



OpenCable Certificate Revocation Policy (CRP)

Policies, Management and Procedures for OpenCable

Notice

This document is a cooperative effort undertaken at the direction of Cable Television Laboratories, Inc. for the benefit of the cable industry in general. Neither CableLabs nor any member company is responsible for any liability of any nature whatsoever resulting from or arising out of use or reliance upon this specification by any party. This document is furnished on an "AS IS" basis and neither CableLabs nor its members provides any representation or warranty, express or implied, regarding its accuracy, completeness, or fitness for a particular purpose.

© Copyright 2006 Cable Television Laboratories, Inc.
All rights reserved.

Table of Contents

1	Introduction.....	1
1.1	Executive Summary.....	1
2	Definitions and Acronyms	2
2.1	Definitions	2
2.2	Acronyms.....	3
3	CableLabs PKI Hierarchies.....	4
3.1	Overview.....	4
3.2	CableLabs Manufacturer Root Hierarchy	5
3.3	CableLabs CVC Root Hierarchy.....	6
4	OpenCable Certificate Revocation Policies and Procedures	6
4.1	Objectives	6
4.1.1	Certificate Archive	9
4.2	CRL Policies and Procedures	9
4.2.1	Certificate Revocation Overview	9
4.2.2	Designated Contacts	10
4.2.3	Revocation Events.....	11
4.2.4	Investigation Request for Possible Revocation.....	11
4.2.5	Investigation, Decision and Appeal Process	14
4.2.6	Revocation Request	16
4.2.7	Root CA CRL Policies	17
4.2.8	CRL Profile	18
4.2.9	CRL Pruning.....	19
5	Certificate Revocation Implementation	19
5.1	OpenCable Certificate Revocation Implementation	19
5.1.1	Selective Denial of Service Overview.....	19
5.1.2	Selective Denial of Service Flow Description.....	20
5.1.3	Selective Denial of Service Record	23

1 Introduction

Several OpenCable specifications include requirements for security services based on the use of X.509 digital certificates. Digital certificates provide a secure mechanism to identify and authenticate an entity via the validation of a digital signature. Certificate validation determines if the certificate and its associated private key should be trusted. Although proper procedures are put in place to maintain the trustworthiness of a certificate, if a certificate should not be trusted, it is revoked and the information is published (e.g., placed on a certificate revocation list (CRL) for use by the relying party. Thus, the cable industry needs to have a defined way to revoke certificates and a common method for communication of the revocation information.

This document addresses certificate revocation for OpenCable devices. This includes certificate revocation of Root CA issued Certification Authorities (CAs) and Code Verification Certificates (CVCs).

1.1 Executive Summary

Certificate revocation is a critical function within a Public Key Infrastructure (PKI) so as to provide information on any invalid certificate. The reasons to revoke a certificate prior to expiration include key compromise, breach of contract, business reasons, technical difficulties, and other reasons as to be defined by the CableLabs revocation policy. Any reason to revoke a certificate is in and of itself not means enough to justify revocation within the cable industry PKI, therefore cable operator participation through the various boards on each project will need to address certificate revocation on a case by case basis until the industry understands the consequences of such an event and can set precedence and enhance the rules for revocation.

OpenCable Certificate Revocation Policies and Procedures addresses identifying the revocation domains of the issuing CA, filing a revocation request, investigating the request, revoking the certificate (if applicable), and publishing the revocation information.

2 Definitions and Acronyms

2.1 Definitions

Asymmetric Key An encryption key or a decryption key used in public key cryptography, where encryption and decryption keys are always distinct.

Authentication The process of verifying the claimed identity of an entity to another entity.

Authenticity The ability to ensure that the given information is without modification or forgery and was in fact produced by the entity that claims to have given the information.

Authorization The act of giving access to a service or device if one has the permission to have the access.

Certificate Archive A record of every certificate issued from the root which includes a copy of the certificate.

Certification Authority (CA) A trusted organization that accepts certificate applications from entities, authenticates applications, issues certificates and maintains status information about the certificates it issues.

Certificate Subscriber The entity, which owns the certificate.

Certificate Revocation List (CRL) A digitally signed list issued by an CA to identify certificates that have been revoked from that authority but have not expired yet.

Certificate Validation The process of checking the validity period, issuer signature and revocation status of the certificate of a requesting party, either by comparing the certificate with its possible occurrence on a CRL.

Code Verification Certificate (CVC) A code verification certificate identifies the authenticity of the software by either the manufacturer or cosigner.

Cosigner A cosigner is an entity authorized to sign code in addition to the manufacturer of the code. CableLabs is authorized to sign certified code images. Service providers are authorized to sign code images to provide authorization for download of software images approved for their particular network customers.

Digital Certificate (or Certificate) A binding between an entity's public key and one or more attributes relating to its identity, also known as a Public Key Certificate.

Digital signature A data value generated by a public key algorithm based on the contents of a block of data and a private key, yielding an individualized cryptographic checksum.

Key Exchange The swapping of public keys between entities to be used to encrypt communication between the entities.

Key Administration The process of securely generating a public/private key pair, properly requesting the X.509 certificate, proper use of the X.509 certificate, proper use and protection of private key.

Non-Repudiation The ability to prevent a sender from denying later that he or she sent a message or performed an action.

Policy Authority (PA) The part of the CableLabs organization that sets the policy rules of how the PKI will operate, including certificate revocation.

Privacy A way to ensure that information is not disclosed to any one other than the intended parties. Information is usually encrypted to provide confidentiality. Also known as confidentiality.

Private Key The key used in public key cryptography that belongs to an individual entity and must be kept secret.

Public Key The key used in public key cryptography that belongs to an individual entity and is distributed publicly. Other entities use this key to encrypt data to be sent to the owner of the key.

Public Key Certificate A binding between an entity's public key and one or more attributes relating to its identity, also known as a digital certificate.

Public Key Cryptography A procedure that uses a pair of keys, a public key and a private key for encryption and decryption, also known as an asymmetric algorithm. A user's public key is publicly available for others to use to send a message to the owner of the key. A user's private key is kept secret and is the only key that can decrypt messages sent encrypted by the user's public key.

Pruning The act of removing certificates from a CRL, usually done upon expiration.

Relying Party It is the relying party who depends upon the PKI to do its part in protecting the valued service.

Root Private Key The private signing key of the highest-level Certification Authority. It is normally used to sign public key certificates for lower-level Certification Authorities or other entities.

Root Public Key The public key of the highest level Certification Authority, normally used to verify digital signatures generated with the corresponding root private key.

Service Provider A CableLabs authorized entity to provide service on a DOCSIS, PacketCable or CableHome network.

Subscriber Certificate Any non-root entity issued a certificate within the CableLabs PKI

X.509 certificate A public key certificate specification developed as part of the ITU-T X.500 standards directory.

2.2 Acronyms

BPI+ Baseline Privacy Plus Interface Specification. The security portion of the DOCSIS 1.1 standard that runs on the MAC layer.

CA Certification Authority. A trusted organization that accepts certificate applications from entities, authenticates applications, issues certificates and maintains status information about certificates.

CM DOCSIS Cable Modem

CMTS Cable Modem Termination System. The device at a cable head-end which implements the DOCSIS RFI MAC protocol and connects to CMs over an HFC network.

CPS Certificate Practices Statement

CVC Code Verification Certificate

DOCSIS Data Over Cable Service Interface Specifications

PKI PA Public Key Infrastructure Policy Authority. The board authorized on behalf of CableLabs to create, maintain and change policy surrounding the creation, use and revocation of its certificates. The PKI PA Officer is the Chief Security Architect for CableLabs.

PKCS Public Key Cryptography Standards. Published by RSA Data Security Inc. These Standards describe how to use public key cryptography in a reliable, secure and interoperable way.

PKI Public Key Infrastructure. A process for issuing public key certificates, which includes standards, Certification Authorities, communication between authorities and protocols for managing certification processes.

RFC Request for Comments. Technical policy documents approved by the IETF which are available on the World Wide Web at <http://www.ietf.cnri.reston.va.us/rfc.html>.

RSA A public-key, or asymmetric, cryptographic algorithm that is used to provide the services of authentication and encryption. RSA stands for the three inventors of the algorithm; Rivest, Shamir, Adleman.

RSA Key Pair

A public/private key pair created for use with the RSA cryptographic algorithm.

3 CableLabs PKI Hierarchies

3.1 Overview

The CableLabs PKI began with a single certificate hierarchy in 2000 to meet the security service requirements of the DOCSIS specification. Since then, to meet the security requirements of other projects, the CableLabs PKI has evolved into five certificate hierarchies: the DOCSIS Root hierarchy, the PacketCable MTA Root hierarchy, the CableLabs Manufacturer Root hierarchy, the CableLabs Code Verification Root hierarchy, and the CableLabs Service Provider Root hierarchy. The CableLabs Manufacturer Root hierarchy and CableLabs Code Verification Root hierarchy are used to satisfy OpenCable requirements.

CableLabs has created these certificate hierarchies to provide:

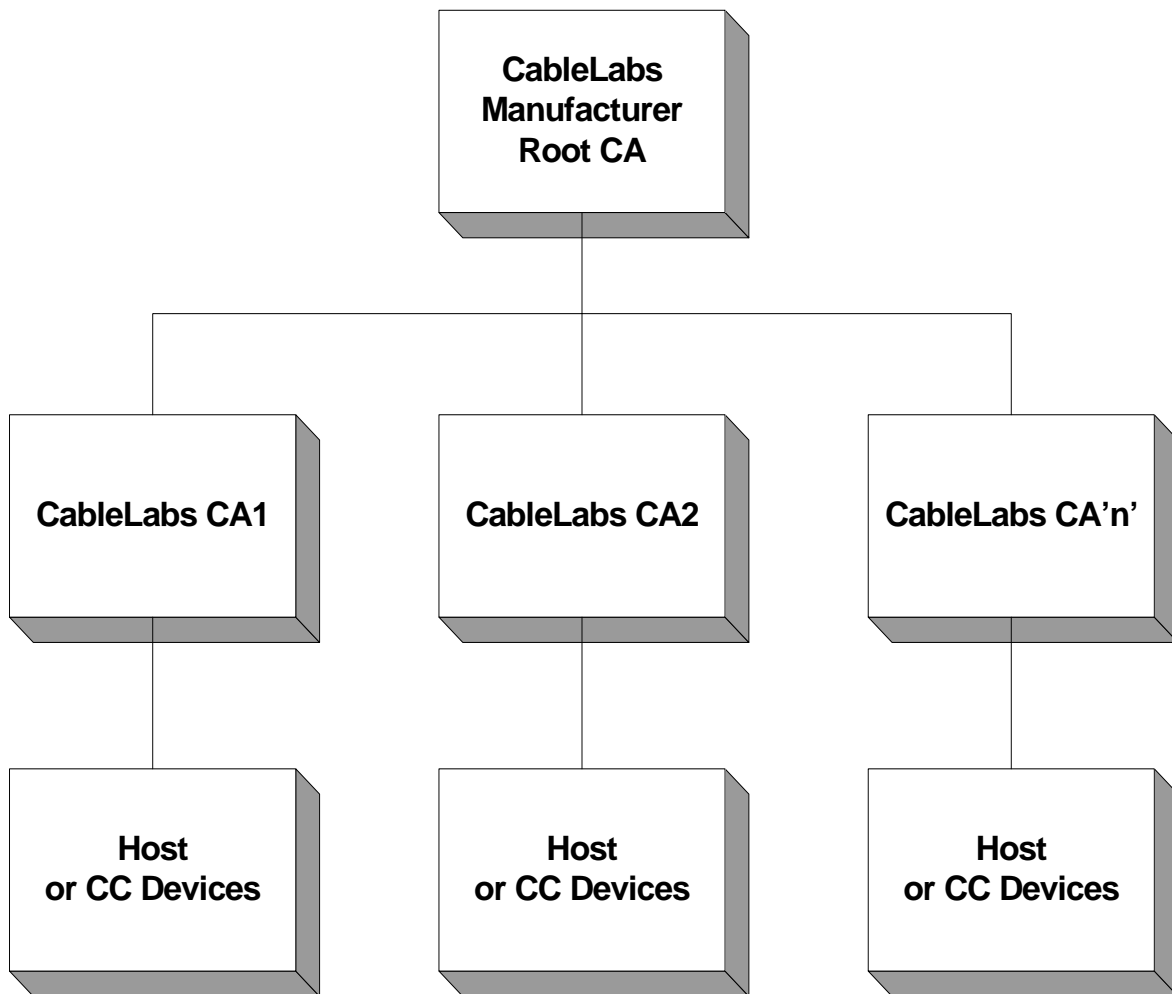
- Authentication for hardware devices (e.g., CableCard–Host authentication);
- Authentication and integrity of software images downloaded into hardware devices (e.g., Common Download)

Hardware device authentication uses a public key X.509 certificate that cryptographically ties the hardware unique ID of the device to the certificate's public key. The hardware authentication is used during the Card-Host binding process prior to granting secure communications to in-home devices on the service provider's network.

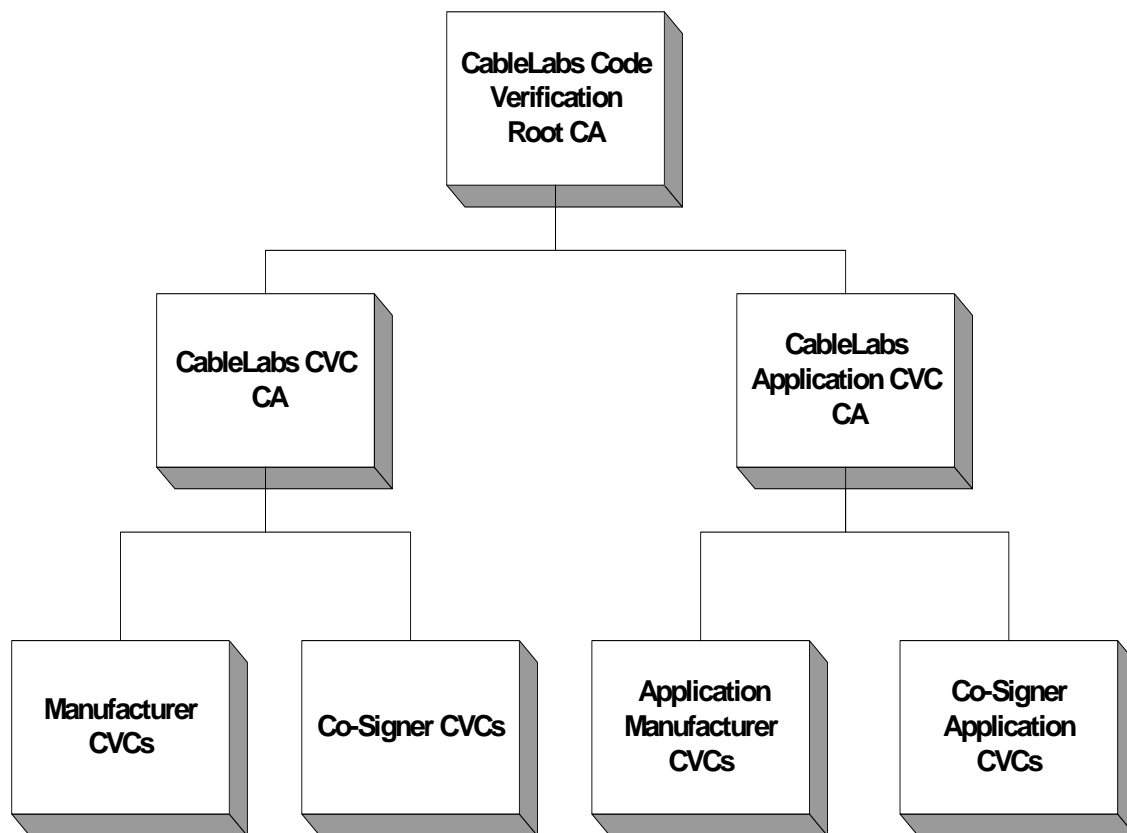
Software authentication uses a public key X.509 certificate that cryptographically ties the signer's subject name to the public key. Software authentication is used during the software download process to the hardware devices to establish appropriate identity of the software prior to acceptance of installation of any download.

It is important to point out that for devices embedded with a DOCSIS CM, there is only one software image for the entire suite of functionality, even if the processes within the box are logically separate. The reader is referred to the DOCSIS and OpenCable specifications for the CableLabs official definition of "embedded".

3.2 CableLabs Manufacturer Root hierarchy



3.3 CableLabs CVC Root hierarchy



4 OpenCable Certificate Revocation Policies and Procedures

4.1 Objectives

The CableLabs PKI serves several CableLabs projects, each providing different cable services. The CableLabs PKI is too large to define policies and procedures for revocation for all certificate types at the same time. The objective of this document is to define certificate revocation policies and procedures for the CableLabs CAs that issue certificates for OpenCable devices.

Revocation of Root CA Issued Certificates: Defines the certificate revocation policies and procedures for all root issued certificates. This is addressed in the CableLabs Certificate Revocation Policy document.

First-tier CA Issued Certificates: Defines the certificate revocation policies and procedures for all First-tier CA issued certificates via CRLs, one CRL corresponding to each First-tier CA. Figure 1 below illustrates the First-tier CA CRLs and the certificates

associated with each CRL. Specifically, CRLs issued by the CableLabs Manufacturer CA, CableLabs CVCs affect OpenCable devices.

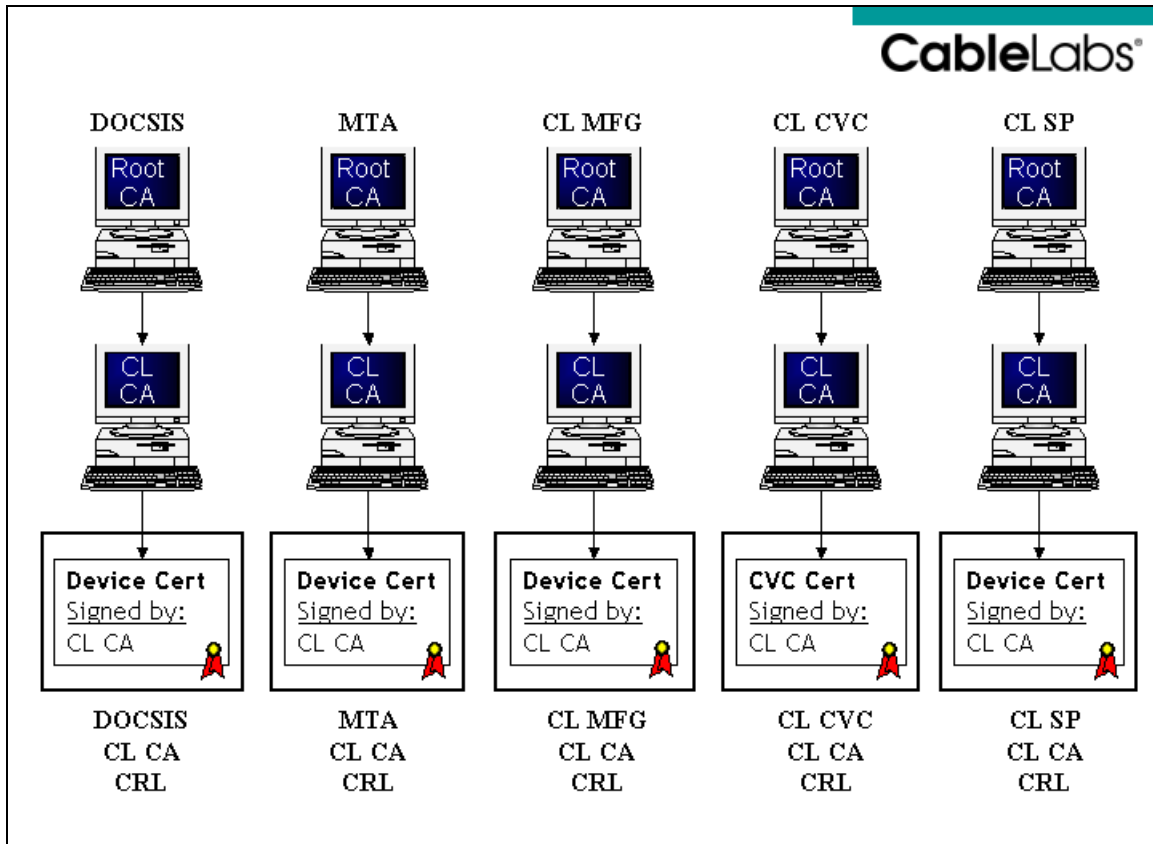
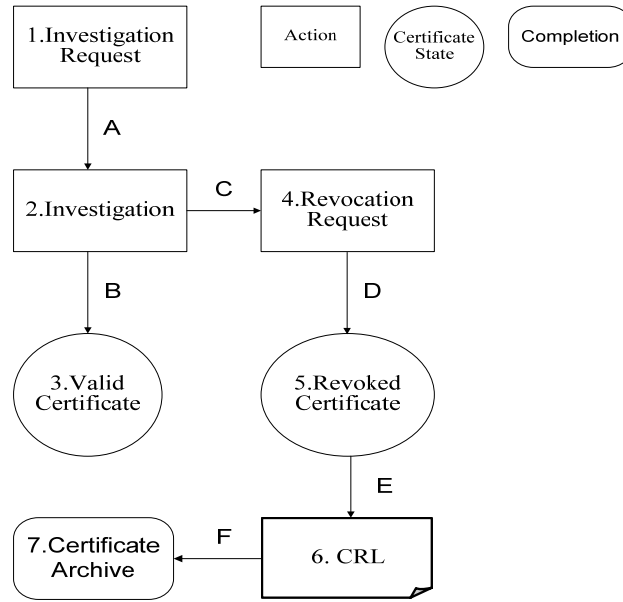


Figure 1 First-tier CableLabs CA issued CRLs

The certificate revocation lifecycle is illustrated in the diagram below.



Each box in the diagram above contains a number which corresponds to the numbers and explanation listed below.

1. Investigation Request – A request for investigation from a certificate subscriber, the Root CA, OpenCable Security, or the OpenCable Certification Board into a possible revocation event for a certificate.
2. Investigation – CableLabs conducts an investigation and holds an OpenCable Security meeting for decision on revocation.
3. Valid Certificate – The state of the certificate if it is valid for use as specified by the appropriate CableLabs specification.
4. Revocation Request – CableLabs requires a certificate to be revoked and requests any contracted parties to carry out the revocation if necessary.
5. Revoked Certificate – The state of the certificate if it has been revoked.
6. CRL – The Certificate Revocation List signed by the appropriate CA.
7. Certificate Archive – A history and copy of all issued certificates and CRLs.

Each line between the boxes is labeled with a letter which corresponds to the letters and explanation listed below.

- A. From investigation request to investigation, a request to investigate for a possible revocation event is sent to CableLabs.
- B. From investigation to valid certificate, the investigation resulted in no revocation event and CableLabs will notify the certificate subscriber and the originator of the request.
- C. From investigation to revocation request, the investigation resulted in a revocation event and CableLabs will notify the certificate subscriber, the originator of the request and the Root CA.

D. From revocation request to revoked certificate, the CA will revoke the certificate by changing the status of the certificate by placing it on the CRL for that CA.

E. From revoked certificate to CRL, the CA will issue a CRL and CableLabs will publish the CRL to the relying parties.

F. From CRL to certificate archive, each CRL created is a unique list created on certain date at specific time. Each unique list is added to the certificate archive as a part of the history of the certificates within the PKI.

4.1.1 Certificate Archive

Upon creation of a certificate from any of the CableLabs CAs, the certificate is placed in a certificate archive along with the history of the certificate. This archive is a database that can be accessed at anytime by the CA organization. The archive gives a complete history of the certificate including the generation (signing) ceremony and the revocation status on all CRLs issued by the CA.

4.2 CRL Policies and Procedures

4.2.1 Certificate Revocation Overview

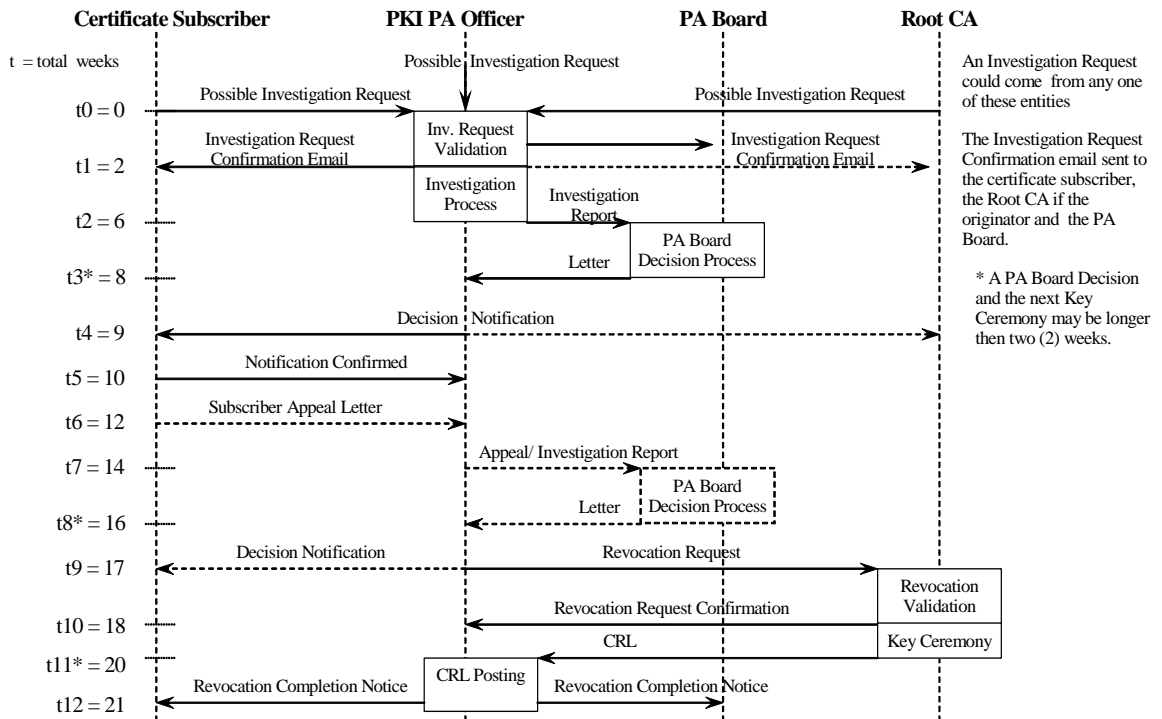
The OpenCable specifications require CableLabs to operate the Root CAs, CableLabs Manufacturer CA, and CableLabs CVC CAs. This operation includes certificate revocation of the certificates issued by the CableLabs controlled CAs for certificates that are no longer valid. This section describes the policy and procedures for the revocation of certificates issued by CableLabs' managed CAs.

Certificate revocation may be necessary when, prior to the expiration of a certificate, there has been a compromise in security or the certificate is no longer valid for legal or business reasons.

CRLs will be created and maintained by the appropriate CA, and each will list the revoked certificates issued from each CA. The CA's private key will sign the CRL issued by that CA. The policies and procedures for revocation from each CA will be the similar. All investigation requests will be investigated by CableLabs and authorized by the PKI Policy Authority (PA) board. The OpenCable PKI PA will consist of OpenCable Security Architect, CableLabs Executive Management for each project, CableLabs Legal Department and Member Participants in the OpenCable Security Team.

The following diagram is an overview of the process. The solid lines are required actions of the certificate revocation process and the dotted lines are optional actions. The first set of lines for the investigation request is solid to represent the mandatory action on the part of one of the parties listed. The investigation request need only come from one party listed not all three possible parties.

Certificate Revocation Process



4.2.2 Designated Contacts

CableLabs Policy Authority Officer:

Oscar Marcia
CableLabs
858 Coal Creek Circle
Louisville, CO 80027
303-661-9100
o.marcia@cablelabs.com

4.2.3 Revocation Events

Certificate revocation begins with the certificate subscriber, the Root CA, the PA Board or the PKI Policy Authority questioning the validity of a particular certificate. Any number of reasons may exist which would invalidate a certificate for its intended purpose. This section describes the events for which a root issued certificates may be considered for revocation.

The CA issued certificates may be revoked under the following circumstances:

- The private key corresponding to the public key in the certificate has been
 - Lost
 - Disclosed without authorization
 - Stolen
 - Compromised in any way
- The certificate subscriber does not meet the obligations of its CableLabs Digital Certificate Authorization Agreement with CableLabs or with the organization holding the Root CA on behalf of CableLabs, which processed the certificate application.
- There is an improper or faulty issuance of a certificate due to:
 - A prerequisite to the issuance of the certificate not being satisfied;
 - A fact 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 certificate subscriber requests the revocation for any reason whatsoever of its certificate.

4.2.4 Investigation Request for Possible Revocation

This section outlines and describes the circumstances and events that would warrant a root issued certificate to be investigated for possible revocation. An investigation always precedes revocation and revocation shall follow only under the specific procedures described in this document. All investigation requests are required to be valid, which shall be determined by their compliance or non-compliance with the procedures of this document.

The investigation involves maintaining a list of all certificates ever under investigation with details outlining the status or history and bringing resolution to the revocation request. While under investigation the CableLabs PKI PA Officer will execute the process as outlined in this document.

An investigation request may come from the certificate subscriber, the Root CA, the PA Board or the PKI Policy Authority. A certificate subscriber may elect another representative to make the investigation request if such representative has been given expressly written authority by the subscriber to make the investigation request. This request is for an investigation only and is not the request for revocation to the issuing organization. The requestor must send a letter to the CableLabs designated legal contact and an email to the designated CableLabs PA Officer.

4.2.4.1 Investigation Schedule

An Investigation Request may be sent to the CableLabs PA Officer at any time. The CableLabs PA Officer sends the Investigation Request Confirmation within ten (10) business days after the reception of the Investigation Request and starts the Investigation Process defined in the following section. The CableLabs PA Officer has thirty (30) business days to complete the investigation and call a PA Board meeting for determination of a revocation event.

4.2.4.2 Investigation Request Letter

An Investigation Request Letter must include the following information:

- The date of the investigation request
- The date the certificate was suspected as invalid
- The contact information must include: name, title, organization name, address, email address, phone and fax number.

For certificate subscribers: This person must be the authorized officer of the company who signed the original agreement with CableLabs, one of the contacts designated in the CableLabs Digital Certificate Authorization Agreement, a replacement for the original signer (verified by CableLabs) or someone of higher authority within the organization.

For the Root CA: This person must be the authorized account manager.

For the PA: This must be the PA Officer.

- The certificate serial number
- Issuer name and subject name on the certificate
- The reason for requesting the revocation
- Acknowledgement that the requestor understands the revocation policies and procedures and intends to comply with the required policies and procedures
- Acknowledgement that if the investigation ends in revocation of the certificate in question, that the consequences of revocation are understood
- If request is from the certificate subscriber: Signature of the authorized officer of the company who signed the original digital certificate agreement with CableLabs.
- If the request is from the CableLabs PA Officer or Root CA Account Manager: That person's signature

An Investigation Request Letter may include the following information:

- Number of signed images or certificates signed.

Note the Investigation Request Letter must be accompanied by the Investigation Request Email.

4.2.4.3 Investigation Request Email

An Investigation Request Email must include the following information:

- The date of the investigation request
- The date the certificate was suspected as invalid
- The contact information must include: name, title, organization name, address, email address, phone and fax number.

For certificate subscribers: This person must be the authorized officer of the company who signed the original agreement with CableLabs.

For the Root CA: This person must be the authorized account manager.

For the PA: This must be the PA Officer.

- The certificate serial number
- Issuer name and subject name on the certificate
- The reason for requesting the revocation
- Attach the certificate in binary DER encoding for email attachments
- Digital Signature (requirements TBD)

An Investigation Request Email may include the following information:

- Number of signed images or certificates signed.

Note the Investigation Request Email must be accompanied by the Investigation Request Letter.

4.2.4.4 Investigation Request Validation

All Investigation Requests to revoke a certificate require one of the following identification and authentication mechanisms prior to acceptance and confirmation of the request.

- If possible, the requestor hand delivers the Investigation Request Letter in person along with a valid state or government issued photo ID card to the CableLabs PA officer and CableLabs Legal Counsel;
- Or, the requestor may send a digitally signed email request to the CableLabs PA Officer and cc the CableLabs Legal Counsel. To confirm this request, a letter must be sent within 5 days of the initial contact with CableLabs to CableLabs Legal Counsel;
- Or, in the event that the above procedures are not available to the requestor they may contact the CableLabs PA Officer directly and request alternative procedures to issue the investigation request. The requestor shall be provided with the procedures to provide sufficient documentation to prove their identity and/or authority to request the revocation. These procedures may include, among other methods, the use of other online procedures, telephone calls, or fax followed by a signed revocation request letter.

Upon receipt of a valid request, the investigation process will be initiated. The investigation request will be included in the documentation of the investigation report.

4.2.4.5 Investigation Request Confirmation

Within ten (10) business days from the official receipt of the Investigation Request Letter, the CableLabs PA Officer validates the Investigation Request and sends an Investigation Request Confirmation via digitally signed mail to the parties listed on

official Investigation Request Letter, the Certificate Subscriber and the PA Board stating that the Investigation Request has been validated and an investigation has begun on the certificate serial number in question and the requestor will be notified upon completion of the investigation.

4.2.5 Investigation, Decision and Appeal Process

This section describes the duties of the PA Officer and the PA Board to process complete an investigation and find resolution to the investigation request for revocation of a certificate. This process may include a request by the requestor to appeal the decision of the PA Board.

4.2.5.1 PA Officer Duties

It shall be the responsibility of the PKI PA Officer to document the investigation process from start to conclusion. Each investigation must include the following steps:

- It is the duty of the PKI PA Officer to investigate the request and send the Investigation Report to the PA Board within 30 days of the Investigation Request Confirmation email.
- The investigation itself must at least consist of direct contact with the requestor to verify the reason for revocation and certificate information.
- At the conclusion of the investigation, the PKI PA Officer must call a meeting of the PA Board to make a determination for revocation.
- Notification in writing to the Requestor and Certificate Subscriber must occur within 5 business days of the creation of the PA Board Decision Letter.

The PA Officer shall create a file to track the necessary documentation, which shall include:

- The Investigation Request Letter along with the date of its receipt
- Investigation Request Confirmation Email along with the date of transmission and the list of addresses.
- The Investigation Report that must contain a description of the dates and status of the investigation upon finding new information that may affect the outcome of the investigation.
- A PA Board Meeting Report must include the date the PA Board met, the attendees and the outcome of the investigation for each certificate in question, along with the signature of the PA Officer on each page of the final report. If revocation is determined, the reason for revocation must be recorded along with a copy of the entire certificate.
- A copy of the PA Board Decision Letter
- For Appeal, all the above documentation plus the Appeal Letter, date of receipt of the appeal letter and any new information.

4.2.5.2 PA Board Duties

It shall be the responsibility of the PA Board will determine the outcome of the investigation.

- Review the investigation report
- Consider the technical and business reasons for revocation
- Discuss possible consequences of revocation
- Make a determination on the investigation request
- The board shall make a determination as quickly as deemed reasonable
- Upon conclusion of a decision, a PA Board Letter must be sent to the PA Officer with the official decision of the Board clearly stating whether the certificate (include the certificate serial number) is to be revoked or not and must be signed and dated by either CableLabs Legal Counsel if attended the board meeting or the Chair of the PA Board.
- The PA Board may request consultation with the requestor or certificate subscriber.

4.2.5.3 The PA Board

The PA Board must consist of the PA Officer, Executive Management for the affected CableLabs project, CableLabs Legal Counsel and the member committee appointed for the affected project.

4.2.5.4 Decision Notification

Upon conclusion of all investigations, the PA Officer shall notify the Certificate Subscriber and the requestor of the outcome within five (5) days after of the creation of the PA Board Decision Letter. The PA Officer will request the subscriber to provide a Notification Conformation Letter within five (5) days of the reception of the PA Board Decision Letter.

4.2.5.5 Subscriber Appeal Process and Schedule

If the Certificate Subscriber wished to appeal the decision made by the PA Board, it must submit an Appeal Letter within ten (10) business days of receipt of the PA Board Letter with the revocation notice from CableLabs to the CableLabs PA Officer.

The PA Officer must call a PA Board Meeting within ten (10) days of receipt of the Appeal Letter.

4.2.5.6 Subscriber Appeal Letter

The Appeal Letter must include the following information:

- In the first sentence of the letter, the request for appeal for the certificate in question with the certificate serial number.
- The Appeal Letter must also include the Investigation Request Letter and the PA Board Letter
- The reason for the appeal
- Acknowledgement that the requestor understands the revocation policies and procedures and intends to comply with the required policies and procedures
- Acknowledgement that if the investigation ends in revocation of the certificate in question, that the consequences of revocation are understood

- If request is from the certificate subscriber: Signature of the authorized officer of the company who signed the original digital certificate agreement with CableLabs.
- If the request is from the CableLabs PA Officer or Root CA Account Manager: Signature

4.2.6 Revocation Request

This section describes the policies and procedures for certificate revocation requests. Based on the decision of the PA Board, the PA Officer will issue a Revocation Request to the CA Contact as listed in this document. A CA issued certificate shall be revoked in all cases through a certificate revocation request issued by the PA Officer and only after going through investigation procedures in accordance with this document.

4.2.6.1 Revocation Request Content

A request for certificate revocation must include the following information:

- The date of the revocation request
- The PA Officer contact information must include: name, title, organization name, address, email address, phone and fax number. This officer must be the authorized PA Officer listed in this document.
- The certificate to be revoked in DER format
- Issuer Name
- Subject Name
- Certificate Serial Number
- The reason for requesting the revocation, which must be one of the following valid reason codes.

unspecified	(0)
keyCompromise	(1)
cACompromise	(2)
affiliationChanged	(3)
superseded	(4)
cessationOfOperation	(5)

keyCompromise is used in revoking an end-entity certificate; it indicates that it is known or suspected that the subject's private key, or other aspects of the subject validated in the certificate, have been compromised. Revoked CVC's would use this reason.

cACompromise is used in revoking a CA-certificate; it indicates that it is known or suspected that the subject's private key, or other aspects of the subject validated in the certificate, have been compromised. All CA-certificates would use this reason.

affiliationChanged indicates that the subject's name or other information in the certificate has been modified but there is no cause to suspect that the private key has been compromised;

superseded indicates that the certificate has been superseded but there is no cause to suspect that the private key has been compromised;

cessationOfOperation indicates that the certificate is no longer needed for the purpose for which it was issued but there is no cause to suspect that the private key has been compromised;

4.2.6.2 The Revocation Event Schedule

The PA Officer must wait at least 10 days after the date of the Confirmation from the Certificate Subscriber to send the revocation request in order to give the Certificate Subscriber 10 days to appeal the process. The PA Officer must send the revocation request within 5 days of receiving an Appeal Board Letter stating that revocation is required. Certificate revocation will take place at the next possible Root CA ceremony.

The Root CA account manager will send the updated CRL to the PA Officer via signed and encrypted email within one (1) business day after the CRL is updated. PA Officer publishes the CRL on the CableLabs web site in the appropriate place for the relying parties within one (1) business day after the reception of the CRL from the CA.

4.2.6.3 PA Officer Duties

Related to the revocation of a certificate, the PKI PA Officer will:

- Record the reason for the revocation in the investigation report
- Include the PA Board Letter, Subscriber Appeal Letter and Appeal Board Letter in the investigation report.
- Send a revocation request to the CA via signed email after ten (10) business days of the date of confirmation from the Certificate Subscriber if no Appeal Letter is received.
- Send a revocation request to the CA via signed email within five (5) business days of an Appeal Board Letter

4.2.6.4 CA Duties

In processing a revocation request for a CA certificate, the CA will:

- Authenticate the certificate revocation request within five (5) days after the reception of the Revocation Request from the PA Officer and send the Revocation Request Confirmation to the PA Officer. Secure email will be used and calls can be used to authenticate requests verbally.
- Update the appropriate CRL based on the CRL profile defined below. During the revocation event the CA will verify it will revoke the correct certificate(s) and specify a revocation reason associated with each revocation as specified in the certificate request form. The CA will set the this Update time to the current time (i.e. the time the CRL signature is created) and set the next Update time to next regularly scheduled CRL update.

4.2.7 CA CRL Policies

4.2.7.1 CRL Update Frequency

To ensure the security of the CA private key, it is important that its exposure is limited and closely guarded. The CRLs will be updated at the monthly ceremony if revoked certificates need to be added to the CRL. At a minimum the CA CRLs will be updated at least once a quarter (i.e. once every three months) with notification to the PA Officer for the scheduled date.

4.2.7.2 CRL Distribution

The CA will securely deliver to PA Officer the CRL. The CRLs will be placed on the CableLabs web site and updated at least once a quarter. The CRLs will be available

for the relying parties to pull the CRL as desired with an HTTP GET in compliance with RFC 2585.

Note that the relying parties consist of CableLabs Members and CableLabs.

4.2.7.3 PA Officer Duties

PA Officer must carry out the following duties for revocation:

- Publish the CRLs on the CableLabs private area of the web site with access for relying parties
- Notify the Certificate Subscriber, as specified on the authorization agreement, the requesting party and the PA Board of the completion of the revocation
- Notify the CableLabs Members via OpenCable Security email alias
- All investigation information will be published on CableLabs private area of the web site for the relying parties.

4.2.7.4 CA Duties

The Root CA must carry out the following duties for revocation:

- Revoke the certificate
- Create/update the CRL according to the schedule
- Maintain the records concerning the revocation request
- Immediately provide the CRL to the PA Officer

4.2.7.5 Subscriber Duties

The duty of the Certificate Subscriber for a revoked certificate is to:

- Continue to safeguard the private key associated with the revoked 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 certificate

4.2.7.6 Authorization to Retrieve CRL

Access to this CRL will be restricted to those authorized by CableLabs. The authorized parties can download the CRL from the URL. The authorized parties will consist of Member organizations to CableLabs and CableLabs itself or any organization that CableLabs assigns to have this information on their behalf.

The CRL authorization list will be a separate from the list of those authorized to receive a certificate from CableLabs.

4.2.8 CRL Profile

The CableLabs CRL profile must comply with RFC 2459. Some CableLabs specific information is described in the table below.

CableLabs 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.

4.2.9 CRL Pruning

There will be no CRL pruning for the CA issued CRLs. The expected size of the CRLs issued by the CAs should be small. Also it is noted that the way certificates and CRLs are used within the cable industry require viewing the revoked CVC certificates beyond the expiration date.

5 Certificate Revocation Implementation

5.1 OpenCable Certificate Revocation Implementation

5.1.1 Selective Denial of Service Overview

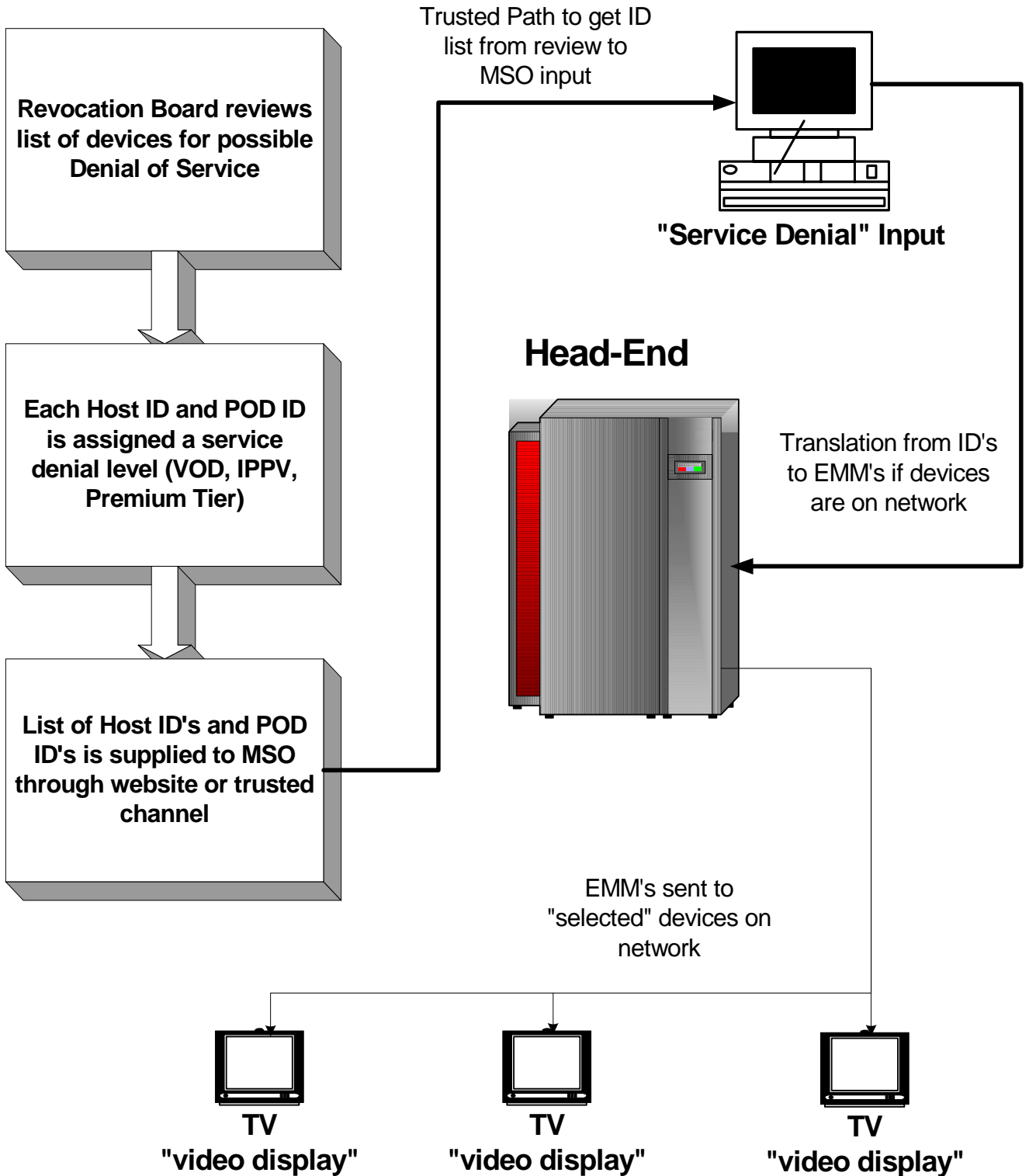
A CableCARD or Host device may be identified and designated to be reviewed by the affected MSO or perhaps a revocation board of MSO's. "Revoked", a term used in classical PKI methods, is a poor choice of words for the process we are defining. What it really means is that the any given ID can be placed on the list which would more accurately be called "Certificate Suspect List" (CSL). This list can be signed with a digital signature however that is probably not necessary since the list will be transferred to the MSO through a "trusted path".

Once an ID or group of ID's get listed on the Certificate Suspect List (CSL), they would need to be entered into the CAS system. An EMM for each of these ID's would be sent to the device to disable some or all premium services, depending on the choices of the MSO's involved in the process.

Finally, a decision would be made to install a new certificate in the field or recover the device from the subscriber to replace the device certificate in the worst security compromise situations.

5.1.2 Selective Denial of Service Flow Description

The following block diagram describes the process from adjudication of the suspect ID's all the way to sending out the EMM from the headend to the device that has been denied service.



Starting with the block in the upper left corner, the Service Denial Review Board meets every 90 days to discuss any possible device certificate problems or security compromises. Each of the suspected certificates are reviewed and the level of severity is discussed. The type of security problem is also discussed such as cloning, exposure of the private key, illegal copying of content, theft of service, and other security related possible issues. Each of the certificates in question are associated with an ID used in the Distinguished Name. The upper 10 bits define the manufacturer of the product. The lower 30 bits can be used to identify the model of the suspected device. All of the information is gathered and used to create a record of the problem including the severity of the problem. The severity will be set to one of four values: low, medium, high or critical. Based on the severity level, a recommended denial of service level will be assigned. The Cable Operator(s) involved in this problem will have the final decision as to the actual denial of service used or the action taken with the subscriber.

At the completion of this review, a list of the records created from the Service Denial Review Board meeting will be posted to an MSO ONLY (restricted access) website. At this point the exact details of how this information will be processed is up to each MSO. However, the website will be accessed by an MSO operations person to enter the appropriate ID's and other necessary record information into the various head-ends for processing. The back-end system will determine if there is a correlation between the problem ID's and the certificate devices on that particular network. If there is a correlation, an EMM is generated in the conditional access system that is addressed to the unit ID of the device which contains the problem certificate. This EMM is sent to the addressed device to remove one or more entitlements for that particular device. The goal is to establish communication with the subscriber and possibly get the problem device returned to the MSO.

5.1.3 Selective Denial of Service Record

The following table defines the information to be obtained about the suspected device certificate:

Host ID or CableCard ID	40 bits containing Mfg info and device info
Manufacturer	Upper 10 bits of ID defines a unique Mfg
Device Model number	Certificate database should contain model information for the range of ID's
Manufacturer Location	Database should contain information on the location
Severity Level	Low, Medium, High, or Critical (Review Board)
Denial of Service	Recommended by review board based on data presented
Certificate Serial Number	If available from certificate database
Certificate Issuer	If available from certificate database
Certificate Subject	If available from certificate database
Certificate Validity	If available from certificate database