

PKI Migration Strategy

CableLabs

1-2004

Agenda

- CableLabs PKI
- Migration Strategy (Objective, Timeline)
- Policy
- PKI Migration
- CableHome PKI Migration
- Certificate Requesting Agent

Public Key Infrastructure (PKI)

- CableLabs PKI evolving to support higher security services such as Content Protection, etc.
- Shared CAs provide higher assurance level CAs
- Initial use of shared CAs is for OpenCable
- Agreement with Host CA service provider allows for cost effective creation of Shared CAs
- Migration to a Shared CA provides a cost-effective, higher assurance device certificate issuance alternative for DOCSIS

Migration Strategy

- Objective:
 - To offer a cost-effective, higher assurance device certificate issuance alternative to DOCSIS, PacketCable, and CableHome vendors via hosted CA model
- Timeline:
 - Create the hosted CAs and Requesting Agents (Nov 03)
 - Promote Migration Strategy to Vendors (Dec 03)
 - Initiate operation of hosted CAs (Mar 04)

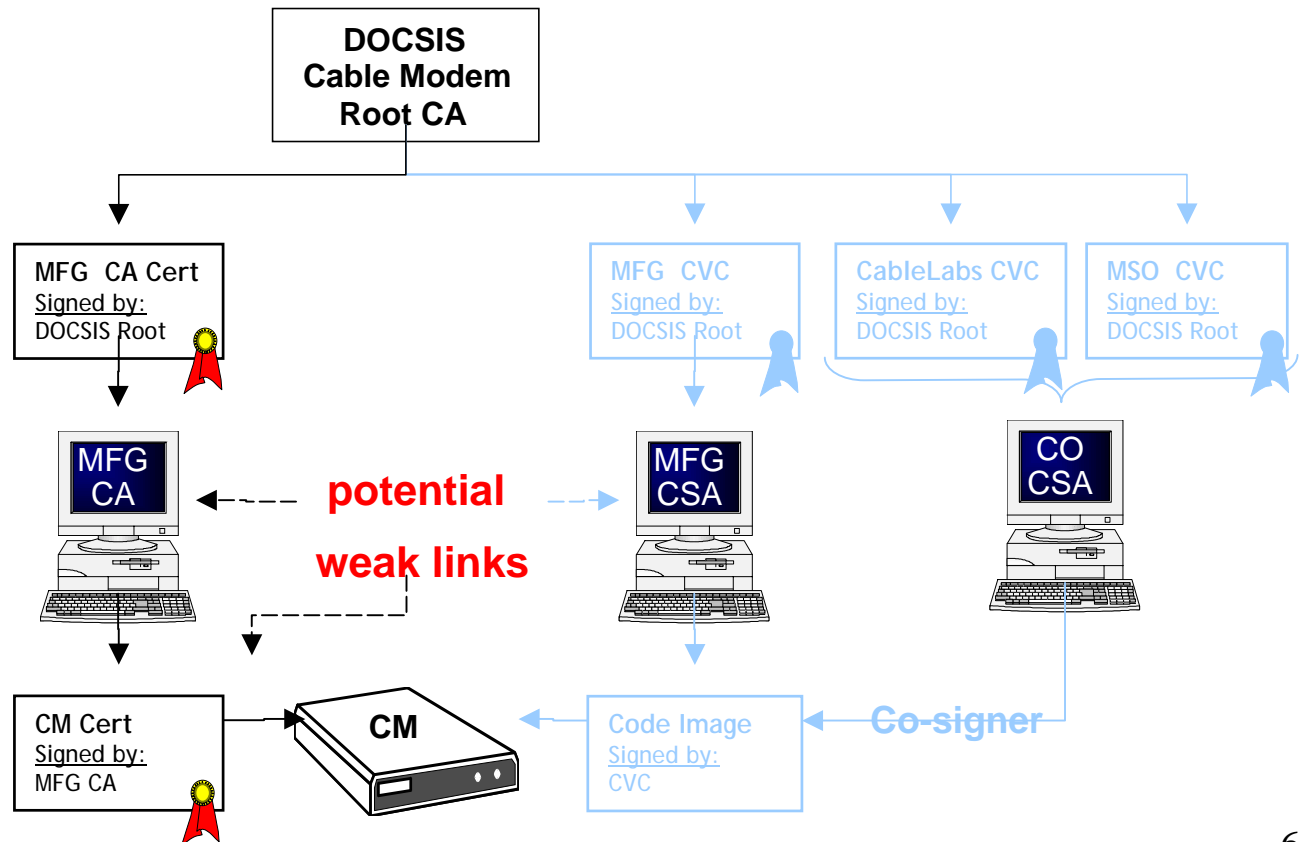
- Pricing:

Category:	Fees:
Certificate Issuance	\$0.07 per Certificate
Annual Administration Fee	\$17,000 per year
Additional Manufacturer Sites	\$7,500 per year

- CableLabs' PKI management is migrating from issuing CAs to issuing device certificates in bulk
- Mfgs with existing CAs can continue using their CAs or opt to receive certificates from the CableLabs hosted CAs
- Mfg needing new CAs will be migrated to appropriate hosted CA
- All new MFGs will receive device certificates from the hosted CA via a web-based Certificate Requesting Agent

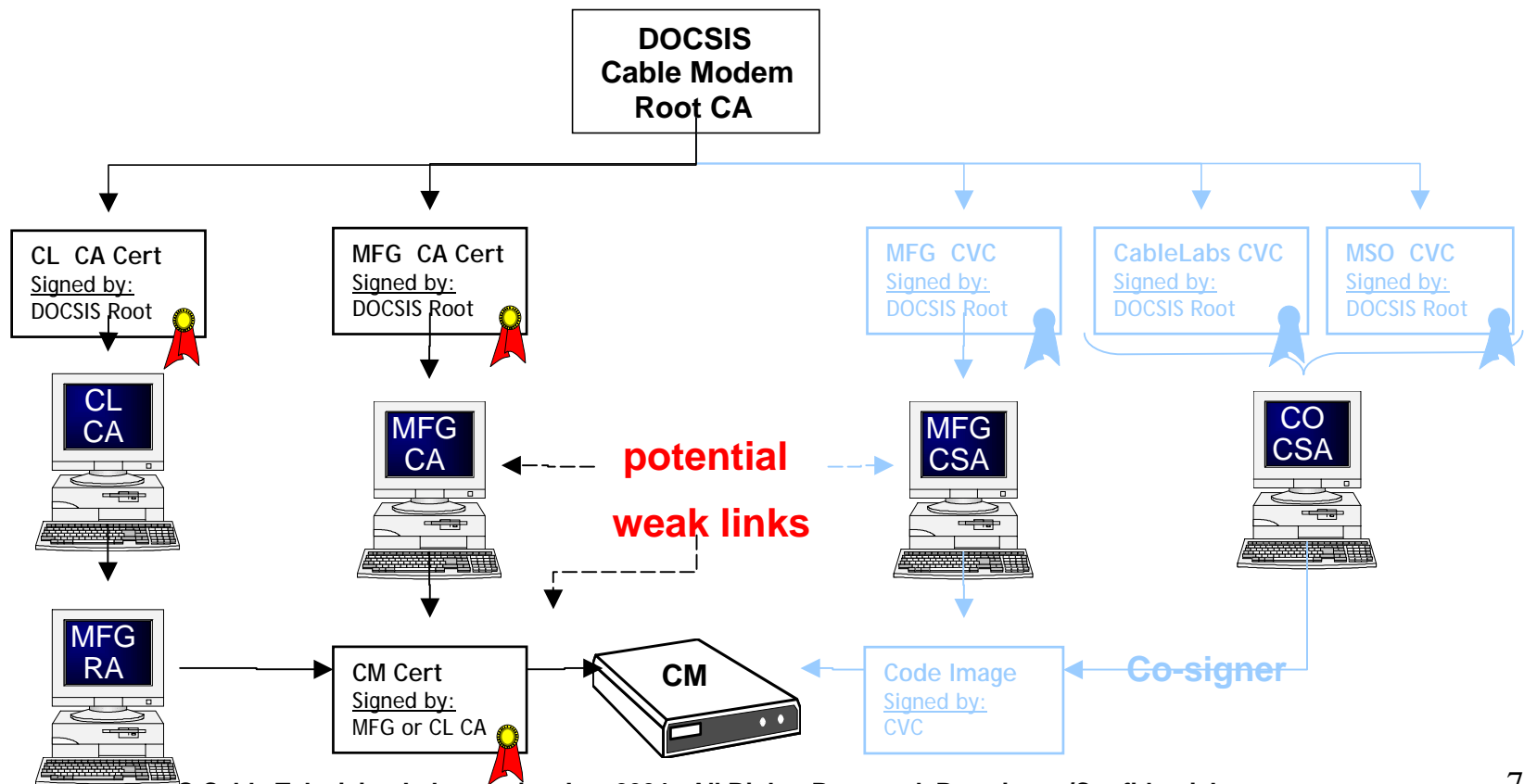
PKI Migration

- Each MFG operates its own Certification Authority (CA)
- MFG CAs issue device certificates to device (e.g., CMs)
- Code Verification Certificates (CVCs) used to sign code



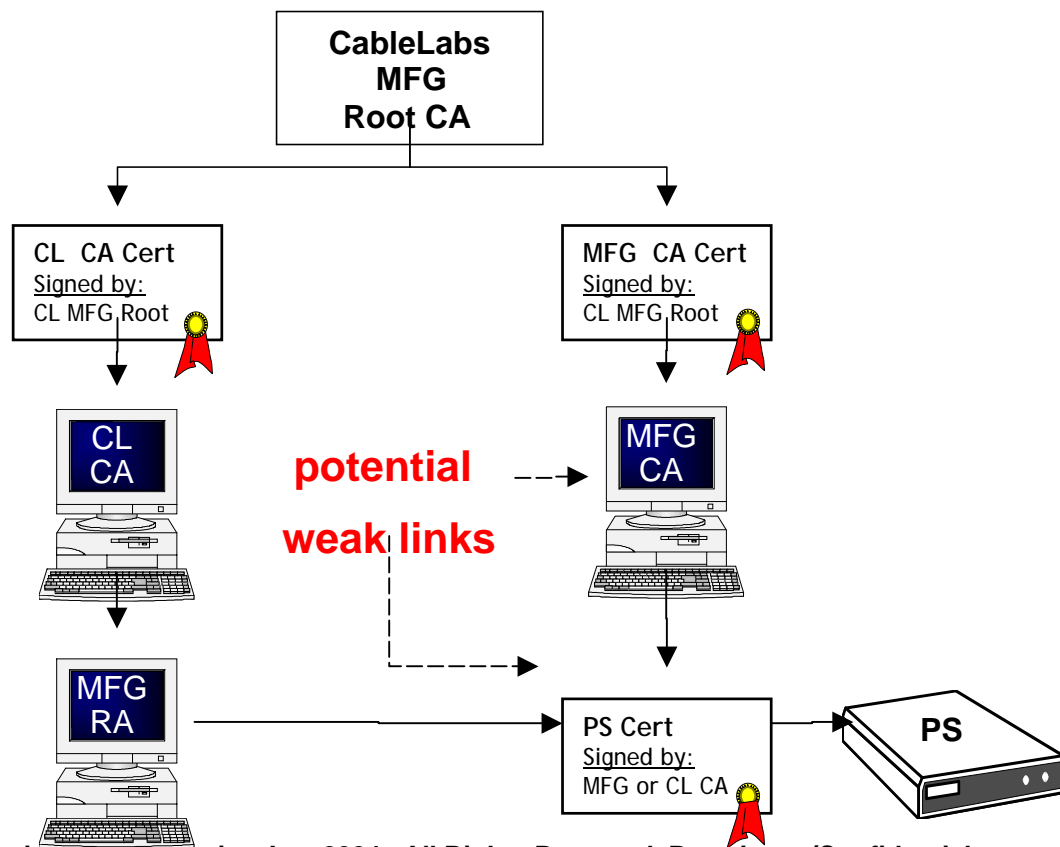
DOCSIS PKI w/Shared CA CableLabs®

- MFG can continue to issue certificates from their own CA
- MFGs can opt to receive certificates from the Shared CA
- New MFGs will receive certificates from the Shared CA



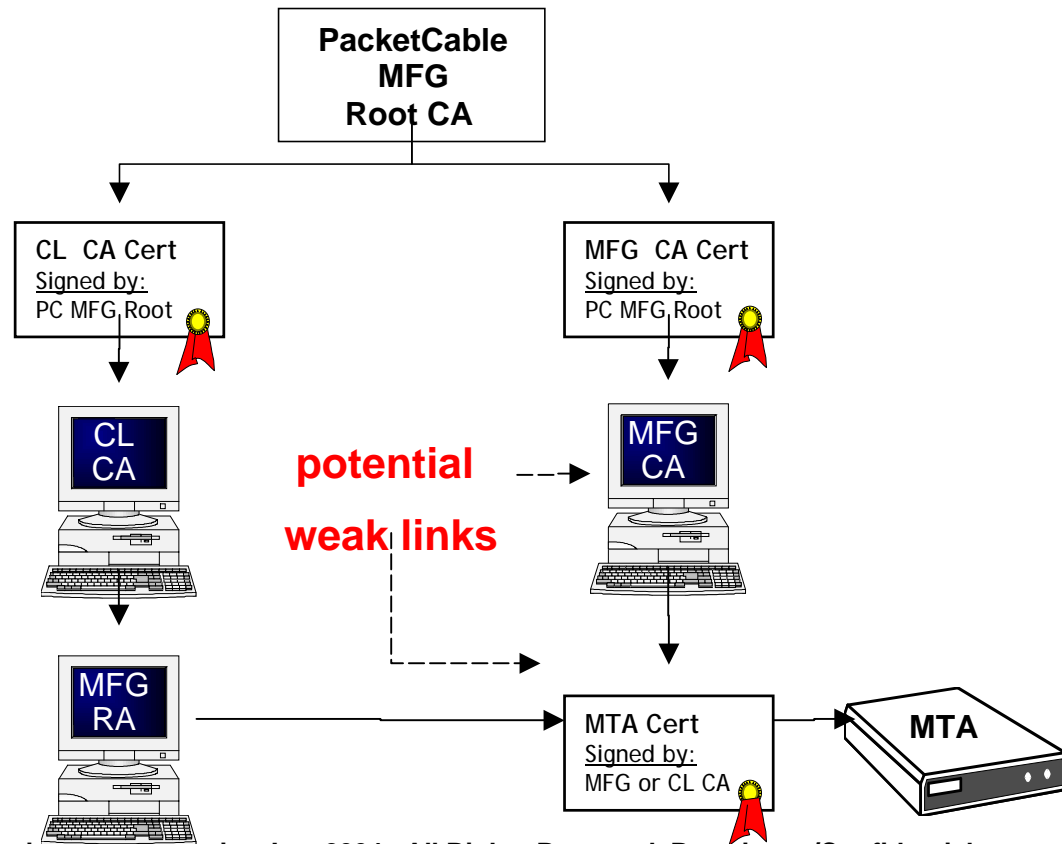
CableHome PKI w/Shared CA

- MFG can issue certificates from their own CA
- MFGs can opt to receive certificates from the Shared CA
- New MFGs will receive certificates from the Shared CA

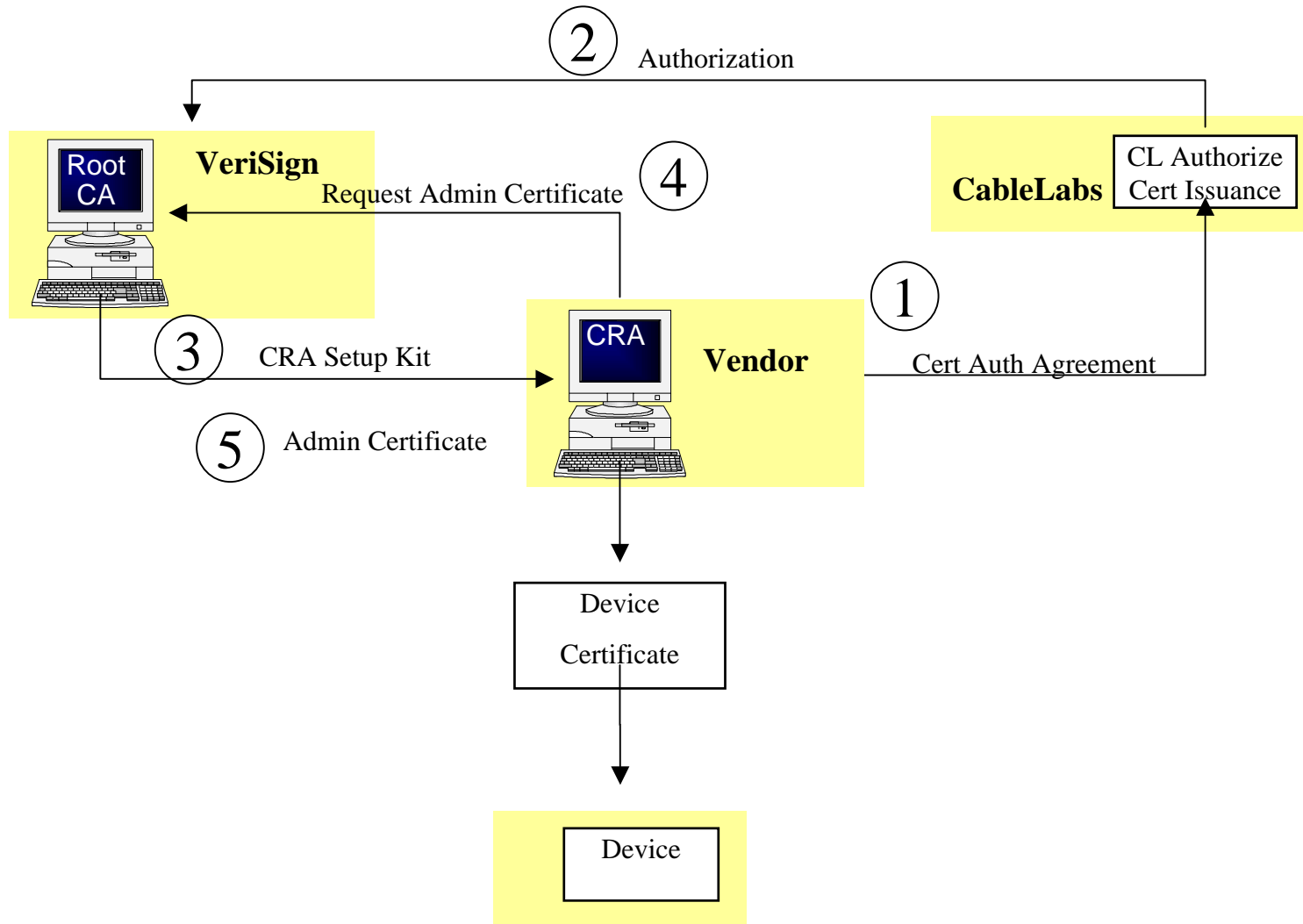


PacketCable PKI w/Shared CA **CableLabs**

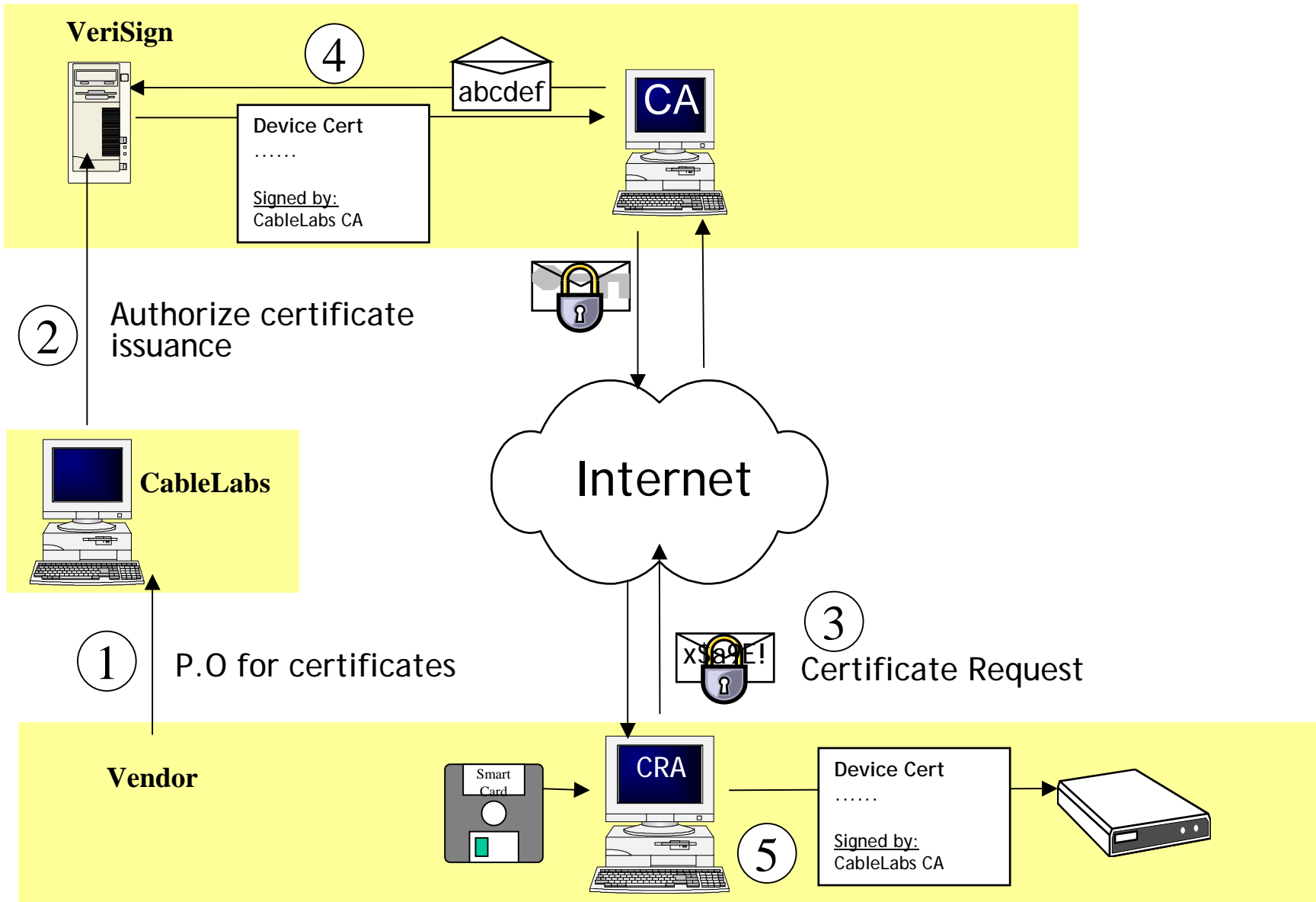
- MFG can issue certificates from their own CA
- MFGs can opt to receive certificates from the Shared CA
- New MFGs will receive certificates from the Shared CA



Certificate Requesting Agent Issuance



Requesting Certificates in bulk



[Home](#)[Request Certificates](#)[Retrieve Certificates](#)[Download Utilities](#)[Help](#)

CableLabs Certificate Requesting Agent

Cable Television Laboratories, Inc. (CableLabs®), a non-profit research and development consortium of the cable industry, manages specifications (DOCSIS®, PacketCable™, CableHome™, and OpenCable™) that require embedding CableLabs Public Key Certificates in compliant devices at the time of manufacture. CableLabs Public Key Certificates provide the basis for a number of security services including data confidentiality, content integrity, and hardware and software authentication.

CableLabs has partnered with VeriSign, to implement a web-based certificate requesting service via the CableLabs Certificate Requesting Agent (CRA). This service enables manufacturers, to request CableLabs Public Key Certificates in bulk via the CRA. The CRA is an integral part of the manufacturer's process of embedding Certificates into their compliant devices.

By requesting certificates and handling the corresponding private keys, manufacturers become part of the CableLabs Public Key Trust Infrastructure.

The CableLabs Certificate Requesting Agent provides the following features:

- Request Certificates** – Certificate request options
- Retrieve Certificates** – Retrieve issued certificates
- Download Utilities** – Links from which to download utilities to help manage the certificates files

[Home](#)[Request Certificates](#)[Retrieve Certificates](#)[Download Utilities](#)[Help](#)

Request Certificates

1. Select the Certificate request type:

By Device ID range:

Starting ID:

Number of certificates:

Increment:

By list of Device IDs:

Example: filename.txt

By Certificate Signing Requests (CSRs):

Example: filename.tar

2. Enter Product Name: (64 Characters max)

3. Select Delivery Mode:

secure download via internet

via CD-ROM (optional, at extra cost)

[Home](#)[Request Certificates](#)[Retrieve Certificates](#)[Download Utilities](#)[Help](#)

Retrieve Certificates

Click on a Certificate request ID to download the batch file of issued Certificates.

Important: Files are removed from the list one week after the files have been retrieved.

<u>Certificate Request ID</u>	<u>Request Date</u>	<u>Response Date</u>	<u>Batch Size</u>
Certificate_10302003144630.download	MM DD YYYY	MM DD YYYY	0
Certificate_10302003145342.download	MM DD YYYY	MM DD YYYY	0
Certificate_11052003120414.download	MM DD YYYY	MM DD YYYY	0

[Home](#)[Request Certificates](#)[Retrieve Certificates](#)[Download Utilities](#)[Help](#)

Download Utilities

Click the links to download free copies of the utilities that help manage the Certificate request upload batch files and the Certificate Retrieval download file.

- **Download the tar utility**

tar (tape archive) utility to unpack batch files.

When using CSRs as the Certificate request type, use the tar utility to package the CSRs into a single file.

- **Download the gzip utility**

gzip utility to uncompress download and upload batch file.

To improve download data transmission time, the CA compresses the download batch file.

When using the CSR option to request certificates, the gzip utility may be used to compress the CSR upload files to improve upload data transmission time.

- **Download the decrypt utility**

Decrypt utility to decrypt the private key data.

When requesting Certificates either by Device ID Range or by list of Device IDs, the CA creates the private keys and encrypts the private key data in the download batch file.