CableLabs®

PKI Onboarding and Delivery Process

CableLabs PKI Operations

January 21, 2025

CableLabs®

Table of Contents

Introduction

CableLabs is the exclusive public key infrastructure (PKI) provider for DOCSIS, PacketCable, DPoE and OpenCable. CableLabs manages and issues production certificates to ensure that devices and systems meet security, encryption and data integrity standards.

If you are ready to place an order, submit the necessary documentation and details to CableLabs PKI Operations team at pkiops@cablelabs.com (See the list below under Ready to go?)

If you are looking for more information, let's walk through the following questions:

Getting Started

This is the first time ordering certificates. What do I do?

If this is your first time, you will need to complete a Digital Certificate Authorization Agreement (DCAA), which details information about your organization that we'll need to issue you certificates. The DCAA can be found on the CableLabs Security Library page.

Depending on the types of certificates you want to purchase, you may need to complete additional document. See the complete list below under Ready to go? .

It has been more than 12 months since I last ordered certificates. What do I need to do?

If it has been more than 12 months since you last ordered certificates AND you did ***not*** renew your account, you will need to first complete the renewal. Please contact the PKI Operations Team (pkiops@cablelabs.com) if you need to renew your account.

Also, if your company contacts have changed (e.g. a new admin or corporate contact, you will need to submit those updates via the Contact Change Form which is available on the CableLabs Security Library page.

Types of Certificates

What type of certificates are available?

Depending on your device's capabilities, you may need one of the following certificates. Generally, the certificates can be grouped into either legacy PKI or the DOCSIS New PKI. The legacy certificates are non-date nested (e.g. device certificate can exceed the date of the issuing or root CA), use smaller key sizes and earlier algorithms/protocols. The New PKI certificates are date nested (e.g. expiration of the device certificate cannot exceed the expiration of the issuing and/or root certificate), use larger key sizes and more modern algorithms.

DOCSIS 3.0 (D3.0)

D3.0 certificates are needed on **ALL** cable modem devices, regardless of the specification (including DOCSIS 4.0). The D3.0 certificates use a legacy PKI specification, which is not compatible with the New PKI specification. Some operators still operate their network using D3.0 and require a D3.0 PKI certificate to authenticate the device with their network.

Note: Starting in January 2025, a new D3.0 CA will be available with an expiration date in 2124. This will allow providers to continue to issue D3.0 device certificates after the existing D3.0 CA expires between July 2029 and June 2036, depending on the CA partner. For more details on this change, please contact PKI Ops (pkiops@cablelabs.com).

DOCSIS 3.1 (D3.1)

D3.1 certificates are needed on cable modems which are compliant with the DOCSIS 3.1 specification. This includes devices which support more than 2 OFDM channels (e.g. products labeled as DOCSIS 3.1 Plus or D3.1+).

DOCSIS 4.0 (D4.0)

D4.0 certificates are needed for cable modems that are compliant with the DOCSIS 4.0 specification. The D4.0 certificates allow D4.0 devices to be backward compatible with D3.1 networks. This means that you ***do not*** need to install a D3.1 certificate on a D4.0 compliant device for it to authenticate with a D3.1 network.

PacketCable

PacketCable certificates are used to authenticate a cable modem device with telephony capabilities to the telephony system. PacketCable certificates are required in addition to the DOCSIS certificates listed above.

DPoE

DOCSIS Provisioning over Ethernet or DPoE certificates are used to authenticate ONU/ONT fiber devices with a DOCSIS provisioning system. There are two variations of this certificate: DPoE which is based on the legacy (e.g. DOCSIS 3.0) PKI and DPoE 2.0 which is based on the New PKI (e.g. DOCSIS 3.1 and later). These certificates ***cannot*** be used interchangeably. Please check with your customer as to which version is needed on their network.

OpenCable

OpenCable certificates are device certificates used to authenticate with legacy systems. They are primarily used today in video-on-demand systems or similar technology provided by the hospitality (i.e. hotel) industry.

If you have questions or needs for OpenCable certificates, please contact the PKI Operations team (pkiops@cablelabs.com).

R-PHY Server/AAA Server

A Remote PHY Device (RPD) must be able to operate in both authenticated and unauthenticated networks. In some cases, the RPD is in an untrusted network, and it must connect to devices inside the trusted network, which presents a potential security vulnerability. The R-PHY Server or AAA Server is introduced to provide authentication services to eliminate the potential security issues. The certificates on these devices facilitate the authentication process.

For R-PHY Server/AAA Server certificates, you will need to complete a Certificate Signing Request (CSR) and a Naming Document. If you need more details on creating a CSR file, See this handy reference.

CMTS and CCAP Core

Historically, the cable modem device authenticated itself with the CMTS in a one-way manner. With DOCSIS 4.0 and BPI+v2, the reverse process happens, where the CMTS authenticates itself with the cable modem (in addition to the cable modem authenticating with the CMTS (or Remote PHY device (RPD). As a result, the CMTS or the CCAP Core in DAA would need their own device certificates to authenticate with the cable modem in the same way the cable modem has a device certificate to authenticate itself.

There are two versions of these certificates: Full, which contain the revocation details like OCSP URL and CRL URL and Non-Revocation Information or NRI, which lacks these fields. Both are fully compliant with the specification and the determination of which one to use is up to the manufacturer and the operator.

The device certificates are issued from the same D4.0 CA as the cable modem certificates. Manufacturers will need to provide the MAC address, fully qualified domain name (FQDN) or another unique identifier when generating the certificate.

What type of certificate do I need?

This section outlines the PKI certificates needed for deployment in the associated devices or components of a DOCSIS network. The intention is to assist manufacturers in their purchasing process, depending on the expected deployment with their operator(s). This is not a comprehensive explanation of the authentication process between components; detail on this can be found in the associated specifications.

The protocols/specifications covered include DOCSIS 3.0, 3.1 and 4.0. It also covers both device certificates as well as code verification certificates. Figure 1 represents the components involved with authentication in a typical DOCSIS network with the cable modem connection directly to the CMTS. Figure 2 highlights a distributed access architecture (DAA) with the inclusion of a Remote PHY device (RPD) that is part of the authentication process.

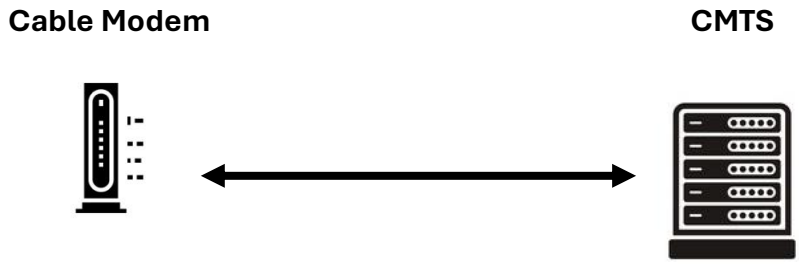

Figure 1 - Basic DOCSIS Components for Authentication

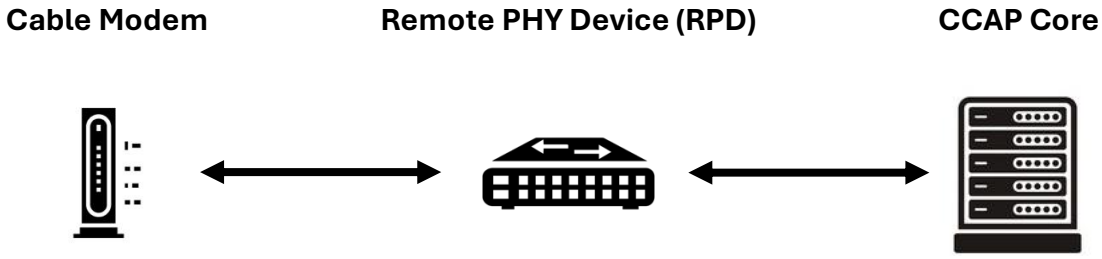

Figure 2 - DAA components for authentication

Table 1 below illustrates the PKI certificates needed by the given device/component in the network. The arrows between the components illustrate the authentication process, notably the device being authenticated (the "from" side of the arrow) and the device doing the authentication (the "to" side of the arrow).

For example, in the first row, the DOCSIS 3.0 cable modem (which has a D3.0 cable modem device certification and its associated issuing CA loaded on the device) is authenticated by the CMTS (which has the D3.0 Root CA loaded). In the last row, the D4.0 device would authenticate with the RPD (and Core) depending on the underlying protocol. The CCAP Core (with the D4.0 CCAP Core cert and associated issuing CA loaded on the device) authenticates with the D4.0 CM (which has the DOCSIS New PKI Root CA installed) at part of the BPI+v2.

DOCSIS 3.0, 3.1 and 4.0

Table 1 - DOCSIS Authentication Scenarios and Associated PKI Certificates

Configuration	Cable Modem		RPD		CMTS/CCAP Core
DOCSIS 3.0	DOCSIS 3.0 CM Device, Issuing CA	→		→	DOCSIS 3.0 PKI Root CA
DOCSIS 3.1 without RPD	DOCSIS 3.0 CM Device + Issuing CA	→		→	DOCSIS 3.0 Root CA
	DOCSIS 3.1 CM Device + Issuing CA	→		→	DOCSIS New PKI Root CA
DOCSIS 3.1 with RPD	DOCSIS 3.0 CM Device + Issuing CA	→			DOCSIS 3.0 Root CA
	DOCSIS 3.1 CM Device + Issuing CA	→	DOCSIS New PKI Root CA		
			DOCSIS R-PHY Device + Issuing CA	→	DOCSIS New PKI Root CA
DOCSIS 4.0 without RPD	DOCSIS 3.0 CM Device +Issuing CA	→		→	DOCSIS 3.0 Root CA
	DOCSIS 4.0 CM Device + Issuing CA	→		→	DOCSIS New PKI Root CA
	DOCSIS New PKI Root CA	←		←	DOCSIS 4.0 CMTS Cert + Issuing CA
DOCSIS 4.0 with RPD	DOCSIS 3.0 CM Device +Issuing CA	→		→	DOCSIS 3.0 Root CA
	DOCSIS 4.0 CM Device + Issuing CA	→	DOCSIS New PKI Root CA		
			DOCSIS R-PHY Device + Issuing CA	→	DOCSIS New PKI Root CA
	DOCSIS New PKI Root CA	←		←	DOCSIS 4.0 CCAP Core Cert + Issuing CA

PacketCable, EuroDOCSIS

Some devices/systems may require additional PKI certificates, depending on the functionality of the device. These are outlined in Table 2.

Table 2 - Additional Certificates for DOCSIS Devices

Configuration	Cable Modem		CMTS/Core
PacketCable	PacketCable Device, Issuing CA*	→	PacketCable Root CA

[*] Note: PacketCable certificates are required on eMTA/telephony devices in addition to the DOCSIS certificates noted above.

Configuration	Cable Modem		CMTS/Core
D3.0 EuroDOCSIS compatible	EuroDOCSIS Device, Issuing CA**	→	EuroDOCSIS Root CA
DOCSIS 3.1 EuroDOCSIS compatible	EuroDOCSIS Device, Issuing CA**	→	EuroDOCSIS Root CA
	DOCSIS 3.1 CM Device + Issuing CA	→	DOCSIS New PKI Root CA

[**] Note: The EuroDOCSIS PKI program is managed by Excentis/DigiCert (not CableLabs). To obtain EuroDOCSIS device certs, you will need to contact DigiCert directly.

What are EuroDOCSIS certificates and where do I get them?

EuroDOCSIS PKI certificates are to authenticate devices to networks where the operator is supporting EuroDOCSIS specification. While this mostly focuses on differences in the channel widths, frequency usage and power levels, it also includes a different PKI certificate. Generally, the EuroDOCSIS PKI is a "sibling" to the DOCSIS 3.0 PKI. Devices supporting EuroDOCSIS would authenticate with the EuroDOCSIS certificate, while a DOCSIS device would use the D3.0 certificate. For devices connecting to a DOCSIS 3.1 (D3.1) network, there is a single D3.1 certificate used (i.e. there is no "EuroDOCSIS 3.1" certificate).

The EuroDOCSIS PKI program is managed by Excentis/DigiCert (not CableLabs). To obtain EuroDOCSIS device certs, you will need to contact DigiCert directly.

What is a code verification certificate (CVC) and do I need one?

Code verification certificates (CVCs) are used to sign the firmware placed on the device and is used to verify the code during initial startup and during any secure software

download processes. CVCs are typically valid for 10 years. Details on current pricing can be found on the CableLabs Security Library page.

CVCs generally align with either the Legacy PKI (e.g. DOCSIS 3.0, PacketCable) or the New PKI (e.g. DOCSIS 3.1 and later). So, depending on your cable modem devices, you may need BOTH a DOCSIS 3.0 and DOCSIS 3.1 (or later) CVC. In general, the following rules would apply:

- DOCSIS 3.0 devices would require signing by a DOCSIS 3.0 CVC
- DOCSIS 3.1 devices could be signed by either a DOCSIS 3.0 or DOCSIS 3.1 CVC
- DOCSIS 4.0 devices would require signing by a DOCSIS 3.1 or later CVC.

Please note, DOCSIS 3.1 CVCs can be used to sign DOCSIS 4.0 firmware. However, DOCSIS 4.0 CVCs ***cannot*** be used to sign DOCSIS 3.1 firmware. Therefore, we suggest if you have both D3.1 and D4.0 compliant devices, you should acquire a D3.1 CVC and use it to sign both D3.1 and D4.0 firmware.

Please note: if you have an existing New PKI CVC (e.g. D3.1 or D4.0) and you need to renew it, we will need to align the *start* date for the validity with the original CVC cert. For example, if you CVC was issued in Mar 1, 20**15** and expires on Feb 28, 20**25**, we will need to align the new CVC to start on Mar 1, 20**15** and expire on Feb 28, 20**35**. To ensure we align this correctly, we will ask you to send us a copy of the ***public*** portion of the cert that we can verify.

For CVCs, you will need to complete a Certificate Signing Request (CSR) and a Naming Document. If you need more details on creating a CSR file, See this handy reference.

Do I need test certificates?

Test certificates are PKI certificates that are compliant to the specification but are issued from a non-production CA. THESE CERTIFICATES SHOULD NOT BE USED IN PRODUCTION DEVICES/SYSTEMS. Test certificates can be found on the CableLabs Security Library page.

Please note, new accounts are given 100 device certificates at no additional costs. These are full production certs that can be used during internal testing, Certification testing, etc.

Account and Certificate Fees

How much do certificates cost? How do I pay for them?

The latest pricing for PKI certificates can be found at here CableLabs Security Library page. If required, the PKI Operations team can provide a quote to your organization so you can issue a purchase order.

Payment is completed through a bank transfer. Payment details (bank details, routing information) can be found on the invoice issued to you with your order.

Is payment required to fulfill an order?

Yes, payment needs to be completed before the certificates will be released to you and/or your account. The PKI Operations team is notified once the payment has cleared and will notify you once the order is completed. (Note: depending on the location of the payment remittance, it may take a few business days to complete). Payment is also required before we will begin any annual account or CVC renewal or initial setup process.

What is the annual account fee for?

The annual account fee is charged for each certificate requesting account (CRA), which is associated with a given specification. For example, if you request certificates for D3.0 and D3.1, you will have two CRAs and would pay for two accounts on an annual basis. These fees are used to maintain your account on the third-party platforms such as Sectigo or DigiCert as well as the overall maintenance of the PKI program itself.

Will I be reminded to renew my certificate accounts or CVCs?

You will be reminded at 60 and 30 days prior to expiration that your certificate account is about to expire. We recommend that payment be sent 3 weeks prior to expiration to avoid a lapse in access. We do not currently send reminders for CVC expirations.

How do I know when my certificate account expires?

The only valid certificate expiration date is the date we provide to you at account setup and renewal. The dates listed in the different portals may not align with the actual renewal date. If you have questions regarding your renewal date, please feel free to ask us at pkiops@cablelabs.com.

Ready to go?

Please complete the following items and send them via email to pkiops@cablelabs.com.

If you are a new **CUSTOMER**:

- Complete and sign the DCAA from the CableLabs Security Library page.
- Complete and sign the necessary exhibits in the DCAA depending on the certificate types you need.
- If required by your organization, generate purchase order (PO) to be added to the invoice.
- Send an email with the above items attached to pkiops@cablelabs.com. If you are purchasing device certificates, please indicate the type and quantity of each certificate type (e.g. 25,000 DOCSIS 3.0, 10,000 PacketCable). If you hold accounts on multiple platforms (e.g. DigiCert and Sectigo), please also indicate which platform the order is to be fulfilled on.

If you are an **EXISTING** customer requesting a **NEW CERTIFICATE TYPE**:

- Complete and sign ONLY the necessary naming document from the DCAA (not the DCAA in its entirety) found on the CableLabs Security Library page.
- If required by your organization, generate purchase order (PO) to be added to the invoice.
- Send an email with the above items attached to pkiops@cablelabs.com. If you are purchasing device certificates, please indicate the type and quantity of each certificate type (e.g. 25,000 DOCSIS 3.0, 10,000 PacketCable). If you hold accounts on multiple platforms (e.g. DigiCert and Sectigo), please also indicate which platform the order is to be fulfilled on.

If you are an **EXISTING** customer **REORDERING** an existing certificate type:

- If required by your organization, generate purchase order (PO) to be added to the invoice
- Send an email to pkiops@cablelabs.com and indicate the type and quantity of each certificate type (e.g. 25,000 DOCSIS 3.0, 10,000 PacketCable). If you hold accounts on multiple platforms (e.g. DigiCert and Sectigo), please also indicate which platform the order is to be fulfilled on.

If you are requesting a **CVC** or **AAA Server Certificate**:

- Complete and sign the ONLY necessary naming document from the DCAA (not the DCAA in its entirety) found on the Security Library page.
- Create a CSR for the CVC. If you need more details on creating a CSR file, See this handy reference. Only send the ***public*** portion of the CSR. Keep the ***private key secure.***
- If this is a CVC renewal, include the public portion of the existing CVC with your request so we can verify and if necessary, align the start dates/time.
- If required by your organization, generate purchase order (PO) to be added to the invoice.
- Send an email to pkiops@cablelabs.com and indicate the type and quantity of each certificate type (e.g. 1 D3.1 CVC)

What happens next?

Once you submit the request and associated documentation, the CableLabs PKI Operations team will process your details to fulfill the order.

Your billing contact (as defined in the DCAA) will receive an invoice for the PKI certificate(s). **All orders must be paid before the order is fulfilled and delivered to you.**

If you are a new customer, we will need to do authentication of both the company and the organization. This typically takes 2-5 business days to complete. Please note that any delays in responding to authentication checks will delay the delivery of your order. Both administrative and corporate contacts should be aware that they will receive emails from the PKI Ops team and should respond to them promptly. Once authentication is

completed, the team will set-up admin account(s) on our partner portals, where users will issue certificates

For CVC requests, a formal ceremony is required and may take up to two weeks to be completed.

For device certificate orders, the balance will be added to your certificate requesting account (CRA) on the partner portal, where you can issue the device certificates. Instructions on using the partner portal can be found on the CableLabs Security Library page.