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

2022 Fall Technical Forum
SCTE • CABLELABS • NCTA

DOCSIS 4.0 Security: A Comprehensive Guide to Successful Deployments

A Technical Paper prepared for SCTE by

Massimiliano Pala
Director, PKI Architectures
CableLabs
858 Coal Creek Cir, Louisville, CO 80027
+1 303.661.3334
m.pala@cablelabs.com

Doug Jones
Principal Architect, Wired Technologies
CableLabs
858 Coal Creek Cir, Louisville, CO 80027
+1 303.661.3326
d.jones@cablelabs.com

Yuan Tian
Security Engineer, PKI Architectures
CableLabs
858 Coal Creek Cir, Louisville, CO 80027
+1 303.661.3330
y.tian@cablelabs.com

Craig Pratt
Lead Architect, Security & Privacy Technologies
CableLabs
858 Coal Creek Cir, Louisville, CO 80027
+1 303.661.3408
c.pratt@cablelabs.com

Table of Contents

Title **Page Number**

List of Figures

Title **Page Number**

List of Tables

Title **Page Number**

1. Introduction

DOCSIS® 4.0 security introduces several important enhancements when compared to previous generations of the protocol [SECv4.0]. To better understand the impact and use of DOCSIS 4.0 new features and how they relate to today's deployments and practices, let's start from reviewing the history of DOCSIS security and its evolution.

The first version of the Data Over Cable Service Interface Specification or DOCSIS® was released in 1997. The document specified the first standard approach to providing Internet access to subscribers over a cable operator's shared-access Hybrid Fiber-Coaxial (HFC) network (i.e., cable network).

The initial DOCSIS security architecture supported two major schemes: the Baseline Privacy Interface (BPI) and the Full Security (FS), a Security System with a removable security module. These two schemes specified the requirements to implement DOCSIS' two main security goals of protecting users and operators from data privacy issues and theft-of-service. The DOCSIS 1.0 specification eventually dropped FS due to a lack of support from the community. DOCSIS 1.1 strengthened BPI with its implementation of BPI+, which later evolved into the DOCSIS Security Specification in DOCSIS 3.0 and 3.1.

1.1. DOCSIS 3.0 and The Enhanced Secure Provisioning (ESP)

The DOCSIS 3.0 Security Specification [SECv3.0] introduced several new components that built upon the BPI+ (V1) Specification such as the Enhanced Secure Provisioning (ESP), extended support for Revocation Status Checking, and PKI Updates.

The Enhanced Secure Provisioning, or ESP, refers to securing the cable operator's operational support systems (e.g., the CM provisioning process, including Dynamic Host Configuration Protocol (DHCP), Time of Day (ToD), and TFTP). Securing these processes played a critical role in protecting the CM and the cable network from unauthorized access and theft-of-service attacks that cable operators were experiencing. Specifically, it prevented hacked modems from requesting unauthorized services.

DOCSIS 3.0 Security Specification also introduced a very important tool: certificate revocation status checking. Specifically, DOCSIS 3.0 supported two standard methods of certificate revocation: Certificate Revocation Lists (CRLs) and Online Certificate Status Protocol (OCSP). DOCSIS 3.0-compliant CMTS-es support configuration of none, one, or both certificate revocation methods.

On the PKI side, DOCSIS 3.0 Security leverages the same infrastructure (PKI) and the same authentication protocol that was used in the previous version of DOCSIS, but it introduces a new CVC infrastructure that supports a three-tier certificate chain architecture (i.e., Root, Intermediate, End-Entity). The support for the new CVC SubCAs was actually employed later in DOCSIS 3.1 security specification as part of the 2nd Gen DOCSIS® PKI, namely the "New PKI".

1.2. DOCSIS 3.1 and The Second Generation DOCSIS® PKI (The New PKI)

The new DOCSIS 3.1 Security Specification [SECv3.1] was introduced to strengthen the cryptographic parameters used during authentication. While DOCSIS 3.1 retains all the DOCSIS 3.0 Security features, it upgrades the PKI to a new infrastructure (2nd Gen DOCSIS® PKI) and increased the allowed size of cryptographic keys for both authentication and encryption.

On the PKI side, for DOCSIS 3.1, CableLabs defined an entirely new PKI hierarchy. The legacy PKI was halfway through its 30-year lifecycle, and it was starting to show its age with key sizes that needed

increasing and Hash Algorithms (i.e., SHA-1) whose use was being deprecated by NIST due to discovered weaknesses in the algorithm. To address this problem, the new PKI introduced the use of SHA-256 for digital signatures.

The overview of the security features of DOCSIS (1.0-3.1) are summarized in Table 1.

Table 1 - DOCSIS Security Evolution (1.0-3.1)

DOCSIS 1.0-3.1 Security Overview					
		DOCSIS 1.0	**DOCSIS 1.1 & 2.0**	**DOCSIS 3.0**	**DOCSIS 3.1**
Baseline Privacy Key Management (BPKM)	CM Public Key	768-bit key, 1024-bit key	768-bit, 1024-bit	768-bit, 1024-bit	768-bit, 1024-bit, 2048-bit key
	Authorization Key (AK)	64-bit key	160-bit key	160-bit key	160-bit key
	AK Generation	Random key generated by the CMTS and sent to the CM			
	AK Encryption	RSAES-PKCS1-v1_5	RSAES-OAEP	RSAES-OAEP	RSAES-OAEP
	KEK	64-bit Key	128-bit key	128-bit key	128-bit key
	KEK Generation	Both CM and CMTS derive KEKs from a function using the Authorization Key and the SHA-1 Hash Algorithm.			
	TEK	64- bit key	64- bit key	64- bit key, 128-bit key	64- bit key, 128-bit key
	TEK Generation	Random key generated by the CMTS and sent to the CM			
	TEK Encryption	56-bit DES	56-bit DES, 112-bit DES	56-bit DES, 112-bit DES	56-bit DES, 112-bit DES
	Message Authentication Key (MAK)	160-bit key	160-bit key	160-bit key	160-bit key
	MAK Generation	Both CM and CMTS derive MAKs from a function using the Authorization Key and the SHA-1 Hash Algorithm.			
	Hash Algorithm	SHA-1	SHA-1	SHA-1	SHA-1
MIC	MIC	HMAC-MD5	HMAC-MD5	MMH-MAC	MMH-MAC
Data	Traffic Encryption	56-bit DES, 40-bit DES	56-bit DES, 40-bit DES	56-bit DES, 40-bit DES, 128-bit AES	56-bit DES, 40-bit DES, 128-bit AES
Auth	CM Authentication	MAC Address	X.509v3 RSA certificate	X.509v3 RSA certificate	X.509v3 RSA certificate
Code	SSD	Proprietary	1024-bit CVC, 1536-bit CVC, 2048-bit CVC	1024-bit CVC, 1536-bit CVC, 2048-bit CVC	1024-bit CVC, 1536-bit CVC, 2048-bit CVC
ESP	ESP	No	No	Yes	Yes

1.3. Distributed Access Architectures and New Security Needs

Since DOCSIS 4.0 relies on the use of distributed architectures to deliver increased speeds both downstream and upstream, it is important to assess and understand the boundaries of this new attack surface and the associated threats.

Distributed Access Architecture (DAA) is an evolved cable network architecture that decentralized the headend network functions by moving the PHY and/or MAC layer functions to the remote node of the access network, while other functions remain in the Converged Cable Access Platform (CCAP). Currently, there are three types of DAA networks: (1) the Remote PHY or R-PHY (2) Remote MACPHY architecture or R-MACPHY, and (3) Flexible MAC Architecture or FMA.

In R-PHY and R-MACPHY, the MSO network is split into "trusted" and "untrusted" domains. The RPD/RMD, coax access network and edge devices (e.g., CMs) are in the "untrusted" domain (i.e., either in the customer's premises or deployed in the field). On the contrary, the CCAP core, authentication server and provisioning servers are located in the "trusted" domain that is usually under strict MSO physical control and where only authorized employees are allowed access (e.g., NetOps and NetSecOps).

With the introduction of FMA, virtualization and containerization techniques are used to ensure service availability and to optimize resource allocation for enhanced services capability. In FMA, the security boundary between trusted and untrusted domains is even more blurred, and, therefore, the need to verify the identity of all elements that are present in the network is critical and necessary. This approach to network security is referred to as Zero Trust Security. Operators may find themselves facing difficult choices when considering tradeoffs between security and service availability: strict revocation checking, frequent software updates, or unnecessarily short certificates' validity periods can cause unexpected service availability issues, while loose security controls and exceptionally long certificate validity periods can put customer and organization assets under the potential risk of compromise.

The original threat model used to design the DOCSIS security protocol did not incorporate or anticipate the kinds of security issues introduced by distributed architectures and without specific hardware protections (e.g., secure key storage), it's still possible to maliciously modify or replace device software and credentials, which might enable attacks such as Modem Cloning or Service Uncapping. For example, attackers could exfiltrate the device's credentials or install malware (e.g., backdoors, bot agents, etc.) to perform active attacks such as ***Denial-of-service*** or ***Man-in-the-middle*** that can have very disruptive effects for the operator's network.

To mitigate the possibility to carry out these new class of attacks, DOCSIS 4.0 introduced two new security controls that are meant to work together: device physical security and network identities.

On the physical security side, the new requirements are described in section 15 of [SECv4.0] and mandate for increased security of stored secrets (keys) (see Section 15.1 of [SECv4.0]) and the use of secure boot processes for CMs (see Section 15.2 of [SECv4.0]). The use of such measures is aimed at reducing the risk of unexpected/malicious changes in the software running on CMs.

When it comes to network identities, before DOCSIS 4.0, only the CMTS could verify the Cable Modem's certificate, not the other way around. In fact, since no verifiable identity is used on the server side (CMTS) in BPI+ V1, an attacker may be able to intercept CMTS functionalities and redirect the messages to its own device or service by targeting, for example, fielded RPDs or RMDs. In this scenario, it is easy to show how an attacker could completely take over large amount of internet connections via malicious network configurations (i.e., DHCP, DNS, etc.) and services (i.e., Web, Mail, etc.). Similarly,

passive attacks are also possible where the customer's session is not actively modified but it is just monitored for "interesting" data.

As discussed in great detail in the next section, DOCSIS 4.0 supports a new version of the authentication protocol, namely BPI+ V2, that greatly reduces the possibility to carry out such attacks by requiring both the CM and the CMTS to verify each other identities before establishing a connection.

2. DOCSIS 4.0 Security Principles

One of the challenges faced in designing DOCSIS 4.0 was how to integrate the needed new security features such as Mutual Authentication or Perfect Forward Secrecy in a minimally disruptive fashion. The answer to this challenge was twofold: (1) provide support for the same BPI+ (V1) authentication protocol in use in previous version of DOCSIS (1.1-3.1) and, (2) introduce a new version of BPI+ (V2) that encapsulate the needed security enhancements.

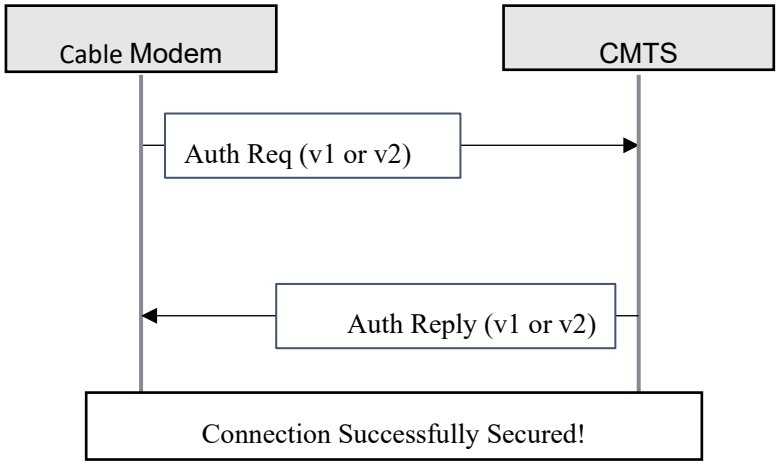


Figure 1 - BPI+ Authentication Messages (V1 and V2)

Figure 1 provides an overview of the BPI+ authentication process (common across BPI+ V1 ad V2) where the Auth Request and Auth Reply messages are used to establish a common encryption key (i.e., AES) between the CM and the CMTS.

To better understand the differences between the security features supported in the two versions of BPI+, let's compare their security features and how they relate to and solve the new threat model.

Message Authentication and Integrity. This security principle is related to protecting the integrity and providing verifiable origin information for exchanged messages during authentication. In BPI+ V1, neither the CM nor the CMTS authenticate (sign) the messages they generate. In BPI+ V1, the CMTS uses the public key of the CM's Device certificate to encrypt the authorization key for the destination CM. The lack of authentication is the source of many possible security vulnerabilities that can lead to very disruptive attacks (i.e., modifying exchanged messages, spoofing device identities, etc.). In BPI+ V2, both the CM and the CMTS are required to sign outgoing authentication messages sent to the other party and authenticating their peer's messages before processing them.

Perfect Forward Secrecy or PFS. This security principle is related to protecting data across sessions. Specifically, when PFS is supported, its use protects against the decryption of pre-recorded data even when the target Cable Modem (CM) private key has been compromised. In BPI+ V1, the session encryption key is directly encrypted under the public key of the CM certificate and an attacker can decrypt any prerecorded sessions between the CM and the CMTS by compromising the certificate's private key at some date in the future. In BPI+ V2 the encryption key is negotiated when establishing a new session by using a Diffie-Hellman key exchange over finite field or Elliptic curves. This prevents an attacker from decrypting previously recorded traffic that was protected under BPI+ V2 even if/when an attacker compromises the CM's private key.

Mutual Authentication or MA. This security principle is related to guaranteeing that no malicious entity is able to impersonate the other party when establishing/authenticating the communication session between the CM and the CMTS. This type of attack is usually referred to as a "Man-In-The-Middle" (MITM) attack and requires the ability to manipulate the traffic on the network. Because BPI+ V1 does not secure the CMTS (or network) identity (it does not provide certificate during connection initiation), BPI+ V1 is vulnerable to such attacks. Malicious actors could impersonate a CMTS without the CM being able to distinguish between the real CMTS and the attacker. In BPI+ V2, the CMTS provides a certificate to prove its identity and the CM can, in this case, easily identify the real CMTS by validating the CMTS' message signature and certificate. The incorporation of this CMTS certificate-based identity allows the CM to properly authenticate the CMTS via a digitally signed Auth Reply, thus preventing any non-authenticated or modified messages to be ignored.

Algorithm Agility. This security principle is related to the possibility to execute the authentication protocol independently from the underlying cryptographic algorithms selected for proving identities (e.g., RSA, Falcon, Dilithium, etc.). In BPI+ V1, as mentioned when describing PFS, the CMTS directly uses the RSA public key associated with the CM's certificate to secure (encrypt) the authorization. In BPI+ V2 the authorization exchange enables a variety of methods to determine an authorization key. This mechanism provides a path for enabling post-quantum-safe cryptography and classic/post-quantum hybrid identity certificates.

Increased size of encryption keys. This security principle is related to the normal evolution of cryptographic algorithms over time where it is understood that larger keys are needed to keep the same level of confidentiality. In BPI+ V1, although there are few options when it comes to negotiating line-rate symmetric ciphers (encryption algorithms), AES-128 is the only supported option that is considered secure according to today's best practices. DOCSIS 4.0 introduces support for negotiating larger key sizes (AES-256) to encrypt user-data traffic that aligns with current best practice and provides the same level of protection against quantum attacks that users enjoy today against classic ones.

Downgrade Protection. This security principle is related to protecting against malicious actors trying to negotiate a more vulnerable version of a protocol when multiple versions are supported. This is a very difficult problem to solve that generally affects Access Networks architectures such 3GPP networks. Since DOCSIS 4.0 supports two different versions of BPI+, without providing any protection, DOCSIS 4.0 could suffer from vulnerabilities similar to ones observed in mobile networks. To address this issue, DOCSIS 4.0 introduces the concept of Trust on First Use (TOFU) that requires a CM to store the minimum allowed version of the BPI+ protocol for subsequent authentications, as indicated by the CMTS, in a secure memory location on the CM after successful authentication. For example, a CM that authenticates with BPI+ V2 can be signaled by the CMTS to only communicate using BPI+ V2 for subsequent sessions – preventing an imposter CMTS from downgrading to BPI+ V1 on a subsequent connection.

In the rest of the section, to better understand the differences and similarities of DOCSIS 4.0 and 3.1, we provide a summary about what changes and what does not change when it comes to deployments.

2.1. From DOCSIS 3.1 to DOCSIS 4.0 Security: What Does NOT Change?

DOCSIS 4.0 supports two versions of the BPI+ authentication protocol: BPI+ V1 and BPI+ V2. While the latest version of the protocol (BPI+ V2) is only available in DOCSIS 4.0 mode, the first version of the protocol, i.e., BPI+ V1, is shared across almost all versions of DOCSIS, including DOCSIS 4.0 (1.1-4.0). A first advantage for retaining support for BPI+ V1 in DOCSIS 4.0 is the possibility to deploy new DOCSIS 4.0 devices without the need for updating existing procedures, thus reducing the extra overhead of deploying new technologies that might come with new requirements. A second advantage is related to the fact that since in BPI+ V1 the CMTS does not need a device certificate, deploying DOCSIS 4.0 with BPI+ V1 does not introduce new requirements (for security) when compared to previous versions of DOCSIS such as DOCSIS 3.0 or DOCSIS 3.1. However, as discussed previously, with the introduction of distributed nodes outside the operator's trusted domain, the attack surface has increased. When enhanced authentications are needed, BPI+ V2 can be enabled to address the new security risks (see Section 2.3 for more details).

From the ***Secure Software Download (SSD) standpoint***, DOCSIS 4.0 design applies the same principle that was used for the authentication protocol: keep support for current procedures and provide the possibility for upgrading to a more efficient one when needed. In fact, in DOCSIS 4.0 *there are two different mechanisms that can be used to enable SSD on a device*. The first one is the same leveraged in DOCSIS 3.1 where the use of a Manufacturer's CVC and/or an Operator's co-signer CVC certificate(s), in the config file (or via SNMP SET), triggers SSD procedures. The second mechanism that directly use the Firmware Authentication Header (FWAH) is detailed in the next section.

Another important similarity between DOCSIS 3.1 and DOCSIS 4.0 is ***the use of the same PKI***. Differently from the previous DOCSIS update (DOCSIS 3.0 → DOICSIS 3.1), DOCSIS 4.0 uses the same Root of Trust that is used in DOCSIS 3.1. This means that DOCSIS 4.0 can use the same procedures and Trust Anchor used in DOCSIS 3.1 to validate device certificates.

When looking at the ***backward compatibility with previous versions of DOCSIS***, it is important to understand what type of certificates might be needed. Specifically, while DOCSIS 4.0 devices use a single certificate to connect to both DOCSIS 4.0 and DOCSIS 3.1 CMTS[1] by using a *Common Cable Modem* certificate profile, they will still need a DOCSIS 3.0 CM certificate to be able to connect to pre-3.1 CMTS. The reason for this is that DOCSIS 3.0 and DOCSIS 4.0 do not share the same Root of Trust and, therefore, separate certificates are still needed, exactly as for DOCSIS 3.1 devices.

Support for revocation also remains untouched from D3.1 and D3.0 specifications. In fact, besides the use of CMTS-related revocation information when BPI+ V2 is enabled, the validation of CM certificates is delegated to the CMTS. During this process the CMTS can use CRLs or OCSPs to check the status of the CM's certificate and take proper action about it (or just report it). Support for revocation status checking for the network (CMTS) certificate is discussed in the next section.

What about EAE? DOCSIS 4.0 support for EAE is backward compatible with previous versions of DOCSIS where the CMTS support for EAE is advertised via TLVs in downstream MDD messages. In DOCSIS 4.0, the usual TLV Type 6 that is used to advertise support for EAE for BPI+ V1 is joined by the

[1] DOCSIS 4.0 certificates are different from DOCSIS 3.1 ones, and a software upgrade might be needed for D4.0 devices to be supported by DOCSIS 3.1 CMTS.

new TLV (Type 23) that allows to specify additional options for BPI+ V1 and BPI+ V2 as described in the next section.

In summary, the security features and operations that remain common to both D3.1 and D4.0 are:

- DOCSIS 4.0 can use the same authentication protocol in use for DOCSIS 3.1 (BPI+ V1)
- DOCSIS 4.0 can use the same PKI in use for DOCSIS 3.1 (2nd Gen DOCSIS® PKI)
- DOCSIS 4.0 can use the same SSD procedures in use for DOCSIS 3.1
- DOCSIS 4.0 devices require, exactly as D3.1 devices, an additional certificate from the 1st Gen DOCSIS® PKI ("legacy" PKI) to authenticate in DOCSIS 3.0 networks (if the device supports D3.0 environments).
- DOCSIS 4.0 supports the same revocation options available in DOCSIS 3.1 and DOCSIS 3.0.

In the next section we look at the aspects that have changed and their impact on DOCSIS 4.0 deployments.

2.2. From DOCSIS 3.1 to DOCSIS 4.0 Security: What Changes?

While support for BPI+ V1 is shared across almost all versions of DOCISS (1.1-4.0), DOCSIS 4.0 is the first version of DOCSIS to support BPI+ V2 that delivers new and enhanced security controls. Since BPI+ V2 introduces the most profound changes in DOCSIS security since the introduction of digital certificates in DOCSIS 1.1, a detailed description is provided in the next section while here we focus on the rest of the differences with DOCSIS 3.1.

On the certificate side, there are four important changes that need to be discussed.

First, although DOCSIS 4.0 uses the same PKI as DOCSIS 3.1, the contents of CM certificates for the two environments are different. In fact, while DOCSIS 4.0 uses the same algorithm (RSA) and key sizes (2048 bit) already in use in DOCSIS 3.1, certificates for D4.0 CMs are larger than their DOCSIS 3.1 counterpart because of the introduction of several standard extensions that deliver new security controls. The first change to notice is the use of the Authority Information Access (AIA) extension to carry the location of the authoritative OCSP server that the CMTS can use to check for the revocation status of certificates. This change fixes the status of revocation in D3.1 and D3.0 where the absence of such data makes revocation checking very hard in practice. Another important change in the certificate profile is related to the introduction of a new concept in DOCSIS: ***roles or functions***. Indeed, D4.0 certificates use a well identified set of Object Identifiers or OIDs inside the Extended Key Usage (EKU) extension that allow the verifier to check, based on the presence of specific values in the extension, if the connecting device is authorized (or not) to provide specific services. DOCSIS 4.0 defines two OIDs to identify CMTS functionality (`svcCMTS`) and CM functionality (`svcCM`) respectively. For example, when a CM is validating the CMTS certificate, it will look for the `svcCM` value in the EKU extension of the certificate and, if not found, rejects the connection if the `svcCMTS` value is not present in the certificate (i.e., the device was not authorized to provide CMTS services). In other words, in DOCSIS 4.0 not all certificates are created equal to prevent attacks where a legit certificate (e.g., a CM certificate) would be used to impersonate different roles (e.g., a CMTS). Table 2 provides the list of the EKU values supported in DOCSIS 4.0.

Second, before the operator enables BPI+ V2, the CMTS needs to be provisioned with a DOCSIS certificate. As we discussed earlier, the availability of CMTS credentials enables the CMTS to authenticate its own messages and, therefore, turning on BPI+ V2 not only lowers the risks of network compromise, but it also enables the possibility for Trusted Services from the network enabled by the

possibility to validate, and subsequently trust, the CMTS identity. The provisioning and management of CMTS certificates (i.e., renewal and installation) is a very new process for the DOCSIS community and it is expected to require dedicated support and/or automation. CMTS certificates have a validity of up to five years.

Four, DOCSIS 4.0 CMs use a single certificate to authenticate in both DOCSIS 4.0 and DOCSIS 3.1 modes. This means that D4.0 devices connecting to existing D3.1 networks will use certificates that although compatible with the DOCSIS 3.1 environment (i.e., same algorithm and key sizes), they may be larger in size than the D3.1 ones because they contain new standard extensions that are not present in D3.1 certificates.

Table 2 - Object Identifiers for EKU enabled functionalities in DOCSIS 4.0

Short Name	Name	Value	Description
svcCMTS	id-cl-pki-eku-CMTS	1.3.6.1.4.1.4491.2021.2.1.1	CMTS functionalities
svcCM	id-cl-pki-eku-CM	1.3.6.1.4.1.4491.2021.2.1.2	CM functionalities

On the CVC side there are some important changes. Differently from the DOCSIS 3.1 environment, DOCSIS 4.0 does not support CVCs from the 1st Gen PKI (or "legacy PKI") when it comes to Secure Software Download and Firmware signing. Because the validation of "legacy" CVCs does not require to check expiration times against the current time, retaining support for "legacy" CVCs would introduce the possibility to modify the code loaded onto D4.0 devices with CVCs that use outdated (and possibly weak) cryptographic parameters such as 1024-bit keys and the SHA-1 algorithm for signatures (any time in the future. To eliminate the security risk, differently from D3.1, DOCSIS 4.0 devices only support CVCs from the 2nd Gen DOCSIS® PKI (i.e., the "modern" PKI). Additionally, a new mechanism to initiate the SSD process has been introduced that optimized validations of the firmware by directly supporting the use of the Firmware Authentication Header (FWAH) in config files or via SNMP SET (see Section 14.2 of [SECv4.0]).

On the revocation side there are also some changes. Although when BPI+ V1 is used there are no changes in how revocation works since D3.0, when BPI+ V2 is enabled and revocation checking is desired there is a new certificate to be validated, the CMTS one. Indeed, in BPI+ V2, the CMTS MUST transmit the OCSP response related to the status of its own certificate in the Auth Reply or Auth Reject message. The CMTS's OCSP response can be cached by the CM and the CMTS for its entire validity time, to minimize the load on revocation infrastructures.

In the previous section we mentioned ***some changes on the EAE side***. Although support for TLV Type 6, i.e., the EAE Enabled/Disable TLV (see Section 6.4.28.1.6 of [MULPIv4.0]), is maintained for backward compatibility, DOCSIS 4.0 devices use the new TLV of Type 23, i.e. BPI+ Supported Version and Configuration (see Section 6.4.28.1.22 of [MULPIv4.0]), to discover which BPI+ versions are enabled on the CMTS and what services are available with each one. This new TLV is a compound TLV that uses two bytes to indicate (a) the enabled version of BPI (i.e., 1-byte integer value), and (b) the associated enabled features (i.e., bitmask where Bit 7, when set to one, indicates EAE support). Multiple TLV 23 can be used to announce the enabled features for each BPI+ version that is enabled on the CMTS.

On the BPKM layer side, DOCSIS 4.0 introduces an important update: enabling fragmentation support to extend the supported maximum size of BPKM payloads to ~28 Kb. This change is implemented by introducing two new MMM messages (i.e., the BPKM-REQ5 and the BPKM-RSP5) in [MULPIv4.0] that leverage MMM V5 (instead of V1 as used in BPI+ V1) to support large BPKM

messages that may span more than one frame (i.e., up to 16 fragments). This solution not only enables the use of extra cryptographic material in the Auth Request / Auth Reply process without the need to add new messages and states in the State Machine, but it also opens up future paths for the deployment of new cryptographic algorithms such as Kyber (for key exchange) and Dilithium (for public/private keys), or even hybrid approaches that combine RSA with new types of algorithms [Pala21].

In summary, the security features and operations that change between D3.1 and D4.0 are:

- DOCSIS 4.0 supports multiple versions of BPI+ (i.e., BPI+ V1 and BPI+ V2)
- DOCSIS 4.0 can use advanced authentication features when enabling BPI+ V2
- DOCSIS 4.0 devices use certificates that are larger in size than D3.1 certificates
- DOCSIS 4.0 can use updated SSD procedures that optimizes early error detection
- DOCSIS 4.0 introduces two new approaches for delivering SSH access to devices without static secrets on devices
- DOCSIS 4.0 can enable or disable, for each enabled BPI+ version, the use of EAE independently.
- DOCSIS 4.0 introduces fragmentation support for BPI+ V2 messages

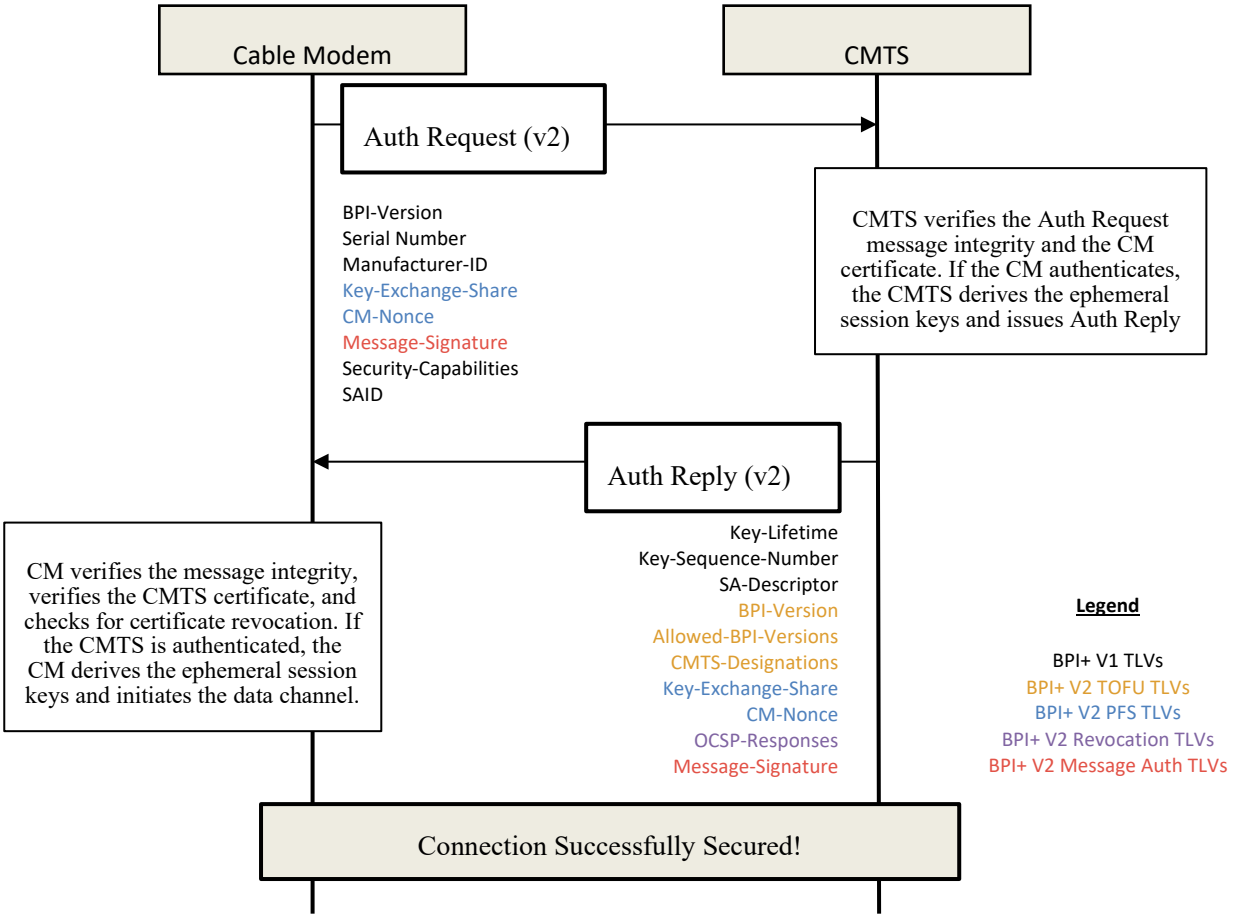


Figure 2 - BPI+ V2 authentication process

2.3. A New Authentication Mode (BPI+ V2)

The new version of the BPI+ authentication protocol supported in DOCSIS 4.0 is called BPI+ V2. Although this new version has the same structure of its predecessor (i.e., it still uses only two (2) messages to establish a secure connection between the CM and the CMTS and there is no change in the state machine), the security properties offered by BPI+ V2 are very different from the ones offered by BPI+ V1. Figure 2 depicts a BPI+ V2 message exchange where the newly defined TLVs are detailed.

A first fundamental difference between BPI+ V1 and V2 is the use of different versions of Mac Manager Messages (MMM) to encapsulate the protocol. In fact, while BPI+ V1 use MMM V1 messages that are limited in size to a single frame, BPI+ V2 defines two new messages, the BPKM-REQ5 and BPKM-RSP5, that leverage version 5 of the MMM headers. The new version of the messages supports payload fragmentation for up to 16 different fragments, thus pushing the maximum supported size for BPKM close to ~28Kb. This change allows for the deployment of larger cryptographic material that may require larger data structures during transport such as post-quantum keys, certificates, and signatures.

A second important feature of BPI+ V2 is the use of digital signatures to authenticate BPKM messages. The `Message-Signature` TLV, depicted in red color in the figure, carries a DER representation of a Cryptographic Message Syntax (CMS) data structure together with the signer's certificate and stores a

detached signature that is calculated over the entire BPKM message (i.e., the code, length, and payload up to, but excluding, the `Message-Signature` TLV itself). The use of this TLV implements the Message Authentication and Integrity principle. Moreover, the use of message authentication on both sides of the communication reflects a very important paradigm shift in DOCSIS security where, up to DOCSIS 3.1, the primary focus has been the authentication of Cable Modems only. As the deployment models for DOCSIS have become more distributed, the new BPI+ V2 introduces the support for Mutual Authentication principle via the presence of the `Message-Signature` TLV in both the Auth Request and Auth Reply (or Auth Reject) messages.

Another important enhancement introduced with BPI+ V2 is the use of the Diffie-Hellman (DH) key exchange mechanism to provide support for Perfect Forward Secrecy (PFS). Indeed, differently from BPI+ V1 where the authorization key is directly encrypted with the RSA public key of the CM's certificate, BPI+ V2 use the `Key-Exchange-Share` TLV to carry the cryptographic material to derive a common key across the CM and the CMTS. This new key exchange mechanism prevents the decryption of pre-recorded traffic for a CM even when the private key of the CM has been compromised, thus implementing the PFS principle.

The combination of Message Authentication and Mutual Authentication principles (implemented in BPI+ V2 via the `Key-Exchange-Share` and `Message-Signature` TLVs), enables a third one, i.e., Algorithm Agility. In fact, because of the separation of the algorithm used for the public key in the certificate and the algorithm used for key exchange, BPI+ V2 is algorithmically agile with respect to the device certificate, thus being able to support not only RSA-based certificates but other classic (e.g., ECDSA), post-quantum (e.g., Dilithium or Falcon), or hybrid (e.g., Composite-Crypto) algorithms.

With the introduction of multiple versions of the BPI+ protocol, a Downgrade Protection mechanism (TOFU) was introduced to provide protection against unauthorized downgrades. To support TOFU, BPI+ V2 uses two TLVs during the authentication process: the `BPI-Version` and the `Allowed-BPI-Versions` whose value can be used to manage which version of BPI+ should the device use after an initial successful connection. For example, during a BPI+ V2 authentication, the CMTS can use the Allowed-BPI-Versions TLV with the value of (1) to indicate that the CM can still use BPI+ V1, if needed, for subsequent authentications (i.e., legit downgrades).

In the rest of the section, we focus on the different options available for managing revocation status checking, an important aspect of successful deployments when it comes to security.

2.4. Certificate Revocations Updates

Support for checking the status of revocation for DOCSIS devices has been integrated into the specifications since DOCSIS 3.0 where both CLRs and OCSP checking were introduced to lower security risks associated with providing services to potentially compromised devices.

In DOCSIS 4.0, there are two main changes in the protocol that affect revocation checking procedures: the introduction of the CMTS (or network) identity, and the updating of certificate profiles.

The first change, the introduction of the network identity, required the definition of a new security control that would allow Cable Modems to know when (or not) to demand OCSP responses from the CMTS (i.e., in DOCSIS 4.0, CMs do not perform OCSP queries directly), and when they can ignore it. Since malicious attackers would try to remove checking of revocation information to make it easier to use compromised credentials, DOCSIS 4.0 does not leverage the usual control interface for configuring CM revocation checking requirements (i.e., config file TLVs or SNMP SETs), but the certificates itself.

Indeed, when CM revocation checking is desired, operators should use CMTS certificates that contain the URL of the OCSP responder (i.e., the Authority Info Access extension with the OCSP access method): when the URL is embedded in the certificate the CM understands that revocation status checking is required and will reject messages that do not carry the needed OCSP responses for the CMTS certificate. Vice versa, when revocation checking is not desired on the CM, operators should install CMTS certificates that do not contain the OCSP URL in them: when the URL of the OCSP responder is not embedded in the CMTS certificate, the CM understands that revocation checking is not required and, therefore, OCSP responses are not needed in the CMTS' messages. CMTS certificates that do not carry any OCSP revocation information are referred to as NRI certificates or No-Revocation Information certificates.

In other words, *the protected value, i.e., the extension, inside the certificate is the secure equivalent of configuring revocation checking on CMs via SNMP or configuration file options* since the presence of the extension in the certificate is protected by the CA signature on the device certificate itself (i.e., even the CMTS cannot lie about the requirement).

In this view, CMTS vendors should consider the possibility to support a dual-certificates configuration for their devices: one certificate for when CMTS certificate revocation checking is enabled and one certificate for when CMTS certificate revocation checking is disabled.

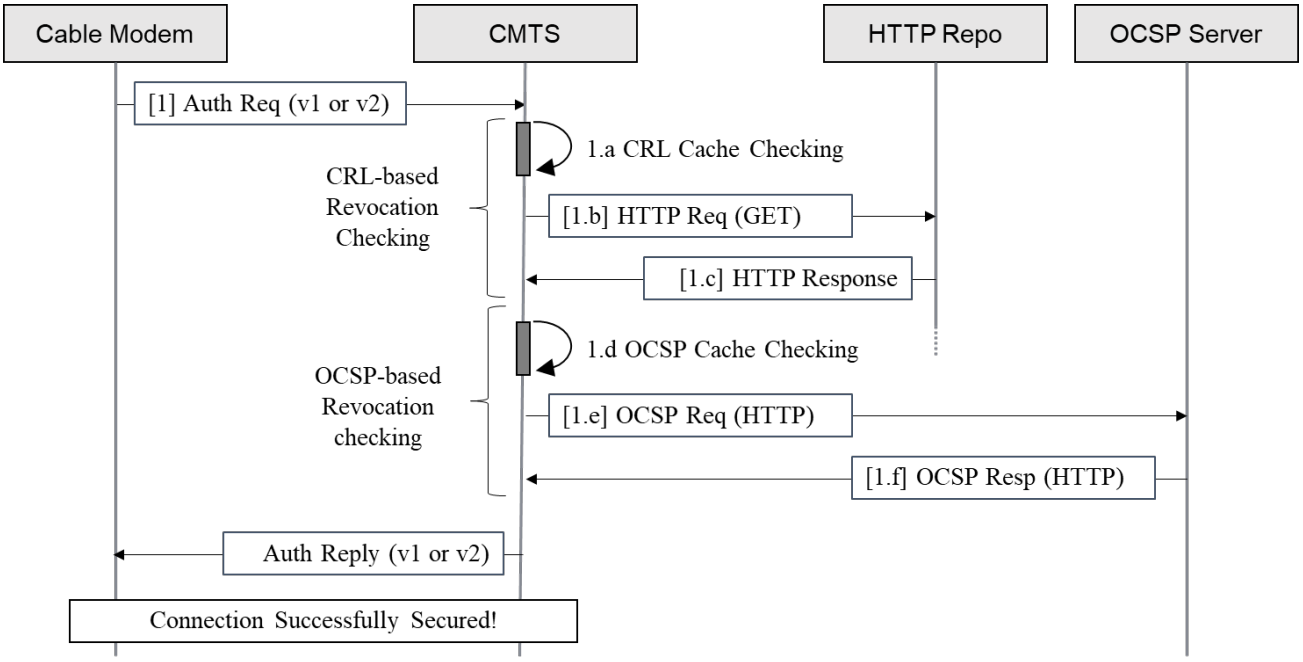


Figure 3 - Integrated BPI+ and Revocation Checking Flow

Figure 3 provides an overview of the generic workflow for the BPI+ protocol basic authentication messages when combined together with the revocation information checking process. We will use this figure throughout this section of the paper to discuss the details of the different deployment options available in DOCSIS 4.0.

As depicted in Figure 3, the retrieval of the revocation information can be triggered by new Authorization Requests coming into the CMTS, however it might be a good practice to keep a caching mechanism on the CMTS to allow for faster authentications (and re-authentications) and reduce the number of external

requests the CMTS issues (and rely upon) to complete the authentication. This is particularly true in the context of OCSP processing when a CMTS is rebooting and, in general, for CRL-based revocation checking where usually the validity period of CRLs is quite long (days or weeks). Since DOCSIS 4.0 explicitly allows for caching the revocation information for their entire validity period, it is important to leverage this option on the CMTS to deliver fast and efficient revocation status checking.

Another important consideration is related to the ability of the CMTS to directly connect to resources on the internet (not directly available on the operator's network). Usually, because of security concerns, CMTS-es are not allowed to access any resource on the Internet. When this is the case, the CMTS would not be able to query CRLs repositories or OCSP responders unless some "intermediary" is used. For example, operators can route all requests for revocation information via an HTTP proxy, thus allowing for easier monitoring (and restrictions) for which resources the proxy can access (e.g., only official OCSP repositories). When OCSP validity period and HTTP caching headers carry the same values, the HTTP caching mechanism can be used for both OCSP and CRLs.

However, when HTTP proxy services are not enough and operators would like to take control over the revocation information for the devices deployed in their own network, operators should consider the possibility to deploy local OCSP servers that can provide OCSP responses (locally) and, moreover, override revocation status (locally). The deployment of such services in the operator's network can enable the possibility to manage the revocation status of device certificates locally. For this option to be enabled, the operator needs an OCSP responder certificate from the DOCSIS infrastructure (for each D4.0 issuing CA) that can be used to setup the local service. Efficient open source implementations for in-line OCSP responders are already available (e.g., OpenSSL [OSSL] or OpenCA OCSPD [OCAOD]).

In the rest of this section, we examine different deployment scenarios for enabling revocation checking on the server side, on the client side, or both.

2.4.1. Enabling Mutual Authentication without Revocation Checking

The simplest and most common deployment model is the one where there is no support for revocation status checking. This is the default deployment scenario in today's DOCSIS network where revocation checking is disabled or practically very difficult to implement because of the lack of OCSP URLs inside D3.0 and D3.1 certificates.

In this authentication mode, when BPI+ V1 or V2 are executed, the CMTS (in both BPI+ V1 and BPI+ V2) does not download any Certificate Revocation List (or CRL) nor any OCSP Responses to validate the revocation status of the device certificate. This means that authentications only rely on the information presented by the device (or the network) to decide if to allow the connection with the device (or the network). This means that the extra steps {*1.a, …, 1.f*} from Figure 3 are not needed and will not be executed in both BPI+ V1 and BPI+ V2.

To achieve this configuration, the CMTS must be first configured to disable CRL and OCSP response (both). Changing the CMTS configuration is sufficient when only BPI+ V1 is enabled. However, to correctly handle the BPI+ V2 case, the CMTS must also be provisioned with a CMTS NRI certificate: the absence of the OCSP URL inside the certificate is used as the security control to communicate to the CM that no revocation checking is needed on this certificate when executing BPI+ V2 only (i.e., BPI+ V1 does not use any network identity and, therefore, there is no CMTS certificate to validate).

2.4.2. Enabling Mutual Authentication with CM's Certificate (client-side) Revocation Checking

Similarly, to D3.0 and D3.1, DOCSIS 4.0 supports checking the revocation status of connected devices when using either BPI+ V1 or BPI+ V2. Similarly, to the previous case, only when executing BPI+ V2 the CMTS NRI certificate is needed to be installed on the CMTS. In this configuration, OCSP responses are not sent inline from the CMTS to the CM during BPI+ authentications (i.e., because NRI certificates do not carry the URL of the OCSP responder), thus limiting the dependencies on the availability of revocation information to the CMTS only.

Since the CMTS is the ultimate controller that can allow or reject a CM during authentication, CMTS vendors have the possibility to implement different authorization policies can be enabled to better accommodate NetOps needs. For example, CMTS vendors could provide the possibility to have strict or permissive policies for allowing devices on the network only after passing revocation checking (strict policy) or allowing them even when revoked and, in that case, report it for monitoring or investigative purposes (permissive policy). Although a strict revocation is the most secure option (e.g., not allowing compromised devices to access any service), permissive policies might be implemented to monitor for potentially compromised or otherwise misbehaving devices. This approach allows for decoupling the decision to provision services to devices from the certificate revocation status (i.e., the revoked status becomes a factor in the decision, not the decision itself).

In this case, although both OCSP and CRL mechanisms can be used for checking the status of devices, it might be more efficient to enable CRL-based validation since a single CRL carries all relevant revocation information for all the certificates issued from the CA while OCSP responses are related to a single certificate entry. When using OCSP, individual request/response roundtrips have to be used for each CM the CMTS needs to validate the revocation status for, while a single CRL can be used to lookup the revocation status of all certificates issued from a CA (with the downside of being quite large if many certificates have been revoked).

2.4.3. Enabling Mutual Authentication with CMTS' Certificate (server-side) Revocation Checking

On the opposite side of the spectrum, this deployment model enables the revocation status checking for the CMTS certificate to authenticate the network. This use-case, because it involves the CMTS certificate, it is relevant only for BPI+ V2 authentications.

To achieve this configuration, operators must disable revocation checking on the CMTS, both CRL-based and OCSP-based mechanisms for the client side. By disabling revocation checking on the CMTS, the CMTS will not execute steps {*1.a, ..., 1.f*} from Figure 3 to validate the CM's certificate.

However, the CMTS still need to procure the OCSP response for its own certificate and send it to the CM in Auth Reply messages during BPI+ V2. Therefore, in this case, the CMTS still needs to execute steps {*1.d, 1.e, 1.f*} to be able to retrieve the OCSP response from the server (if not cached).

Differently from the two previous use-cases, the CMTS certificate must carry the URL of the OCSP responder in it to communicate to the CM that OCSP responses validation is required for this certificate. CMTS certificates that contains revocation information are referred to as "Full" or "Full CMTS" certificates.

As described in Section 2.3, that when validation checking is to be performed by the CM, the CMTS must provide the OCSP response inline during BPI+ authentications and that means that if a response cannot be fetched (or the cached version is expired), the CM will reject the CMTS certificate.

2.4.4. Enabling Mutual Authentication with Mutual Revocation Checking

The last use-case we want to explore is the scenario where both the client-side (CMs) and the server-side (CMTS-es) are required to check the validation status of the other party. This setting, as the previous one, is only relevant when BPI+ V2 is used.

To achieve this setup, the CMTS must be configured to enable the revocation checking of CMs' certificates (either via CRLs or OCSP) must be enabled on the CMTS. Moreover, the CMTS, exactly as the previous case, must be provisioned with a Full CMTS certificate to enable revocation checking on the CM.

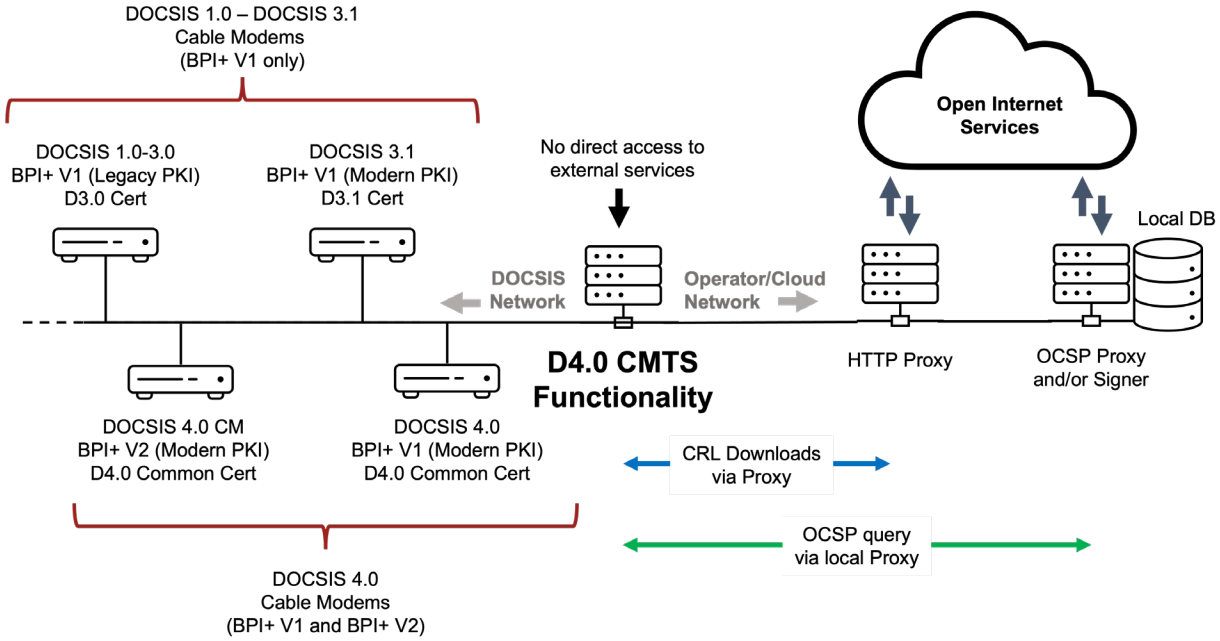
In this configuration, the authentication message flow will actually use steps {1.a, 1.b, and 1.c} to validate the CM's certificate when the CRL mechanism is used or steps {1.d, 1.e, 1.f} to validate the CM's certificate when the OCSP mechanism is enabled. Additionally, steps {1.d, 1.e, 1.f} must be repeated to gather the revocation information of the CMTS certificate that needs to be sent inline when executing BPI+ V2.

3. Deployment Examples

As we have seen, DOCSIS 4.0 offers a series of new security features that can be independently enabled to lower the network's security risks. This section provides an overview of one of the possible paths to DOCSIS 4.0 deployment. We start by providing considerations on how to support D4.0 devices in existing networks (such as DOCSIS 3.1 or earlier) and then we focus on the impact of enabling the new security features when deploying new DOCSIS 4.0-enabled networks. The envisioned architecture is depicted in Figure 4 where it is assumed that the CMTS (i.e., or where the functionality is provided such as the CCAP Core or MAC-NE elements in distributed architectures) does not have direct access to external services. In this architecture, the CMTS can route all the HTTP request for CRLs and OCSP processing via the HTTP Proxy where strict access rules can be easily enforced.

Additionally, to improve network reliability, operators may deploy local OCSP Proxies and/or responders that can directly sign (or cache) valid responses locally. This solution can be used not only to improve the network reliability, but also to provide support for locally managed revocations that are specific for the operator's ecosystem such as tracking (permissive policy) or reject (strict policy) cloned or otherwise potentially compromised devices.

Figure 4 - Example Deployment with revocation checking support and local overrides



3.1. Preparing Your Networks for D4.0 CMs

To prepare the network for operating with DOCSIS 4.0 devices, there are important details that operators need to be aware of for successful deployments planning.

In Section 2.2, we discussed the additions made to DOCSIS 4.0 certificates when compared to DOCSIS 3.1 or earlier profiles (or configurations). It is therefore evident why DOCSIS 4.0 certificates are bigger in size than their DOCSIS 3.1 equivalent.

Because of the increased size of the certificates, even BPI+ V1 messages might hit the software limit imposed on the size of BPKM messages (1490 bytes)[2]. The relaxation of the software limitation on BPKM messages is needed to enable the use of a common certificate when operating in DOCSIS 4.0 and DOCSIS 3.1 modes. Although this choice lowers devices cost because of the use of a single certificate, in some cases DOCSIS 3.1 CMTS-es might require a software update to enable processing BPKM messages that are larger than 1490 bytes. It is important to notice that the same issue does not affect pre-D3.1 backward compatibility: the common certificate cannot be used in this case, and, exactly as for DOCSIS 3.1 devices, a separate certificate issued from the 1st Gen DOCSIS PKI (i.e., the "legacy" PKI) is still needed

When operators are ready to offer higher speed tiers and additional services that come with it, networks can be upgraded by deploying new DOCSIS 4.0 CMTS (or their DAA equivalent), thus enabling new speeds and the possibility to upgrade the security features, if needed, at a later time. Let's see how.

[2] The software limit stems from limitations in the frame size of DOCSIS 3.0 MAC and Phy layers that was wrongly directly imported in the DOCSIS 3.1 specifications without any update.

3.2. Upgrading Speeds, Not Security

When the time is right for a network upgrade, new DOCSIS 4.0 CMTS services can be enabled on the network. Besides the needed work to configure and upgrade the PHY layer to be able to deliver the new speeds, DOCSIS 4.0 does not require any changes from the currently used deployment model when it comes to security.

In previous Sections of the paper, we have shown how DOCSIS 4.0 networks can be configured to leverage the same authentication protocol used in DOCSIS 3.1 (and previous) networks (i.e., BPI+ V1) and how, additionally, it is possible to duplicate the existing networks configuration for revocation checking in the new environment. The combination of these two controls allows DOCSIS 4.0 deployments to leverage new speeds without requiring changes in NetOps because of security: a feature aimed at ease the transition, on the operator's time, to more secure options.

In other words, only when and if new security features are needed (i.e., PFS or MA), operators may decide to enable the use of BPI+ V2 according to their own deployment plans and schedule.

3.3. Enabling Advanced Security Features With BPI+ V2

During the development of DOCSIS 4.0, the need for providing trusted networks where the identity of the network is validated was quite evident: not only the use of a network identity enables more secure authentication and privacy options, but it also introduces the concept of authenticated and trusted networks that is the basis on top of which networks can offer trusted services. The need for trusted networks, combined with the need to mitigate new attack vectors related to new distributed deployment models, are some of the core reasons for enabling the new BPI+ V2.

When the new authentication protocol is enabled, a new set of controls is available to the operator via the configuration of the Persistent Security Attributes (PSAs). PSAs are stored in the secure memory of the CM and allow operators to further restrict accepted network/CMTS identities and protocol's versions during authentications (i.e., via the `Allowed-BPI-Versions` TLV) and are used to implement the downgrade protection mechanisms for BPI+. Additionally, PSA attributes are used to restrict what is considered valid with respect of network identities by requiring, in the CMTS certificate, the presence of specific values. For example, it is possible to configure a CM to only accept "Operator A" as the Organization field (O) in the certificate's subject name by using the `CMTS-Designations` TLVs in the Auth Reply message from the CMTS.

Enabling BPI+ V2, however, requires the provisioning and management of the CMTS certificate as discussed earlier. This means that managing CMTS (only when BPI+ V2 is enabled) will require supporting a new set of operations: from requesting the initial certificate (if not already installed by the Vendor) to regularly renewing it before expiration (i.e., once every 5 years). Although not part of DOCSIS 4.0 specifications, it is expected that automated certificate renewal protocols and tools will be developed and integrated with the increased enablement of BPI+ V2 across networks.

3.4. Enabling Revocation Checking and DOCSIS 4.0

As discussed throughout the paper and specifically in Section 2.4, DOCSIS 4.0 allows for very flexible configurations when it comes to revocation status checking. In fact, it is important to notice how enabling or disabling revocation status checking can be done independently from enabling or disabling the use of BPI+ V2. This capability is the key for empowering operators to choose the deployment path that is more relevant for their networks today and their upgrade path(s) tomorrow – even if they need to change it

during execution. In other words, because of the different options available in DOCSIS 4.0, revocation checking should not be considered a limiting factor for its deployment.

This said, because revocation checking has not been widespread enabled in the broadband community, enabling support for it (especially when requiring CMs to check revocation status of CMTS certificates) should be carefully planned and might require additional infrastructure services such as HTTP proxies or local OCSP responders as depicted in Figure 3.

4. Acknowledgments

The work described in this paper is the ultimate result of the contributions to DOCSIS 4.0 design and specifications from the whole community. We would like to recognize the many great contributions from both the Operators and the Vendors community without which DOCSIS 4.0 could not have happened. We would also like to recognize the continuous support and commitment to the DOCSIS 4.0 SEC WG activities from Ali Negahdar, Colin Dearborn, Dan Torbet, David Taylor, Margo Dolas, Jeff DeMent, Jeff Finkelstein, Owen Parsons, Onur Zengin, Pawel Sowinski, Philip Anderson, Ramy Elmoneiry, Sasha Medvinsky, and Satish Mudugere.

5. Conclusion

In this paper, we provide an overview of the many new security features in DOCSIS 4.0 with particular attention to the impact of its deployment on existing and new networks.

After a brief introduction where we describe the history of DOCSIS security together with considerations about new deployment models, the paper continues with a description of the security principles adopted in DOCSIS 4.0 and how they address new possible threats when considering distributed architectures. In particular, we have seen how DOCSIS 4.0 can be deployed by using the same authentication protocol and procedures that are in use in today's DOCSIS 3.1 networks and how operators can enable existing and new features by enabling BPI+ V2.

When it comes to revocation status checking, we also provided important considerations on how to support efficient revocation checking and described how to support different degrees of enforcement (i.e., strict vs. permissive policies).

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).

Abbreviations

3GPP	3rd Generation Partnership Project
AES	Advanced Encryption Standard
AIA	Authority Information Access
AK	Authorization Key
BPKM	Baseline Privacy Key Management
BPI	Baseline Privacy Interface
BPI+	Baseline Privacy Interface Plus
CA	Certificate Authority

CCAP	Converged Cable Access Platform
CM	Cable Modem
CMTS	Cable Modem Termination System
CRL	Certificate Revocation Lists
CVC	Code Verification Certificate
DOCSIS	Data Over Cable Service Interface Specification
EAE	Early Authentication and Encryption
EKU	Extended Key Usage
ESP	Enhanced Secure Provisioning
FMA	Flexible MAC Architecture
FS	Full Security
FWAH	Firmware Authentication Header
HFC	Hybrid Fiber-Coaxial
HMAC	Keyed-Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
KEK	Key Encryption Key
MA	Mutual Authentication
MAC	Media Access Control
MAK	Message Authentication Key
MD5	Message-Digest algorithm 5
MDD	MAC Domain Descriptor
MITM	Man-In-The-Middle
MMM	MAC Management Message
MSO	Multiple Systems Operator
NetOps	Network Operations
NetSecOps	Network and Security Operations
NIST	National Institute of Standards and Technology
NRI	No Revocation Information
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PFS	Perfect Forward Secrecy
PKI	Public Key Infrastructure
R-PHY	Remote PHY
R-MACPHY	Remote MACPHY
RMD	R-MACPHY Device
RPD	Remote PHY Device
RSA	Rivest, Shamir, Adleman (a public key cryptographic algorithm)
SA	Security Association
SCTE	Society of Cable Telecommunications Engineers
SHA-1	Secure Hash Algorithm 1
SHA-256	Secure Hash Algorithm 256-bit
SSD	Secure Software Download
SSH	Secure Shell
TEK	Traffic Encryption Key
TFTP	Trivial File Transfer Protocol
TLV	Type/Length/Value
ToD	Time of Day
TOFU	Trust on First Use

URL	Uniform Resource Locator
ZTN	Zero Trust Networks

Bibliography & References

[SP-SSI] MCNS Data Over Cable Security System Specification SP-SSI-I01-970506 (SP-SSI) May 6, 1997. Cable Television Laboratories, Inc.

[RSMI] MCNS Cable Modem Removable Security Module Interface Specification SPRSMI01-970425 April 25, 1997. Cable Television Laboratories, Inc.

[BPI] Data-Over-Cable Service Interface Specifications 1.0, Baseline Privacy Interface Specification, SP-BPI-C01-011119, November 19, 2001. Cable Television Laboratories, Inc.

[BPI+08] Data-Over-Cable Service Interface Specifications, Baseline Privacy Plus Interface Specification, CM-SP-BPI+-C01-081104, November 4, 2008.

[MULPIv4.0] Data-Over-Cable Service Interface Specifications, DOCSIS 4.0 MAC and Upper Layer Protocols Interface Specification, CM-SP-MULPIv4.0-I05-220328, March 28, 2022, Cable Television Laboratories, Inc.

[SECv3.0] Data-Over-Cable Service Interface Specifications 3.0, Security Specification, CM-SP-SEC3.0-I16-160602, June 2, 2016, Cable Television Laboratories, Inc.

[SECv3.1] Data-Over-Cable Service Interface Specifications 3.1, Security Specification, CM-SP-SECv3.1-I10-2111110, November 11, 2021, Cable Television Laboratories, Inc.

[SECv4.0] DOCSIS 4.0 Security Specification, CM-SP-SECv4.0-I04-220328, March 28, 2022, Cable Television Laboratories, Inc.

[Pala21] Massimiliano Pala. Enabling Encryption and Algorithm Revocation for Pos-Quantum DOCSIS Certificates. SCTE Cable-Tech Expo, September 2021.

[OSSL] The OpenSSL project. https://www.openssl.org

[OCAOD] The OpenCA OCSPD project. https://www.openca.org

