Creating Infinite Possibilities.

SCTE
a subsidiary of CableLabs

DOCSIS 4.0 Security: A Comprehensive Guide to Successful Deployments

Yuan Tian

Security Engineer
CableLabs
+1 303.661.3330 | y.tian@cablelabs.com

SCTE CABLE-TEC EXPO 22
SEPTEMBER 19-22 • PHILADELPHIA, PA

2022 Fall Technical Forum
SCTE • CABLELABS • NCTA

DOCSIS Evolution

A group of CMs went into the “Wise Cable” bar and asked for some drink:

The D1.1 CM told the bartender its **date of birth** (MAC Address), the bartender nodded.

The D2.0 CM showed **a paper napkin with its date of birth and signature**, the bartender nodded.

The D3.0 CM showed its **library card**, the bartender checked with cautious and then nodded.

The D3.1 CM showed its **driving license**, the bartender checked with cautious and a UV light, then nodded.

They all got the services.

Now here comes the D4.0 CM, it told the bartender the date of birth and showed him the its driving license. The bartender promptly served up a beer, but the 4.0 CM didn’t take it.

“What?” the bartender asked, “ anything wrong with your order, pal?”

“No. ” The D4.0 CM opened the UV light, “Now it’s **your turn**.”

Yes, in DOCSIS4.0, we now have **mutual authentication** in BPI+V2!

DOCSIS 4.0 Security Overview

What does NOT change?

BPI+ V1 Authentication: DOCSIS 4.0 continues to support BPI+ V1. There is **NO** new security change to the BPI+V1 in D4.0.

Early Authentication and Encryption (EAE): EAE in 4.0 is backward compatible with BPI+V1 in previous versions of DOCSIS (3.0-3.1).

Secure Software Download (SSD): DOCSIS 4.0 keeps support for current procedures (i.e., CVC Chain) and provide the possibility for upgrading to a more efficient one.

1st Gen DOCSIS® PKI: DOCSIS 4.0 devices require an additional certificate from the 1st Gen DOCSIS® PKI to authenticate in DOCSIS 3.0 networks (if the device supports D3.0 environments).

2nd Gen DOCSIS® PKI: DOCSIS 4.0 continues to use 2nd Gen DOCSIS® PKI as defined in DOCSIS 3.1;

Certificate Revocation Options: DOCSIS 4.0 supports the same revocation options available in DOCSIS 3.1 and DOCSIS 3.0.

DOCSIS 4.0 Security Overview

What changes?

DOCSIS 4.0 Security Is **Upgradable**

- **BPI+ V1** - Same Authentication Protocol used in DOCSIS 1.1-3.1
- **BPI+ V2** – Aligns Authentications to today's Best Practices (especially for Distributed Access Architecture threats)

Specifically, **BPI+ V2 Authentication** brings **new** security features:

- Mutual Authentication (verify CM and CCAP's identity and role)
- Full Revocation Checking Support (BPI+ & SSD)
- Downgrade Protection (TOFU)
- Perfect Forward Secrecy (PFS) and Algorithm Agility
- Add AES 256 support
- CCAP Designation

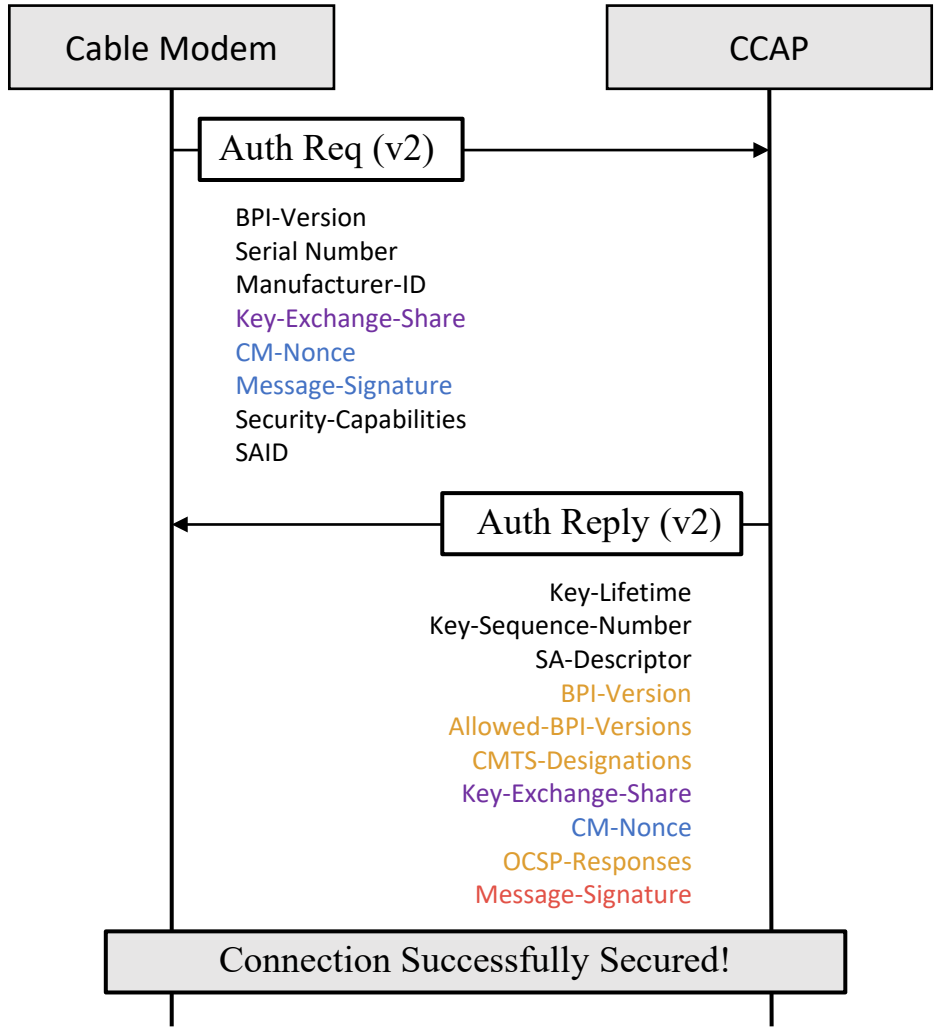

Fig.1 BPI+V2 Authentication Process

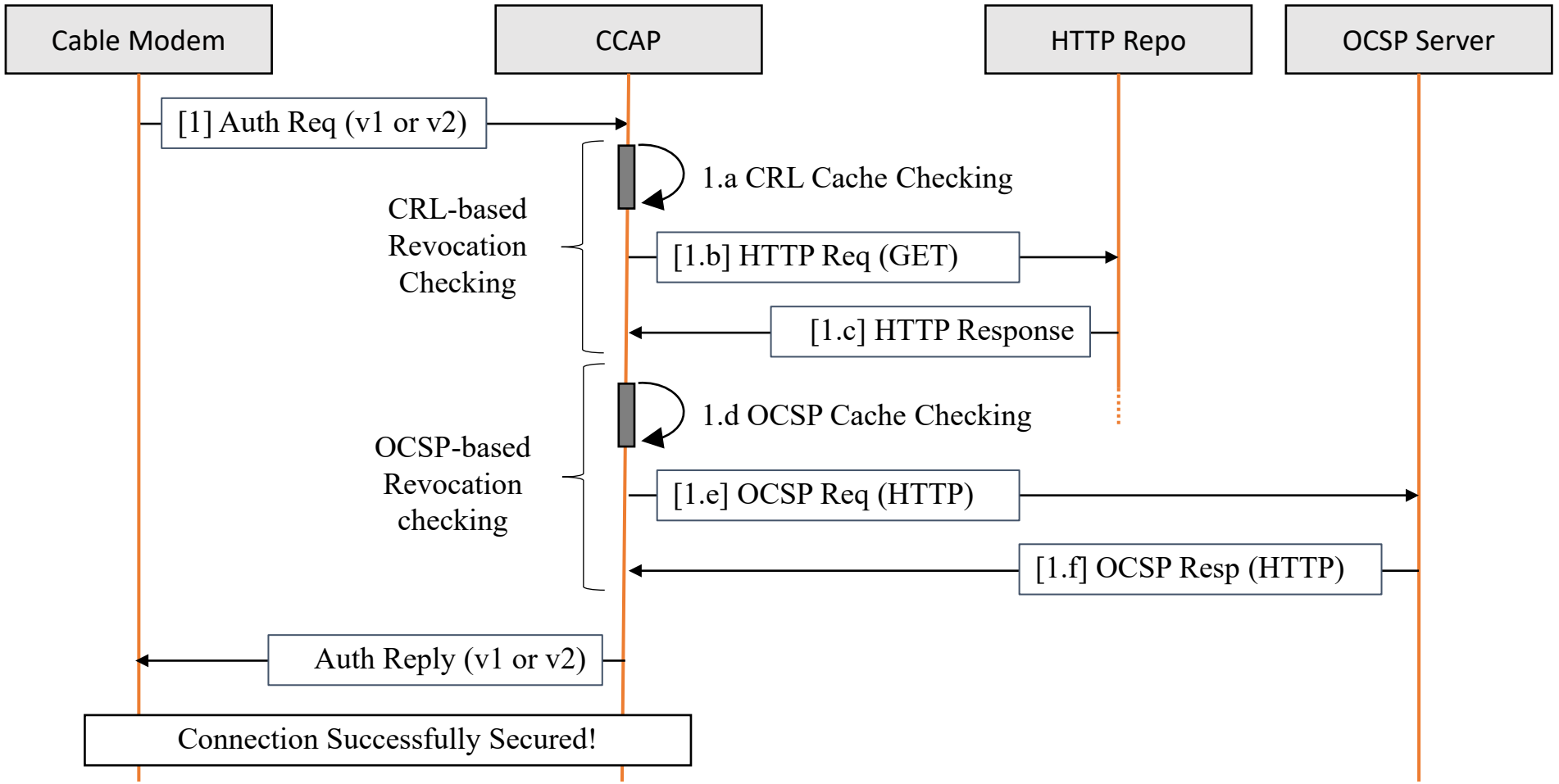

Fig.2 Integrated BPI+ and Revocation Checking Flow

Many Deployment Modes…

- **No Revocation Checking:**
  - Easy for bartender to offer faster services
  - Licenses (certs) may be revoked already
- **Client-Side Revocation Checking**
  - The bartender needs a phone to call DMV
  - If the license is revoked, no beer for D4.0 CM
  - Cannot verify bartender's identity
- **Server-Side Revocation Checking (BPI+V2 only)**
  - The bartender needs to show his license
  - He also needs to prove his license is not revoked
  - Cannot verify the CM's identity
- **Mutual Revocation Checking (BPI+V2 only)**
  - Both license are now required to check the revocation status
  - Need the support from the infrastructure (e.g., a 7/24 hotline to DMV)

And More…

- **Authority Information Access (AIA) extension:** carry the location of the authoritative OCSP server that the CMTS can use to check for the revocation status of the certificate
  - The DMV's number
- **Extended Key Usage (EKU):** allow the verifier to check if the connecting device is meant to provide specific services (e.g., svcCMTS).
  - Must be the bartending license
- **Early Authentication and Encryption (EAE):** EAE in 4.0 defines new Bitmask TLV to support BPI+V1 and/or BPI+V2
  - Show your license to a guard before get into the bar
- **Secure Software Download (SSD) with FWAH:** Additionally, D4.0 provides the possibility for using the Firmware Authentication Header (FWAH) to optimize early error detection.
  - The D4.0 CM obtains a receipt for its order, verify the beer with the info on the receipt

DOCSIS 4.0 Deployment Steps

Step 1: Preparing Your Networks for D4.0 CMs

- **DOCSIS 4.0 certificates** have **bigger size** than their DOCSIS 3.1 equivalent (i.e., updated cert profile for supporting revocation and identity check and increased key size).
- **DOCSIS 3.1 CMTS-es** might require a software update to enable processing BPKM messages that are **larger than 1490 bytes** and new type of BPKM that supports. **fragmentation** (i.e., version 5 MMM).
- **DOCSIS 4.0 CMs**, if need to support 3.0 and earlier environment, will still need to be provisioned with a DOCSIS 3.0 certificate.

Step 2: Upgrading Speeds, Not Security

- Configure and upgrade the PHY layer to be able to deliver new speeds.
- Enable the use of BPI+ V2 according to your own deployment plans and schedule only when new security features are needed.

DOCSIS 4.0 Deployment Steps

Step 3: Enabling Advanced Security Features With BPI+ V2

- Enable **Trust On First Use (TOFU)** for downgrade protection
- **Manage Persistent Security Attributes (PSAs)** to specify allowed BPI+ version for illegal downgrade protection
- Use PSAs for **CMTS Designation**, restrict CMTS Certificate's value (i.e., from Operator A or O = A)

Step 4: Support Revocation Checking

- Enable revocation checking according to your own deployment plans and schedule only when new security features are needed, and the infrastructure/services are ready.
- **Additional** Infrastructures and services might be needed (e.g., OCSP responder and HTTP CRL repository)
- Choose the modes that suits the actual needs:
  - Strict policy and Permissive policy
  - No revocation, Client-Side, Server-Side, or both

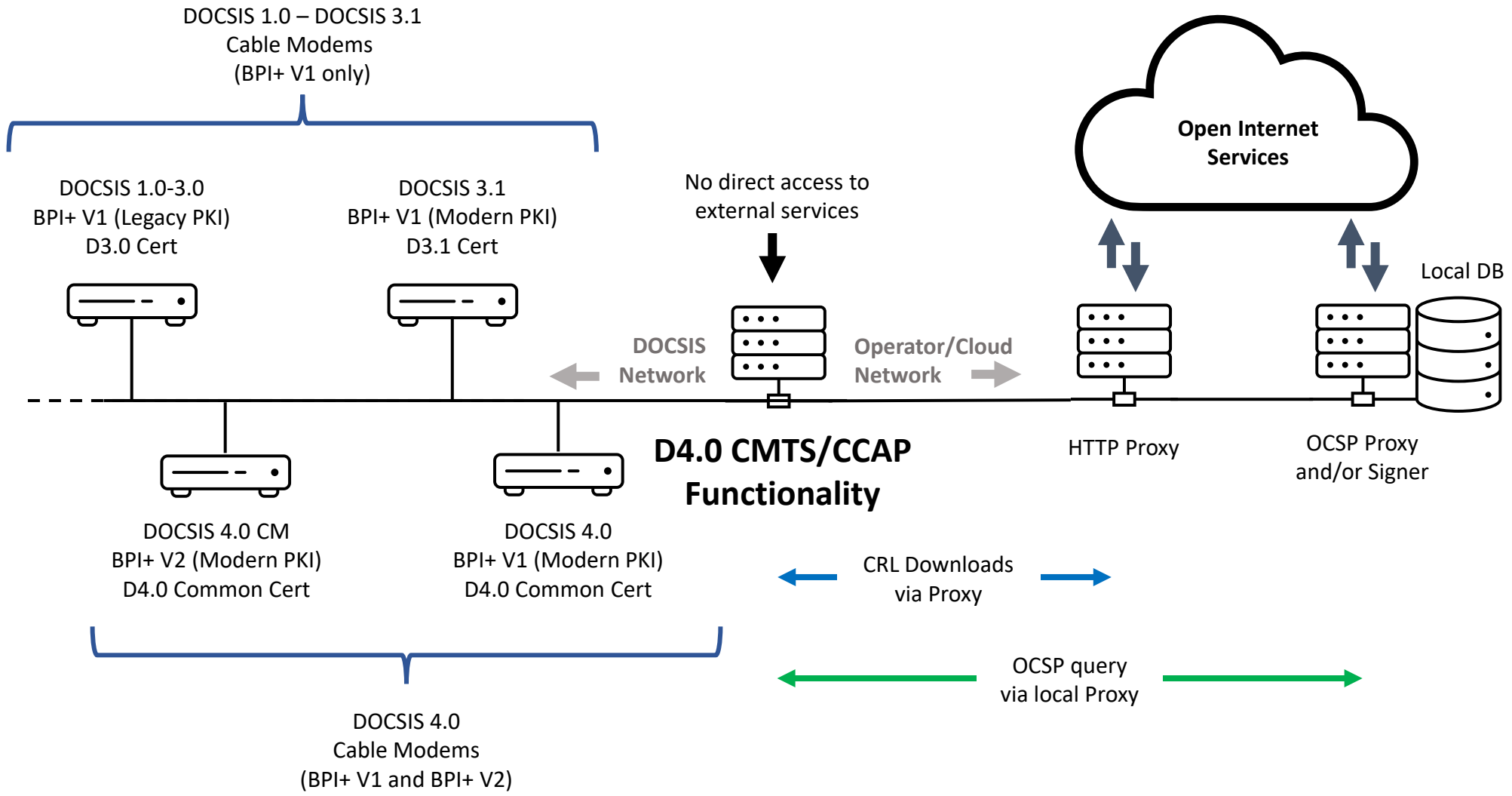

Fig 3. Example Deployment with revocation checking support and local overrides

Conclusions

- DOCSIS 4.0 provides many new security features and controls to lower the security risks of DOCSIS networks such as **BPI+ V2** or **TOFU**.
- DOCSIS 4.0 design implements new security principles such as **Perfect Forward Secrecy** and **Mutual Authentication** that can effectively address new security threats stemming from the introduction of distributed architectures.
- DOCSIS 4.0 builds on top of the options supported in previous version of DOCSIS when it comes to **revocation status checking** and fixes the revocation information discoverability by adding **standard extensions** to device certificates.
- Ultimately, DOCSIS 4.0 and BPI+ V2 open new future possibilities for the broadband industry and paves the road for practical solutions to address **upcoming security issues or threats** (such as post-quantum cryptography deployment for DOCSIS) while providing a cost-effective and efficient path to get there (algorithm agility).

Creating Infinite Possibilities.

Thank You!

Yuan Tian

Security Engineer
CableLabs
+1 303.661.3330 | y.tian@cablelabs.com