

CableLabs Certificate Issuance Process

Notice

This document is furnished by Cable Television Laboratories, Inc. (CableLabs) in an "AS IS" basis. CableLabs does not provide any representation or warranty, express or implied, regarding its accuracy, completeness, infringement of intellectual property, or fitness for a particular purpose. CableLabs is not responsible for any liability of any nature whatsoever resulting from or arising out of use or reliance upon this document by any party.

© Copyright 2005 Cable Television Laboratories, Inc. All rights reserved.

Document Status Sheet

Document Title: CableLabs Certificate Issuance Process

Revision History: 03/22/2004 – Draft

04/12/2004 – V1

6/28/2005 – V2

3/03/2006 – V3

Date: March 3, 2006

Contents

1	INTRODUCTION	1
1.1	Document Purpose	1
1.2	CableLabs Device Public Key Infrastructure.....	1
1.2.1	Root CA	2
1.2.2	First-tier CA	2
2	DOCUMENTS AND CONTACT INFORMATION.....	4
2.1	CableLabs Documents.....	4
2.2	CableLabs Contacts.....	4
2.2.1	Certificate Issuance Service Contact.....	4
2.2.2	Technical Contact.....	4
2.2.3	Legal Contact	4
3	MFG CRA ISSUANCE PROCESS.....	5
3.1	Introduction	5
3.2	Authorization	7
3.3	CRA Issuance	8
3.4	MFG CRA Issuance Schedule	9
3.5	Device Certificate requests via the CRA	9

1 INTRODUCTION

1.1 Document Purpose

This document describes the digital certificate issuance process of device certificates via the Manufacturer (MFG) Certificate Requesting Agent (CRA).

1.2 CableLabs Device Public Key Infrastructure

CableLabs manages specifications (*e.g.*, DOCSIS[®], PacketCable[™], CableHome[™], and OpenCable[™]) that require embedding digital certificates in devices at the time of manufacture. These certificates provide the basis for a number of security services including data confidentiality, content integrity, and device authentication. For example, a digital certificate, embedded into a cable service device (*e.g.*, Cable Modem, Media Terminal Adapter, or Set Top Box), prevents the pirating of cable services by allowing the Cable Service Provider to authenticate the device requesting services.

In order for a certificate to be in compliance with CableLabs specifications, it must properly chain up to the appropriate CableLabs Root Certification Authority (CA) as defined by the specifications. At present, CableLabs has five active Root CAs, four of these roots (*i.e.*, the DOCSIS Root CA, MTA Root CA, CableLabs MFG Root CA, and the Service Provider Root CA) issue device certificates.

Figure 1 illustrates the major components of the CableLabs Device Public Key Infrastructure (PKI). The Root CA is the apex of the PKI which issued the first-tier CA certificates to Manufacturers in the legacy distributed architecture and now issues first-tier CA certificates of the CableLabs hosted CAs in the centralized architecture. CableLabs no longer issues first-tier CAs to Manufacturers.

In the centralized architecture, Manufacturers receive their device certificates via a web-based Certificate Requesting Agent (CRA). The certificate profiles for the CableLabs PKI are defined in the applicable CableLabs specification (*e.g.*, DOCSIS[®], PacketCable[™], CableHome[™], and OpenCable[™]).

Manufacturers, by requesting device certificates and handling the corresponding private keys, become part of the CableLabs PKI. Before receipt of production device certificates, CableLabs requires that manufacturers execute a Digital Certificate Authorization Agreement (DCAA), which governs the Manufacturer's practice for requesting certificates and their handling of the corresponding private keys.

CableLabs is migrating its PKI from the distributed to the centralized architecture and is employing the following policies:

- MFGs with existing CAs may continue to use their CAs to meet the certificate needs for existing specifications that allow the use of MFG CAs (*e.g.*, DOCSIS 1.x, 2.0)
- MFGs with existing CAs may opt to receive all their device certificates from a hosted CA via a web-based CRA.

- MFGs with existing CAs for one project (e.g., DOCSIS) that would like to obtain certificates for another CableLabs project (e.g., PacketCable) will need to receive the new project's device certificates from a hosted CA via a CRA.
- MFGs with existing CAs that have been compromised or that need to replace their existing CA will be migrated to the appropriate hosted CA.
- MFGs without existing CAs will receive device certificates from the appropriate hosted CA via a CRA.
- As appropriate, new specification versions (e.g., DOCSIS 3.0) may require that device certificates be issued from CableLabs hosted CAs.

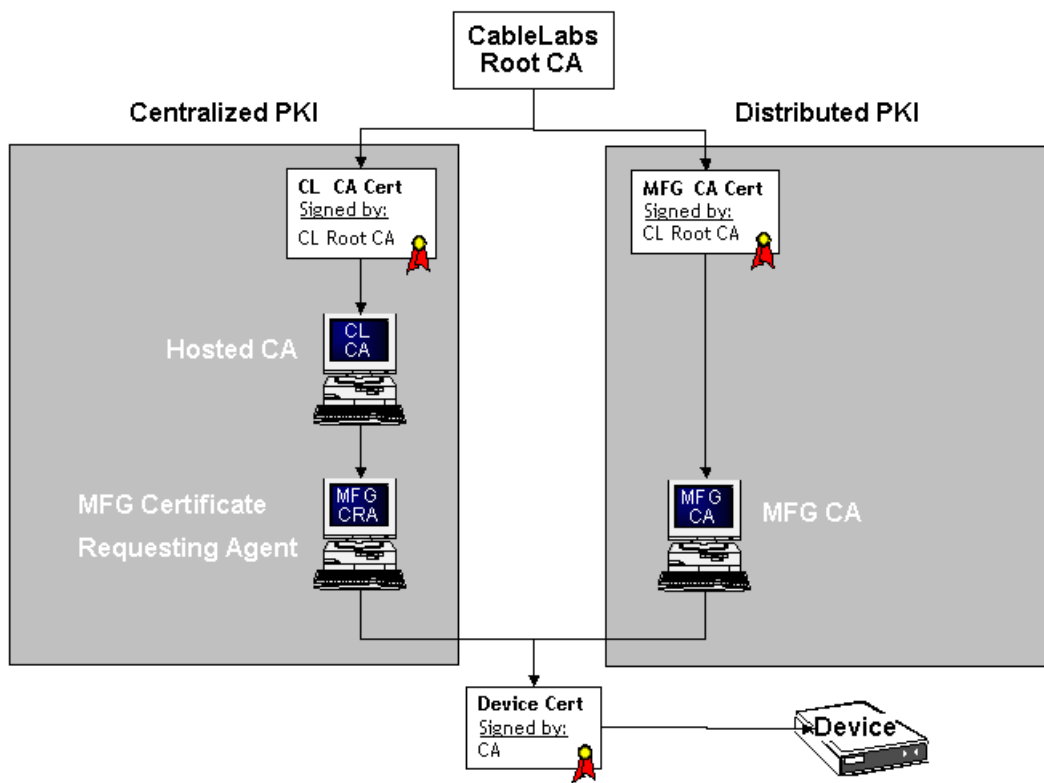


Figure 1: CableLabs PKI Hierarchy

1.2.1 Root CA

The Root Certification Authority (CA) is used to issue first-tier CA certificates. VeriSign, Inc. operates the CableLabs Root CAs on behalf of CableLabs.

1.2.2 First-tier CA

First-tier CA (i.e., a hosted CA or a MFG CA) certificates must chain up to the Root CA. Under the distributed (legacy) PKI architecture, a vendor chooses whether to operate

their CA, or have a third party operate the CA on their behalf. For the centralized PKI architecture, Manufacturers request device certificates from the CableLabs Hosted CAs via the MFG CRA.

2 DOCUMENTS AND CONTACT INFORMATION

2.1 CableLabs Documents

The following documents can be found at <http://www.cablelabs.com>:

1. CableLabs Certificate Issuance Process (This Document)
2. CableLabs Digital Certificate Authorization Agreement
3. CableLabs Project Specifications
4. Public Key Certificates for CableLabs Root CAs

2.2 CableLabs Contacts

2.2.1 Certificate Issuance Service Contact

Tara Gratz
Digital Certificate Account Coordinator
Cable Television Laboratories, Inc.
858 Coal Creek Circle
Louisville, CO 80027-9750
Tel: (303) 661-3320
Fax: (303) 664-8131
Email: t.gratz@cablelabs.com

2.2.2 Technical Contact

Oscar Marcia
Vice President, Security
Cable Television Laboratories, Inc.
858 Coal Creek Circle
Louisville, CO 80027-9750
Tel: 303-661-3350
Fax: 303-664-8170
Email: o.marcia@cablelabs.com

2.2.3 Legal Contact

Simon L. Krauss
Sr. Counsel
Cable Television Laboratories, Inc.
858 Coal Creek Circle
Louisville, CO 80027-9750
Tel: (303) 661-3836
Fax: (303) 661-9199
Email: s.krauss@cablelabs.com

3 MFG CRA ISSUANCE PROCESS

3.1 Introduction

The CableLabs web-based Certificate Requesting Agent (CRA) has the capability to issue device certificates in bulk with very low attendant cost to Manufacturers throughout the certificate management lifecycle. The CRA service enrolls a Manufacturer quickly. The following diagram presents a high level view of the CableLabs CRA:

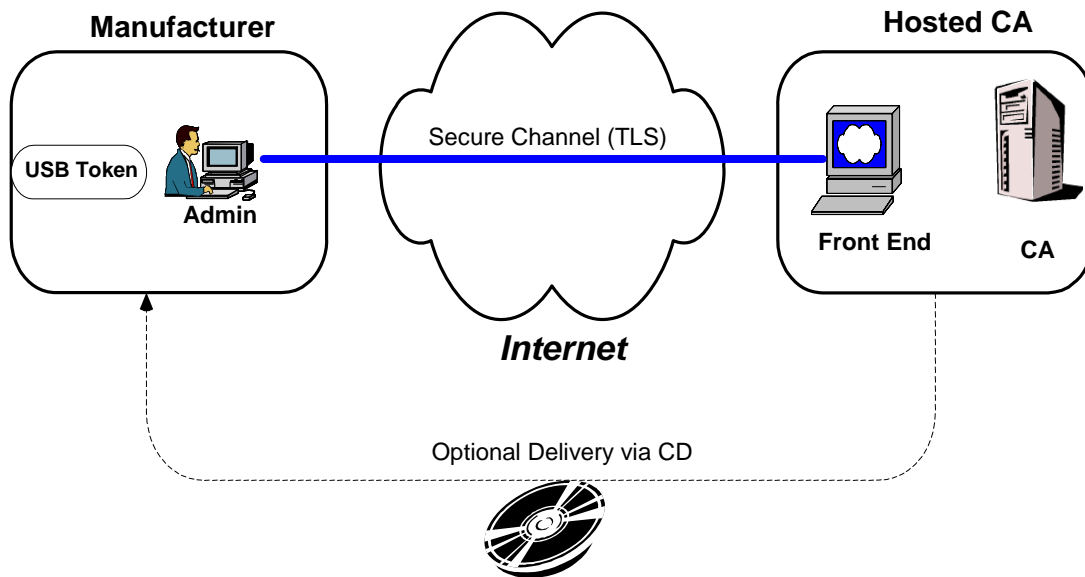


Figure 2 MFG CRA Overview

In the centralized architecture, the manufacturer uses a standard web browser and hardware token (e.g., USB token) to connect to the CableLabs Hosted CA's web interface. Via this interface, the Manufacturer may request device certificates and pick up batched signed certificates. Optionally, a manufacturer can specify that issued certificates be delivered via postal mail on a CD-ROM.

The CRA will not require any deployment at the manufacturer's site, other than the installation of the lightweight standalone client software needed to decrypt download file content. Therefore, immediate setup for a Manufacturer to request and receive device certificates is realized.

Figure 3 illustrates the process for issuance of a Manufacturer CRA under the appropriate Root. The process consists of two sequences, Authorization and Issuance. Section 3.2 describes the authorization steps, and section 3.3 describes the issuance steps.

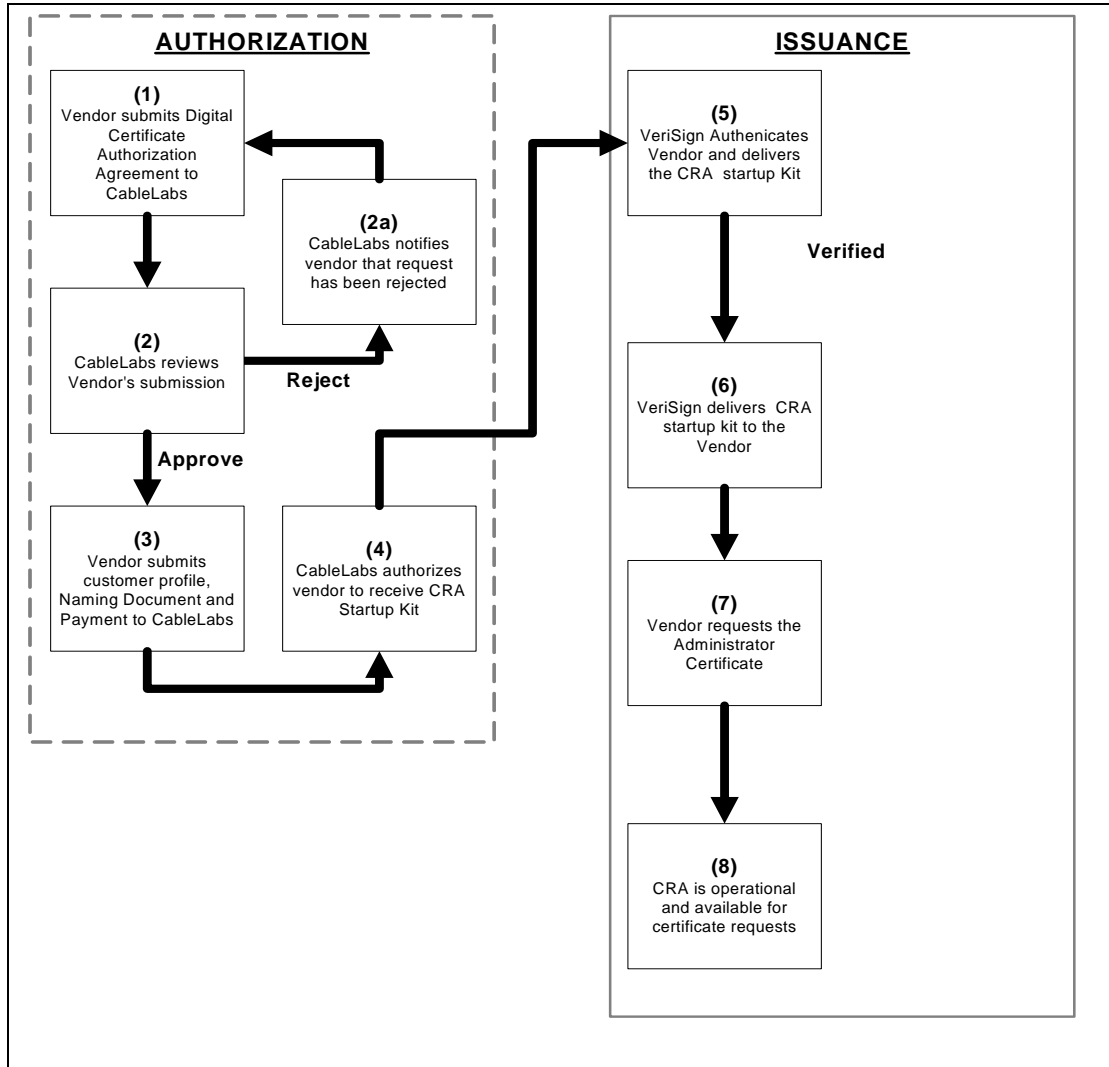


Figure 3: Manufacturer CRA Flow

3.2 Authorization

Step 1	<p>Manufacturers wishing to enroll in the CRA service must execute a “CableLabs Digital Certificate Authorization Agreement (DCAA)”, including completion of the customer profile and naming document.</p> <p>Manufacturers must submit a signed DCAA to the CableLabs Legal Contact listed in 2.2.1.</p> <p>The agreement can be sent via facsimile with follow-on of original documents by tracked delivery service.</p>
Step 2	CableLabs will review the submission and either accept or reject it.
Step 2a	If the submission is rejected, CableLabs will notify the vendor’s Legal Contact and provide a reason for the rejection. The vendor may go back to step one after the reason for rejection has been addressed.
Step 3	CableLabs will authorize a Manufacturer to receive a CRA once CableLabs has received an executed agreement, a complete customer profile and naming document, and received payment for the first year’s maintenance.
Step 4	CableLabs notifies VeriSign of vendors authorized to receive a CRA startup kit.

3.3 CRA Issuance

Step 5	<p>VeriSign will authenticate and verify the identity of the manufacturer as follows:</p> <p>First, VeriSign will verify that the corporate and administrator contacts are, in fact, employees of the company; either by speaking with them or another verifier, i.e., receptionist.</p> <p>Delays may be caused if we are not able to reach the employee(s) or if a potential verifier will not, or cannot verify employment.</p> <p>Second, VeriSign will look up the Dun and Bradstreet number to assure that the address and name of the company are the same as that under which they enrolled.</p> <p>A delay may be caused if there are any discrepancies in the address information.</p> <p>In most instances, Verification and Authentication can be accomplished within 24-48 hours. However as stated above, some situations may occur that may cause delays.</p>
Step 6	<p>VeriSign delivers the CRA startup kit (A blank hardware token (e.g., a USB token) and instructions on how to request the Administrator's certificate) to the Administrator specified by the vendor in the customer profile.</p>
Step 7	<p>The manufacturer installs the token reader and drivers and is directed to an enrollment page that generates the private key and provisions the administrator certificate onto the token. The Administrator Certificate will be used to authenticate the Administrator to the CA web interface and to upload certificate request files.</p>
Step 8	<p>The CRA system is now operational. The manufacturer's designated Administrator may now request device certificate (see section 3.5).</p>

3.4 MFG CRA Issuance Schedule

CRA startup kits are delivered to the Manufacturer five business days after completion of VeriSign’s authentication process. Figure 4 illustrates the sequence of events required to obtain a MFG CRA. MFGs authorized to receive a CRA must initiate the process at least one to two months before the scheduled certification wave submission date the MFG plans to attend.

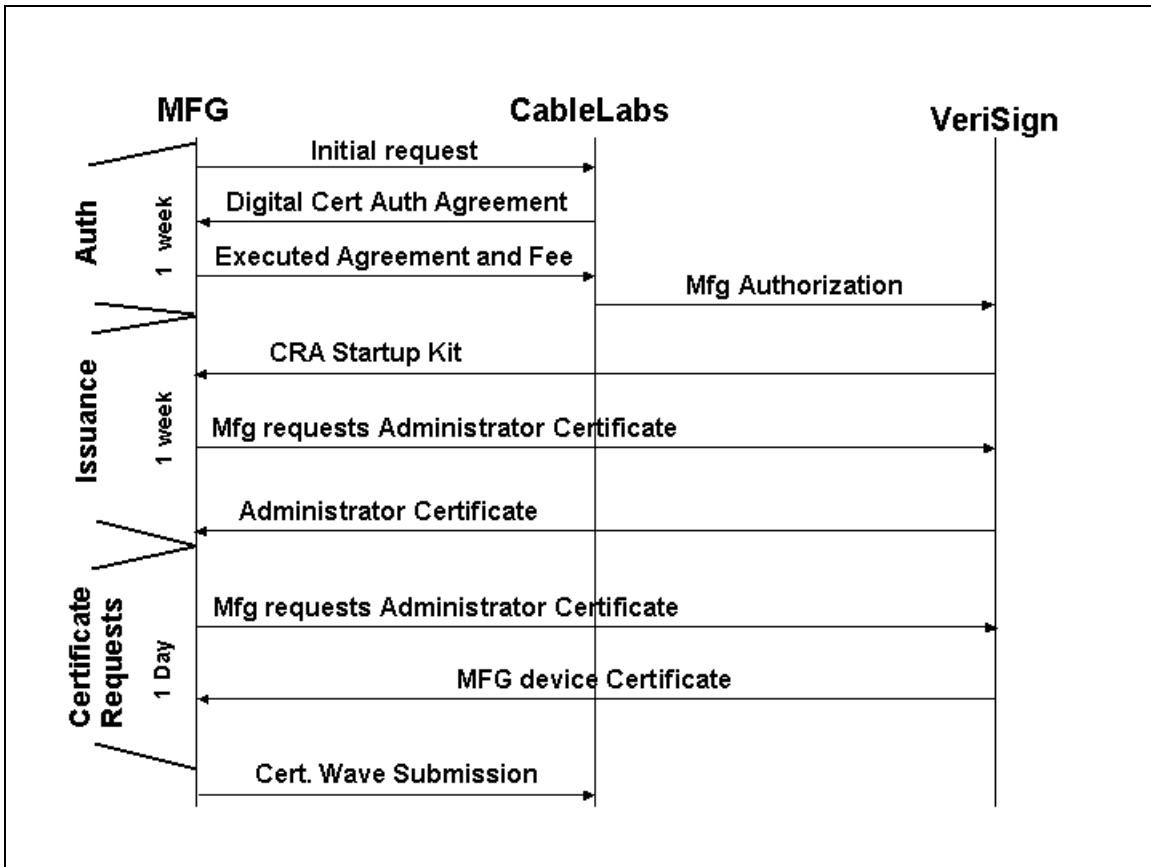


Figure 4 MFG CRA Issuance Process

3.5 Device Certificate requests via the CRA

Once the Manufacturer is enrolled for the CRA service, the Manufacturer’s Administrator may request device certificates using the process described in this section.

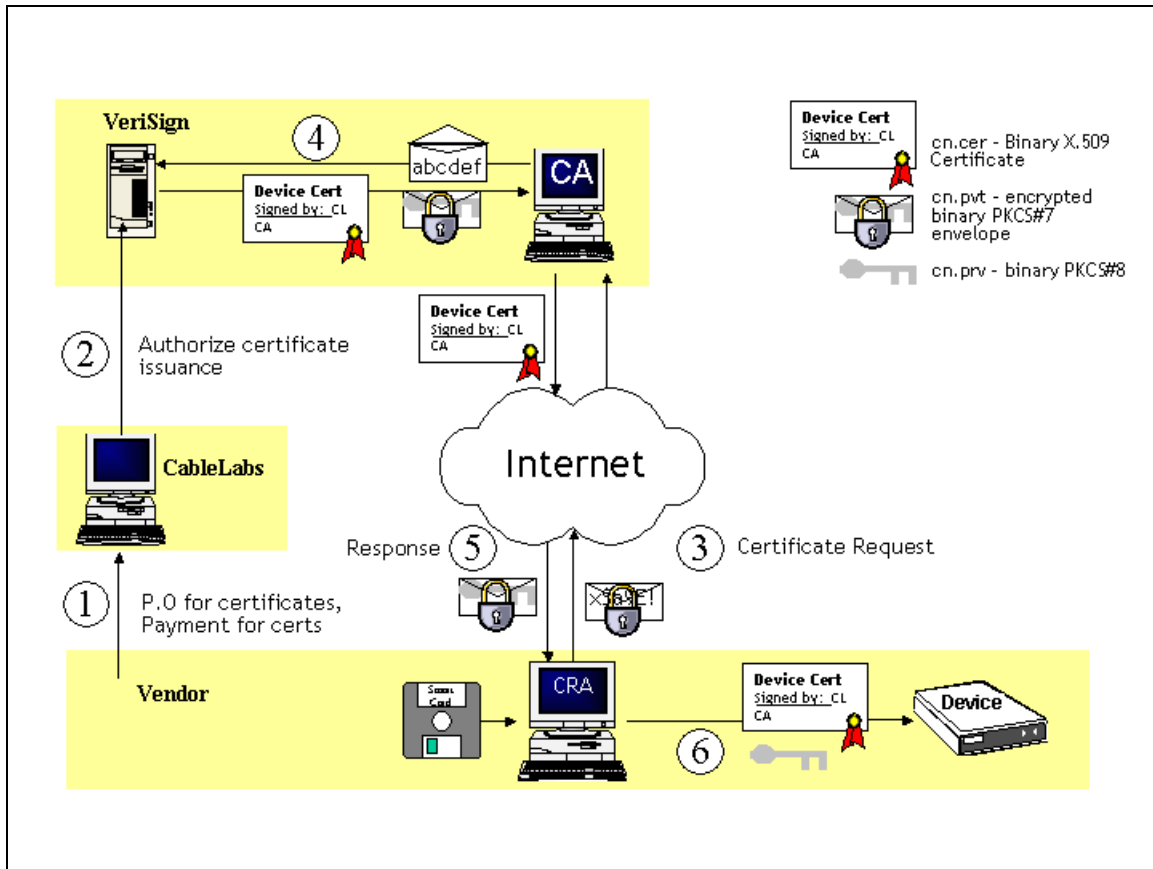


Figure 5 Device Certificate Request Process

Certificate Request Process (See Figure 5):

1. Manufacturer issues a P.O. for the number of certificates it wishes to purchase. CableLabs sends advance invoice to manufacturer.
2. Once payment is received, CableLabs authorizes VeriSign to load the number of purchased certificates onto the account.
3. The Administrator authenticates to the CA web page. The communication to this web page is encrypted and authenticated using the key and certificate on the Administrator's token. The Administrator may request the number of certificates up to but not exceeding the number of certificate the Manufacturer has purchased. The Administrator receives an acknowledgement of the request and is presented with a numbered receipt that identifies this particular request.
4. The CA checks the request against the number of certificates authorized by CableLabs for the Manufacturer. If the manufacturer has not exceeded its limit, the CA generates the certificates (and optionally keys) based on the information contained in the request. If fulfilling the entire request would exceed the

Manufacturer's limit, then the CA will only generate certificates up to the Manufacturer's limit.

5. Once the request is complete, the CA informs the Administrator, via email, that their request has been completed. The response file is delivered to the manufacturer via one of the following mechanisms:
 - a. Certificate response is placed on an access-controlled website. The Administrator is sent the URL where this batch of certificates may be picked up. Access to this URL is protected via client and server authenticated TLS and requires the correct manufacturers' administrator certificate for access.
 - b. Or, the CA burns the encrypted response onto a CD-ROM, which is sent via postal mail to the address listed as the Administrator's address in the customer profile.
6. If the manufacturer has asked the CA to generate the key pairs, the certificate request response is encrypted by the CA into a binary PKCS#7 envelope. The response is decrypted using a lightweight client utility and the manufacturer's key on the token. Responses to certificate requests submitted as PKCS#10 certificate requests, will contain only certificates, thus will not be encrypted. Manufacturer can now embed the device certificates and corresponding private key into compliant cable service devices.