Manufacturer in a safe and secure manner may take up to 4 weeks to complete.* Manufacturer shall cooperate with CableLabs and/or the Certification Authority to implement such secure account and automated system (*e.g.*, RA or PKCS#10 messaging, online access).

9.2 Request and Issuance of End-Entity Certificates

In order to maintain the overall integrity of the PKI, Manufacturers requesting Certificates from the Cablelabs Device CA MUST comply with the following:

- Each digital signature created using the private key corresponding to the public key listed in the Certificate is the digital signature of the Manufacturer and the Certificates have been accepted and is operational (not expired or revoked) at the time the digital signature is created;
- No unauthorized person has ever had access to the Manufacturer's private key;
- All information supplied by the Manufacturer and contained in the Certificates is true;
- The Certificates are being used exclusively for authorized and legal purposes, consistent with this Enclosure and the DFAST License Agreement; and
- The Manufacturer 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.

9.3 Certificate Delivery and Acceptance

Upon Certificate generation, the CableLabs Device CA notifies the Manufacturer that the Certificates are available and notifies the Manufacturer of the means for obtaining the Certificates.

Upon issuance, Certificates are made available to Manufacturers by allowing Manufacturers to download the Certificates from a Web site or Certificates may be sent to the Manufacturer via secure e-mail. Downloading a Certificate or receiving the Certificate via e-mail, constitutes the Manufacturer's acceptance of the Certificate.

9.4 Key Pair Generation and Installation

9.4.1 Key Pair Generation

Key pair generation is performed by multiple pre-selected, trained and Trusted Personnel using Trustworthy Systems and processes that provide for the security and required cryptographic strength for the generated keys.

9.4.2 Private Key Delivery to Entity

End-Entity key pairs are typically generated by the Manufacturer and embedded into the manufacturer's cable service device at the time of production. Manufacturers may generate their key pairs in hardware or software.

9.4.3 Public Key Delivery to CA

Manufacturers submit their public key to the CableLabs Device CA for certification electronically through the use of a PKCS#10 Certificate Signing Request (CSR) or another secure manner as determined by the CableLabs Device CA. (Note: This is not required since Manufacturers may choose to have the key pairs generated at the CableLabs Device CA prior to Certificate signing.)

9.4.4 Public Key Delivery to Manufacturer

The CableLabs Device CA will provide the full certificate chain (including the Root CA certificate, the issuing CA certificate and any CA certificates in the chain) to the Manufacturer upon Certificate issuance via email. CA Certificates are available upon request from the Contact Person.

9.4.5 Key Sizes

The Root CA Certificate, CableLabs Device CA Certificate and the End-Entity Certificate key sizes are defined in sections 5.3, 5.4 and 5.5 of the System Security Specification [6].

9.4.6 Key Usage Purposes

KeyUsage extension for Certificates are populated in accordance with the System Security Specification [6].

9.5 Private Key Protection

Manufacturers should implement a combination of physical, logical, and procedural controls to ensure the security of private keys. Logical and procedural controls are described in this section. Physical access controls are described above.

9.5.1 Private Key Entry into Cryptographic Module

Manufacturers may generate their key pairs in hardware or software. When generated in hardware cryptographic modules, manufacturers should make copies of such key pairs for routine recovery and disaster recovery purposes. Where key pairs are backed up to another hardware cryptographic module, such key pairs shall be transported between modules in encrypted form.

9.5.2 Method of Destroying Private Key

At the conclusion of its operational lifetime, one or more copies of the private key are archived. Remaining copies of the private key are securely destroyed. In addition, archived private keys are securely destroyed at the conclusion of their archive periods. Key destruction activities require the participation of multiple trusted individuals.

Private keys must be destroyed in a manner that reasonably ensures that there are no residual remains of the key that could lead to the reconstruction of the key. When performed, key destruction activities are logged.

9.6 Validity Periods for the Public and Private Keys

The Validity Period of a Certificate is 30 years unless revoked. The Validity Period for key pairs is the same as the Validity Period for the associated Certificates, except that private keys may continue to be used for decryption and public keys may continue to be used for signature verification. Except as noted, Manufacturers shall cease all use of their key pairs after their usage periods have expired.

10 Rekey, Renewal, and revocation

Prior to the expiration of an existing Certificate, it is necessary for the Manufacturer to obtain a new certificate to maintain continuity of Certificate usage. To accomplish this, a new key pair is generated to replace the expiring key pair (technically defined as "rekey"). However, in certain cases (*e.g.*, for test Certificates) the CableLabs Device CA permits Manufacturers to request a new certificate for an existing key pair (technically defined as "renewal").

Generally speaking, both "Rekey" and "Renewal" are commonly described as "Certificate Renewal," focusing on the fact that the old Certificate is being replaced with a new Certificate and not emphasizing whether or not a new key pair is generated.

10.1 Routine Rekey and Renewal for End-Entity Certificates

For Certificate rekey, the Manufacturer will need to repeat the process used to obtain the original Certificate.

For a Certificate renewal, the Manufacturer mainly follows the process used to obtain the original Certificate. Except, the Manufacturer may make changes to the subject's status (*e.g.*, subject name), but not other information in the Certificate (*e.g.*, validity period). The CableLabs Device CA will issue a new Certificate retaining the public key of the original Certificate. The

original Certificate will be revoked and the new Certificate will have a matching start and end validity date. Renewal is permitted up until 30 working days from the expiration date of a Certificate. The public key used in the original Certificate may be used up to three times in consecutive renewal Certificates before the same public key may no longer be used. The remainder of the renewal process is as described for obtaining the original Certificate.

10.2 Rekey After Revocation

End-Entity Certificates, if and when revoked, may be replaced (*i.e.*, rekeyed) in accordance with Table 1 below. Note: CA Certificate Rekey is not permitted after Certificate Revocation.

Table 1. Requirements for Certificate Replacement After Revocation

Timing	Requirement
Rekey of a revoked Certificate prior to Certificate expiration	The requirements specified in this Enclosure for the authentication of an original Certificate shall be used for replacing a Manufacturer End-Entity Certificate. Such Certificates contain the same Subject distinguished name as the Subject distinguished name of the Certificate being replaced.
Rekey of a revoked Certificate after Certificate expiration	The requirements specified in the Enclosure for the authentication of an original Certificate shall be used for replacing a Manufacturer End-Entity Certificate.

10.3 Certificate Revocation

A device Certificate issued by the CableLabs Device CA may be revoked in accordance with the policy entitled Revocation Of Certificates Corresponding to Cloned, Lost, or Stolen Private Keys Or Pursuant To Government Order For End-Entity Digital Certificates in Unidirectional Digital Cable Product, attached hereto

11 Audit Logging and Records

11.1 Audit Logging

11.1.1 Types of Events Logged

Manufacturers MUST manually or automatically log the following significant events in the handling of keys:

- Key lifecycle management events, including: key generation, backup, storage, recovery, archival, and destruction;
- Certificate installation;
- Authentication or lack of authentication (retries) for accessing the RA computer/software;
- Manufacturer certificate lifecycle management events, including:
  - Certificate Applications, receipt, renewal, rekey, and revocation;
  - Successful or unsuccessful processing of requests; and
- Security-related events including:
  - Security sensitive files or records read, written or deleted (in summary form);
  - Security profile (security environment) changes;
  - System crashes, hardware failures and other anomalies that are related to security; and
- IT software and hardware maintenance and updates which are not related to security.

Log entries include the following elements:

- Date and time of the entry;
- Serial or sequence number of entry, for automatic journal entries;

- Identity of the entity making the journal entry; and
- Kind of entry.

11.1.2 Frequency of Processing Log

Audit logs SHALL be examined on a timely basis (*e.g.,* at least monthly) for significant security and operational events. In addition, Manufacturers must review their audit logs for suspicious or unusual activity in response to alerts generated based on irregularities and incidents.

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

11.1.3 Retention Period for Audit Log

Audit logs shall be retained onsite at least two (2) months after processing and thereafter archived in accordance with Section § 11.2.2.

11.1.4 Protection of Audit Log

Electronic and manual audit log files shall be protected from unauthorized viewing, modification, deletion, or other tampering through the use of physical and logical access controls.

11.1.5 Audit Log Backup Procedures

Incremental and full backups of audit logs shall be performed as needed and shall be stored in a secure storage site.

11.1.6 Audit Collection System

If an automated audit data system is utilized, audit data shall be generated and recorded at the application, network and operating system level. Manufacturer personnel may record audits manually.

11.2 Records Archival

11.2.1 Types of Events Recorded

In addition to the audit logs specified in 11, Manufacturers must maintain records that include documentation of:

- Actions and information that are material to each Certificate Application and to the creation, issuance, use, revocation, expiration, and rekey or renewal of all certificates received by the Manufacturer.

Certificate lifecycle events include:

- The identity of persons requesting Certificate revocation;
- Other facts represented in the Certificate;
- Time stamps; and
- Certain foreseeable material facts related to issuing Certificates including, but not limited to, information relevant to successful completion of a Compliance Audit.

Records may be maintained electronically or in hard copy, provided that such records are accurately indexed, stored, preserved, and reproduced.

11.2.2 Retention Period for Archive

Records associated with certificates are retained for at least a time period of ten (10) years following the date the Certificate expires or is revoked.

11.2.3 Protection of Archive

Manufacturers shall protect record archives in a manner to restrict access to only Trusted Persons, and shall protect against modification, deletion or tampering.

Archive Backup Procedures: The archive shall be incrementally and/or fully backed-up. The backups shall be stored in a separate facility in a secure manner as detailed above.

11.2.4 Requirements for Time-Stamping of Records

Certificates and other revocation database entries shall contain time and date information. It should be noted that such time information is not cryptographic-based.

12 Key Compromise

Manufacturers must implement a robust combination of physical, logical, and procedural controls to minimize the risk and potential impact of a key Compromise. In addition, Manufacturers must implement Key Compromise response procedures described below. Compromise Recovery procedures should be developed to minimize the potential impact of such an occurrence and restore the operations within a reasonable period of time.

12.1 Key Compromise

Upon the suspected or known Compromise of a private key, the Manufacturer shall enact its Key Compromise Response procedures. This team handling the procedures assesses the situation, develops an action plan, and implements the action plan with approval from the Security Group. Please see Figure 2 below.

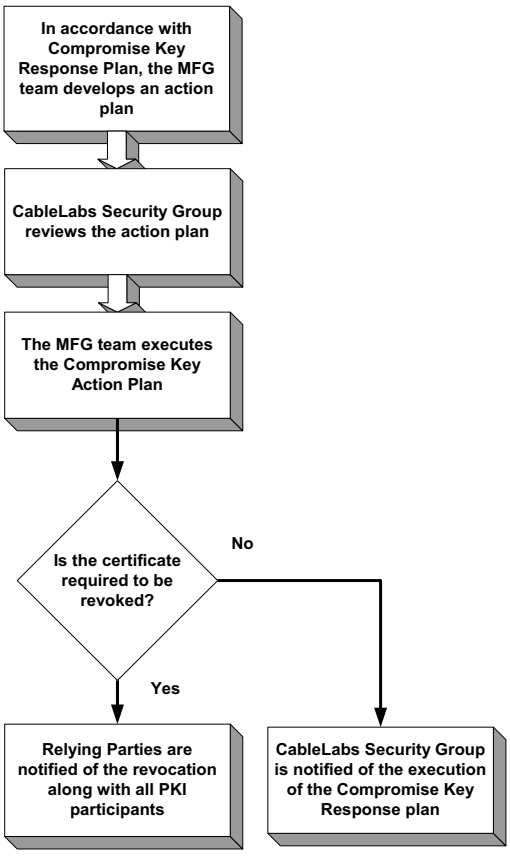

Figure 2. Compromise Key Response Process

As noted above, if a Manufacturer discovers or has reason to believe that there has been a loss of the Manufacturer's private keys, a Compromise of the Manufacturer's private keys, or the information within the Certificate is incorrect or has changed, the Manufacturer MUST promptly:

- Notify the CA; and
- Notify any Relying Party that reasonably may be expected to rely on or to provide services in support of the Manufacturer's certificates or a digital signature verifiable with reference to the Manufacturer's certificates.

12.2 Corruption of Computing Resources, Software, and/or Data

In the event of the corruption of computing resources, software, and/or data, such an occurrence is reported to the CableLabs Device CA and incident handling procedures are enacted. Such procedures require appropriate escalation, incident investigation, and incident response. Manufacturer's key compromise recovery procedures will be enacted.

13 Security Controls

Manufacturers SHALL use commercial practices for managing keys, such measures to include, at a minimum, physical, procedureal, peronnel, and computer security controls.

13.1 Physical Controls

Detailed Security Policy and Procedures should be developed by the Manufacturer to address the following subsections.

13.1.1 Media Storage

All media containing production software and data, audit, archive, or backup information should be securely stored within the Manufacturer facilities or in a secure off-site storage facility with appropriate physical and logical access controls designed to limit access to authorized personnel and protect such media from accidental damage (*e.g.*, water, fire, and electromagnetic).

13.1.2 Waste Disposal

Sensitive documents and materials should be shredded before disposal. Media used to collect or transmit sensitive information should be rendered unreadable before disposal. Cryptographic devices should be physically destroyed or zeroized in accordance to the cryptographic manufacturers' guidance prior to disposal. Other waste should be disposed of in accordance with normal waste disposal requirements.

13.1.3 Off-Site Backup

Manufacturers should perform routine backups of critical system data, audit log data, and other sensitive information. Offsite backup media should be stored in a physically secure manner.

13.2 Procedural Controls

13.2.1 Trusted Roles

Trusted Persons include all employees, contractors, and consultants that have access to or control authentication or cryptographic operations that may materially affect:

- The validation of information in Certificate Applications;
- The issuance, or revocation of Certificates, including personnel having access to restricted portions of its repository;
- Or the handling of Manufacturer information or requests.

Trusted Persons include, but are not limited to:

- Security personnel;
- Legal personnel;
- System administration personnel;
- Designated engineering personnel; and

- Executive Management.

13.2.2 Number of Persons Required Per Task

Manufacturers must maintain a policy and rigorous control procedures to ensure segregation of duties based on job responsibilities. The most sensitive tasks, such as access to private key material, require specific processes to avoid compromise. Depending on the specific nature of the operational evironment, Manufacturers may have two-man rules or other systems to ensure appropriate security levels.

13.2.3 Identification and Authentication for Each Role

Manufacturers shall maintain security practices that ensure that each individual which has access to sensitive information gains access through an approval and authorization process designed to strictly control access and avoid compromise of sensitive information and materials.

13.3 Personnel Controls

13.3.1 Background, Qualifications, Experience, and Clearance Requirements

Manufacturers shall establish relevant procedures for qualifing personnel for designation as Trusted Persons, which may include identity, background and other processes.

13.3.2 Training Requirements

Manufacturers must provide its personnel with training upon hire and the requisite on-the-job training needed for personnel to perform their job responsibilities competently and satisfactorily. Manufacturers should periodically review and enhance their training programs as necessary.

Manufacturers training programs should be tailored to the individual's responsibilities and may include the following as relevant:

- Basic PKI concepts;
- Job responsibilities;
- Security and operational policies and procedures;
- Use and operation of deployed hardware and software;
- Incident and compromise reporting and handling.

13.3.3 Limited Roles of Non-Trusted Personnel

In limited circumstances employess, independent contractors, or consultants who have not completed the procedures specified in 13.3.1 are permitted to fill Trusted Positions. Any such Non-Trusted Personnel is held to the same functional and security criteria that apply to Trusted Personnel in a comparable position. Any Non-Trusted personnel used to fill a Trusted Position must be escorted and directly supervised by Trusted Personnel.

13.3.4 Documentation Supplied to Personnel

Manufacturers shall provide its personnel the requisite documentation needed to perform their job responsibilities competently and satisfactorily.

13.4 Computer Security Controls

13.4.1.1 Specific Computer Security Technical Requirements

Manufacturers must ensure that the systems maintaining RA software and data files are Trustworthy Systems, secure from unauthorized access.

Manufacturers must use passwords that have a minimum character length and a combination of alphanumeric and special characters. Manufacturers must change passwords on a periodic basis, at least once every six months.

14 Privacy and Confidentiality

14.1 Types of Information to be Kept Confidential and Private

The following records shall be kept confidential and private by the Manufacturer ("Confidential/Private Information"):

- Audit trail records created or retained by the Manufacturer;
- Audit reports created by the Manufacturer or their respective auditors (whether internal or public);
- Compromise Key and Recovery Plan;
- Security measures controlling the operations of hardware and software and the administration of Certificate services; and
- Private Keys.

14.2 Types of Information Not Considered Confidential

Manufacturers acknowledge that Certificates, Certificate revocation and other status information, CableLabs Device CA's repository, and information contained within them are not considered Confidential/Private Information. Certificate Revocation information also may be disclosed.

14.3 Release to Law Enforcement Officials, Court Order, or Request

Manufacturers acknowledge that the CableLabs Device CAs shall be entitled to disclose Confidential/Private Information if, in good faith, the CableLabs Device CA believes disclosure is necessary in response to subpoenas and search warrants. This section is subject to applicable privacy laws.

Manufacturers acknowledge that the CableLabs Device CAs shall be entitled to disclose Confidential/Private Information if, in good faith, the CableLabs Device CA believes disclosure is necessary in response to judicial, administrative, or other legal process during the discovery process in a civil or administrative action, such as subpoenas, interrogatories, requests for admission, and requests for production of documents. This section is subject to applicable privacy laws.

The CableLabs Device CAs may disclose Confidential/Private Information to the person disclosing it to the CableLabs Device CA, or upon the request of the disclosing party, to any third party. This section is subject to applicable privacy laws.

15 Intellectual Property Rights

15.1 Property Rights in Certificates and Revocation Information

The Cablelabs Device CA retains all Intellectual Property Rights in and to the Certificates and revocation information that they issue. Manufacturers are granted permission to copy for back-up purposes and distribute Certificates on a nonexclusive royalty-free basis. Manufacturers shall grant permission to use revocation information to perform Relying Party functions subject to the applicable Certificate Revocation Policy.

15.2 Property Rights in Names

A Manufacturer retains all rights it has (if any) in any trademark, service mark, or trade name contained in any Certificate Application and distinguished name within any Certificate issued to such Manufacturer. Nothing contained in this Enclosure shall be construed as conferring any right to use in advertising, publicity, or other promotional activities any name, trade name, trademark or other designation of any party (including any contraction, abbreviation or simulation of any of the foregoing).

15.3 Property Rights in Keys and Key Material

Key pairs corresponding to Certificates of Manufacturers are the property of the Manufacturers regardless of the physical medium within which they are stored and protected, and Manufacturers retain all Intellectual Property Rights in and to these key pairs. Without limiting the generality of the foregoing, CableLabs' PKI and the Cablelabs Device CA root public keys and the root certificates containing them are the property of CableLabs. Finally, without limiting the generality of the foregoing, Secret Shares

of the Cablelabs Device CA private key are the property of Cablelabs, and the CA retains all Intellectual Property Rights in and to such Secret Shares.

16 Compliance Audits

As detailed in Section 7(1)b of the DFAST License, CableLabs shall have the right to review, upon five (5) business days notice, or such earlier time as may be reasonable and required due to special circumstances, the implementation of all security measures at the secure location(s) required hereunder for Highly Confidential Information on an ongoing basis, at reasonable times as agreed between Manufacturer and CableLabs, subject to a mutually agreed upon reasonable non-disclosure agreement prior to CableLabs' release of Highly Confidential Information to Manufacturer. Should Manufacturer prefer that such review be conducted by a third-party auditor, Manufacturer and CableLabs may agree upon one or more acceptable third-party auditors and a reasonable non-disclosure agreement, prior to CableLabs' release of Highly Confidential Information to Manufacturer.

16.1 Topics Covered by Audit

Audit topics shall be limited to compliance with this enclosure and the DFAST License

16.2 Actions Taken as a Result of Deficiency

Significant exceptions or deficiencies identified during the Compliance Audit will result in a determination of corrective actions to be taken, if any. The determination of such corrective actions shall be the result of an evaluation of the cirumstances jointly by CableLabs, the auditor and the Manufacturer. Manufacturer shall submit a plan for executing the correction actions within 30 days of completion of the joint evaluation detailed in the preceding. If CableLabs reasonably determines that such exceptions or deficiencies pose an immediate threat to the security or integrity of the CableLabs PKI, a corrective action plan must be developed within 30 days and implemented within a commercially reasonable period of time. For less serious exceptions or deficiencies, CableLabs, the Auditor and the Manufacturer shall jointly evaluate the significance of such issues and determine the appropriate course of action.

17 Administration

17.1 Change Procedures

From time to time this Enclosure may be modified subject to mutual approval of the parties.

17.2 Contact Person

The Contact Person for CableLabs for security issues should be addressed to:

CableLabs
858 Coal Creek Circle
Louisville, CO 80027-9750
Attn: –Chief Security Architect
(303) 661-9100 (voice)

18 Supplemental Manufacturer Security Policies and Procedures

This Enclosure is supplemental to each Manufacturer's own internal security and operational documents. The following sections define policy and practice documents needed to manage key material and secrets used in the CableLabs PKI. Conformance to this uniform level of security is required to maintain a level of security to adequately protect the cable industry, other manufacturers, content providers, and cable subscribers. All Manufacturers SHALL develop and maintain the following security documents in accordance with commercial practices for managing private keys:

18.1 Security Policies and Procedures

Manufacturers shall create policies and procedures regarding their security operations, policies and procedures to be used in the day to day operations and actions with regard to protection of sensitive information, and such policies and procedures will include cyrptographic key security. .

18.2 Personnel Security Practices

Manufacturers shall create policies and procedures as appropriate to ensure that personnel designated to handle, process or control sensitive information are appropriately qualified and deemed trustworthy. In addition, Manufacturers shall ensure that such designated personnel are appropriately trained with regard to their functional responsibilities and appropriate security practices.

18.3 Key Pair Generation Policies and Practices

The Manufacturer is required to have procedures for generating key pairs, private key delivery, and public key delivery. Key sizes and all technical security controls used for key pair generation and usage should be addressed in the Key Pair Generation Policies and Practices document, or equivalent thereof.

18.4 Private Key Protection Plan

Associated with the Key Pair Generation Polices and Procedures above, the Private Key Protection Plan, or equivalent thereof, consists of a combination of physical, logical, and procedural controls to ensure the security of End-Entity private keys used in the devices.

18.5 Audit Logging and Procedures

The Audit Logging and Procedures should meet or exceed the requirements set forth in this enclosure. The Audit Procedure should include all aspects of the audit logging process including the types of events recorded, the frequency of processing the log, and notification. Protection, vulnerability and retention of audit logs should also should be addressed.

18.6 Compromise Key and Recovery Plan

A Compromise Key and Recovery Plan should contain the procedures needed to handle a Compromise and recovery along with the procedures for developing an action plan specific to the case of a key Compromise. This plan must define the overall process used to create the action plan, get it approved and implemented and also define the details related to destruction of the compromised key material and creation of new key pairs. Manufacturers are required to have a detailed Compromise Key and Recovery Plan that covers the following issues:

- Notification requirements;
- Action Plan Requirements;
- Requirements from the revocation of the Certificate;
- Key distribution and installation requirements; and
- Final reporting requirements.

18.7 Rekey and Renewal Procedures

The Manufacturer is required to have procedures for renewing and rekeying key pairs, private key delivery, and public key delivery. The requirements are defined in section 5.9.

Revocation Of Certificates Corresponding to Cloned, Lost, or Stolen Private Keys Or Pursuant To Government Order

For

End-Entity Digital Certificates in Digital Cable Product [1]

[1] Other cable products may use the same or similar PKI hierarchy for issuing digital certificates. Certificate revocation for these products, as well as certificates and certificate revocation for software, CAs, and service denial in general, are outside the scope of this document.

1 Introduction

The X.509 specification defines the use of a certificate revocation list (CRL). The CRL is used to distribute the list of digital certificates revoked by the issuing Certification Authority (CA). This document addresses the criteria for certificate revocation, and the processes and procedures that must be used by users of the digital certificates in the certificate hierarchy to effect such revocation. Failure to adhere to this policy may compromise the integrity and security of the certificate hierarchy for all users of the certificate hierarchy: cable operators, manufacturers, content providers, and consumers.

The purpose of this document is to set forth a clearly defined process to revoke digital certificates, and a common method for communication of the CRLs.

The following assumptions are applicable to this document:

- The reader should be familiar with PKI, this document does not attempt to teach PKI.
- The reader should be familiar with the applicable specifications, and, in particular the sections identifying the digital certificates. Technical process requirements for CRLs are listed in the specifications.

2 Definitions

Affected Manufacturer	A Manufacturer holding one or more Digital Certificates that are Revoked or are sought for Revocation.
Cable Operator	A cable operator having one or more DFAST-licensed devices connected to their cable network.
Certification Authority (CA)	A trusted organization, as defined in this Agreement, that accepts certificate applications from entities, authenticates applications, issues certificates and maintains status information about the certificates it issues.
Certificate Revocation List (CRL)	A digitally signed list issued by a CA to identify certificates that have been revoked from that authority (but have not expired yet).
Digital Certificate	An X.509 end-entity device digital certificate used in a DFAST-licensed device.
Manufacturer	A manufacturer that is a party to this Agreement.
Private Key	The key used in public key cryptography that belongs to an individual entity and must be kept secret.
Public Key Infrastructure (PKI)	A process for issuing Digital Certificates, which includes standards, Certification Authorities, communication between authorities and protocols for managing Digital Certificate processes.
Revocation or Revoked	A means by which Digital Certificates of certain devices may be invalidated, rendering such devices unable to exchange data via the POD ("CableCARD") Interface.

3 Revocation Procedures

3.1 **Request for Revocation**. Any party or beneficiary of a DFAST Technology License Agreement ("Revocation Initiators") may seek Revocation by providing proof in a sworn affidavit (the "Manufacturer Affidavit") of any of the facts relating to any particular Digital Certificate and/or associated private keys issued to Manufacturer

hereunder pursuant to this Agreement that would warrant Revocation of such Digital Certificate and satisfy one or more of the Revocation Criteria. The Manufacturer Affidavit shall be sufficiently detailed that it can be determined solely on the basis of such affidavit whether the facts averred on their face would satisfy one or more of the Revocation Criteria.

3.2 **Revocation Criteria**.

3.2.1 a Private Key and corresponding Digital Certificate have been cloned such that the same Device Key and corresponding Digital Certificate are found in more than one device or product;

3.2.2 a Private Key (with or without its corresponding Digital Certificate) has been lost, stolen, intercepted or otherwise misdirected, or made public or disclosed;

3.2.3 the CA is required to revoke a Digital Certificate by the National Security Agency, court order, or other competent government authority;

3.2.4 The Affected Manufacturer requests the Revocation of its Digital Certificate;

3.3 **Indemnification.** The Revocation Initiator(s) shall indemnify and hold harmless and defend, the Affected Manufacturer, Cable Operators, or any party that carries the Certificate Revocation List applicable to such Revocation and each of their officers, directors, equivalent corporate officials, employees, representatives and agents ("Indemnified Parties," if not the Revocation Initiator) from and against any and all (i) claims, actions, suits, proceedings or litigation and any losses, deficiencies, damages, liabilities, costs and expenses associated therewith, including but not limited to reasonable attorneys' fees and expenses, arising out of the Revocation or rescission of Revocation of any Digital Certificate for which Revocation Initiators had sought Revocation and (ii) other costs or expenses incurred by the Indemnified Parties in connection with such Revocation or rescission of Revocation, including but not limited to any costs and expenses associated with the generation and distribution of information necessary to affect such Revocation or rescission and any amounts paid to the Affected Manufacturer (or to Manufacturers' affected customers) or any other party on account of such Revocation. A bond or security for reasonably anticipated costs may be required.

3.4 **Notice of Revocation to Affected Manufacturer.** In the event that Revocation is requested, the CA shall provide the Affected Manufacturer to whom the affected Digital Certificate was issued with notice of such requested Revocation. If the Manufacturer notifies the CA that the Manufacturer consents to such Revocation of such Digital Certificate, or if the CA is required to Revoke pursuant to Section 3.2.3 above, the CA may take steps to Revoke the applicable Digital Certificate.

3.5 **Assent to Revocation/Dispute Resolution.** No more than 30 (30) calendar days after the receipt of notice from the CA, the Affected Manufacturer shall notify the CA whether Manufacturer desires to contest the grounds for such Revocation. If the Affected Manufacturer notifies the CA that it does not wish to contest the requested Revocation, or if Manufacturer fails to respond timely to the notice from the CA, the Revocation shall be deemed to be without objection and may proceed. If the Affected Manufacturer timely notifies the CA of its intent to object to the requested Revocation, Manufacturer shall submit a written statement, under oath, which sets out any facts which disprove or contradict the Revocation Initiator's stated grounds for Revocation ("Revocation Objection"). Within ten (10) business days after receipt of the Revocation Objection, the CA shall provide notice of the Revocation Objection and the Revocation Objection itself to the Revocation Initiator(s). Within thirty (30) days after receipt from the CA of the notice of the Revocation Objection, the Revocation Initiator(s) may initiate an arbitration in accordance with the provisions of Section 3.7 below to determine whether the requested Revocation may proceed.

3.6 **Affected Manufacturer Remedies**. Affected Manufacturer’s sole recourse with respect to Revocation shall be the objection and arbitration procedures set out herein. The CA, other Manufacturers, and Cable Operators shall each have no liability whatsoever with respect to any Revocation. Without limiting the foregoing, the

CA, other Manufacturers, and Cable Operators shall not have any liability with respect to any Revocation, and no compensation shall be made to Affected Manufacturer, except that if the CA determines that it has performed a Revocation in error it may, at the request of Manufacturer, (a) rescind the Revocation through substantially the same means as were used to effect the Revocation, or (b) provide for compensation to the Affected Manufacturer (or Manufacturer's affected customers) for each of its affected devices in an amount equal to the least of (i) the fair market value of each device, (ii) the cost of reworking each device to incorporate a new Digital Certificate and Private Keys or (iii) $25 per device.

3.7 **Arbitration Procedures.**

3.7.1 The parties to the arbitration shall be the Revocation Initiator(s), the Affected Manufacturer(s), and at its discretion, the CA (collectively, the "Arbitrating Parties"). The Revocation Initiator(s) shall bear the burden of proof in demonstrating, by a preponderance of the evidence, that one or more of the Revocation Criteria have been satisfied.

3.7.2 There shall be a sole arbitrator, who shall be selected by the Arbitrating Parties from the National Panel of Commercial Arbitrators of the American Arbitration Association within fourteen (14) days of the initiation of arbitration; provided, however, that in the event the Arbitrating Parties cannot agree on a sole arbitrator within such fourteen (14)-day period, the Revocation Initiator(s), on the one hand, and the other Affected Manufacturer, on the other hand, shall each, promptly thereafter, select one arbitrator from the National Panel of Commercial Arbitrators of the American Arbitration Association and those two arbitrators shall jointly select a third arbitrator from the National Panel of Commercial Arbitrators of the American Arbitration Association, who shall serve as the presiding arbitrator and chairperson of such arbitration.

3.7.3 The arbitration shall be conducted in New York, New York, in accordance with the International Arbitration Rules of the American Arbitration Association. The language of the arbitration shall be English.

3.7.4 The arbitrator(s) may conduct the arbitration in such manner as he, she or they shall deem appropriate, including the imposition of time limits that he, she or they consider(s) reasonable for each phase of the proceeding, but with due regard for the need to act, and make a final determination, in an expeditious manner. The arbitrator(s) shall set a schedule to endeavor to complete the arbitration within one (1) month.

3.7.5 The arbitrator(s) shall permit and facilitate such limited discovery as he, she or they shall determine is reasonably necessary, taking into account the needs of the Arbitrating Parties and the desirability of making discovery as expeditious and cost-effective as possible, recognizing the need to discover relevant information and that only one party may have such information.

3.7.6 The Arbitrating Parties and the arbitrator(s) shall treat the arbitration proceedings, any related discovery, documents and other evidence submitted to, and the decision of, the arbitrator(s) as confidential information. In addition, and as necessary, the arbitrator(s) may issue orders to protect the confidentiality of proprietary information, trade secrets and other sensitive information disclosed in discovery or otherwise during the arbitration.

3.7.7 Any decision by the arbitrator(s) shall be final and binding on the Arbitrating Parties, except that whether the arbitrator(s) exceeded his, her or their authority, as specifically described in this Agreement, shall be fully reviewable by a court of competent jurisdiction. Judgment upon any award shall be entered in a court of competent jurisdiction.

3.7.8 The arbitrator(s) shall be compensated at his, her or their hourly rates, determined at the time of appointment, for all time spent in connection with the arbitration, and shall be reimbursed for

reasonable travel and other expenses. The arbitrator(s) shall determine all costs of the arbitration, including the arbitrator(s)' fees and expenses, the costs of expert advice and other assistance engaged by the arbitrator(s), the cost of a transcript and the costs of meeting and hearing facilities.

3.7.9 The arbitrator(s) is (are) empowered solely to determine whether one or more of the Revocation Criteria have been satisfied. In the event that the arbitrator(s) determine(s) that the Revocation Criteria have been satisfied, Revocation shall be deemed warranted. Any such determination by the arbitrator(s) shall be final and binding on the Arbitrating Parties, except that whether the arbitrator(s) exceeded his, her or their, authority as specifically described in this Section, such decision shall be fully reviewable by a court of competent jurisdiction. In any such arbitration, the Affected Manufacturer(s) may introduce evidence solely to support the position that one or more of the Revocation Criteria have not been satisfied.

3.7.10 All costs and fees shall be shared equally as between the Revocation Initiator(s), on the one hand, and the Affected Manufacturer, on the other; provided, however, the arbitrator(s) may otherwise apportion such costs and fees among such Revocation Initiator(s) and Affected Manufacturer as the arbitrator(s) may determine. The prevailing party in such arbitration shall provide to the CA a copy of the arbitrator(s) decision. If Revocation is warranted, the CA may, after it receives such decision, take steps to cause such Revocation.

4 Certificate Revocation Logistics

4.1 See generally the ITU X.509 specification and RFC 3280.

4.2 CRL Update Frequency

For security reasons, update and access to the Root CA CRL should be minimal. The CA will reasonably determine when and if the Root CA CRL should be updated with the current CRL. CableLabs shall affect any updates to the Root CA CRL.

4.3 CRL Distribution

The CRLs will be placed on the CableLabs web site private area and updated at least once a quarter. The CRLs will be available for PKI users (Manufacturers, Cable Operators, CableLabs) to pull the CRL as desired with an HTTP GET in compliance with RFC 2585.

4.4 Affected Manufacturer Duties

Upon Revocation (after arbitration as the case may be), the Affected Manufacturer shall continue to safeguard the Private Key associated with the Revoked Digital Certificate, until the certificate expires, at which time the Private Key should be securely destroyed, or securely destroy the Private Key associated with the Revoked Digital Certificate.

4.5 CRL Profile

The CRL profile complies with RFC 2459. The specific information for this application of X.509 CRLs is described in the table below.

CRL Profile		
Field	**Value**	**Comments**
CertificateList ..tbsCertList		
....version	1	Integer value of 1 for a version 2 CRL
....algorithmIdentifier	sha1WithRSAEncryption	Must match the Algorithm Identifier in the signatureAlgorithm field.

....issuer	Subject Name of CA certificate	Must exactly match the subject name in the CA certificate.
....thisUpdate	YYMMDDHHMMSSZ or YYYYMMDDHHMMSSZ	UTCTime: For dates up to and including 2049 generalTime: For dates after 2049
....nextUpdate	YYMMDDHHMMSSZ or YYYYMMDDHHMMSSZ	UTCTime: For dates up to and including 2049 generalTime: For dates after 2049
....RevokedCertificates		
......serialNumber	INTEGER[1..20]	Serial number of revoked certificate
......revocationDate	YYMMDDHHMMSSZ or YYYYMMDDHHMMSSZ	UTCTime: For dates up to and including 2049 generalTime: For dates after 2049
....crlExtensions		
......CRL Number	INTEGER	Monotonically increasing sequential number
..Signature		
..signatureAlgorithm	sha1WithRSAEncryption	Must match the Algorithm Identifier in the tbsCertList.algorithmIdentifier field.
..signature	BITSTRING	The signatureValue field contains a digital signature computed upon the ASN.1 DER encoded tbsCertList.