CableLabs® Certification Wave Requirements and Guidelines

June 2017   Revision 4.11

These Guidelines are for devices built to the Specifications for DOCSIS®, DPoE, EuroDOCSIS®, EuroPacketCable™, PacketCable™ and OpenCable™. For "verification" guidelines applicable to Unidirectional Digital Cable Products ("Plug and Play") devices built in accordance with FCC regulations, please see http://www.cablelabs.com/wp-content/uploads/2014/01/UDCP-Guidelines.pdf

Cable Television Laboratories, Inc.
858 Coal Creek Circle
Louisville, CO 80027-1266
www.cablelabs.com

TABLE OF CONTENTS

2

OVERVIEW

Working in cooperation with cable operators and cable equipment manufacturers, Cable Television Laboratories, Inc. ("CableLabs") has developed various specifications to facilitate the manufacture of interoperable cable devices used in the cable network ("Specifications"). The Specifications, and other information, can be found at www.cablelabs.com. Interoperable devices based on common specifications facilitate consumer choice, wide spread deployment of new technologies, and lower costs to both cable operators and consumers.

The Certification process defined herein has been developed to provide cable operators, retail distributors, and consumers' confidence that Certified products interoperate with products made by other manufacturers, and that the integrity and security of the cable operators' network is maintained. As used herein, "Certification" of devices for retail sale also covers "Qualification" of devices that are sold to cable operators. Manufacturers are required to internally test their products for conformance to the Specifications. CableLabs then performs independent audit testing to verify compliance with the Specifications. CableLabs has ownership of Certification programs, however compliance testing will be performed under contract to Kyrio, a wholly owned subsidiary and/or other 3rd parties based on the type of submission. Although testing is performed by the manufacturer, with audit testing by CableLabs, the benchmark for all devices is compliance with the Specifications. All Certification decisions are made by respective Certification Boards comprised of technical cable operator personnel.

Certification "Waves" are scheduled throughout the year to identify which specification and associated specification changes (ECNs) apply for each device submission. Please see the Certification Wave Schedule posted on our website for the appropriate ECN cutoff date associated with each Certification Wave. CableLabs manages different types of waves for Cable Modem based devices. A Fixed Wave submission has a fixed start and end date. A Flex submission allows the device to come in anytime during the wave. This is summarized in the following table:

	DOCSIS Device Type	Wave Start	Wave End
D3.0 Fixed Wave Submission	3.0 / 2.0	Fixed dates[1]	Fixed dates
D3.0 Flex Wave Submission	3.0 / 2.0	Anytime	Open
D3.1 Flex Wave Submission	3.1	Each Monday	Open

[1] See Certification Wave Schedule

The CableLabs Certification process determines equipment compliance with the Specifications. The Certification process does not test for performance, quality, or other subjective characteristics.

Non-Consumer Premises Equipment (non-CPE), e.g., cable network element devices such as CableCARDs or CMTS are determined to be "Qualified" rather than Certified because they are only purchased by cable operators and not the consuming public at retail. Similarly, certain test tools and other devices that are purchased only by cable operators and may present deviations from the "full" specification may be submitted to CableLabs for testing. These devices, if approved, will be labeled "Verified for Interoperability".

A separate process of "Verification" is performed for so-called "Plug & Play" devices; also called Unidirectional Digital Cable Products, or UDCPs. See http://www.cablelabs.com/wp-content/uploads/2014/01/UDCP-Guidelines.pdf

"CableLabs Certified®", "CableLabs Qualified™", or "Verified for Interoperability" means that the device has passed a series of tests for compliance with the applicable Specification, and has thus demonstrated interoperable functionality with other CableLabs certified devices. Manufacturers are encouraged to add additional functions and features to their devices to meet the requirements of

other industry specifications and standards. However, "CableLabs Certified®", "CableLabs Qualified™", or "Verified for Interoperability" should not be understood as an endorsement of these other attributes, or that the device is certified to such other specifications or standards. Such claims are solely the responsibility of the manufacturer making the additional claims. In addition, testing hereunder does not certify or indicate that the product is in conformance with FCC rules, any applicable license agreements, or the manufacturer's claims.

Unless otherwise specified, the terms certification, qualification, and verification are used indistinctively in the document. Similarly, unless explicitly specified, certified, qualified, and verified all share the meaning, certification board approved.

For purposes of clarification, the reference to Annex A is to devices compatible to the European channelization, aka EuroDOCSIS; as opposed to Annex B which refers to the North American, aka DOCSIS. CableLabs offers a Certification Program for both Annex A and Annex B devices.

1 PRODUCT SUBMISSION CATEGORIES

CableLabs has developed the following product submission categories to meet the needs of vendors and cable operators to speed the availability of products suitable for deployment in an end-to-end, interoperable, high-speed cable network.

1.1 Certification/Qualification Submissions

A product **MUST** be submitted for certification/qualification if any **one or more** of the following conditions apply:

1. Any product that has not achieved certification/qualification status for all the requested specification(s), including:
   - Products submitted for the first time for any of the requested specification(s).
   - Products that did not achieve certification/qualification status for any of the requested specification(s) in previous wave(s).
2. Any previously Certified product that has undergone major changes that are not acceptable under Recertification option. This may include, for example, changes to power supply, hardware (silicon, tuner, active components, etc.), software, or other major changes as determined at the sole discretion of CableLabs and the Certification Boards.

The product must have an applicable manufacturing label (color, logo, artwork, model number, etc.) as it will be marketed. It is intended these units should be of production quality, not pre-production quality. The model number must match the application form and the model, SW, and HW revs shown on the application must appear in the sysDescr field or "internal readout". Additionally, the submitted product must have a CableLabs Product ID label as outlined in section 4.6. This label must be clearly visible and readable (do not place this label on the bottom or port side of the unit). Please ensure the label is of satisfactory quality. The label should remain affixed to the units and printing should not deteriorate over the course of testing due to handling.

1.2 Recertification/Requalification Submissions

The following sections describe the different requirements and procedures for the recertification submissions. Each submission will be considered on a case-by-case basis based upon board approval and may be submitted at any time.

Unless explicitly addressed below, all requirements and guidelines for regular Certification Waves and submissions apply to Recertification submissions. A product **MAY** be submitted for recertification or requalification under the following condition:

Minor changes to a previously certified/qualified product may be presented to the Certification Board for consideration. Minor changes are determined through the sole discretion of CableLabs and its Certification Boards.
Vendors considering a recertification submission must submit a formal letter (including a signed statement from an Officer and/or Quality Assurance Manager) on Vendor company letterhead.

The letter should include:

1. The model number of the product and date the product was previously certified

2. Details of all changes from the previously certified product

3. Acknowledgement that Vendor has completed regression testing and has retained the test results

4. Acknowledgement that Vendor is able to provide such test results to CableLabs within one day of CableLabs' request

5. Acknowledgement that, based on such tests, Vendor in good faith believes that the product submitted for Recertification complies with the appropriate CableLabs specifications

Recertification submissions MUST be compliant to current specifications including ALL applicable ECNs. Resulting changes to the original software must be part of the document previously mentioned. CableLabs must receive the request via email at labs@kyrio.com.

1.3 Verified for Interoperability

Certain CPE devices and test tools that are purchased only by cable operators may be submitted to CableLabs for testing. These devices are not eligible to become certified because of specific, previously approved specification compliance exceptions; instead they must be submitted to be "Verified for Interoperability." Devices accepted for such testing currently include DSG eCMs, line power test tools, MDUs, and special DPoE devices, among others. A DSG eCM is a set-top device with embedded Conditional Access (CA) that includes an embedded cable modem (eCM) that complies with the requirements of the DSG specification.

Products that are "Verified for Interoperability" undergo a series of tests for compliance with the applicable Specification and demonstration of interoperable functionality with other CableLabs Certified, Qualified, and/or Verified for Interoperability devices. Functionality that is outside of the applicable Specification is not tested.

The product must have an applicable manufacturing label (color, logo, artwork, model number, etc.) as it will be marketed. It is intended that these units should be of production quality not pre-production quality.   The model number must match the application form; and the model, SW and HW revs shown on the application must appear in the sysDescr field or "internal readout". Additionally, the submitted product must have a CableLabs Product ID label as outlined in section 4.6. This label must be clearly visible and readable (do not place this label on the bottom or port side of the unit.) Please ensure the label is of satisfactory quality. The label should remain affixed to the units and printing should not deteriorate over the course of testing due to handling.

Vendors desiring to submit a product for "Verified for Interoperability" must complete the following a minimum of 30 days prior to submission:

1. Request Certification Board approval to submit.
2. Provide an executive summary detailing functionality included in the product, areas of non-conformance to the CableLabs specifications, and summary of why of the product is ineligible for certification and why "verified for interoperability" is being requested.
3. Describe any known limitations that will prevent testing in the CableLabs test environment.
4. Verified for Interoperability submissions will be considered on a case-by-case basis based upon board approval. Please contact us at labs@kyrio.com regarding submission details.

The submission process for "Verified for Interoperability" is the same as for a regular certification wave including its fees. The product will undergo a complete testing cycle except for the functionality explicitly excluded by the vendor and approved by the Certification board. If approved, the product will be added to the CableLabs website listing of "Verified for Interoperability" devices.

1.4   CMTS Qualification

CMTS Qualification testing has been designed to align with the way in which CMTSs are developed and deployed by cable operators: with an initial base set of features, followed by individual features as needed. This is referred to as CMTS Feature Set Testing, which permits the testing and Qualification of individual CMTS Features (as distinct from CPE Certification testing, which verifies compliance to the full specification). Note that there are some important differences in how CMTS Feature Set Testing is implemented for different versions and regional variants of DOCSIS, which is detailed in the sections that follow.

Within CMTS Feature Set Testing, CMTS vendors have the choice of applying either for Qualification or just for a report. These two outcomes are defined as follow:

1. **Feature Set Qualification (FQ):** CMTS devices submitted for Feature Set Qualification should fully support the Feature Set being submitted and tested for. At the completion of testing the results will be reviewed by the appropriate Certification Board, which will determine whether the device is awarded Feature Set Qualification status. If successful, the device will get listed as "Functionally Qualified" for the given functionality;
2. **Functional Report (FR):** CMTS devices that do not fully comply with the requirements of a given Feature Set, or for which the manufacturer does not want to have the Certification Board make a formal decision, may be submitted for a Functional Report. Upon the completion of testing, results are provided only to the manufacturer, and are only shared by CableLabs with members at the request of the manufacturer purely for informational purposes (no decision will be made). There is no label or listing associated with this option.

For the purpose of FQ, CableLabs creates and posts Compliance Checklists for each of the Feature-Sets listed below, which are then validated with the Certification Board. Notice that the testing conducted for a FR can be flexible, and is not limited just to the listed Feature Sets; in this case, the expected list of tests to be performed – and the number of test point equivalent fees (minimum one) – will be determined via discussion between CableLabs and the manufacturer.

The current fee schedule for CMTS Qualification submissions is posted on the Kyrio website; it can be found under the heading "Certification and Qualification Fees" at Kyrio Certification Testing. With the exception of DOCSIS 3.0 Annex A submissions (aka EuroDOCSIS 3.0), the testing is paid for with "Test Units", which can be purchased in bulk for a discount by manufacturers. Each Feature Set costs 1 or more Test Units, as detailed on the http://www.kyrio.com/testing-services/#certification-testing. Please note that all Test Units are valid for 12 months from the day of finishing the first report.

1.4.1 DOCSIS 2.0 (ANNEX B) Qualification program (aka North American DOCSIS 2.0)

For DOCSIS 2.0 compliant devices, only submissions for full compliance to the DOCSIS 2.0 specifications are permitted. No additional Feature Sets for DOCSIS 2.0 have been defined.

DOCSIS 2.0 CMTS Feature Sets	1. DOCSIS 2.0

1.4.2 DOCSIS 3.0 (ANNEX B) Qualification program (aka North American DOCSIS 3.0)

For DOCSIS 3.0 Annex B, the specification has been broken into several Feature Sets. CMTS vendors can apply for FQ or FR for any Feature Set independently of any other.

The following table includes all Feature Sets currently available for DOCSIS 3.0 (Annex B) Feature Qualification:

DOCSIS 3.0 CMTS Feature Sets	DOCSIS 3.0 CORE	1. D3.0_MAC_Base 2. PHY 3. DRFI 4. Provisioning (IPv4 & IPv6) 5. DSCB 6. USCB 7. Advanced QoS 8. Dynamic Operations 9. Security
	DOCSIS 3.0 additional sets	10. SCDMA 11. Multicast 12. EM1x1 13. OSS 14. Optional Features

"DOCSIS 3.0 CORE Qualified" will refer to devices that achieve FQ for D3.0 MAC Base, DRFI, PHY, Provisioning (IPv4 and IPv6), DSCB, USCB, Advanced QoS, Dynamic Operations, and Security under the same HW and SW. If they successfully complete Feature Qualification for these Feature Sets with the same hardware and software, an additional notation will be added to their listing on the Certified/Qualified list to indicate that achievement.

1.4.3 DOCSIS 3.0 (ANNEX A) Qualification program

For DOCSIS 3.0 Annex A (aka EuroDOCSIS 3.0), the specification has been broken into several Feature Sets. However, unlike with the DOCSIS 3.0 Annex B (aka North American DOCSIS 3.0) Qualification program, CMTS must be submitted for the "Base Feature Set" as a part of any Qualification submission, and can then also apply for one or more additional Feature Sets.

The following table includes all Feature Sets available for EuroDOCSIS 3.0 Qualification:

Base Feature Set	Topology resolution, SG discovery, fiber node configuration Cable modem (re)initialization (in IPv4) Downstream Channel Bonding, DSIDs Dynamic Channel Change CM-STATUS Legacy modem support All MIBs to support the above features
UCB	Upstream Channel Bonding, TCC assignment, continuous concatenation and fragmentation, queue depth requesting, multiple requests outstanding, SID clusters, all MIBs to support the above features

DBC	Dynamic Bonding Change operations, DBC-based load balancing If the UBC feature module is not supported, then only the downstream related DBC operations will be verified. All MIBs to support the above features
IPv6	CM provisioning (IPv6 only, dual stack, Alternate Provisioning Mode) CPE traffic, IPv6 SF classifiers and Upstream Drop Classifiers
Multicast	Multicast per 3.0 spec: Multicast DSID Forwarding, Source Specific, Multicast, Multicast QoS, and Authorization. If the IPv6 feature module is not supported, then only the tests in IPv4 will be done. All MIBs to support the above features
Security	Early Authentication and Encryption, AES Certificate Revocation Lists, Online Certificate Status, Protocol, TFTP proxy, Config file (name) learning, TFTP Options, Extended MIC. All MIBs to support the above features
S-CDMA	All S-CDMA functionality All MIBs to support the above features.
OSS	Diagnostic Log Enhanced Signal Quality Monitoring, IPDR All MIBs to support the above features
LI	Lawful Intercept functionality

CMTSs that pass the requirements for the features submitted for testing will get the label "verified for" together with the list of feature groups that the submitted CMTS passed. Since passing the Base Feature Set is always a minimum requirement, no product can pass other feature groups if the Base Feature Set is failed.

On the EuroDOCSIS participants portal of the InfoZone, a document is available that provides a mapping of the 3.0 ATPs to the different feature sets: https://community.cablelabs.com/wiki/pages/viewpage.action?pageId=121667968 in the European Certification Information section.

1.4.4 DOCSIS 3.1 Qualification program

For DOCSIS 3.1, the specification has been broken in several Feature Sets. A DOCSIS 3.1 CMTS must pass "DOCSIS 3.1 Base" Qualification before it can be Qualified for any additional Feature Sets. After achieving Base Qualification, the device does not have to be re-submitted for "DOCSIS 3.1 Base" Qualification with each subsequent Feature Set submission, so long as the same hardware is used. The device may be submitted for additional Feature Sets concurrently with Base or at a later time.

The following table includes all Feature Sets available for DOCSIS 3.1 CMTS Qualification:

DOCSIS 3.1 CMTS Feature Sets	DOCSIS 3.1 BASE	1. Minimum viable product for field deployment
	Additional Feature Testing available	2. Downstream PHY & DSCB 3. Upstream PHY & USCB 4. Advanced QoS 5. Dynamic Operations (includes Profile changes, DBC, DCC, DPD Change, DSX, UCD Change) 6. Multicast 7. Security 8. EM (includes EM1x1 & DLS) 9. OSS 10. Fault Conditions (includes CM-STATUS) 11. PNM 12. Profile testing & Probing

1.4.5 PacketCable 1.5 Qualification program

For PacketCable 1.5 Qualification testing, the specification has been broken in several Feature Sets. For DOCSIS 3.0 Annex B devices *(aka North American DOCSIS 3.0)*, the CMTS may be submitted for Qualification of any one or more of these Feature Sets independently of any other. For DOCSIS 3.1 devices, the CMTS must first be qualified for "DOCSIS 3.1 BASE" and "Advance QoS" before it can be qualified for any PacketCable 1.5 Feature Sets.

The following table includes all Feature Sets available for PacketCable 1.5 Qualification:

PacketCable CMTS Feature Sets	1. PC-DQoS 2. PC-SEC 3. PC-CALEA 4. PCMM 5. PC-EM

1.4.6 Modular Headend Architecture Qualification program

For CMTS devices that comply with one or more of the Modular Headend Architecture specifications, they may be submitted for Qualification of any one or more of those specifications independently of any other Qualification submission.

The following table includes the Feature Sets currently available for MHA Qualification:

Modular Headend Architecture	1. VSI 2. DTI 3. DEPI

1.4.7 Qualification program for DOCSIS Independent Feature Sets

There are additional specifications for which a DOCSIS CMTS may be tested for Qualification compliance. A CMTS may be submitted for Qualification of any one or more of these specifications independently of any other Qualification submission. The following table includes the Feature Sets that are independent of the DOCSIS variant of the CMTS that are available for Qualification:

DOCSIS Version Independent Features	1. L2VPN 2. DSG 3. CBI

1.5 Paper or OEM Certification

Submissions for Paper and OEM have the same requirements; however:

- Paper Submissions apply when the manufacturer is under the same name and branding as the original device.
- OEM Submissions are for devices that are from manufacturers who resell another company's product under their own name and branding.

Manufacturers may request that their Device (other than OpenCable devices, which have their own requirements as detailed in Section 1.6) be submitted for a Paper/OEM Certification if they meet all the following conditions:

- Identical software as certified/qualified product
- Identical hardware as certified/qualified product
- Identical docsDevSwCurrentVers as certified/qualified product (for DOCSIS cable modem products)

The **only** acceptable differences permitted between the certified/qualified product and the Paper/OEM submissions are the System Descriptor (sysDescr), and the product OUI (vendor portion of the MAC address).

The sysDescr of the submitted device may be changed from that of the originally certified device, enabling differentiation between products. In addition, a device could use an "on the fly" method to compile the sysDescr. For example, the method can consist of implementing code in the software image that would compose the contents of the sysDescr MIB "on the fly." In this case, certain

fields would be obtained from the software image (such as the software version), while others could be obtained from non-volatile memory, set at the time of manufacture (such as hardware version or vendor name).

Paper/OEM submissions may be made at any time and are not tied to any specific Certification Wave. A request to submit must be approved by the Certification Board prior to the actual submission. Acceptance of a Paper/OEM submission is not a guarantee of achieving certified status.

Note that if the Certification Board has requested specific fixes for the original Certified device, that device is not eligible for an OEM/Paper submission.

1.6 Paper Certification for OpenCable Devices

A product may be submitted for OpenCable Paper Certification under the following conditions:

- Minor changes to a previously certified product may be presented to the Certification Board for consideration. Minor changes are determined at the sole discretion of CableLabs and its Certification Boards.
- Software maintenance upgrades or a new code version of a previously certified device that consist of changes representing functionality entirely outside the scope of the then-current Specifications.
- Host devices with different model numbers submitted in the same Certification Wave. The first product submission will require full certification testing. For **concurrent** submissions in the same Certification Wave with no hardware or software changes, but with different screen sizes or power supply, a paper submission may be submitted along with two devices for regression testing.

Vendors may make and distribute Certified Host Devices with such minor changes concurrently with submission for Paper Certification; provided that Vendor acknowledges that any upgrades made to Certified Host Devices prior to the grant of Paper Certification shall be undertaken at Licensee's sole risk and Licensee will remain responsible for any breach of applicable license agreements, Compliance Rules, Robustness Rules, and Specifications.

Paper Certification is not associated with a particular Certification Wave, may be submitted at any time, and will be evaluated independently of the regular certification wave testing schedule. Paper Certification submissions will be considered on a case-by-case basis, based upon Certification Board approval. Applications will be evaluated within two to three weeks of submission. If approved, the product will be added to the CableLabs website listing of certified products. If not approved for paper submission, applicant may submit under the other submission categories described in this section. Please contact us at labs@kyrio.com regarding submission details.

Vendors considering a Paper Certification must complete and have a company officer sign the Paper Certification Application, which is available through the online admission application. The application includes affirmative statements that:

- Vendor has completed testing under the then-current test suite and test plan, and has retained the test results;
- Vendor is able to provide such test results to CableLabs within one day of CableLabs' request;
- Based on its own test results, Vendor in good faith believes that the product submitted for Paper Submission complies with the appropriate Specifications.
- Vendor confirms the availability of one (1) unit of the upgraded device for audit testing at CableLabs' request.

1.7 "Self Certification" for OpenCable Devices

Certification testing for OCAP/tru2way devices ended June 30, 2014. Only Licensees that have obtained "Self Certification" status prior to June 30, 2014 will be considered for "Self Certification."

Licensees who have demonstrated that they are consistently capable of obtaining Certification of OpenCable Host Devices may apply for Self Certification status. Subject to the conditions of this section, successful Certification of three (3) unique Host Devices in three (3) separate CableLabs Certification Waves within a two (2) year period, together with no Certification failures or breaches of the applicable Agreements (CHILA, OCAP, tru2way) over a two (2) year period, shall serve as *prima facia* evidence of such capability. After successful Certification in a third Certification Wave, Vendor may apply to the Certification Board for Self-Certification status by written request. Once granted, the Certification Board may revoke Self-Certification status for any material breach of the applicable Agreements. The Self-Certification election is optional under the sole discretion of the Vendor, who may, notwithstanding the acquiring of the Self-Certification status, continue to use CableLabs Certification.

For Self Certification of an OpenCable Host Device, see the Self Certification Submission Form available in the online-application form: https://www.cablelabs.com/newpst/login.php.

1.8   Practice Run Submissions

Practice Run product submissions may be made at any time, without correlation to a specific Certification Wave. A product submitted for a Practice Run is tested under the following conditions:

- All Certification/Qualification submission guidelines apply to Practice Run submissions (including the fee structure).
- Practice Run submissions are tested the same way and at the same time as product submitted for Certification/Qualification.
- Failing results are provided as they occur, after they are verified. All collected test results will be provided at the end of the wave.
- Practice Run products are allowed to upgrade software only one time during the Certification Wave. The upgrade must be completed prior to the end of the wave, and vendors must identify which tests they would like to run after the upgrade, as we cannot guarantee that a complete set of tests will be executed.
- We will discuss any test results at the end of the wave cycle, when testing is complete.
- Practice Run test results may be shared with the respective Certification Boards for information only.
- Practice Run submissions are not eligible for Certification/Qualification decision by any Certification Board.

1.8.1 Converting from Certification/Qualification or Recertification/Requalification to Practice Run

- A product submitted to a Certification Wave for Certification/Qualification or Recertification/Requalification may switch to "Practice Run" at any time during the wave.
- The "Practice Run" product may upgrade one time. This is the only opportunity to perform a software upgrade on the product.
- CableLabs, at its discretion, will complete as much testing as possible and will attempt to honor a single request for a specific prioritized list of tests to be conducted.
- The "Practice Run" product will no longer be eligible to receive a Certification/Qualification decision by the Certification Board, and all other Practice Run submission considerations will apply.
- A product submitted for Practice Run may not be transitioned to Certification/Qualification status during a Certification Wave.

2 SPECIAL TESTING CONSIDERATIONS

2.1 Combined (add-on) Product Certification

DOCSIS based devices submitted for Certification of compliance can apply for additional specifications as "add-ons". Add-on Certifications are currently available for PacketCable, L2VPN, and Cable Gateway. A DOCSIS based device may be submitted for one or more add-ons, in any combination.

For example, an EMTA can also be submitted for L2VPN Certification, a CM can be submitted for Cable Gateway Certification, and so on.

A device must pass DOCSIS Certification in order to be eligible for Certification of any submission add-ons. All add-ons pass or fail independently of each other at the Certification Boards' discretion.

2.2 Results During the Wave

Kyrio, on behalf of CableLabs, will provide updates throughout testing. Final results will be provided after the Certification Board decision. The vendor will be notified of all failures and will be provided with associated data. Kyrio may also provide additional information to follow-up questions as needed. Kyrio will continue testing regardless of failures unless the vendor requests that Kyrio stop during their evaluation. Any issues that require troubleshooting could impact the expected schedule.

2.3 Failures Resolution Process

The following options are available for vendors who have devices exhibiting one or more failure during testing. Note that these processes may result in delays in the test schedule and the certification process.

2.3.1 Troubleshooting a Failure

During testing, when a failure is identified, our test team will work with the vendor to understand the scope of the failure. During the troubleshooting process, the vendor may update their software to determine whether a change addresses the issue found. CableLabs may, with vendor approval, share the existence of any working solution to the Certification Board. However, please be aware that if an update is not tested as per the process in Section 2.3.2 below, the Certification Board will still be making their decision based on the submitted version and associated results.

2.3.2 Device Update Process

Vendors may elect to update their device during a wave to resolve issues that have been reported during Certification Testing up to that point. This is referred to as the Device Update Process. If a vendor takes advantage of the Device Update process, all testing from that point forward will be conducted using the updated device; in addition, some amount of regression testing will also be conducted on the updated device.

Device updates may consist of software and/or hardware changes to the submitted device; however, the Certification Board must approve hardware changes in advance.

Note that exercising the Device Update Process will adversely impact the test schedule for your device.

2.3.2.1 Device Update Process Eligibility for D3.0 (Annex B) CPE devices (aka North American DOCSIS 3.0)

DOCSIS 3.0 (Annex B) CPE devices submitted for full Certification are eligible for this process if requested by the vendor during the first six (6) weeks of testing; devices submitted for Recertification are eligible for this process if requested by the vendor within the first two (2) weeks of testing. This process can only be utilized one time for a given submission. Failures will continue to be reported throughout the test cycle. Devices that are no longer eligible for the Device Update Process are eligible to perform a Resubmission for the appropriate fee.

2.3.2.2 Device Update Process Eligibility for D3.0 (Annex A) CPE devices (aka EuroDOCSIS 3.0)

DOCSIS 3.0 (Annex A) CPE devices submitted for full Certification are eligible for this process if requested by the vendor within the first four (4) weeks of testing; it is not applicable for Recertification submissions. This process can only be utilized one time for a given submission. Failures will continue to be reported throughout the test cycle. Devices that are no longer eligible for the Device Update Process are eligible to perform a Resubmission for the appropriate fee.

13

2.3.2.3   *Device Update Process Eligibility for DPoE equipment (ONU and OLT)*

DPoE devices submitted for full Certification are eligible for this process if requested by the vendor during the first six (6) weeks of testing; devices submitted for Recertification are eligible for this process if requested by the vendor within the first two (2) weeks of testing. This process can only be utilized one time for a given submission. Failures will continue to be reported throughout the test cycle. Devices that are no longer eligible for the Device Update Process are eligible to perform a Resubmission for the appropriate fee.

2.3.2.4   *Device Update Process Eligibility for D3.0 (Annex B) CMTS equipment*

DOCSIS 3.0 (Annex B - aka North American DOCSIS 3.0) CMTS devices submitted for Feature Qualification testing may be updated one time during the wave for no charge at any time before testing is completed. After the first update, or after testing is completed, any updates require a new Feature Set Qualification submission.

2.3.2.5   *Device Update Process Eligibility for D3.1 CPE devices*

During testing of DOCSIS 3.1 CPE devices submitted for DOCSIS 3.1 Certification, a manufacturer may apply for an update at any time. Any failure(s) found during Core testing will require an update. For any failures found during secondary testing, the vendor may update at their discretion. All updates/resubmissions may consist of software and/or hardware changes to the submitted device. However, for updates (beyond the core test set) the Certification Board must approve hardware changes in advance.

Regression testing will be conducted in all cases at the discretion of CableLabs and the Certification Board.

2.3.2.6   *Device Update Process Eligibility for D3.1 CMTS equipment*

DOCSIS 3.1 CMTS devices submitted for DOCSIS 3.1 Base Qualification are eligible to be updated at any time during Qualification testing. These updates (if any) will be free of charge. Regression testing will be conducted in all cases at the discretion of CableLabs and the Certification Board. Failures will continue to be reported throughout the test cycle. The intent of this process is to allow vendors to continue to update their devices until they are able to pass Base Qualification.

DOCSIS 3.1 CMTS devices submitted for DOCSIS 3.1 Feature Qualification are also eligible to be updated at any time for no fee, but only FOR A LIMITED TIME; the expiration of this process will be announced via the appropriate reflector in advance of the expiration date.

2.4   Resubmission of Failed Devices

Devices that fail the certification process may be resubmitted within 30 days of the board decision for the cost of the resubmission fee. These products may be resubmitted to the same wave, without consideration of new ECNs.

2.5   Resubmission after a Practice Wave

Devices that complete a wave under the practice wave program may be resubmitted within 30 days for the cost of the resubmission fee. These products may be resubmitted to the same wave, without consideration of new ECNs.

2.6   Resubmission of Retained Headend Devices

A vendor may resubmit retained headend hardware units for qualification testing if the following conditions are met:

- The retained headend hardware is a CMTS or an EQAM.
- The retained hardware will be submitted along with the new software.
- There is a reliable mechanism to change (upgrade/downgrade) the software images on the retained hardware.
    - The special instructions of the submitted product must include a detailed description of the mechanism to switch between the two software images.
    - CableLabs will hold copies of both the previously qualified and the newly submitted software images.
    - The vendor must successfully demonstrate to CableLabs' personnel the mechanism and procedure to switch between the two software images held by CableLabs.
- If the submitted hardware requires any changes to auxiliary hardware components, then there must be a reliable mechanism to change (upgrade/downgrade) the auxiliary hardware components.

- - The special instructions of the submitted product must include a detailed description of the steps to switch the auxiliary hardware components.
  - CableLabs will hold both the retained and the newly submitted auxiliary hardware components.
  - The vendor must successfully demonstrate to CableLabs personnel the mechanism and procedure to switch between the auxiliary hardware components.
- The application for the newly submitted product shows the "hardware revision" of the retained hardware.
- In addition to using the retained hardware, vendors may need to submit additional hardware units to fulfill the number of units required for submission.
  - Qualification submissions: Most product submissions will require a vendor to supply between 1 and 4 additional units.
  - OEM or Paper submissions: Most product submissions will not require additional units; however, in some cases a vendor may need to supply one additional unit.
  - Upon qualification, the current retention policy will apply.

3 APPEALS PROCESS

The Certification Board will consider appeals for products that do not achieve Certification.

For a valid appeal, the vendor must follow these steps, in the order listed:

1. After the Certification Board(s) decision, participate in an optional conference call with Kyrio technical staff for detailed discussions of test results. Kyrio will schedule this call at the request of the vendor.

2. If the conference call does not resolve all questions about why the product did not achieve Certification, Kyrio will schedule an optional visit (at a mutually agreed time) for the vendor to view the results of tests performed.

3. If the vendor believes there are grounds for an appeal, the vendor may submit a formal appeal request to CableLabs, **complete with backup data to document any test results the vendor believes the Certification Board should consider**. The formal appeal and backup data will be forwarded to the Certification Board(s) for review.

4. The appropriate appeals fee equivalent to the recertification fee must accompany the formal appeal request. The fee will be refunded to the vendor if the Certification Board(s) grants the appeal.

5. The deadline for filing an appeal to the Certification Board(s) must be completed within 10 business days of the vendor notification of the Certification Board(s) decision.

The Certification Board(s) will evaluate appeals fairly and in a non-discriminatory manner. The Certification Board(s) may request whatever additional information or tests from the vendor and/or CableLabs it deems necessary to resolve the issue on appeal.

 CableLabs will communicate the decision of the Certification Board to the appealing vendor. Vendors should be aware that, while the Certification Board makes every effort to act on a timely basis, it might take several weeks before any decision is reached on an appeal.

Devices will be retained until after the appeal process is completed so that additional testing and lab visits may be supported, as needed.

4   SUBMISSION REQUIREMENTS

4.1   Specification Compliance Requirements

Unless stated otherwise, CableLabs verifies compliance against the current version of the applicable Specifications for which the product is submitted.

The most recent, published version of CableLabs Specifications can be found on the CableLabs webpage applicable to the product in question. Issued Specifications undergo changes through an open Engineering Change Process involving Engineering Change Requests (ECRs), Engineering Change Orders (ECOs), and Engineering Change Notices (ECNs) as detailed on the applicable CableLabs webpage. Engineering Change Notices are considered to be part of the applicable Specification, even though they may not yet be included in a published version of that Specification.

Therefore, for purposes of compliance testing, CableLabs considers the current version of a Specification to consist of the most recent, published version of the Specification, as it appears on CableLabs' website, modified by any and all ECNs that are applicable for that Certification Wave as noted in the ECN.

To allow vendors an appropriate period to comply with Engineering Change Notices, the Certification Wave Schedule indicates a "Mandatory ECNs Accepted" cutoff date, typically 60 days before the start of a Certification Wave. ECNs that are accepted after the cutoff date are not considered mandatory for Certification/Qualification in the Certification Wave to which the date applies except in unusual circumstances, in which case an announcement will be made as far in advance of the Certification Wave as possible detailing any additional ECNs that will be mandatory for a wave.

4.2   Pre-Submission Requirements

Before submitting products to the certification process, the vendor must conduct internal testing, preferably using standard off-the-shelf testing equipment, to show conformance with the applicable CableLabs Specifications. A vendor's internal testing should be as rigorous as possible. Conformance tests are generally made available by CableLabs prior to Certification testing. Vendors are encouraged to add functionality outside the scope of the applicable Specification, but such enhancements will not be tested or certified as part of the certification wave process, nor should such proprietary enhancements interfere with interoperability or compliance with the Specification.

Payment is expected by the submission date along with the completed online application. If payment has not been received within 30 days of Submission Day, CableLabs reserves the right to stop testing until payment is received. Testing periods will be extended with any delay in payment.

The web-based application is available at https://apps.cablelabs.com/newpst/. To request a vendor login/password to access the web-based application, please contact labs@kyrio.com.

4.3   Certification Wave Schedule

CableLabs publishes Certification Wave Schedules, which can be found at Certification Wave Schedule. CableLabs reserves the right to alter the schedules as necessary.

The Certification Wave Schedule provides several key pieces of information associated with each Certification Wave:
1.   The name of the Certification Wave, which will be used to label submissions and results for the Wave.
2.   The date by which ECNs (Engineering Change Notifications) need to be accepted in order to apply to a particular Certification Wave. This defines the specification requirements for products submitted to that Wave.
3.   The Submission Day or Days. This defines the beginning of a particular Certification Wave, as well as the entry point for DOCSIS and PacketCable CPE devices to be submitted for D3.0 Fixed Wave Submissions. All submissions of other product types – or DOCSIS and PacketCable CPE devices outside of these dates – will be considered Flex submissions.
4.   The Certification Results Notification date, which is the latest date by which 3.0 Fixed Wave Submissions will receive notification of the results of their testing (all other submission results will be provided as they are completed).

Any device may be submitted at any time. Note that DOCSIS 3.0 and PacketCable CPE devices have separate fees for "Regular Wave" vs. "Flex Wave" submissions; all other submission types have only a single fee regardless of when they are submitted.

CableLabs requests at least two-weeks' notice of intent to submit via email to labs@kyrio.com. Submitting to a certification wave on the posted submission date is the only guarantee to a specific end date. Testing on devices submitted outside of the normal wave cycle may take longer to complete.

4.4   Fees

The fee schedule for all types of Certification submissions and other submissions (such as OEM submissions) can be found at http://www.kyrio.com/testing-services/#certification-testing and looking for the Certification & Qualification Fees section. Kyrio reserves the right to change fees by posting changes to the applicable website 30 days prior to commencement of an event to which the fee relates. Fees are non-refundable, and are due on submission day. If payment has not been received within 30 days of Submission Day, Kyrio reserves the right to stop testing until payment is received. Testing periods will be extended with any delay in payment.

To request an invoice prior to Submission, please contact labs@kyrio.

Payment for submission indicates acceptance of the terms and conditions of Kyrio's application process. When making a payment, please include the following information for all products that the payment applies to:

1. Make payment to Kyrio
2. Include the CableLabs Product ID as listed on the application (See section 4.6 below for details)
3. Provide the corresponding invoice number (if known)

4.5   Product

Unless otherwise noted, devices submitted for certification must be of production quality, as they would be marketed and sold, and must be labeled as manufactured. Products risk rejection otherwise.

All products submitted for certification testing shall be configured for 120 volts, 60 hertz, 20 or 30 amps. Devices utilizing other power requirements shall be submitted with the necessary transformers, power adapters, etc., to ensure compatibility to the existing Kyrio power distribution system.

Devices submitted to Ghent must be capable of supporting 230v 50Hz; the set of devices submitted to Louisville must be capable of supporting 120v 60Hz. Exceptions to this will be considered if the device uses internal power supplies. European to North American plug adapters (and vice versa) are welcome, but not mandatory.
Vendors requiring a UPS (uninterruptible power supply) must submit the UPS along with their product.

All products must support all functionality for all requested Specification(s).

4.5.1 Products with Battery Power

The executive summary must state whether the hardware and/or software supports operation under battery power and if so, must describe any functional or operational differences from operation on main power. Specifically, information on usage ('Battery Backup' only or 'Battery Backup and UPS') and any deviations from operations on A/C power (e.g. Ethernet port disabled during battery being used for 'backup' only) is encouraged.

CableLabs compliance testing does not mandate that CPE products be capable of operating on battery power. However, if the product is capable of operating on battery power, cable operators encourage vendors to include the appropriate batteries with the CPE product when submitted for testing. All submitted units must be identical and must be capable of operating on battery power. CableLabs reserves the right to test such product while it is operating on a second power source (i.e. batteries). Failure to submit batteries and/or pertinent information in the executive summary can result in delays in testing and the certification process.

Note: 'Battery Backup' functionality in the context of this document refers to the ability to switch to 'backup power' only when the primary power source to the device fails, provided secondary power sources are present. 'UPS' (Uninterruptible Power Supply) functionality is defined as the ability to provide power using either the primary or secondary power sources at all times, provided additional sources are present.

4.5.2 Units required for Certification

See separate submission types in sections 5-7 for tables showing the number of units that must be submitted for a Certification Wave.

Vendors agree that CableLabs and Kyrio shall bear no liability for loss for damage or injury to vendor's staff, employees or agents, or to the property of the vendor, including but not limited to the product being submitted and other equipment, tools, supplies, or records, from any cause or causes whatsoever, while in or on the premises of CableLabs, Kyrio or elsewhere.

4.5.3 Number of units required for Retention

The table below shows the minimum number of units that will be retained by CableLabs following the Certification Wave. CableLabs reserves the right to request permanent retention of additional units beyond the minimum.

As new vendors come into the market, interoperating with previously certified equipment is paramount. After certification is awarded, CableLabs will keep units of products as described below. CableLabs will conduct testing to resolve technical difficulties that may arise from product deployment at CableLabs or one or more other laboratories under CableLabs' control and supervision. At its option, CableLabs reserves the right to retain units of failing components, as well as a limited number of practice run devices, and will contact the vendor if such a need becomes evident. Retained devices will be used at the discretion of CableLabs.

Vendors are responsible for the cost of shipping all returned units. The return of vendor products is dependent upon the workload of the staff, and as such does not adhere to any implied date. Also, in the event that an appeal is filed, devices will be retained until after the entire process is completed so that additional testing and lab visits can be supported, as needed.

Vendors have the option of requesting disposal of all units not to be retained by CableLabs.

Base DOCSIS submission:

	Certification	Re-Certification	OEM / Paper
DOCSIS 3.1 CM D3.0 (Annex B) **DOCSIS 3.0 CM** **DOCSIS 3.0 DSG eCM** **DOCSIS 3.0 eCMM**	10 10 units in Louisville	5 5 units in Louisville	5 5 units in Louisville
DOCSIS 3.1 CM ED3.0 (Annex A)	20 10 units in Louisville 10 units in Ghent	10 5 units in Louisville 5 units in Ghent	5 3 units in Louisville 2 units in Ghent
EuroDOCSIS 2.0 CM/STB **EuroDOCSIS 3.0 CM/STB**	15 12 units in Louisville 3 units in Ghent	15 12 units in Louisville 3 units in Ghent	5 12 units in Louisville 3 units in Ghent
DOCSIS eCMM-based	5 5 units in Louisville	5 5 units in Louisville	1 1 units in Louisville
EuroDOCSIS eCMM-based	5 4 units in Ghent 1 unit in Louisville	5 4 units in Ghent 1 unit in Louisville	2 1 unit in Ghent

	1 unit in Louisville

In addition, the following units will be retained for the following applicable add-ons:

	Certification	Re-Certification	OEM / Paper
Packet Cable 1.5 EMTAs	5	5	5
	5 units in Ghent	5 units in Ghent	5 units in Ghent
Euro Packet Cable 1.5 EMTAs	5	5	5
	5 units in Ghent	5 units in Ghent	5 units in Ghent
L2VPN CPE	0	0	0
	N/A	N/A	N/A
Cable Gateway	0	0	0
	N/A	N/A	N/A

Other submissions:

	Certification	Re-Certification	OEM / Paper
DPoE ONU	5	5	5
	In the case of units requiring an Ethernet adapter, as per section 8.4, 5 adapters will be retained.	In the case of units requiring an Ethernet adapter, as per section 8.4, 5 adapters will be retained.	In the case of units requiring an Ethernet adapter, as per section 8.4, 5 adapters will be retained.
	5 units in Louisville	5 units in Louisville	5 units in Louisville
DPoE System	2	0	0
	2 units in Louisville	N/A	N/A
DOCSIS CMTS **DOCSIS CMTS + MM** **EQAM** **CCAP** **PacketCable CMTS** **PacketCable + Multimedia CMTS**	2	0	0
	2 units in Louisville	N/A	N/A
EuroDOCSIS CMTS	3	0	0
	2 units in Ghent 1 units in Louisville	N/A	N/A
EuroDOCSIS CMTS + MM **EuroPacketCable CMTS** **EuroPacketCable + Multimedia CMTS**	5	0	0
	4 units in Ghent 1 units in Louisville	N/A	N/A

OpenCable Unidirectional Receiver	4	4	0
	All units to Louisville	All units to Louisville	N/A
CableCARD	20	20	0
	All units to Louisville	All units to Louisville	N/A
Tuning Resolver	2	2	0
	All units to Louisville	All units to Louisville	N/A

4.6   Labeling and Product IDs

The Product ID label will identify each product submitted for certification and is automatically created when submitting an application. The Product ID convention is used to track products submitted for certification:
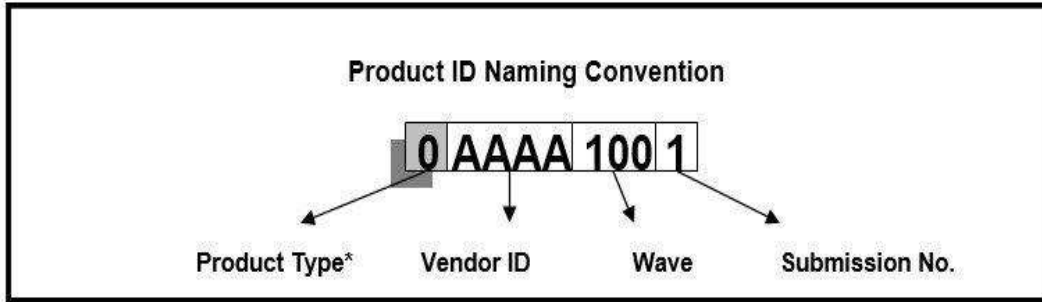
The eight+ character "product id" will be used as the tracking identifier for the physical products submitted (including ancillary hardware), all submission documentation, and all test data.

The last position in the product ID is the Submission number. Use the following as a guide to create the submission number.

1 = First model submitted
2 = Second model submitted
3 = Third model submitted

Product Type	Example Label for a device submitted for CW120 and ECW65	Additional Requirements
DOCSIS CM	ABCD1201 Unit:01 CMx.x RF: XXXX:XXXX:XXXX USB: XXXX:XXXX:XXXX ETH: XXXX:XXXX:XXXX =========================== ABCD1201 Unit: 29 CMx.x (Test DRCA) RF: XXXX:XXXX:XXXX USB: XXXX:XXXX:XXXX ETH: XXXX:XXXX:XXXX	Clearly mark ON THE FRONT OF EACH PRODUCT: 1) MAC addresses of each unit being submitted for certification. Note that if there is more than one MAC address for the individual modem (i.e. RF, Ethernet and USB), each must be shown and clearly identified as "RF", "Eth", or "USB". <u>Note: Submissions must correspond to the numbers and MAC addresses shown on the MAC Address Form included with the application.</u> 2) A unit number 3) Label as "CMx.x", according to the version of DOCSIS Specification. 4) Units 29 and 30 must be labeled as "Test DRCA" units.
EuroDOCSIS CM	ABCD65E Unit: 01 CM x.x (Console Port) RF: XXXX:XXXX:XXXX USB: XXXX:XXXX:XXXX ETH: XXXX:XXXX:XXXX Serial # HW Version ABCD65E Unit: 25 CMx.x (Test EDRCA) RF: XXXX:XXXX:XXXX USB: XXXX:XXXX:XXXX ETH: XXXX:XXXX:XXXX Serial # HW Version	Clearly mark ON THE FRONT OF EACH PRODUCT: 1) MAC addresses of each unit being submitted for certification. Note that if there is more than one MAC address for the individual modem (i.e. RF, Ethernet and USB), each must be shown and clearly identified as "RF", "Eth", or "USB". <u>Note: Submissions must correspond to the numbers and MAC addresses shown on the MAC Address Form included with the application.</u> 2) A unit number 3) Label as "CMx.x", according to the version of DOCSIS Specification. 4) Units 25 and 26 MUST also be labeled as "TEST EDRCA" The diagnostic unit with console port access (#1) must be labeled with "CONSOLE PORT".
D-ONU	ABCD1201 Unit:01 DONUx.x Device MAC: XXXX:XXXX:XXXX USB: XXXX:XXXX:XXXX ETH: XXXX:XXXX:XXXX	Clearly mark ON THE FRONT OF EACH PRODUCT: 1) MAC addresses of each unit being submitted for certification. If there is more than one MAC address for the individual D-ONU (i.e. RF, Ethernet and USB), each must be shown and clearly identified as "RF", "Eth", or "USB". <u>Note: Submissions must correspond to the numbers and MAC addresses shown on the MAC Address Form included with the application.</u> 2) A unit number 3) Label as "DONUx.x", according to the version of DPoE Specification.

PacketCable E-MTA	For an E-MTA: ABCD1201 Unit:01 CMx.x/E-MTAy.y RF: XXXX:XXXX:XXXX USB: XXXX:XXXX:XXXX ETH: XXXX:XXXX:XXXX MTA MAC: XX:XX:XX:XX:XX:XX	Clearly mark ON THE FRONT OF EACH PRODUCT: 1) MAC addresses of each unit being submitted for certification. If there is more than one MAC address for the individual modem (i.e. RF, Ethernet and USB), each must be shown and clearly identified as "RF", "Eth", or "USB". Both the CM and E-MTA MAC addresses must be shown. <u>Note: Submissions must correspond to the numbers and MAC addresses shown on the MAC Address Form included with the application</u>
	For an E-MTA: ABCD1201 Unit: 29 CMx.x/E-MTAx.x (Test DRCA) RF: XXXX:XXXX:XXXX USB: XXXX:XXXX:XXXX ETH: XXXX:XXXX:XXXX MTA MAC: XX:XX:XX:XX:XX:XX ============================= For an E-MTA: ABCD1201 Unit: 44 CMx.x/E-MTAx.x (Test SPRCA) RF: XXXX:XXXX:XXXX USB: XXXX:XXXX:XXXX ETH: XXXX:XXXX:XXXX MTA MAC: XX:XX:XX:XX:XX:XX	2) A unit number 3) Label as "CMx.x/E-MTA y.y", according to the version of DOCSIS (x.x) and PacketCable (y.y) Specifications. 4) Units 29 and 30 must be labeled as "test DRCA" units 5) Units 44 and 45 must be labeled as "test SPRCA" units
EuroPacketCable EMTA	ABCD65E Unit:01 CMx.x/E-MTAx.x (Console Port) RF: XXXX:XXXX:XXXX USB: XXXX:XXXX:XXXX ETH: XXXX:XXXX:XXXX MTA MAC: XX:XX:XX:XX:XX:XX Serial #: HW Version:	Clearly mark ON THE FRONT OF EACH PRODUCT: 1) MAC addresses of each unit being submitted for certification. If there is more than one MAC address for the individual modem (i.e. RF, Ethernet and USB), each must be shown and clearly identified as "RF", "Eth", or "USB". Both the CM and E-MTA MAC addresses must be shown. <u>Note: Submissions must correspond to the numbers and MAC addresses shown on the MAC Address Form included with the application</u>
	For an Euro E-MTA: ABCD65E Unit: 34 CMx.x/E-MTAx.x (Test EDRCA) RF: XXXX:XXXX:XXXX USB: XXXX:XXXX:XXXX ETH: XXXX:XXXX:XXXX MTA MAC: XX:XX:XX:XX:XX:XX Serial #: HW Version:	2) A unit number 3) Label as "CMx.x/E-MTA y.y", according to the version of DOCSIS (x.x) and PacketCable (y.y) Specifications. 4) Units #34 and #35 MUST also be labeled as TEST EDRCA. 5) Units #44 and #45 MUST also be labeled as TEST SPRCA. The diagnostic unit with console port access (#1) must be labeled with "CONSOLE PORT"
	For an Euro E-MTA: ABCD65E Unit: 44 CMx.x/E-MTAx.x (Test SPRCA) RF: XXXX:XXXX:XXXX USB: XXXX:XXXX:XXXX ETH: XXXX:XXXX:XXXX MTA MAC: XX:XX:XX:XX:XX:XX Serial #: HW Version:	

24

DSG eCM	ABCD1201 Unit:01 CMx.x DSG Advanced RF: XXXX:XXXX:XXXX USB: XXXX:XXXX:XXXX ETH: XXXX:XXXX:XXXX ============================ ABCD1201 Unit: 29 CMx.x DSG Advanced (Test DRCA) RF: XXXX:XXXX:XXXX USB: XXXX:XXXX:XXXX ETH: XXXX:XXXX:XXXX	Clearly mark ON THE FRONT OF EACH PRODUCT: 1) MAC addresses of each unit being submitted for certification. Note that if there is more than one MAC address for the individual modem (i.e. RF, Ethernet and USB), each must be shown and clearly identified as "RF", "Eth", or "USB". Note: Submissions must correspond to the numbers and MAC addresses shown on the MAC Address Form included with the application. 2) A unit number 3) Label as "CMx.x" according to the version of DOCSIS Specification. 4) The notation "DSG Advanced," "DSG Basic," or "DSG Both" must appear on the label. 5) Units 29 and 30 must be labeled as "Test DRCA" units.
DOCSIS CMTS **EuroDOCSIS CMTS**	2ABCD1201 Unit:01 CMTS x.x MAC: XXXX:XXXX:XXXX 2ABCD65E Unit:01 CMTSx.x MAC: XXXX:XXXX:XXXX	Clearly mark ON THE FRONT OF EACH PRODUCT: 1) MAC addresses of each unit being submitted for qualification. Submissions must correspond to the numbers & MAC addresses shown on the MAC Address Form included with the application. 2). A unit number 3) Label as "DOCSIS x.x", according to the version of the DOCSIS Specification.
DOCSIS CMTS w/DSG Agent	2ABCD1201 Unit:01 CMTS x.x DSG MAC: XXXX:XXXX:XXXX	Clearly mark ON THE FRONT OF EACH PRODUCT: 1) MAC addresses of each unit being submitted for qualification. Submissions must correspond to the numbers & MAC addresses shown on the MAC Address Form included with the application. 2) A unit number 3) Label as "DOCSIS x.x DSG", according to the version of the DOCSIS Specification.
DPoE System	23ABCD1201 Unit: 01 MAC: XXXX:XXXX:XXXX	Clearly mark ON THE FRONT OF EACH PRODUCT: 1) MAC addresses of each unit being submitted for qualification. Submissions must correspond to the numbers & MAC addresses shown on the MAC Address Form included with the application. 2) A unit number Label as "DPoE x.x", according to the version of the DPoE Specification.
PacketCable CMTS **PacketCable Multimedia CMTS** **PacketCable + Multimedia CMTS** **EuroPacketCable CMTS**	2ABCD1201 Unit:01 CMTSx.x/PCy.y/MM MAC: XXXX:XXXX:XXXX 2ABCD65E Unit:01 CMTSx.x/PCy.y MAC: XXXX:XXXX:XXXX	Clearly mark ON THE FRONT OF EACH PRODUCT: 1) MAC Addresses of each unit being submitted for qualification. Submissions must correspond to the numbers & MAC addresses shown on the MAC Address Form included with the application. 2) A unit number 3) Label as "CMTS x.x/PCx.x/MM", according to the version of DOCSIS (x.x) and PacketCable (y.y) Specifications.
OpenCable Unidirectional Receiver	16ABCD1201 Unit:01 OC x.x RF: XXXX:XXXX:XXXX USB: XXXX:XXXX:XXXX	Clearly mark ON THE FRONT OF EACH PRODUCT: 1) MAC addresses of each unit being submitted for certification. Note that if there is more than one MAC address for the individual modem (i.e. RF and USB), each must be shown and clearly identified as "RF" or "USB". 2) A unit number.

CableCARD Multi-Stream	12ABCD1201 Unit:01 OC x.x Code Version: XXX.XXX	Clearly mark ON THE FRONT OF EACH PRODUCT: Code Version being submitted
Tuning Resolver	19ABCD1201 Unit : 01 OC xx Code Version : XXX.XXX	Clearly mark ON THE FRONT OF EACH PRODUCT: Code Version being submitted
EQAM	14ABCD1201 Unit:01 MAC: XXXX:XXXX:XXXX	Clearly mark ON THE FRONT OF EACH PRODUCT: 1) MAC addresses of each unit being submitted for qualification. Submissions must correspond to the numbers & MAC addresses shown on the MAC Address Form included with the application. 2) A unit number.
L2VPN CPE	ABCD65E Unit: 01 L2VPN (Console Port) RF: XXXX:XXXX:XXXX USB: XXXX:XXXX:XXXX ETH: XXXX:XXXX:XXXX Serial # HW Version	Clearly mark ON THE FRONT OF EACH PRODUCT: 1) MAC addresses of each unit being submitted for certification. If there is more than one MAC address for the individual modem (i.e. RF, Ethernet and USB), each must be shown and clearly identified as "RF", "Eth", or "USB". Note: Submissions must correspond to the numbers and MAC addresses shown on the MAC Address Form included with the application. 2) A unit number The diagnostic unit with console port access (#1) must be labeled with "CONSOLE PORT".
Cable Gateway	ABCD65E Unit: 01 L2VPN (Console Port) RF: XXXX:XXXX:XXXX eRouter: XXXX:XXXX:XXXX USB: XXXX:XXXX:XXXX ETH: XXXX:XXXX:XXXX Serial # HW Version	Clearly mark ON THE FRONT OF EACH PRODUCT: 1) MAC addresses of each unit being submitted for certification. If there is more than one MAC address for the individual modem (i.e. RF, Ethernet and USB), each must be shown and clearly identified as "RF", "eRouter", "Eth", or "USB". Note: Submissions must correspond to the numbers and MAC addresses shown on the MAC Address Form included with the application. 2) A unit number The diagnostic unit with console port access (#1) must be labeled with "CONSOLE PORT".
Power Supplies, E-MTA Batteries, UPS, & other Support products		**All** products must be supplied with a means to power the device with 120v AC. Label the front of each accompanying power supply, and personal computer with the corresponding Product ID as described above. Backup batteries must also be tagged with printed labels clearly showing the Product ID and the CPE unit number. AC adaptor labels do not need to include the corresponding unit number. Unlabeled batteries or AC adaptors will not be accepted. AC power cords do not require labels.

4.7   Product Delivery Requirements

Please note that on-site vendor representation is not required for product drop-off. Submitted products not accompanied by the vendor are not guaranteed to be checked-in when the product arrives. Shipping all of the required equipment is acceptable. Vendors choosing to ship incomplete submissions or submissions for which the actual products do not correspond to the products described in the documentation risk rejection and return of their product prior to the wave, unless an on-site vendor representative is present and can correct the submission immediately prior to submission cut-off. The mode of delivery is up to the vendor's discretion.

North American Product Delivery
All materials must be delivered by noon Mountain Time on the designated day.

Please address submissions to:

> Cable Television Laboratories, Inc.
> Attn: Kyrio Test Lab
> 858 Coal Creek Circle
> Louisville, CO 80027-9750 USA

European Product Delivery
All materials for EuroDOCSIS 3.0, 2.0, 1.1 and 1.0 and EuroPacketCable 1.5, 1.0, L2VPN and Cable Gateway testing are required to be delivered by noon CET on the designated day. CMTS vendors MUST also have all required equipment set up and running. At least one engineer per CMTS vendor will be required to personally set up the equipment (this may also be done in advance).

Please address submissions to:
> Excentis
> Attn: Kristof Sercu
> Gildestraat 8
> B-9000 Ghent
> Belgium

As with submissions to Louisville, manufacturer is responsible for all customs/shipping risk, paperwork, and costs for devices sent to Ghent.

Note that devices for European testing must also include additional devices to Louisville no later than two weeks after the initial submission.

4.8   Submission Documentation

All the information listed in this section is required for product submission.

4.8.1 Submission Information provided via web-form

The web-based application is available at https://www.cablelabs.com/newpst/. To request a vendor login/password to access the web-based application, please contact labs@kyrio.com.

The following submission information must be provided via the web-based application:

Certification Wave Admission Application

- The vendor must use the current version of the web-based form to provide all necessary product submission information.
- When submitting for the first time, the vendor must submit a signed, original, signature page to be accessed from the web-based form. An Officer and Quality Assurance Manager of the vendor company must sign this document to affirm the accuracy of all Admission Application information related to the product.
- Hardware and software revisions and SysDescriptor, or internal software readouts, **must** match the product as submitted or resubmission will be required.
- DOCSIS and PacketCable optional functionality must be provided via the web-based application. Misrepresentation of such information may impact certification/qualification test reporting and results. Note that optional functionality may be listed on the CableLabs public certification/qualification list.
- MAC Address and/or Serial Number List. A soft-copy of the MAC Address and/or Serial Number List must be submitted on the website. Note that all product units should exhibit the same OUI (organizational unique identifier).

4.8.2 Additional Submission Information provided via web-form upload utility

The additional documentation listed below must be provided via the web-form file upload utility.

To best assist our certification team, all documentation must be organized according to the folder hierarchy shown below:

Create a top-level folder with the same name as the product ID, for example: "VEND1051". This top-level folder contains high-level information about the product, such as the executive summary, interoperability test report, etc.

Create a sub-folder for information specific to each specification (DOCSIS, DPoE, and PacketCable). Note that some products require multiple sub-folders. For example, an E-MTA will require two sub-folders: "DOCSIS" and "PacketCable".

Executive Summary: The Executive Summary should not exceed four pages. For certification requests, vendors must include a list of the test cases performed and verified against the product being submitted. Also included should be any exceptions or additional information that a vendor believes the Certification Board should know, or that is required for testing.

Submission Documentation Folder Hierarchy:

<table>
<tr><td>

Example: VEND1201 or VEND65E

</td></tr>
<tr><td>

Executive Summary

</td></tr>
<tr><td>

Images
(subfolder)
Image and Driver Files: DOCSIS, PacketCable, OpenCable (Manufacturer-signed OCAP image in object code form)

</td></tr>
<tr><td>

DOCSIS/EuroDOCSIS (subfolder)
CM:
- Requirements Checklist (DOCSIS, eDOCSIS and DSG, if applicable)
- Digital Certificates for DOCSIS CM
- DSG eCM Special Instructions (if applicable)
- Wi-Fi configuration manual & MIBs (if applicable)
- MPEG stream (for EuroDOCSIS STB/CM)

CMTS:
- Requirements Checklist (DOCSIS, and DSG, if applicable)
- DOCSIS CMTS Special Instructions
- CMTS Operations Manual

EQAM:
- Requirements Checklist (M-CMTS and DRFI)
- DOCSIS M-CMTS EQAM Special Instructions

</td></tr>
<tr><td>

PacketCable/EuroPacketCable (subfolder)
- Requirements Checklist (formally known as a Component Checklist)
- Test Case Checklist
- Vendor's ATP (if applicable)
- Interoperability Report
- PacketCable CMTS Vendor Product Operating Instructions

</td></tr>
<tr><td>

DPoE (subfolder)
D-ONU:
- Requirements Checklist (Applicable DPoE requirements)
- Digital Certificates for D-ONU
- D-ONU Special Instructions (if applicable)
- D-ONU Operations Manual

DPoE System:
- Requirements Checklist (Applicable DPoE requirements)
- DPoE System Special Instructions (if applicable)
1. DPoE System Operations Manual

</td></tr>
</table>

M-UDCP or UDCP (subfolder)
▪   Completed Requirements Checklist ▪   Detailed ATP   Vendor Submitted Documentation Recommendations

Tuning Resolver (subfolder)
▪   Completed Requirements Checklist ▪   Detailed ATP

OCUR (subfolder)
▪   Completed Requirements Checklist ▪   Detailed ATP ▪   Production Signed Code Object (Signed by Submitting Manufacturer) ▪   Unsigned development object (To be signed by evaluation certificate at CableLabs)

Cable Gateway (subfolder)
▪   Completed Requirements Checklist ▪   Detailed ATP ▪   eRouter documentation: how to reset the device to its default behavior for all functionality, how to enable/disable any Customer Facing IP Interfaces, how to enable/disable the local DHCPv4 and DHCPv6 server, how to configure/disable the firewall, how to configure the Wi-Fi, etc. (i.e., via proprietary MIBs, webpage or other). ▪   If TR-069 is supported: supported data models

L2VPN (subfolder)
▪   Completed Requirements Checklist ▪   Detailed ATP

DOCSIS Documentation Requirements. Products submitted for DOCSIS certification testing may submit a signed declaration stating compliance to the applicable specifications in lieu of submitting the normally required supporting documentation as detailed in the guidelines, with the exception of the applicable Special Instructions and the Requirements Checklist. Any exceptions to the Requirements Checklist should be clearly noted within the declaration document. Digital certificates, drivers and image files are also required.

In the event that additional documentation is required to provide the test team with more data, CableLabs reserves the right to request this information with vendor response within a 48-hour time frame at any time during the wave.

Note that this applies to DOCSIS devices only, and submissions must adhere to PacketCable, DPoE and OpenCable documentation requirements as detailed.

Interoperability Test Report. The Interoperability Test Report is a summary of all the testing performed at CableLabs, MSO locations (field trial), other Interops, third-party locations and other vendor sites. The testing performed and summarized in the Interoperability Test Report should demonstrate that the product submitted for certification interoperates with multiple vendor products. E-MTA submissions should demonstrate interoperability with a minimum of three qualified CMTS products. PacketCable CMTS submissions should list all interoperable PacketCable network products.

Completed Conformance and Requirements Checklists
The "Requirements Checklist" is available on the InfoZone web site at
https://community.cablelabs.com/wiki/display/TECHPUBS/DOCSIS+PICs+and+REQs# . "Completed" means each line item is clearly marked with a "Yes" or "No". Each Requirements line item must refer to a given test procedure that was used to verify that specific Requirement item. The Requirements Checklist is a vendor's formal declaration to the level of the product's conformance to the specifications. The document *must* match the product.

Detailed Acceptance Test Plan (ATP) / Compliance Test Plan (CTP)
Each vendor is responsible for its own product, writing and verifying each test procedure on each line item of the DOCSIS, DSG, and PacketCable Requirements Checklist, and testing the product against it. The actual data gathered for each test must be attached to support each of the verifying Requirement item. The various sources of test procedures for product vendors are: 1) silicon vendors (for chip conformance to specs); 2) commonly used or widely available ATPs for the cable industry, such as the CableLabs ATP, which is available via the project websites; 3) the vendor's internally developed ATPs. The Certification Board requests that each test procedure be documented in a similar manner to the CableLabs ATP.

The "PacketCable Test Case" is available on the PacketCable InfoZone web site in "Certification Wave Documentation", then "CW## Documentation". The PacketCable Test Case Checklist is a listing of all PacketCable test cases and requirements contained in the PacketCable Compliance/Acceptance Test Plans (CTPs/ATPs). PacketCable CTPs/ATPs are available on the PacketCable InfoZone website. By executing these test plans and supplying CableLabs with the results in the format provided in the appendices, vendors will expedite results reporting process to the board for evaluation. In the event vendors choose to utilize their own proprietary test plans, they must submit those test plans, results and a traceability matrix depicting how every applicable PacketCable requirement is addressed by test case.

Image and Driver Files.

Image and Driver Files for all products must be included in the "images" folder and must adhere to the file naming convention per section 5.2.

- If the CPE product contains a CM component: The MAC-14 and BPI-23 test image file and an original image file must be included in the uploaded .zip file. If the cable modem is a USB or internal, device drivers must also be provided in the file upload. See Section 5.2 for details.

Digital Certificates.

For testing of DOCSIS and/or EuroDOCSIS 3.1, 3.0, or 2.0 cable modems, the images must contain all of the certificates and signatures required for secure software downloading and authentication. For testing of CableCARDs, such devices must contain all of the certificates and signatures required for device authentication... See Sections 7 and 9 for details.

Special Instructions Documents:

DOCSIS CMTS Special Instructions: For testing DOCSIS and/or EuroDOCSIS CMTSs, and/or CCAP, the special instructions posted under the *Special Instructions Documents* header found at
https://community.cablelabs.com/wiki/display/CERTQUAL/DOCSIS+Testing+Information must be included in the uploaded .zip file. Vendors must include in this form a list of "Conditional MUSTs" and Programmable Features that the product supports.

CMTS Operations Manual: CMTS vendors should also provide a soft-copy of the operations manual. If one is not available, a hard copy should be provided with the submission materials upon delivery of the units.

DOCSIS M-CMTS EQAM Special Instructions: For testing DOCSIS M-CMTS EQAMs, the special instructions posted under the *Special Instructions Documents* header found at
https://community.cablelabs.com/wiki/display/CERTQUAL/DOCSIS+Testing+Information must be included in the uploaded .zip file.

DPoE System Special Instructions: For testing DPoE System, the special instructions posted under the *Special Instructions Documents* header found at https://community.cablelabs.com/wiki/display/CERTQUAL/DOCSIS+Testing+Information must be included in the uploaded .zip file. Vendors must include in this form a list of "Conditional MUSTs" and Programmable Features that the product supports.

DPoE System Operations Manual: DPoE System vendors should also provide a soft-copy of the operations manual. If one is not available, a hard copy should be provided with the submission materials upon delivery of the units.

D-ONU Special Instructions: For testing D-ONU, the special instructions posted under the *Special Instructions Documents* header found at https://community.cablelabs.com/wiki/display/CERTQUAL/DOCSIS+Testing+Information must be included in the uploaded .zip file. Vendors must include in this form a list of "Conditional MUSTs" and Programmable Features that the product supports.

D-ONU Operations Manual: **D-ONU** vendors should also provide a soft-copy of the operations manual. If one is not available, a hard copy should be provided with the submission materials upon delivery of the units.

DSG eCM Special Instructions: For testing DSG eCMs, the special instructions posted under the *Special Instructions Documents* header found at https://community.cablelabs.com/wiki/display/CERTQUAL/DOCSIS+Testing+Information must be included in the uploaded .zip file.

PacketCable/EuroPacketCable CMTS Vendor Product Operating Instructions: The submission must include the CMTS Operating Instructions, as appropriate. The Vendor Product Operating Instructions must be provided for product submitted to the Certification Wave, as well as for supporting product necessary to support off-net functionality. Templates for the Vendor Product Operating Instruction documents can be found on the PacketCable InfoZone web page at
https://community.cablelabs.com/wiki/display/CERTQUAL/PacketCable+Testing+Information .

5 DOCSIS SUBMISSION REQUIREMENTS

5.1 DOCSIS PRODUCTS

Each submission follows these general rules:

- "Diagnostic" unit and it is a regular unit with an active diagnostic port (may include special SW load)

- "Test DRCA" units substitute the DOCSIS ROOT PUBLIC KEY for TEST DOCSIS ROOT PUBLIC KEY

- "Test EDRCA" units substitute the EURODOCSIS ROOT PUBLIC KEY for TEST EURODOCSIS ROOT PUBLIC KEY

- "Test CRCA" units substitute the CABLELABS ROOT CA units for TEST CABLELABS ROOT CA

- "Test SPRCA" units substitute the EUROPACKETCABLE SERVICE PROVIDER ROOT CA for TEST EUROPACKETCABLE SERVICE PROVIDER ROOT CA

- The submission, for check-in purposes, must provide read-only access to the MIB objects listed as a MAY in Section 8.5.4.1 in the current OSSI specification: sysDescr, sysUptime and ifTable.

The following information provides specific product submission requirements.

5.1.1 DOCSIS 1.1 Cable Modem Submissions

To submit a DOCSIS 1.1 device of any kind, please contact labs@kyrio.com

5.1.2 DOCSIS 3.0 or 2.0 Cable Modem Submissions (CM,DSG eCM, eCMM)

Certification Level	Units	Shipping Location	Details differences among units		Common to all units
CERTIFICATION	30	Louisville	#1	"Diagnostic" unit	DOCSIS MFG CA CERTIFICATE DOCSIS CM CERT DOCSIS CM PRIVATE KEY
			#1 through #28	DOCSIS ROOT PUBLIC KEY	
			#29 and #30	TEST DOCSIS ROOT PUBLIC KEY	
RE-CERTIFICATION	15	Louisville	#1	"Diagnostic" unit	DOCSIS MFG CA CERTIFICATE DOCSIS CM CERT DOCSIS CM PRIVATE KEY DOCSIS ROOT PUBLIC KEY
OEM / PAPER	5	Louisville	#1	"Diagnostic" unit	DOCSIS MFG CA CERTIFICATE DOCSIS CM CERT DOCSIS CM PRIVATE KEY DOCSIS ROOT PUBLIC KEY

5.1.3 EuroDOCSIS 3.0/2.0/1.1 Cable Modem (CM, STB/CM)

Certification Level	Units	Shipping Location	Details differences among units		Common to all units
CERTIFICATION	26	Ghent	#1	"Diagnostic" unit	EURODOCSIS MFG CA CERTIFICATE EURODOCSIS CM CERT EURODOCSIS CM PRIVATE KEY
			#1 through #24	EURODOCSIS ROOT PUBLIC KEY	
			#25 and #26	TEST EURODOCSIS ROOT PUBLIC KEY	
	4	Louisville	#27	"Diagnostic" unit	
			#27 through #30	EURODOCSIS ROOT PUBLIC KEY	
RE-CERTIFICATION	13	Ghent	#1	"Diagnostic" unit	EURODOCSIS MFG CA CERTIFICATE EURODOCSIS CM CERT EURODOCSIS CM PRIVATE KEY
			#1 through #11	EURODOCSIS ROOT PUBLIC KEY	
			#12 and #13	TEST EURODOCSIS ROOT PUBLIC KEY	
	2	Louisville	#14 through #15	EURODOCSIS ROOT PUBLIC KEY	
OEM / PAPER	3	Ghent	#1 through #3	NA - all units are the same.	EURODOCSIS MFG CA CERTIFICATE EURODOCSIS CM CERT EURODOCSIS CM PRIVATE KEY EURODOCSIS ROOT PUBLIC KEY
	2	Louisville	#4 and #5		

5.1.4 DOCSIS 3.0 or 2.0 embeded Cable Modem Module Submissions based (eCMM-based)

Certification Level	Units	Shipping Location	Details differences among units		Common to all units
Any	5	Louisville	#1	"Diagnostic" unit	DOCSIS MFG CA CERTIFICATE DOCSIS CM CERT DOCSIS CM PRIVATE KEY DOCSIS ROOT PUBLIC KEY

5.1.5   EuroDOCSIS 3.0/2.0/1.1 embeded Cable Modem Module Submissions based (eCMM-based)

Certification Level	Units	Shipping Location	Details differences among units		Common to all units
Any	5	Louisville	#1	"Diagnostic" unit	EURODOCSIS MFG CA CERTIFICATE EURODOCSIS CM CERT EURODOCSIS CM PRIVATE KEY EURODOCSIS ROOT PUBLIC KEY

5.1.6   DOCSIS 3.1 Cable Modem Submissions

Each DOCSIS 3.1 cable modem submission must include all unit certificate configurations for a DOCSIS 3.0 or 2.0 cable modem submission from the legacy PKI as detailed above in 5.1.2 for North American and Asian devices and 5.1.3 for European devices to support backward compatibility testing. In addition, units must also include certificates and keys from the new PKI.

5.1.6.1 DOCSIS 3.1 backward compatible to D3.0

Certification Level	Units	Shipping Location	Details differences among units		Common to all units
CERTIFICATION	30	Louisville	#1	"Diagnostic" unit	DOCSIS MFG CA CERTIFICATE DOCSIS CM CERT DOCSIS CM PRIVATE KEY CABLELABS DEVICE CA CERTIFICATE CM DEVICE CERT CM DEVICE PRIVATE KEY
			#1 through #28	DOCSIS ROOT PUBLIC KEY CABLELABS ROOT CA CERTIFICATE	
			#29 and #30	TEST DOCSIS ROOT PUBLIC KEY TEST CABLELABS ROOT CA CERTIFICATE	
RE-CERTIFICATION	15	Louisville	#1	"Diagnostic" unit	DOCSIS MFG CA CERTIFICATE DOCSIS CM CERT DOCSIS CM PRIVATE KEY DOCSIS ROOT PUBLIC KEY CABLELABS DEVICE CA CERTIFICATE CM DEVICE CERT CM DEVICE PRIVATE KEY CABLELABS ROOT CA CERTIFICATE
OEM / PAPER	5	Louisville	#1	"Diagnostic" unit	DOCSIS MFG CA CERTIFICATE DOCSIS CM CERT DOCSIS CM PRIVATE KEY DOCSIS ROOT PUBLIC KEY CABLELABS DEVICE CA CERTIFICATE CM DEVICE CERT CM DEVICE PRIVATE KEY CABLELABS ROOT CA CERTIFICATE

5.1.6.2 DOCSIS 3.1 backward compatible to ED3.0

Certification Level	Units	Shipping Location	Details differences among units		Common to all units
CERTIFICATION	30	Louisville	#1	"Diagnostic" unit	EURODOCSIS MFG CA CERTIFICATE EURODOCSIS CM CERT EURODOCSIS CM PRIVATE KEY CABLELABS DEVICE CA CERTIFICATE CM DEVICE CERT CM DEVICE PRIVATE KEY
			#1 through #28	EURODOCSIS ROOT PUBLIC KEY CABLELABS ROOT CA CERTIFICATE	
			#29 and #30	TEST EURODOCSIS ROOT PUBLIC KEY TEST CABLELABS ROOT CA CERTIFICATE	
	10	Ghent	#31	"Diagnostic" unit	
			#31 through #40	EURODOCSIS ROOT PUBLIC KEY CABLELABS ROOT CA CERTIFICATE	
RE-CERTIFICATION	15	Louisville	#1	"Diagnostic" unit	EURODOCSIS MFG CA CERTIFICATE EURODOCSIS CM CERT EURODOCSIS CM PRIVATE KEY CABLELABS DEVICE CA CERTIFICATE CM DEVICE CERT CM DEVICE PRIVATE KEY
			#1 through #13	EURODOCSIS ROOT PUBLIC KEY CABLELABS ROOT CA CERTIFICATE	
			#14 and #15	TEST EURODOCSIS ROOT PUBLIC KEY TEST CABLELABS ROOT CA CERTIFICATE	
	5	Ghent	#16 through #20	EURODOCSIS ROOT PUBLIC KEY CABLELABS ROOT CA CERTIFICATE	
OEM / PAPER	3	Louisville	#1 through #3	NA - all units are the same.	EURODOCSIS MFG CA CERTIFICATE EURODOCSIS CM CERT EURODOCSIS CM PRIVATE KEY EURODOCSIS ROOT PUBLIC KEY CABLELABS DEVICE CA CERTIFICATE CM DEVICE CERT CM DEVICE PRIVATE KEY CABLELABS ROOT CA CERTIFICATE
	2	Ghent	#4 and #5		

5.1.1   DOCSIS Add-Ons Submissions

Specific Packet Cable Submission requirements are listed in Section 6.

The following programs can be standalone or add-on submissions.

	Certification	Re-Certification	OEM / Paper
L2VPN CPE	5	2	0
	5 units to Ghent	2 units to Ghent	
Cable Gateway	5	2	0
	5 units to Ghent	2 units to Ghent	

5.1.1.1 L2VPN CPE Testing

L2VPN CPE testing is available as an add-on or as a stand-alone option to EuroDOCSIS or DOCSIS Certification testing. Only previously-certified devices may be submitted for stand-alone testing, using the same hardware and software versions as were originally certified. Devices may be submitted at any time and are not required to adhere to the posted Certification Wave schedule. Samples are to be delivered to Excentis at the aforementioned address.

The requirements for an L2VPN CPE device are found in the CableLabs L2VPN specification found at http://www.cablelabs.com/specification/business-services-over-docsis-layer-2-virtual-private-networks/ and the associated Requirements Checklist. Please note that at the present time L2VPN testing does not include testing of Section 8 "Service Operations, Administration, and Maintenance (OAM)", although it is expected to be added at a future time. This difference will be reflected in the Requirement Checklist, which should be used as the definitive guide for the requirements for an L2VPN CPE device.

5.1.1.2 Cable Gateway CPE Testing

Cable Gateway CPE testing is available as an add-on or as a stand-alone option to EuroDOCSIS or DOCSIS Certification testing. Only previously certified devices may be submitted for stand-alone testing, using the same hardware and software versions as were originally certified. Devices may be submitted at any time and are not required to adhere to the posted Certification Wave schedule. Samples are to be delivered to Excentis at the aforementioned address

The requirements for a Cable Gateway device are based on, and must comply with, the eRouter specification found at. http://www.cablelabs.com/specification/ipv4-and-ipv6-erouter-specification/. There are a few differences where some optional features have been made mandatory or a particular option from a list of choices is expected as compared to the Cable Gateway Requirements Checklist. The specifics of these differences are detailed below and include (but are not limited to) the following:

- Narrow, or tighten:
    1. Reduce the scope using three DUID types (RFC-3315), to a DUID that is type DUID-LL only.
    2. Specify the IPv6 prefix delegation from any prefix to a /48 or higher (/48 through /64).
- As an option:
    1. support a webpage or use a Proprietary MIB for enabling/disabling the firewall.
    2. use a Proprietary MIB to disable its DHCPv4 and/or DHCPv6 server.
    3. support 6rd as an alternative to DS-Lite to support transfer of both IPv6 packets and IPv4 packets across a network. If 6rd is used, it MUST adhere to RFC-5969.

These are only examples; the definitive list of requirements can be found in the Cable Gateway Requirements Checklist. The above list is subject to change at any time.

5.1.2 STB/CM without external Ethernet interface

In the case of an STB/CM product that will be brought in production without any external Ethernet port the following additional requirements are applicable:

- Of the 23 normal samples (i.e. non test EDRCA samples) samples #1-5 must be production ready samples (i.e. without CPE interface) and the other 18 samples (sample # 6-23) must have an external Ethernet interface (so that all certification tests can be executed).
- The ifTable structure MUST NOT differ between products without Ethernet interface and products with external Ethernet interface.

In case the external Ethernet interface is provided through an extra interface on the eCM, then this interface MUST have ifIndex 1. For the samples without Ethernet interface the ifAdminStatus for the Ethernet interface (ifIndex 1) MUST then be set to "down" and the ifOperStatus MUST then be set to "notPresent".

5.1.3 eDOCSIS Products

Products being submitted with an embedded cable modem must comply with the Embedded DOCSIS (eDOCSIS) Specification, in addition to the DOCSIS 3.1, 3.0, or 2.0 specifications as they may apply.

PacketCable E-MTAs are classified as eDOCSIS devices, and must comply with the eDOCSIS Specification.

The following is a summary of the key requirements of the eDOCSIS Specification:

- It contains specific requirements for the embedded cable modem component of the E-MTA for the reporting of a "logical interface" to represent the data path between the CM and the E-MTA. This logical interface is given a well-known ifIndex and is required to follow the same data forwarding and address learning rules as a "normal" CPE interface (e.g. Ethernet).

- It requires that the DOCSIS device-specific MIBs not be made available to an SNMP manager that queries the E-MTA IP address. Similarly, the E-MTA device-specific MIBs are not to be made available to an SNMP manager that queries the CM IP address.

- For the complete set of requirements, please refer to the eDOCSIS Specification published in the CableLabs website at http://www.cablelabs.com/specification/edocsis-specification/ . Note that these requirements apply to the embedded cable modem regardless of which version of the DOCSIS specification to which it is compliant.

5.1.4 DSG eCM Requirements

Products being submitted with a DSG eCM to be Verified for Interoperability must comply with the DSG specification, in addition to the eDOCSIS Specification and the DOCSIS 3.0 or 2.0 specifications as they may apply.

The DOCSIS, eDOCSIS, and DSG Requirements Checklist documents must be completed.

The document *DSG eCM Special Instructions* available on InfoZone (https://community.cablelabs.com/wiki/display/CERTQUAL/DOCSIS+Testing+Information under "Special Instructions Documents") must be completed.

The devices must include a CPE Interface, such as an accessible Ethernet port. Note that per DSG requirements, this interface must not bridge DSG traffic. This port is for the purpose of sending two-way data traffic to verify DOCSIS functionality.

In order to support DOCSIS testing, the device must support a "non-DSG" mode (commonly referred to as 'DOCSIS mode'), in which the device will not require the presence of DSG messages or traffic in order to lock to a downstream channel. The method for switching between modes must be described in the document *DSG eCM Special Instructions* available on InfoZone (https://community.cablelabs.com/wiki/display/CERTQUAL/DOCSIS+Testing+Information) under *Special Instructions Documents*. It is assumed that this will be the only difference between this mode and the device's normal operating mode. If there are other differences that place constraints upon device testing, please describe them in the special instructions as well.

In the case where the support of DOCSIS–mode requires vendor intervention and the units must adhere to the table in section 7.1.1, a method for querying the CM diagnostic address must be provided for use on submission day.

In the event the method for switching between modes requires manual intervention by the vendor, the DRCA units must be configured to boot;

- one in DOCSIS only test mode
- one in DSG mode.

The requirements for Stand Alone Cable Modems as defined in Sections 5.1.2 and 5.1.2.1 must also be followed.

5.1.5 Embedded Cable Modem Modules (eCMMs) and eCMM-Based Devices

An embedded DOCSIS cable modem module (eCMM) is a cable modem, functionally equivalent to a stand-alone cable modem, except that, because it is intended to be embedded into another device (eCMM-based device), it has a vendor-specific CPE interface rather than the DOCSIS-required CMCI. An eCMM-based device consists of an eCMM and an embedded CPE device that provides the application-specific function of the eCMM-based device. eCMMs may be submitted to CableLabs only for qualification.

eCMM requirements vary depending upon the eCMM-based device they are embedded in. For example, an eCMM embedded in an OpenCable Host 2.1 eCMM-based device will have different requirements than one embedded in a stand-alone DOCSIS cable modem eCMM-based device. An eCMM submitted for qualification must support all the requirements of the eCMM-based device it will be embedded in (see appropriate specification and Certification Guidelines section).

Any eCMM-based device that then incorporates a qualified eCMM may be submitted for an "eCMM based-device Certification" with reduced fees. This doesn't preclude a vendor from submitting an eCMM based-device for full certification.

It is strongly recommended for the safety and integrity of the vendor equipment, collection of test data, and testing staff, that these devices be submitted in an enclosed housing. This recommendation could be fulfilled by the usage of non-production quality clear plastic housings, with the appropriate holes to reach interfaces.

Each eCMM-based device implementation must be certified by CableLabs in order to be labeled as CableLabs Certified. Certification of one particular eCMM-based device implementation does not automatically convey certification to another, even if the two devices are built with identical eCMMs.

Qualification Submission Guidelines for eCMMs:

1. Each eCMM, if submitted with a vendor-specific CPE interface, must be submitted with an appropriate CMCI translator to convert the vendor-specific CPE interface (e.g. MII) to an Ethernet interface.

2. Detailed descriptions of all vendor-specific CPE interfaces and their functions must be included in the Executive Summary (note that CMCI access requirements for an eCMM are the same as for a standalone cable modem).

3. Each eCMM with CMCI and power supply is equivalent to a standalone cable modem.

4. All other requirements applicable to the eCMM-based device in which it will be embedded apply.

5. The full DOCSIS certification fee applies.

Requalification Submission Guidelines for eCMMs:

1. eCMM products may be submitted for requalification in the event of hardware and /or software changes.

2. Each eCMM, if submitted with a vendor-specific CPE interface, must be submitted with an appropriate CMCI translator to convert the vendor-specific CPE interface (e.g. MII) to an Ethernet interface.

3. Detailed descriptions of all vendor-specific CPE interfaces and their functions must be included in the Executive Summary (note that CMCI access requirements for an eCMM are the same as for a standalone cable modem).

4. Each eCMM with CMCI and power supply is equivalent to a standalone cable modem.

5. All other requirements applicable to the eCMM-based device it will be embedded in apply.

6. The full DOCSIS recertification fee applies.

Certification Submission Guidelines for eCMM-based devices:

1. In order to be considered for certification, an eCMM-based device must be based on a qualified eCMM (no eCMM hardware or software changes are allowed from the originally submitted product).

2. The eCMM-based device may be submitted for certification during the same wave that the eCMM is submitted for qualification or at any future wave within one year of the original qualification.

3. The eCMM-based device is expected to have the same sysDescr as the originally qualified eCMM, with the exception of the model number.

4. The certification requirements that apply to eCMM-based devices are the same as for any other device submitted for certification. However, a reduced certification fee applies.

5. An eCMM-based device is not required to have an externally exposed CMCI interface.

6. Vendor must supply vendor-specific instructions on:

   a. enabling and disabling the embedded CPE device,
   b. generating typical traffic through the CPE interface when the embedded CPE is active.

Recertification Submission Guidelines for eCMM-based devices:

An eCMM-based device may be considered for recertification under either or both of the following conditions:

1. An eCMM was requalified due to a hardware modification to the eCMM itself.

2. A modification of the hardware of the eCMM-based device, excluding the eCMM.

3. If an eCMM is requalified due to a software change *only*, the eCMM-based device does not need to be recertified.

4. The submission requirements are the same as the submission requirements for eCMM-based device certification.

5.1.6 Wireless Devices

For CPE products that contain an 802.11x wireless interface, this interface must by default be configured in disabled mode on all submitted units. Default signal strength must be set as the submission is intended to be deployed. Dynamic Frequency Selection (if supported) must be disabled by default. All wireless enabled products must not transmit the following SSID or any other SSID. If special equipment is required for wireless interface testing appropriate devices must be included with the submission.

The default SSID for an 802.11x wireless device submitted should be the Product ID concatenated with the unit number, concatenated with _2G or _5G depending on the radio. (i.e. for a product submitted in CW1051 by ABCD, the SSID of the unit 12 should read ABCD1051-12_2G); **please use all capital letters.**

Detailed instructions must be provided on how to enable/disable the Wi-Fi and how to configure all settings (SSID, username/password, security, etc.). The testing facility will use submitted documentation (Wi-Fi MIBs, web interface, etc.) to configure the Wi-Fi settings. If configuration is via web interface, the user name for a wireless device should be set to "cablelabs" and the password to "admin".

5.1.7 Bridges

If the product utilizes any other data interface, please submit two bridges for Ethernet. Exceptions include USB or 802.11a/b/g, for which bridges are not required.

5.1.8 DOCSIS CMTS (Annex B)

Documentation as detailed in Section 4.8, including one operations manual.

CMTS vendors must also submit the 'CMTS Special Instructions and Programmable Features' available for download from InfoZone (https://community.cablelabs.com/wiki/plugins/servlet/appfusions/alfresco/download?id=358bc92a-70e2-4a3d-b5be-8f903f463ca9;1.0 under *Special Instructions Documents)*.

Four console cables (one per CMTS) must be provided. As required in the CMTS Special Instructions, detailed instructions on how to configure the CMTS using the console port **must** be provided.

On the CMTS application form, the supplier must list the MIB object(s) that contains the CMTS hardware and software revisions. The revisions listed in these MIB objects must match what is on the application for certification.

All of the four submitted CMTSs must be pre-configured with the DOCSIS Root CA Certificate and the Test DOCSIS Root CA Certification so that they appear in the docsBpi2CmtsCACertTable. For further information of the Test DRCA, see Section 9.1.

DOCSIS 3.0 and 2.0 compliant products must support the current version of the DOCSIS Testing MIB as posted on InfoZone https://community.cablelabs.com/wiki/display/TECHPUBS/DOCSIS+MIB+Current

In order to support "CMTS Load Balancing and DCC Operation" testing, a DOCSIS 3.1, DOCSIS 3.0 or 2.0 compliant product must support a rule/policy that demonstrates load balancing operations in the conditions defined in the ATP, either by default or via a vendor specific rule/policy. If the latter, instructions for configuring this rule/policy must be included in the CMTS Special Instructions document.

For a CMTS that supports more than one downstream in a single unit, at least one of the four CMTS units submitted for qualification must be configured with at least two active downstream ports. For a chassis/blade based CMTS, this could be done with multiple blades, or with multiple downstream ports on the same blade. However, all cards/blades in the CMTS must be consistent from unit to unit (i.e., it is not permissible for one CMTS to have a blade with two downstreams, and all others to have different blades with a single downstream). The unit that has multiple downstreams active must be labeled appropriately to indicate this.

5.1.9 EuroDOCSIS CMTS (Annex A)

EuroDOCSIS 3.0 CMTSs may be submitted using a "feature based" approach. This is further described in Section 1 of this document.

CMTS vendors must submit the completed CMTS Special Instructions documentation available on InfoZone (https://community.cablelabs.com/wiki/plugins/servlet/appfusions/alfresco/download?id=358bc92a-70e2-4a3d-b5be-8f903f463ca9;1.0 under *Special Instructions Documents)*. Further, a CMTS vendor must submit the following additional items:
- A labeled console cable for each unit
- A CMTS Operations manual
- The CMTS must be submitted with at least a 1000Base-T NSI interface

All submitted units must be pre-configured with the EuroDOCSIS Root CA certificate. The CMTS must be capable of supporting the EuroDOCSIS test Root CA certificate and the CMTS must be either pre-configured with the EuroDOCSIS test Root CA certificate in addition to the EuroDOCSIS Root CA certificate or capable of replacing the pre-configured EuroDOCSIS Root CA certificate in the CMTS with the special EuroDOCSIS test ROOT CA certificate.

In order to support "CMTS Load Balancing and DCC Operation" testing, a EuroDOCSIS 3.0 or 2.0 compliant product must support a rule/policy that demonstrates load balancing operations in the conditions defined in the ATP, either by default or via a vendor specific rule/policy. If the latter, instructions for configuring this rule/policy must be included in the CMTS Special Instructions document.

For a CMTS that supports more than one downstream in a single unit, at least one of the four CMTS units submitted for qualification must be configured with at least two active downstream ports. For a chassis/blade based CMTS, this could be done with multiple blades, or with multiple downstream ports on the same blade. However, all cards/blades in the CMTS must be consistent from unit to unit (i.e., it is not permissible for one CMTS to have a blade with two downstreams, and all others to have different blades with a single downstream). The unit that has multiple downstreams active must be labelled appropriately to indicate this.

A EuroDOCSIS 3.0 CMTS or a CMTS that supports multiple downstream channels per RF port must support the requirements in the DRFI specification.

5.1.9.1 CMTSs with DSG Agent Functionality

In addition to the requirements in Section 5.1.7 for a DOCSIS CMTS, a CMTS that also implements DSG Agent functionality must meet the following requirements:

- These products must comply with the DSG specification, in addition to the DOCSIS 3.0 or 2.0 specifications as they apply.

- The DOCSIS and DSG Requirements Checklist documents must be completed.

- The DSG section of the *CMTS Special Instructions* document available on InfoZone under the section titled *Special Instructions documents* (https://community.cablelabs.com/wiki/plugins/servlet/appfusions/alfresco/download?id=358bc92a-70e2-4a3d-b5be-8f903f463ca9;1.0) must be completed.

5.1.10 EQAM

The DEPI, DRFI, and M-OSSI specifications must be supported.

A DTI Client as defined in the DTI Specification must be supported.

Documentation as detailed in Section 4.8, including DEPI, DRFI, and M-OSSI Requirements Checklists, must be included.

If the ERMI specification is supported, the ERMI Requirements Checklist must be included as well.

EQAM vendors must also submit the 'EQAM Special Instructions' available for download from InfoZone under the section titled *Special Instructions documents* at
https://community.cablelabs.com/wiki/plugins/servlet/appfusions/alfresco/download?id=358bc92a-70e2-4a3d-b5be-8f903f463ca9;1.0

5.2   Software Images and Digital Certificates

Note that there are specific software and digital certificate requirements per project.

5.2.1 DOCSIS 3.0 or 2.0 Cable Modems and EuroDOCSIS 3.0 or 2.0 Cable Modems:

Two software image files must be provided to CableLabs in the submission .zip file.

First is the current image for the certification wave, **with a file name according to the following convention**:

> **<Product_ID>.img**

The current image is digitally signed by the manufacturer CVC.

The second file is a test image that is a duplicate of the current image except that, when the following MIB element is queried,

> iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).system(1).sysDescr(1)

the response from the modem contains the text "MAC-14 test image for CW##."

Note that, as a result of this modification to the sysDescr MIB object, the docsDevSwCurrentVers MIB object is also required to display a different software version number for this second image file containing the text "**MAC14_ver"** relative to the first image file.

The test image must also have the same signing time as the current image.

The second file name must follow the following convention:

> **<Product_ID>-MAC-14.img**

5.2.2 Additional Files for DOCSIS 3.0 or 2.0 Cable Modems

5.2.2.1 Software Image Files

In the case of the DOCSIS 3.0 or 2.0 cable modem submission, in addition to the Current Image and MAC-14 image file for products (unit #1-#28), the following two (2) additional software images must also be provided in the submission .zip file.

The third and fourth image files are for Test DRCA devices which are digitally signed by a test manufacturer CVC issued from the Test DRCA. These are for Units #29 - #30.

The third file is the current image for the Test DRCA products, **with a file name according to the following convention:**

> **<Product_ID>-TestDRCA.img**

The fourth file is a test image that is a duplicate of the current image for the Test DRCA products except when the following MIB element is queried,

> iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).system(1).sysDescr(1)

the response from the modem contains the text "BPI-23 test image for CW##".

Note that, as a result of this modification to the sysDescr MIB object, the docsDevSwCurrentVers MIB object is also required to display a different software version number for this fourth image file containing the text "**BPI23_ver"** relative to the third image file.

The fourth file name must follow this convention:

> **<Product_ID>-TestDRCA-BPI-23.img**

5.2.2.2 Digital Certificate Files

Digital Certificate File: In the case of the DOCSIS 3.1, 3.0, or 2.0 cable modem submission, in order to download the MAC-14 image file (<Product_ID>-MAC-14.img) and the current image file (<Product_ID>.img) to the product cable modems (unit #1-#27), these two image files must contain:

    a)   the identical Manufacturer CVC (Code Verification Certificate) issued by the DOCSIS Root CA

    b)   the same signingTime values of the CVS (Code Verification Signature).

For further information on the Manufacturer CVC issuance by the DOCSIS Root CA, see the Section 9. This Manufacturer CVC must also be provided in the submission .zip file, with a file name according to the following convention:

> **<Product_ID>-CVC.der**

Digital Certificate Test File: In order to download the fourth image file (<Product_ID>-TestDRCA-BPI-23.img) and the third current image file (<Product_ID>-TestDRCA-BPI-23.img) to the Test DRCA cable modems (unit #29-#30), these two image files must contain:

a) the identical Test Manufacturer CVC signed by the Test DRCA private key, and

b) the same signing Time values of the CVS.

For further information on the Test DRCA, see Section 9.3. This Test Manufacturer CVC must also be provided in the submission documentation, with a file name according to the following convention:

<Product_ID>-TestDRCA-CVC.der.

5.2.3 Additional Files for EuroDOCSIS 3.0 or 2.0 Cable Modems

5.2.3.1 Software Image Files

In the case of a submission of a EuroDOCSIS 2.0 or 3.0 cable modem or STB/CM that uses the EuroDOCSIS software upgrade mechanism, two additional software images must also be provided in the file upload.

The **third file** is the current image for the Test EDRCA cable modems (see above), with a file name according to the following convention:

⟨**Product ID⟩-TestEDRCA.img**

The current image for Test EDRCA products is digitally signed by a test manufacturer CVC issued from the Test EDRCA.

The **fourth file** is a test image that is a duplicate of the current image for the Test EDRCA cable modems except that it is named differently:

⟨**Product ID⟩-TestEDRCA-BPI-23.img**

This BPI.23 test image must contain special text in the following fields:

• System descriptor:

iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).system(1).sysDescr(1): "BPI.23 test image of CW X"

• Software version: reference to BPI.23 test image

5.2.3.2 Digital Certificate Files

Digital Certificate File: In the case of a EuroDOCSIS 3.0 or 2.0 cable modem submission, in order to download the MAC-14 image file (<Product_ID>-MAC-14.img) and the current image file (<Product_ID>.img) to the product cable modems (unit #1-#24), these two image files must contain:

a) the identical Manufacturer CVC (Code Verification Certificate) issued by the EuroDOCSIS Root CA

b) the same signingTime values of the CVS (Code Verification Signature).

For further information on the Manufacturer CVC issuance by the EuroDOCSIS Root CA, see the Excentis website:
https://www.excentis.com/testing/certification/programs/eurodocsis/digital-certificates.
This Manufacturer CVC must also be provided in the submission .zip file, with a file name according to the following convention:

<Product_ID>-CVC.der

Digital Certificate Test File: In order to download the fourth image file (<Product_ID>-TestEDRCA-BPI-23.img) and the third current image file (<Product_ID>-TestEDRCA.img) to the Test EDRCA cable modems (unit #25-#26) these two image files must contain:

a) the identical Test Manufacturer CVC signed by the Test EDRCA private key

b) the same signing Time values of the CVS.

For further information on the Test EDRCA, see Section 9.3. This Test Manufacturer CVC must also be provided in the submission documentation, with a file name according to the following convention:

<Product_ID>-TestEDRCA-CVC.der.

5.2.4 DOCSIS 3.1 Cable Modems:

Image files created from the new DOCSIS 3.1 PKI:

Two software image files must be provided to CableLabs in the submission .zip file.

First is the current image for the certification wave, w**ith a file name according to the following convention**:

<Product_ID>-NewPKI.img

The current image is digitally signed by the manufacturer CVC from the new PKI.

The second file is a test image that is a duplicate of the current image except that, when the following MIB element is queried,

iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).system(1).sysDescr(1)

the response from the modem contains the text "MAC-14 test image signed by the New PKI for CW##."

Note that, as a result of this modification to the sysDescr MIB object, the docsDevSwCurrentVers MIB object is also required to display a different software version number for this second image file containing the text "**MAC14_NewPKI_ver**" relative to the first image file.

5.2.5 Additional Files for DOCSIS 3.1Cable Modems

5.2.5.1 Software Image Files

In the case of the DOCSIS 3.1 cable modem submission**, in addition to the Current Image and MAC-14 image** for the products (unit #1-#28), the following two (2) additional software images must also be provided in the submission .zip file.

The third and fourth image files are for the Test CRCA products (unit #29-#30), devices which are digitally signed by a test manufacturer CVC issued from the Test CRCA. These are for Units #29 - #30.

The third file is the current image for the Test CRCA products, **with a file name according to the following convention:<Product_ID>-TestCRCA-NewPKI.img**

The fourth file is a test image that is a duplicate of the current image for the Test CRCA from the New PKI products except when the following MIB element is queried,

iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).system(1).sysDescr(1)

the response from the modem contains the text "BPI-23 test image signed by the New PKI for CW##".

Note that as a result of this modification to the sysDescr MIB object, the docsDevSwCurrentVers MIB object is also required to display a different software version number for this fourth image file containing the text "**BPI23_NewPKI_ver**" relative to the third image file.

The fourth file name must follow this convention:

<Product_ID>-TestCLCA-BPI-23-NewPKI.img

5.2.5.2 Digital Certificate Files

Digital Certificate File: In the case of the DOCSIS 3.1 cable modem submission, in order to download the MAC-14 image file (<Product_ID>-MAC-14-NewPKI.img) and the current image file (<Product_ID>-NewPKI.img) to the product cable modems (unit #1-#27), the signature header of these two image files must contain:

a) Manufacturer CVCs (Code Verification Certificates) with identical subject names and validity periods issued by the CableLabs CVC CA,

b) the issuing CableLabs CVC CA certificate

c) the same signingTime values of the CVS (Code Verification Signature).

For further information on the Manufacturer CVC issuance by the CableLabs CVC CA, see Section 9. This Manufacturer CVC must also be provided in the submission .zip file, with a file name according to the following convention:

<Product_ID>-CVC-NewPKI.der

Digital Certificate Test File: In order to download the fourth image file (<Product_ID>-TestCLCA-BPI-23-NewPKI.img) and the third current image file (<Product_ID>-TestCLCA-BPI-23-NewPKI.img) to the Test CRCA cable modems (unit #29-#30) the signature header of these two image files must contain:

a) Test Manufacturer CVCs with identical subject names and validity periods signed by the Test CableLabs CVC CA private key

b) the issuing Test CableLabs CVC CA certificate

c) the same signing Time values of the CVS.

For further information on the Test CableLabs CVC CA, see Section 9.3. This Test Manufacturer CVC must also be provided in the submission documentation, with a file name according to the following convention:

<Product_ID>-TestCRCA-CVC-NewPKI.der.

5.3   CMTS and Other DOCSIS Headend Submission Requirements

	Certification	Re-Certification	OEM / Paper
DOCSIS CMTS **DOCSIS CMTS + MM** **EQAM** **CCAP** **PacketCable CMTS** **PacketCable + Multimedia CMTS**	**2** May need more units based on vendor timeline requirements and feature sets requested. Additional units (strongly recommended for Escort Engineer work in the Visiting Engineer lab area.)	**0**	**0**
	All units to Louisville	N/A	N/A
EuroDOCSIS CMTS	**3**	**0**	**0**
	2 units to Ghent 1 units to Louisville	N/A	N/A
EuroDOCSIS CMTS + MM **EuroPacketCable CMTS** **EuroPacketCable + Multimedia CMTS**	**5**	**0**	**0**
	4 units to Ghent 1 units to Louisville	N/A	N/A

5.3.1   CMTS SNMP Coexistence Modes of Operation and Event Notifications

The following setup is required for CMTS OSS testing to cover SNMP modes of operation requirements contained in RFC 3411 through RFC 3416 and RFC 3584.

5.3.1.1 CMTS Configuration

The vendor must configure one CMTS and provide written step-by-step instructions for that purpose in case of a full configuration reset. The vendor may use any of the following or another procedure:

- CLI script with the specific parameters contained in the CMTS Special Instructions and Programmable Features
- Automated Application/script
- Config File
- SNMP commands (provide the details as object-by-object SNMP SET commands)
- usmUserTable from RFC 3414, for Authentication and Privacy Passwords: if the CLI or any other procedure requires localize the keys from the passwords, provide the tools and procedures.

5.3.2   Default Operation for pre-3.0 DOCSIS CMTSs

If SNMPv1/v2c NmAccess or proprietary mode is supported, the CMTS should be in SNMPv1/v2c NmAccess or proprietary mode by default, including instructions for switching between SNMPv1/v2c NmAccess or proprietary mode and SNMP Coexistence Mode. Proprietary mode stands for a SNMPv1/v2c setup that doesn't configure docsDevNmAccessTable or any table in RFC 3411 through RFC 3415 and RFC 2576.

5.3.2.1 SNMPv1/v2c NmAccess/Proprietary Mode if supported for pre-3.0 DOCSIS CMTSs

The following community strings are used:

Community string   "public"   with read-only/traps access

Community string   "private"   with read-write access

5.3.3 SNMP Notifications and syslog

Syslog must be set for an IP that will be supplied on submission day and syslog event reporting must be active, including instructions for changing the syslog IP address.

SNMP Notifications for all required events, including DOCSIS events, must be enabled. SNMP Notifications must only be enabled for the SNMPv1/v2c users/community strings. SNMPv3 users must have SNMP Notifications disabled by default (see snmpTargetAddrRowStatus 'notInService' in snmpTargetAddrTable of RFC 3413).

The IP address of the SNMP Notification receiver will be supplied on submission day. Instructions for changing the SNMP Notification receiver IP address must be supplied.

5.3.4 SNMP access list, if required

All nodes on the 10.50.1.x subnet should have access (a list of specific nodes will be provided on submission day). The CMTS vendor must provide instructions to change the access list.

5.3.5 SNMPv3 Coexistence Mode

Users must have the following setup:

securityName:"rotesting"	v1/v2c read-only/traps
securityName:"rwtesting"	v1/v2c read-write/traps
User: "noAuthNoPrivUser"	v3 read-write/traps access
	security level: "noAuthNoPriv"
User: "AuthNoPrivMD5User"	v3 read-write/traps access
	security level: "AuthNoPriv"
	authProtocol: MD5
	authPassword: "AuthPassword"
User: "AuthNoPrivSHAUser"	v3 read-write/traps access
	security level: "AuthNoPriv"
	authProtocol: SHA
	authPassword: "AuthPassword" (if SHA is supported)
User:"AuthPrivMD5User"	v3 read-write/traps access
	security level: "AuthPriv"
	authProtocol: MD5
	authPassword: "AuthPassword"
	privProtocol: DES
	privPassword: "PrivPassword"
User "AuthPrivSHAUser"	v3 read-write/traps access
	security level: "AuthPriv"
	authProtocol: SHA
	authPassword: "AuthPassword" (if SHA is supported)
	privProtocol: DES
	privPassword: "PrivPassword"

Views: All coexistence users must have a view named "docsisManagerView" with access to the entire MIB tree starting with "internet" or below.

After setup, the snmpCommunityTable, snmpTargetAddrExtTable, usmUserTable, vacmSecurityToGroupTable, vacmAccessTable, vacmViewTreeFamilyTable, vacmContextTable, snmpTargetAddrTable, snmpTargetParamsTable, snmpNotifyTable, snmpNotifyFilterProfileTable and snmpNotifyFilterTable, should resemble the tables in Appendix A of the OSSIv3.0 ATP.

5.3.6 Notes

Please provide the following additional information:

- Objects and indexes taking values other than the solicited because of CLI auto setup
- Objects/Tables not supported by the implementation
- Special operation conditions and requirements

5.4   DOCSIS CMCI Data Port Verification Guidelines

CMCI data ports must adhere to the following guidelines:

All visible data ports must be labeled appropriately. If a modem with covered ports is submitted, the cover must be permanent (temporary tape is not acceptable) and remain covered in order to retain certification status. If a visible port is not active, a full disclosure of such condition is required and will not be listed as a tested interface, in the event of successful certification\qualification. The Certification Board(s) will have final decision; therefore it is highly recommended to make such a disclosure available to CableLabs and the board prior to submission.

Data ports that are not explicitly defined in the CMCI Specification (e.g. HomePNA, wireless, etc.) will be verified for proper operation by CableLabs, utilizing equipment submitted by the vendor as part of that vendor's submission to the wave.

All products with non-specified data ports must have a means to convert to an Ethernet interface, using a vendor-supplied electronic translation adapter or exhibit an Ethernet data port, in addition to the non-specified data port.

Kyrio will provide only a CMTS and a cable plant to connect the device. The vendor must provide required data port-specific test equipment.

Products may contain ports for other uses beyond data ports. For example, a PacketCable™ E-MTA will contain RJ-11 phone jacks and an OpenCable™ Set Top Box may contain digital video ports. Such ports must be both labeled and operational, and may be used to provide stimulus to a device for DOCSIS certification testing.

Any exception to these guidelines must be presented to CableLabs in advance of submission for approval by the Certification Board(s) and noted in the Executive Summary for submission.

Note: Console and/or serial ports are not allowed on cable modems. These ports, whether active or inactive, should not be physically present on the cable modem. Cable modems that are submitted for certification which include a console and/or serial port will be returned upon submission, except as defined in section 5.1.

6 PACKETCABLE SUBMISSION REQUIREMENTS

Vendors submitting for certification are required to identify optional functionality that has been implemented in the application form.

6.1   E-MTA

Each submission follows these general rules:

- "Diagnostic" unit and it is a regular unit with an active diagnostic port (may include special SW load)
- "Test DRCA" units substitute the DOCSIS ROOT PUBLIC KEY for TEST DOCSIS ROOT PUBLIC KEY
- "Test EDRCA" units substitute the EURODOCSIS ROOT PUBLIC KEY for TEST EURODOCSIS ROOT PUBLIC KEY
- "Test CRCA" units substitute the CABLELABS ROOT CA units for TEST CABLELABS ROOT CA
- "Test Packet Cable SPRCA" units substitute the Packet Cable SPRCA for the TEST Packet Cable SPRCA

The following information provides specific product submission requirements.

6.1.1 DOCSIS 3.0 PacketCable 1.5 EMTA

Certification Level	Units	Shipping Location	Details differences among units		Common to all units
CERTIFICATION	30	Louisville	#1	"Diagnostic" unit	DOCSIS MFG CA CERTIFICATE DOCSIS CM CERT DOCSIS CM PRIVATE KEY PC MTA MFG CA CERT PC MTA CERT PC MTA PRIVATE KEY
			#1 through #28	DOCSIS ROOT PUBLIC KEY PC SERVICE PROVIDER ROOT CERTIFICATE	
			#29 and #30	TEST DOCSIS ROOT PUBLIC KEY TEST PC SERVICE PROVIDER ROOT CERTIFICATE	
	15	Ghent	#31	"Diagnostic" unit	
			#31 through #43	DOCSIS ROOT PUBLIC KEY PC SERVICE PROVIDER ROOT CERTIFICATE	
			#44 and #45	TEST DOCSIS ROOT PUBLIC KEY TEST PC SERVICE PROVIDER ROOT CERTIFICATE	
RE-CERTIFICATION	15	Louisville	#1	"Diagnostic" unit	DOCSIS MFG CA CERTIFICATE DOCSIS CM CERT DOCSIS CM PRIVATE KEY PC MTA MFG CA CERT PC MTA CERT PC MTA PRIVATE KEY
			#1 through #13	DOCSIS ROOT PUBLIC KEY PC SERVICE PROVIDER ROOT CERTIFICATE	
			#14 and #15	TEST DOCSIS ROOT PUBLIC KEY TEST PC SERVICE PROVIDER ROOT CERTIFICATE	
	10	Ghent	#11	"Diagnostic" unit	
			#11 through #23	DOCSIS ROOT PUBLIC KEY	

Certification Level	Units	Shipping Location	Details differences among units		Common to all units
				PC SERVICE PROVIDER ROOT CERTIFICATE	
			#24 and #25	TEST DOCSIS ROOT PUBLIC KEY TEST PC SERVICE PROVIDER ROOT CERTIFICATE	
OEM / PAPER	5	Louisville	#1 through #5	NA - all units are the same.	DOCSIS MFG CA CERTIFICATE DOCSIS CM CERT DOCSIS CM PRIVATE KEY DOCSIS ROOT PUBLIC KEY PC MTA MFG CA CERT PC MTA CERT PC MTA PRIVATE KEY PC SERVICE PROVIDER ROOT CERTIFICATE
	5	Ghent	#6 through #10		

6.1.2 EURODOCSIS 3.0 EUROPacketCable 1.5 EMTA

Certification Level	Units	Shipping Location	Details differences among units		Common to all units
CERTIFICATION	35	Ghent	#1	"Diagnostic" unit	EURODOCSIS MFG CA CERTIFICATE EURODOCSIS CM CERT EURODOCSIS CM PRIVATE KEY EURO PC MTA MFG CA CERT EURO PC MTA CERT EURO PC MTA PRIVATE KEY
			#1 through #33	EURODOCSIS ROOT PUBLIC KEY EURO PC SERVICE PROVIDER ROOT CERTIFICATE	
			#34 and #35	TEST EURODOCSIS ROOT PUBLIC KEY TEST EURO PC SERVICE PROVIDER ROOT CERTIFICATE	
	10	Louisville	#36	"Diagnostic" unit	
			#36 through #43	EURODOCSIS ROOT PUBLIC KEY EURO PC SERVICE PROVIDER ROOT CERTIFICATE	
			#44 and #45	TEST EURODOCSIS ROOT PUBLIC KEY TEST EURO PC SERVICE PROVIDER ROOT CERTIFICATE	
RE-CERTIFICATION	15	Ghent	#1	"Diagnostic" unit	EURODOCSIS MFG CA CERTIFICATE EURODOCSIS CM CERT EURODOCSIS CM PRIVATE KEY PC MTA MFG CA CERT
			#1 through #13	EURODOCSIS ROOT PUBLIC KEY EURO PC SERVICE PROVIDER ROOT CERTIFICATE	
			#14 and #15	TEST EURODOCSIS ROOT PUBLIC KEY	

Certification Level	Units	Shipping Location	Details differences among units		Common to all units
				TEST EURO PC SERVICE PROVIDER ROOT CERTIFICATE	PC MTA CERT PC MTA PRIVATE KEY
	5	Louisville	#16	"Diagnostic" unit	
			#16 through #20	EURODOCSIS ROOT PUBLIC KEY EURO PC SERVICE PROVIDER ROOT CERTIFICATE	
OEM / PAPER	5	Ghent	#1 through #5	NA - all units are the same.	EURODOCSIS MFG CA CERTIFICATE EURODOCSIS CM CERT EURODOCSIS CM PRIVATE KEY EURODOCSIS ROOT PUBLIC KEY EURO PC MTA MFG CA CERT EURO PC MTA CERT EURO PC MTA PRIVATE KEY EURO PC SERVICE PROVIDER ROOT CERTIFICATE
	5	Louisville	#6 through #10		

6.1.3 DOCSIS 3.1 PacketCable 1.5 EMTA

Certification Level	Units	Shipping Location	Details differences among units		Common to all units
CERTIFICATION	30	Louisville	#1	"Diagnostic" unit	DOCSIS MFG CA CERTIFICATE DOCSIS CM CERT DOCSIS CM PRIVATE KEY PC MTA MFG CA CERT PC MTA CERT PC MTA PRIVATE KEY CABLELABS DEVICE CA CERTIFICATE CM DEVICE CERT CM DEVICE PRIVATE KEY
			#1 through #28	DOCSIS ROOT PUBLIC KEY PC SERVICE PROVIDER ROOT CERTIFICATE CABLELABS ROOT CA CERTIFICATE	
			#29 and #30	TEST DOCSIS ROOT PUBLIC KEY TEST PC SERVICE PROVIDER ROOT CERTIFICATE TEST CABLELABS ROOT CA CERTIFICATE	
	15	Ghent	#31	"Diagnostic" unit	
			#31 through #43	DOCSIS ROOT PUBLIC KEY PC SERVICE PROVIDER ROOT CERTIFICATE	

				CABLELABS ROOT CA CERTIFICATE	
			#44 and #45	TEST DOCSIS ROOT PUBLIC KEY TEST PC SERVICE PROVIDER ROOT CERTIFICATE TEST CABLELABS ROOT CA CERTIFICATE	
RE-CERTIFICATION	15	Louisville	#1	"Diagnostic" unit	DOCSIS MFG CA CERTIFICATE DOCSIS CM CERT DOCSIS CM PRIVATE KEY PC MTA MFG CA CERT PC MTA CERT PC MTA PRIVATE KEY CABLELABS DEVICE CA CERTIFICATE CM DEVICE CERT CM DEVICE PRIVATE KEY
			#1 through #13	DOCSIS ROOT PUBLIC KEY PC SERVICE PROVIDER ROOT CERTIFICATE CABLELABS ROOT CA CERTIFICATE	
			#14 and #15	TEST DOCSIS ROOT PUBLIC KEY TEST PC SERVICE PROVIDER ROOT CERTIFICATE TEST CABLELABS ROOT CA CERTIFICATE	
	10	Ghent	#11	"Diagnostic" unit	
			#11 through #23	DOCSIS ROOT PUBLIC KEY PC SERVICE PROVIDER ROOT CERTIFICATE	
			#24 and #25	TEST DOCSIS ROOT PUBLIC KEY TEST PC SERVICE PROVIDER ROOT CERTIFICATE	
OEM / PAPER	5	Louisville	#1 through #5	NA - all units are the same.	DOCSIS MFG CA CERTIFICATE DOCSIS CM CERT DOCSIS CM PRIVATE KEY DOCSIS ROOT PUBLIC KEY PC MTA MFG CA CERT PC MTA CERT PC MTA PRIVATE KEY PC SERVICE PROVIDER ROOT CERTIFICATE CABLELABS DEVICE CA CERTIFICATE CM DEVICE CERT CM DEVICE PRIVATE KEY CABLELABS ROOT CA CERTIFICATE
	5	Ghent	#6 through #10		

6.1.4 DOCSIS 3.1 EuroPacketCable 1.5 EMTA (EURODOCSIS 3.0)

Certification Level	Units	Shipping Location	Details differences among units		Common to all units
CERTIFICATION	30	Louisville	#1	"Diagnostic" unit	EURODOCSIS MFG CA CERTIFICATE EURODOCSIS CM CERT EURODOCSIS CM PRIVATE KEY EURO PC MTA MFG CA CERT EURO PC MTA CERT EURO PC MTA PRIVATE KEY CABLELABS DEVICE CA CERTIFICATE CM DEVICE CERT CM DEVICE PRIVATE KEY
			#1 through #28	EURODOCSIS ROOT PUBLIC KEY EURO PC SERVICE PROVIDER ROOT CERTIFICATE CABLELABS ROOT CA CERTIFICATE	
			#29 and #30	TEST EURODOCSIS ROOT PUBLIC KEY TEST EURO PC SERVICE PROVIDER ROOT CERTIFICATE TEST CABLELABS ROOT CA CERTIFICATE	
	25	Ghent	#31	"Diagnostic" unit	
			#31 through #53	EURODOCSIS ROOT PUBLIC KEY EURO PC SERVICE PROVIDER ROOT CERTIFICATE CABLELABS ROOT CA CERTIFICATE	
			#54 and #55	TEST EURODOCSIS ROOT PUBLIC KEY TEST EURO PC SERVICE PROVIDER ROOT CERTIFICATE TEST CABLELABS ROOT CA CERTIFICATE	
RE-CERTIFICATION	15	Louisville	#1	"Diagnostic" unit	EURODOCSIS MFG CA CERTIFICATE EURODOCSIS CM CERT EURODOCSIS CM PRIVATE KEY PC MTA MFG CA CERT PC MTA CERT PC MTA PRIVATE KEY CABLELABS DEVICE CA CERTIFICATE CM DEVICE CERT CM DEVICE PRIVATE KEY
			#1 through #13	EURODOCSIS ROOT PUBLIC KEY EURO PC SERVICE PROVIDER ROOT CERTIFICATE CABLELABS ROOT CA CERTIFICATE	
			#14 and #15	TEST EURODOCSIS ROOT PUBLIC KEY TEST EURO PC SERVICE PROVIDER ROOT CERTIFICATE TEST CABLELABS ROOT CA CERTIFICATE	
	10	Ghent	#16	"Diagnostic" unit	
			#16 through #23	EURODOCSIS ROOT PUBLIC KEY EURO PC SERVICE PROVIDER ROOT CERTIFICATE CABLELABS ROOT CA CERTIFICATE	

OEM / PAPER					
			#24 and #25	TEST EURODOCSIS ROOT PUBLIC KEY TEST EURO PC SERVICE PROVIDER ROOT CERTIFICATE TEST CABLELABS ROOT CA CERTIFICATE	
	5	Louisville	#1 through #5	NA - all units are the same.	EURODOCSIS MFG CA CERTIFICATE EURODOCSIS CM CERT EURODOCSIS CM PRIVATE KEY EURODOCSIS ROOT PUBLIC KEY EURO PC MTA MFG CA CERT EURO PC MTA CERT EURO PC MTA PRIVATE KEY EURO PC SERVICE PROVIDER ROOT CERTIFICATE CABLELABS DEVICE CA CERTIFICATE CM DEVICE CERT CM DEVICE PRIVATE KEY CABLELABS ROOT CA CERTIFICATE
	5	Ghent	#6 through #10		

6.1.5 PacketCable High Definition Voice

For PacketCable E-MTA devices submitted for certification that include the optional High Definition Voice feature the following will apply:
- The device must implement an Embedded DECT Interface or a Wideband SLIC Interface or both an Embedded DECT Interface and a Wideband SLIC Interface.
- For devices with Embedded DECT Interface, each unit must be submitted with at least one DECT handset for testing purposes. The vendor must supply proof that the Embedded DECT Components have successfully been certificated by the DECT Forum for highest level of CAT-iq certification at the time of production. The devices will be tested using DECT handsets form a range of vendors for interoperability and results will be reported to the Certification Board.
- The device may have voice quality testing performed and results will be presented as supplemental information to the Certification Board. If such testing is preformed, all devices submitted for that certification wave will be tested equally.

6.2 PacketCable 1.5 and PacketCable Multimedia Certification

PacketCable products may be submitted for PacketCable 1.5 Certification or Qualification and PacketCable Multimedia Qualification.

The following products are eligible for PacketCable 1.5 Certification/Qualification: E-MTA, CMTS. The table below shows the PacketCable 1.5 required interfaces.

The following product is eligible for PacketCable Multimedia Qualification: CMTS.

The table below shows the PacketCable 1.5, PacketCable Multimedia and PacketCable Residential SIP Telephony required interfaces.

Component	PacketCable 1.5	PacketCable Multimedia
E-MTA	NCS, DQoS, SEC, Prov, CODEC, **MEM, Battery Backup MIBs**	N/A

CMTS PacketCable	DQoS, SEC, **LAESS, EM**	MM
CMTS Multimedia	N/A	MM
CMTS PacketCable + Multimedia	DQoS, SEC, **LAESS, EM**	MM

6.2.1 *EuroPacketCable CMTS*

Each EuroPacketCable CMTS submission must contain 3 units for Ghent plus 1 unit for Louisville and includes a EuroDOCSIS 3.0 or 2.0 submission.

Details on the EuroDOCSIS configuration and requirements can be found in the previous section. Details on the EuroPacketCable CMTS special instructions can be found on InfoZone.

Each EuroPacketCable submission must also include a detailed 'operations manual' with details on configuration.

6.2.2 *EuroPacketCable Multimedia CMTS*

Each EuroPacketCable Multimedia CMTS submission must contain 3 units for Ghent plus 1 unit for Louisville and includes a EuroDOCSIS 3.0 or 2.0 submission.

Details on the EuroDOCSIS configuration and requirements can be found in the previous section. Details on the EuroPacketCable Multimedia CMTS special instructions can be found on InfoZone.

Each EuroPacketCable Multimedia submission must also include a detailed 'operations manual' with details on configuration.

6.2.3 *EuroPacketCable and EuroPacketCable Multimedia CMTS*

Each combined EuroPacketCable and EuroPacketCable Multimedia CMTS submission must contain 3 units for Ghent and 1 unit for Louisville and includes a EuroDOCSIS 3.0 or 2.0 submission.

7 OPENCABLE SUBMISSION REQUIREMENTS

NOTE: Certification testing for OCAP/tru2way devices ended June 30, 2014. Any device submission that includes OCAP/tru2way specifications will no longer be accepted for certification testing. OCAP/tru2way specification references within this guide have been removed. Qualification of CableCARDs and Certification of OpenCable Unidirectional Receivers (OCUR) is still available under these Guidelines. For "verification" guidelines applicable to Unidirectional Digital Cable Products ("Plug and Play") devices built in accordance with FCC regulations, please see http://www.cablelabs.com/wp-content/uploads/2014/01/UDCP-Guidelines.pdf

7.1 Product Documentation

Manufacturer must provide CableLabs with the following documentation in one .zip file.

1. **Executive Summary.** The Executive Summary should include the following:
   a. **Product Summary.** A high-level description of the product being submitted for certification and why the product should be accepted for certification. Details on tasks and efforts conducted by the vendor may be highlighted here.
   b. **Testing Efforts Description**: A summary of the activities the Manufacturer has undertaken to ensure the product is compliant to OpenCable specifications and is stable and ready to proceed for certification testing. The summary should include a list of all of the testing activities conducted not just the effort to test for Requirements compliance. Note, *prior to* formal Certification testing submission, it is *highly recommended* that the device be submitted to the OpenCable Interoperability and Integration Testing process.
   c. **Test Results Summary.** A report of the applicable Requirements Checklist results shall be provided which summarizes the results of the Manufacturer's testing (actual completed Requirements Checklist data is also required for submission). The report should include;
      - Total Requirements Items Compliant
      - Total Requirements Items Non-Compliant
      - Total Requirements Items Not Applicable
      - The detailed test procedure used for each REQ
      - A detailed explanation and justification of compliant items that were passed based on design reviews or implied success based on indirect testing. Such design review or indirect testing should be minimized.
      - A detailed explanation of any Non-Compliant items with justification why the requirement will not impact the certification process results
      - An explanation of why any Not Applicable items are not relevant to the certification testing process

2. **OpenCable Certification Admission Application Form ("Application").**
   The web-based application is available at https://www.cablelabs.com/newpst/. To request a vendor login/password to access the web-based application, please contact labs@kyrio.com.

   The following submission information must be provided via the web-based application:

      a. The vendor must use the current version of the web-based form to provide all necessary product submission information
      b. When submitting for the first time, the vendor must submit a signed original signature page to be downloaded from the web-based form. An Officer and Quality Assurance Manager of the vendor company must sign this document to affirm the accuracy of all Admission Application information related to the product.
      c. Hardware and software revisions and sysDescr, or internal software readouts, **must** match the product as submitted or resubmission will be required

3. **Completed Vendor Checklist.** The Vendor Checklist should be a completed version of the latest OpenCable Vendor Checklist document available at:
   https://community.cablelabs.com/wiki/display/TECHPUBS/OpenCable+PICS+Requirements+Checklists# .
   "Completed" means each line item is clearly marked with a "Yes" or "No" or "N/A". Each REQ line item must refer to a given test procedure that was used to verify that specific REQ item. The Vendor Checklist is a manufacturer's formal declaration to the level of the product's conformance to the Specification. Vendor Checklist and support documents must accurately represent the product submitted.

4. **Detailed Acceptance Test Plan (ATP).** Each manufacturer is responsible, with respect to its own product, for writing and verifying each test procedure on each line item of the Vendor Checklist, and for testing the product against it. The actual data gathered for each test must be attached to support each of the verifying REQs. Acceptable sources of test procedures for product manufacturers are: (1) Silicon manufacturers (for chip conformance to specs); (2) Commonly used or widely available ATPs for the cable industry, such as the CableLabs ATP, which is available via the project websites; (3) The manufacturer's internally developed ATPs. The Certification Board requests that each test procedure be documented in a similar manner as the CableLabs ATP located at:

. (Note that manufacturer is responsible for providing to CableLabs an appropriate "DRM plug-in" for the OCUR test tool, as applicable.)

5. **Interoperability Test Report.** The Interoperability Test Report is a summary of all the testing performed at CableLabs or Kyrio (e.g., Dry Runs), MSO locations (field trial), other Interops, third-party locations and other manufacturer sites. The testing performed and summarized in the Interoperability Test Report should demonstrate that the product for which certification is applied operates with as many other products as possible. Specifically, interoperability goals are as follows:

   CableCARD Modules: demonstrate interoperability with the available OpenCable features on at least three (3) Host devices or appropriate test platforms.

   OCUR Devices: demonstrate interoperability with the available OpenCable features on (1) at least two CableCARD Modules based on different hardware platforms and (2) each of the deployed headend networks (currently Motorola, Scientific Atlanta, Conax, NDS and Nagravision).

6. **Digital Certificates.** OCUR and CableCARD products require signed X.509 Device Digital Certificates for authentication purposes. The monolithic code image used for software download must be signed with a Manufacturer Code Verification Certificate (CVC) issued under the CableLabs CVC CA (not the Manufacturer CVC issued under the DOCSIS Root CA).

7. **DFAST Parameters**. Host and CableCARD products submitted for certification require production DFAST parameters. See the OpenCable Security Specification (http://www.cablelabs.com/specifications/specification-search/) and the Digital Certificate Authorization Agreement (DCAA) (http://www.cablelabs.com/resources/digital-certificate-issuance-service/) for details.

7.1.1 *OpenCable Submissions:*

	Certification	Re-Certification	OEM / Paper
OpenCable Unidirectional Receiver	4	4	0
	All units to Louisville	All units to Louisville	N/A
CableCARD	20	20	0
	All units to Louisville	All units to Louisville	N/A
Tuning Resolver	2	2	0
	All units to Louisville	All units to Louisville	N/A

7.1.1.1 *OpenCable Host Submissions:*

OpenCable Host Devices submitted for certification must include production:
- DFAST secrets
- Host Device certificate
- Code Verification Certificate
- Any other production certificates, Root CAs, CAs and other Critical Security Parameters required by specifications

Products submitted for Practice Runs must have production DFAST secrets and host device certificates, and the monolithic code image provided must be signed using the CableLabs Manufacturer CVC.

7.1.1.2 *OCUR Submissions*

OpenCable Unidirectional Receiver products submitted for certification must include production:
- DFAST secrets
- OCUR device certificate
- Any other production certificates, Root CAs, CAs and Critical Security Parameters required by specifications

OpenCable Unidirectional Receivers may only be submitted for certification with aa CableLabs-approved Digital Rights Management (DRM) solutions. Manufacturer is responsible for ensuring that the DRM is submitted to CableLabs for review and approval prior to the submission of product for certification testing. In addition, the manufacturer is responsible for ensuring that applicable licenses are in place with CableLabs, and that a suitable "DRM plug-in" is provided to CableLabs for use in the OCUR test tools used for certification testing.

7.1.1.3 Tuning Resolver (Adapter) Submissions

These requirements are for stand-alone Tuning Resolver submissions. Requirements for M-UDCP devices with tuning resolvers are available in the guidelines available at: http://www.cablelabs.com/wp-content/uploads/2014/01/UDCP-Guidelines.pdf

Tuning resolver products submitted for Qualification must include:
- Completed Requirements Checklist
- Detailed ATP

7.1.2 Additional Submission InstructionsOperational Code Image (OCUR)

Manufacturer must provide one signed operational code image as specified in the OCUR specification. The signed image in the .zip file must exactly match the operational code image included in the product(s) being submitted for testing. If the OCUR product is certified, CableLabs will co-sign the operational code image provided in the .zip file and will return the signed code to the manufacturer.

8 DPOE SUBMISSION REQUIREMENTS

8.1 DPoE PRODUCTS

The following information provides specific product submission requirements.

8.1.1 DPoE 1.0 Submissions

All DPoE 1.0 ONU units must contain the real device certificate and real CableLabs DPoE Mfr CA certificate (DPoE CA00008).

		Certification	Re-Certification	OEM / Paper
DPoE ONU	15		5	5
	In the case of units requiring an Ethernet adapter, as per section 8.4, 15 adapters should be provided.			
	15 units to Louisville		5 units to Louisville	5 units to Louisville
DPoE System	2		2	2
	May need more units based on vendor time needs and feature sets requested. Additional units (strongly recommended for Escort Engineer work in the Visiting Engineer lab area.)			
	2 units to Louisville		2 units to Louisville	2 units to Louisville

8.1.2 eDOCSIS Products

eDOCSIS products being submitted must comply with the Embedded DOCSIS (eDOCSIS) Specification, in addition to the DPoE 1.0 specifications as they may apply.

The following is a summary of the key requirements of the eDOCSIS Specification:

- It contains specific requirements for the embedded cable modem component of the E-MTA for the reporting of a "logical interface" to represent the data path between the ONU component and the E-MTA. This logical interface is given a well-known ifIndex and is required to follow the same data forwarding and address learning rules as a "normal" CPE interface (e.g. Ethernet).

- It requires that the DPoE device-specific MIBs not be made available to an SNMP manager that queries the E-MTA IP address. Similarly, the E-MTA device-specific MIBs are not to be made available to an SNMP manager that queries the vCM IP address.

- For the complete set of requirements, please refer to the eDOCSIS Specification published in the CableLabs website at http://www.cablelabs.com/specs/specification-search/. Note that these requirements apply to the embedded cable modem regardless of which version of the DOCSIS specification it complies with (DOCSIS 3.0 or 2.0).

8.1.3 DPoE System

Documentation as detailed in Section 4.8, including one operations manual.

DPoE System vendors must also submit the 'DPoE System Special Instructions and Programmable Features' available for download from InfoZone (https://community.cablelabs.com/wiki/display/CERTQUAL/DOCSIS+Testing+Information) under "Special Instructions Documents".

DPoE System equipment must be submitted with a 100Base-T NSI interface or functional equivalent.

Two console cables (one per DPoE System) must be provided. As required in the DPoE System Special Instructions, detailed instructions on how to configure the DPoE System using the console port **must** be provided.

On the DPoE System application form, the supplier must list the MIB object(s) that contains the DPoE System hardware and software revisions. The revisions listed in these MIB objects must match what is on the application for certification.

All of the four submitted DPoE Systems must be pre-configured with:

- Real CableLabs Mfr Root CA certificate. Used for ONU authentication testing (DSEC-01)
- Test CableLabs Mfr Root CA certificate. Used for ONU authentication testing (DSEC-01)
- Real CableLabs CVC Root CA certificate and real CableLabs CVC CA certificate. Used by vCMs to validate signed code images (DSEC-06)
- Test CableLabs CVC Root CA certificate and test CableLabs CVC CA certificate. Used by vCMs to validate signed code images (DSEC-05)

8.2   Software Images and Digital Certificates

Note that there are specific software and digital certificate requirements per project.

8.2.1 DPoE 1.0 ONUs:

Two software image files must be provided to CableLabs in the submission .zip file.

First is the current image for the certification wave, **with a file name according to the following convention:**

> **<Product_ID>.img**

The current image is digitally signed by the DPoE manufacturer CVC.

The second file is a test image that is a duplicate of the current image except that it has a different software version number.

The test image must also have the same signing time as the current image.

The second file name must follow the following convention:

> **<Product_ID>-DSEC-06.img**

8.2.2 Additional Files for DPoE 1.0 ONUs:

8.2.2.1 Software Image Files

In the case of the DPoE 1.0 ONU submission, in addition to the above two (2) software images, the following two (2) additional software images must also be provided in the submission .zip file.

The third file is the current image with a file name **according to the following convention:**

> **<Product_ID>-TestCLCA.img**

This file is digitally signed by a test DPoE manufacturer CVC issued from the test CableLabs CVC CA certificate.

The fourth file is a duplicate of the current image except that it has a different software version number.

The fourth file name must follow this convention:

> **<Product_ID>-TestCLCA-DSEC-05.img**

This file is digitally signed by a test DPoE manufacturer CVC issued from the test CableLabs CVC CA certificate.

8.2.3 Digital Certificate Files

Digital Certificate File: In the case of the DPoE 1.0 ONU submission, in order to download the DSEC-06 image file (<Product_ID>-DSEC-06.img) and the current image file (<Product_ID>.img) to the ONUs, these two image files must contain: (a) the identical DPoE Manufacturer CVC (Code Verification Certificate) issued by the CableLabs CVC CA, and (b) the same signingTime values of the CVS (Code Verification Signature). For further information on the DPoE Manufacturer CVC issuance by the CableLabs CVC CA, see the Section 9. This DPoE Manufacturer CVC must also be provided in the submission .zip file, with a file name according to the following convention:

> **<Product_ID>-CVC.der**

Digital Certificate Test File: In order to download the fourth image file (<Product_ID>-TestCLCA-DSEC-05.img) and the third current image file (<Product_ID>-TestCLCA.img) to the ONUs these two image files must contain: (a) the identical Test DPoE Manufacturer CVC signed by the Test Cablelabs CVC CA private key, and (b) the same signingTime values of the CVS. For further information on the Test CableLabs CVC CA, see Section 9.3. This Test DPoE Manufacturer CVC must also be provided in the submission documentation, with a file name according to the following convention:

> **<Product_ID>-TestCLCA-CVC.der.**

57

8.3 DPoE System Submission Requirements for SNMP Coexistence

The following setup is required for DPoE System OSS testing to cover SNMP modes of operation requirements contained in RFC 3411 through RFC 3416 and RFC 3584.

8.3.1 DPoE System Configuration

The vendor must configure one DPoE System and provide written step-by-step instructions for that purpose in case of a full configuration reset. The vendor may use any of the following or other procedure:

- CLI script with the specific parameters contained in the DPoE System Special Instructions and Programmable Features
- Automated Application/script
- Config File
- SNMP commands (provide the details as object-by-object SNMP SET commands)
- usmUserTable from RFC 3414, for Authentication and Privacy Passwords: if the CLI or any other procedure requires localize the keys from the passwords, provide the tools and procedures.

8.3.2 Default Operation for DPoE Systems

If SNMPv1/v2c NmAccess or proprietary mode is supported, the DPoE System should be in SNMPv1/v2c NmAccess or proprietary mode by default, including instructions for switching between SNMPv1/v2c NmAccess or proprietary mode and SNMP Coexistence Mode. Proprietary mode stands for a SNMPv1/v2c setup that doesn't configure docsDevNmAccessTable or any table in RFC 3411 through RFC 3415 and RFC 2576.

8.3.3 SNMPv1/v2c NmAccess/Proprietary Mode

The following community strings are used:

Community string "public"   with read-only/traps access
Community string "private"   with read-write access

8.3.4 SNMP Notifications and syslog

Syslog must be set for an IP that will be supplied on submission day, and syslog event reporting must be active, including instructions for changing the syslog IP address.

SNMP Notifications for all required events, including DOCSIS and DPoE events, must be enabled. SNMP Notifications must only be enabled for the SNMPv1/v2c users/community strings.

The IP address of the SNMP Notification receiver will be supplied on submission day. Instructions for changing the SNMP Notification receiver IP address must be supplied.

8.3.5 SNMP access list, if required

All nodes on the 10.50.1.x subnet should have access (a list of specific nodes will be provided on submission day). The DPoE System vendor must provide instructions to change the access list.

8.3.6 Notes

Specify information about:

- Objects and indexes taking values other than the solicited because CLI auto setup
- Objects/Tables not supported by the implementation
- Special operation conditions and requirements

8.4 DPoE ONU CMCI Data Port Verification Guidelines

CMCI data ports must adhere to the following guidelines:

All visible data ports must be labeled appropriately. If a DPoE ONU with covered ports is certified, the cover must remain intact in order to retain certification status. If a visible port is not active, a full disclosure of such condition is expected. The Certification Board(s) will have final decision; therefore it is highly recommended to make such a disclosure available to CableLabs and the CableLabs Certification board prior to submission.

Data ports that are not explicitly defined in the CMCI Specification (e.g. HomePNA, wireless, etc.) will be verified for proper operation by Kyrio, utilizing equipment submitted by the vendor as part of that vendor's submission to the wave.

All products with non-specified data ports must have a means to convert to an Ethernet interface, using a vendor-supplied electronic translation adapter or exhibit an Ethernet data port, in addition to the non-specified data port.

Kyrio will provide only a DPoE System and a cable plant to connect the device. The vendor must provide required data port-specific test equipment.

Products may contain ports for other uses beyond data ports. For example, a PacketCable™ E-MTA will contain RJ-11 phone jacks and an OpenCable™ Set Top Box may contain digital video ports. Such ports must be both labeled and operational, and may be used to provide stimulus to a device for DOCSIS certification testing.

Any exception to these guidelines must be presented to CableLabs in advance of submission for approval by the Certification Board(s) and noted in the Executive Summary for submission.

Note: Console and/or serial ports are not allowed on DPoE ONUs. These ports, whether active or inactive, should not be physically present on the DPoE ONU. DPoE ONUs that are submitted for certification which include a console and/or serial port will be returned upon submission.

9 DIGITAL CERTIFICATE PROCESSES AND CERTIFICATION

This section describes Digital Certificate Processes for Certification Wave submissions. Additional supporting documentation may be found at the CableLabs Certification and Qualification website at http://www.kyrio.com/digital-certificate-issuance-service/.

Digital Certificate Processes **for EuroDOCSIS and EuroPacketCable** can be found at Excentis website at https://www.excentis.com/testing/certification/programs/eurodocsis/digital-certificates and https://www.excentis.com/testing/certification/programs/europacketcable/digital-certificates

9.1 Obtaining CableLabs Digital Certificates and CVCs

One month in advance of submission date*:
1. Complete the appropriate Digital Certificate Authorization Agreement(s) (DCAAs) (listed below):
   a. DOCSIS (all DOCSIS included)
   b. PacketCable
   c. DPoE
   d. OpenCable
2. Submit agreement to CableLabs for approval.
   a. CableLabs authenticates contacts listed on the Customer Profile and invoices manufacturer for the appropriate fee.
   b. CableLabs must receive completed DCAA agreement, naming document, responses to contact authentication emails and payment prior to authorizing activation of the Certificate Requesting Account. Completion is reliant upon prompt vendor response time and document accuracy.
   c. Account activation for device certificates will take approximately one week from the authorization date.
3. CVC Issuance
   a. DOCSIS, DPoE, OCUR and Manufacturer (OCAP) CVC Signing Ceremonies occur on a periodic basis.
   b. CableLabs must receive the Code Signing Request (CSR) – (PKCS#10 file)

Contact security@cablelabs.com regarding questions about obtaining certificates.

9.2 CableLabs Root CA

Symantec, on behalf of CableLabs, operates the following CableLabs Root Certification Authorities:

1. DOCSIS Root Certification Authority (DRCA) for the DOCSIS 3.0 and 2.0 systems.
2. PacketCable Root CA (PRCA) for PacketCable
3. CableLabs Manufacturer Root CA (CMRCA) for OpenCable and DPoE
4. CableLabs Service Provider Root CA (CSPRCA) for PacketCable
5. CableLabs Code Verification Certificate Root CA (CCVCRCA) for OpenCable, DPoE and OCUR CVCs
6. CableLabs Root CA (CRCA) used by DOCSIS 3.1

All of the above CableLabs Root CAs can be downloaded at the following location:
http://www.cablelabs.com/resources/digital-certificate-issuance-service/

CableLabs also maintains a set of Test Root CAs for testing purposes:

1. Test DOCSIS Root CA (Test DRCA)
2. Test CableLabs Service Provider Root CA
3. Test CableLabs Manufacturer Root CA
4. Test CableLabs CVC Root CA
5. Test CableLabs Root CA (Test CRCA) used by DOCSIS 3.1

All of the above CableLabs Test Root CAs can be downloaded at the following location under the appropriate project:

http://www.cablelabs.com/resources/digital-certificate-issuance-service/

Please note that OpenCable Terminal equipment or OpenCable Set-top boxes designated for OCAP testing must have OpenCable Test CAs.

9.3 CableLabs CA

CableLabs supports a Centralized CA model, whereby CableLabs manages a shared CA, and issues device certificates to manufacturers, who are then responsible for embedding the certificates into the appropriate devices. Manufacturers that already have a CA may continue to use it, or may transition to the new centralized model. Manufacturers that do not have a CA will be provided certificates through the Centralized model.

Manufacturers who continue to operate their own CAs to issue DOCSIS 3.0 CM device certificates are required to successfully complete a CableLabs audit. This audit must be performed before submitting DOCSIS 3.0 cable modems for certification testing. To schedule an audit, please contact security@cablelabs.com at least one month before the desired date. The DOCSIS Certification Authority Audit Policy document is posted on the InfoZone website: (https://community.cablelabs.com/wiki/display/TECHPUBS/DOCSIS+Support+Docs#).

Symantec, on behalf of CableLabs, operates the following Shared CAs in support of the Centralized model:

1. CableLabs Shared DOCSIS CA for DOCSIS 3.0 and 2.0
2. CableLabs Shared PacketCable CA for PacketCable
3. CableLabs Shared Manufacturer CAs for OpenCable products
4. CableLabs Shared Manufacturer CA for DPoE
5. CableLabs Shared CVC CAs for OpenCable, OCUR and DPoE
6. OCAP App CVC CA for OpenCable
7. CableLabs Shared Service Provider CA for PacketCable
8. CableLabs Shared DOCSIS CA for DOCSIS 3.1

CableLabs Shared CAs can be downloaded at the following location:

http://www.cablelabs.com/resources/digital-certificate-issuance-service/

CableLabs also maintains a set of Test CAs, for testing purposes, which can be downloaded at the following location:

http://www.cablelabs.com/resources/digital-certificate-issuance-service/

Within this document, the term Manufacturer CA will mean either the Manufacturer's CA, or the Shared CA, depending on which model the manufacturer is in.

9.4 Certificate Requirements

9.4.1 Digital Certificate Necessary for DOCSIS 3.0 and 2.0 Cable Modem Vendor

Compliant cable modems must contain the Manufacturer CA issued by the DOCSIS Root CA, and the CM device certificate issued by the Manufacturer CA. They must also contain the DOCSIS Root CA public key for validating Secure Software Download CVCs.

For BPI-21.1 (CM Authentication by CMTS) and BPI-23.1 (Secure Software Download), CableLabs uses the Test DOCSIS Root CA (Test DRCA) and the digital certificates generated by it. The Test DRCA cable modems (units #27-28) must contain the Test DRCA public key for CVC verification of Secure Software Download as specified in Section 9. The submitted CMTS must be capable of supporting the Test DRCA Certificate as specified in Section 9.

Test DRCA Data including the Test DRCA Certificate, its PSA Private Key and additional information can be found at the CableLabs Certification/Qualification website at http://www.cablelabs.com/resources/digital-certificate-issuance-service/ .

9.4.2 Digital Certificate Necessary for the PacketCable E-MTA

As defined in the PacketCable Security specification, E-MTAs must contain the PacketCable Manufacturer CA certificate issued by the PacketCable MTA Root CA, and the E-MTA device certificate issued by the Manufacturer CA. E-MTAs must also contain either the CableLabs Service Provider Root CA certificate or Test CableLabs Service Provider Root CA certificate (refer to the table in Section 6.1 for more information). E-MTAs are embedded with DOCSIS 3.0 and 2.0 compliant cable modems. Refer to Section 9.3 for information on DOCSIS 3.0 and 2.0 cable modem certificate requirements.

9.4.3 Digital Certificate Necessary for OpenCable Host Devices and OCAP

The CableCARD Copy Protection Specification requires the use of X.509 digital certificates in accordance with the OpenCable Security Specification (both specifications at http://www.cablelabs.com/specifications/specification-search/). Test/evaluation certificates for hosts are provided by CableLabs when Manufacturer signs the CableCARD-Host Interface License Agreement (CHILA). See the table in Section 4.6 for information on which submitted units require test certificates. See the table in Section 7.1.1 for information on test/evaluation certificate configurations. Access to production digital certificates requires execution of either the OpenCable Host Device Digital Certificate Authorization Agreement or the OCUR Digital Certificate Authorization Agreement. All required OpenCable licenses can be obtained by providing the information in the following form: https://www.cablelabs.com/forms/forms/Video%20Licensing%20Questionnaire_01312021_631.html

9.4.4 Digital Certificates Necessary for DPoE 1.0 ONU & DPoE System Devices

Compliant ONUs must contain the production DPoE Manufacturer CA certificate (CA00008) issued by the real CableLabs Mfr Root CA, and the production ONU device certificate (along with its associated private key) issued by the DPoE Manufacturer CA.

For DSEC-01 (ONU Authentication by DPoE System) CableLabs uses the production CableLabs Mfr Root CA certificate and the Test CableLabs Mfr Root CA certificate. For DSEC-05 (Secure Software Download), CableLabs uses the Test CableLabs CVC Root CA, Test CableLabs CVC CA and the digital certificates generated by them. The submitted DPoE System must be capable of supporting these production and test CA certificates. CA certificates can be found at CableLabs Certification/Qualification website at http://www.cablelabs.com/resources/digital-certificate-issuance-service/ under DPoE.

9.6 Digital Certificate Authorization Agreements (DCAAs)

The following DCAAs can be found at:

http://www.cablelabs.com/resources/digital-certificate-issuance-service/
- DOCSIS DCAA (all DOCSIS included)
- PacketCable DCAA
- OpenCable DCAAs*
- DPoE DCAA

* Note: For OpenCable the DCAAs are not posted online. The above link under "Video" leads to a licensing questionnaire. CableLabs will follow up with the appropriate agreement.

9.7 Digital Certificate for the OEM Cable Modems

Neither the Certification Process nor the CableLabs Digital Certificate Authorization Agreement prohibits the digital certificates issued by Root CA's from being used for the third-party cable modems, as long as the digital certificates are used in compliance with the CableLabs DOCSIS Specification and the Digital Certificate Authorization Agreement. The manufacturer specified in the digital certificate shall be responsible for the usage of the digital certificate.

9.8 CableLabs Certified Cable Modem Code Files

CableLabs may sign the DOCSIS 3.1, 3.0, or 2.0 certified cable modem code files. The code-signing procedure shall take place at CableLabs under industry standard certificate policies and procedures. In spite of such security procedures, there is always a risk of security breach or error. The vendor agrees that CableLabs is not liable under any legal theory for any problems arising from or related to the CableLabs' code signing.

E-MTAs are embedded in DOCSIS 3.0 or 2.0 cable modems. Thus, CableLabs may sign certified E-MTA images using the CableLabs DOCSIS CVC.

10 QUESTIONS

Email: labs@kyrio.com

Fax: 303-661-3830
Phone: 303-661-9100

12 SUBMISSION CHECKLISTS

CPE DEVICES:

Stand-alone Cable Modems and eCM devices	❑ The required number of products complete with power supplies with required labeling
	❑ Fee
	To be uploaded via the web form:
	❑ Required documentation
	    ❑ Executive summary
	    ❑ Completed Requirements Checklist
	    ❑ Image & Driver Files for MAC-14 & Test DRCA
	    ❑ Cable Modem Device Certificates and DOCSIS Code Verification Certificate (CVC)
	    ❑ eCM Special Instructions (for eCM products only)
	❑ Successful completion of a CableLabs audit if you operate your own CA (distributed model) to issue DOCSIS 3.0 CM device certificates.
	❑ For Re-certification and OEM/Paper include a copy of the original request letter

E-MTA	❑ The required number of products complete with power supplies with required labeling
	❑ Fee
	To be uploaded via the web form:
	❑ Required documentation
	  (Main Folder)
	    ○ Executive summary for both DOCSIS and PacketCable functionality
	    ○ Interoperability Test Report for PacketCable functionality
	    ○ PacketCable/DOCSIS Image and Driver files
	  DOCSIS (Sub Folder)
	    ❑ Completed Requirements Checklist (DOCSIS)
	  PacketCable (sub-folder)
	    ❑ Component Checklist (PacketCable)
	    ○ ATP (PacketCable)

DPoE ONU	❑ The required number of products complete with power supplies with required labeling
	❑ Fee
	To be uploaded via the web form:
	❑ Required documentation
	    ❑ Executive summary
	    ❑ Completed Requirements Checklist
	    ❑ Device Certificates and Code Verification Certificate (CVC)
	    ❑ Special Instructions, if applicable

EuroDOCSIS CM or EuroPacketCable EMTA	❑ Delivery of required number of samples (with label as required) and power supplies
	❑ Fee
	To be uploaded via the web form:
	❑ Required documentation
	    ❑ Executive summary
	    ❑ Completed Requirements Checklist
	    ❑ Detailed Interoperability and ATP test reports
	    ❑ Image files (Original, MAC.14 test image, 2 BPI.23 images)
	    ❑ Code Verification Certificates (CVCs)
	    ❑ Login and password for the web admin page on the CM
	    ❑ For ED3.0 CMs: operating manual for the unit with console access
	    ❑ For STB devices: MPEG stream together with configuration settings
	    ❑ For STB devices: instructions to enable echo application
	  ❑ For products with USB support: drivers required for equipment operation
	  ❑ For products with Wi-Fi support: wireless interface information (username, passwords, SSIDs); instructions on how to enable/disable the Wi-Fi interface (Wi-Fi must by default be disabled)
	    ❑ MIB definitions of all supported MIBs (e.g., proprietary MIBs to configure the Wi-Fi)
	    ❑ If applicable, Import papers

OpenCable Unidirectional Receiver	❑ The required number of products complete with power supplies with required labeling ❑ OpenCable Certification Admission Application – signed original, ***complete*** ❑ Fee *To be uploaded via the web form:* ❑ Required documentation

	❑ Executive Summary ❑ Completed Requirements Checklist ❑ Detailed ATP ❑ Host Device Certificates and OpenCable Code Verification Certificate (CVC) ❑ DRM Plug-in for OCUR test tool

OpenCable CableCARD	❑ The required number of products complete with power supplies with required labeling.
	❑ OpenCable Certification Admission Application – signed original, ***complete***
	❑ Fee
	To be uploaded via the web form:
	❑ Required documentation
	    ❑ Executive Summary
	    ❑ Completed Requirements Checklist
	    ❑ Detailed ATP
	    ❑ CableCARD Device Certificates
	    ❑ Interoperability Test Report

Tuning Resolver	❑ The required number of products complete with power supplies with required labeling
	❑ Fee
	To be uploaded via the web form:
	❑ Required documentation
	    ❑ Executive Summary
	    ❑ Completed Requirements Checklist
	    ❑ Detailed ATP

L2VPN CPE	❑ Same as for stand-alone DOCSIS or EuroDOCSIS Cable Modem (see above)
Cable Gateway	❑ Same as for stand-alone DOCSIS or EuroDOCSIS Cable Modem (see above) **+** ❑ eRouter configuration documentation: how to reset the device to its default behavior for all functionality, how to enable/disable any Customer Facing IP Interfaces, how to enable/disable the local DHCPv4 and DHCPv6 server, how to configure/disable the firewall, how to configure the Wi-Fi, etc. (i.e., via proprietary MIBs, webpage or other). ❑ If TR-069 is supported: supported data models

HEADEND DEVICES:

DOCSIS CMTS
 	
CCAP
	❏ The required number of products complete with power supplies with required labeling
	❏ 100Base-T Interface or equivalent
	❏ Four console cables (one per CMTS)
	❏ Fee
	To be uploaded via the web form:
	❏ Required documentation
	    ❏ Executive summary
	    ❏ Software Image File(s) required to rebuild the system
	    ❏ Completed Requirements Checklist
	    ❏ CMTS Special Instructions & Programmable Features
	    ❏ Operations manual

CMTS (EuroDOCSIS, EuroPacketCable and EuroPacketCable Multimedia)	❏ The required number of products (including power supply) to Ghent and Louisville
	❏ Console cable for each unit
	❏ Fee
	To be uploaded via the web form:
	❏ Required documentation
	    ❏ Executive summary
	    ❏ Completed Requirements Checklist
	    ❏ Detailed Interoperability and ATP test reports
	    ❏ Software images to rebuild the systems
	    ❏ CMTS Special instructions and operations manual
	    ❏ If applicable, Import papers

DPoE System	❏ The required number of products complete with power supplies with required labeling
	❏ 100Base-T Interface or equivalent
	❏ Two console cables (one per DPoE System)
	❏ Fee
	To be uploaded via the web form:
	❏ Required documentation
	    ❏ Executive summary
	    ❏ Software Image File(s) required to rebuild the system
	    ❏ Supported data rates (1G/1G, 10G/1G, 10G/10G)
	    ❏ Completed Requirements Checklist
	    ❏ DPoE System Special Instructions & Programmable Features
	❏ Operations manual

EQAM	❏ The required number of products complete with power supplies with required labeling
	❏ Fee
	To be uploaded via the web form:
	❏ Required documentation
	    ❏ Executive summary
	    ❏ Software Image File(s) required to rebuild the system
	    ❏ Completed Requirements Checklist
	    ❏ EQAM Special Instructions & Programmable Features

PacketCable CMTS
 	
DOCSIS + PacketCable Multimedia CMTS
 	
PacketCable + Multimedia CMTS
	❏ The required number of products complete with power supplies with required labeling
	❏ 100Base-T Interface or equivalent
	❏ Six console cables (one per CMTS)
	❏ Fee
	To be uploaded via the web form:
	❏ Required documentation
	  (Main Folder)
	    o Executive summary for both DOCSIS and PacketCable functionality
	    o Interoperability Test Report for PacketCable functionality
	    o Software Image File(s) required to rebuild the system
	DOCSIS (sub-folder)
	    o Completed Requirements Checklist DOCSIS)
	    o CMTS Special Instructions & Programmable Features (DOCSIS)
	    o Operations Manual
	PacketCable (sub-folder)
	    o Component Checklist (PacketCable)
	    o ATP (PacketCable)
	        o PacketCable CMTS Vendor Product Operating Instructions