CableLabs®

DIGITAL CERTIFICATE AUTHORIZATION AGREEMENT

For Devices Built in Compliance with the
DOCSIS® 3.0, 3.1, 4.0, PacketCable, DPoE & Remote PHY Specifications

This Digital Certificate Authorization Agreement ("Agreement"), is made effective as of _____ (the "Effective Date"), by and between Cable Television Laboratories, Inc. ("CableLabs"), a Delaware non- stock membership corporation with offices at 858 Coal Creek Circle, Louisville, Colorado 80027-9750, and the party identified below ("Manufacturer").

Manufacturer Organization Name (Full Legal Name of Entity executing this Agreement):	
Main Corporate Headquarters Address: (city, state or province, postal code, country)	Phone:

CableLabs maintains and operates a secure Public Key Infrastructure (PKI) for issuing Digital Certificates for use in a cable network. Digital Certificates assist the cable operator in deterring theft of cable services, or unauthorized access to cable services, and help protect subscriber privacy. CableLabs Code Verification Certificates allow for secure download of Device code into Devices operating on a cable network. CableLabs hereby grants to Manufacturer the right to obtain and use the Digital Certificates Code Verification Certificates to sign Manufacturer's code for download into its Devices in accordance with the terms and conditions of this Agreement.

CableLabs hereby grants to Manufacturer the right to obtain and use the appropriate Digital Certificates in its Devices in accordance with the terms and conditions of this Agreement. Please check one or more of the following options:

Legacy PKI (DOCSIS 1st Gen PKI)		
☐	**DOCSIS 3.0 CM Device Certs or earlier**	**Complete Exhibits A, D1**
☐	**DOCSIS 3.0 CM Device Certs (Extended CA)**	**Complete Exhibit A, D2**
☐	**DOCSIS 3.0 CVC**	**Complete Exhibit C1**
☐	**PacketCable CM Device Certs**	**Completed Exhibits A, D3**
☐	**DPoE (Legacy PKI) CM Device Certs**	**Complete Exhibits, A, D4**
☐	**DPoE (Legacy PKI) CVC**	**Complete Exhibit C2**
New PKI (DOCSIS 2nd Gen PKI)		
☐	**DOCSIS 3.1 CM Device Certs**	**Complete Exhibits A, D5**
☐	**DOCSIS 3.1 or Remote PHY CVC**	**Complete Exhibits A, C3**
☐	**Remote PHY Device Certs**	**Complete Exhibits A, D6**
☐	**DOCSIS 4.0 CM Device Certs**	**Complete Exhibits A, D7**
☐	**DOCSIS 4.0 CVC***	**Complete Exhibits A, C4**
☐	**DPoE 2.0 (New PKI) CM Device Certs**	**Complete Exhibits A, D8**
☐	**DPoE 2.0 (New PKI) CVC**	**Complete Exhibits C5**
Server Certificates (DOCSIS 2nd Gen PKI)		
☐	**Remote PHY Server/AAA Server Certs**	**Complete Exhibits A, S1**
☐	**DOCSIS 4.0 CMTS NRI Cert**	**Complete Exhibit A, S2**
☐	**DOCSIS 4.0 CMTS Full Cert**	**Complete Exhibit A, S3**
☐	**Remote PHY CCAP Core NRI Cert**	**Complete Exhibit A, S4**
☐	**Remote PHY CCAP Core Full**	**Complete Exhibit A, S5**

[*] DOCSIS 3.1 CVCs can be used to sign DOCSIS 4.0 firmware.

MANUFACTURER HAS READ AND AGREES TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT, INCLUDING THOSE TERMS CONTAINED ON THE FOLLOWING PAGES HEREOF.

In consideration of the mutual promises and covenants contained herein, and other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the parties have entered into this Agreement as of the Effective Date.

CABLE TELEVISION LABORATORIES, INC.	**MANUFACTURER NAME:**
By:	By:
Name:	Name:
Title:	Title:
Date:	Date:

Agreement

1.0 Definitions

1.1. "Certificate Manager" means a service manager identified by CableLabs that manages certain aspects of the CableLabs PKI.

1.2. "Compliant" means that the Device is Certified or Qualified (as defined in the CableLabs' Certification Wave Guidelines) by the DOCSIS Certification Board; or the device, in CableLabs' ultimate determination, is constructed to the appropriate DOCSIS specification.

1.3. "CVC" means a code verification certificate that is signed by the DOCSIS Root CA for DOCSIS 3.0 and earlier Devices, signed by the CableLabs CVC CA for DOCSIS 3.1 Devices or signed by the Remote PHY CA, as is appropriate. A CVC is a type of Digital Certificate.

1.4. "Device" means a Manufacturer's Compliant product.

1.5. "Device Certificate" means a Digital Certificate installed in a Device to authenticate the Device to the cable network.

1.6. "Digital Certificate" means an electronic identification key that allows for the authentication of Devices on the cable network or, in the case of a CVC, ensures secure software downloads from a cable operator to a cable subscriber.

1.7. "CA" means a Certification Authority, which is hosted by a third party and is signed by the Root CA.

1.8. "Root CA" means the highest CA in the DOCSIS PKI and is the trust point for all certificates that are issued by the DOCSIS PKI.

1.9. "Public Key Infrastructure" (PKI) means the architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a digital certificate-based public key cryptographic system.

1.10. "Wrongful Use" means Manufacturer has knowingly or with gross negligence embedded a Digital Certificate in any other product or application that is not Compliant.

2.0 Digital Certificate Authorization

2.1. Upon receipt of a complete and executed Agreement, payment of appropriate fees (see section 5.0), the Manufacturer's information (see **Exhibit A**), the Naming Documents (see **Exhibit D1-D8, C1-C5, & S1-S4**), a Certificate Signing Request (CSR) file in PKCS#10 format (for **Exhibit C1-C5, S1-S5**), and verification of Manufacturer's identity for security purposes, CableLabs will authorize Manufacturer to receive Digital Certificates.

3.0 Use of Digital Certificates and Request/Receipt of Certificates

3.1. **Embedding of Digital Certificates.** Manufacturer shall not embed the Digital Certificates in any Device that is not Compliant or that is associated with a private key that Manufacturer knows or should have known was stolen, intercepted or otherwise compromised in any way.

3.2. **Security of Digital Certificate Private Keys.** Manufacturer shall safeguard the Digital Certificates and associated private keys to ensure that the private keys are not lost, stolen, embedded in a product other than a Device, or otherwise used in a manner that may compromise, or actually does compromise, the CableLabs PKI, as CableLabs may determine in its sole discretion. Manufacturer shall immediately notify CableLabs at pkiops@cablelabs.com if Manufacturer's digital certificates, including the CVC, are thought to be or are actually, lost, stolen or otherwise compromised.

3.3. **Manufacturer is solely liable for all code signed with the Manufacturer's CVC.** Manufacturer is responsible to ensure that the code signed with the Manufacturer's CVC works appropriately, does not cause harm to those who rely upon the code, that the code operations are lawful, and that the code does not infringe intellectual property rights. **Manufacturer shall ensure that its CVC shall only be used**

to sign its own Device code.

3.4. **Automated Request/Receipt of Digital Certificates.** Within thirty (30) days after receipt of the Annual Maintenance Fee, CableLabs shall cause the Certificate Manager to activate a Manufacturer account for securely obtaining Digital Certificates in an automated fashion.

3.5. **No Other Rights.** CableLabs retains all right, title, and interest in and to CableLabs' Root CAs and CableLabs' Intermediate CAs and any associated trade secrets or other proprietary information associated therewith that is provided by CableLabs to Manufacturer herein. CableLabs grants no rights in any trademark, trade name, service mark, business name or goodwill in the trademarks "CableLabs" or "DOCSIS".

4.0 Term and Termination

4.1. **Term**. The term of this Agreement shall begin on the Effective Date and shall continue until terminated earlier under the provisions of this Section.

4.2. **Termination by Manufacturer.** Manufacturer may terminate this Agreement, with or without cause, by giving CableLabs sixty days written notice of such termination.

4.3. **Termination by CableLabs.** CableLabs may terminate this Agreement for material breach of this Agreement by Manufacturer, where such breach is not cured within sixty days of notice to Manufacturer; or, where such breach is incapable of cure at the time of the material breach. Examples of breach include, but are not limited to: Manufacturer's Device Certificate private keys have been lost, stolen, intercepted or otherwise compromised in any way, a court or governmental agency orders CableLabs to revoke Manufacturer authorization, or a series of non-material breaches of this Agreement by Manufacturer.

4.4. **Termination for Wrongful Use.** If this Agreement is terminated due to Wrongful Use, in addition to revoking CableLabs' authorization for Manufacturer to receive Digital Certificates, CableLabs shall receive all revenue Manufacturer receives from Wrongful Use. CableLabs' receipt of revenue from Wrongful Use is in addition to any damages CableLabs is entitled to receive by law.

4.5. **Effect of Agreement Termination or Certificate Revocation.** If this Agreement is terminated, or Digital Certificates are revoked, Manufacturer shall discontinue using such Digital Certificate(s) and cease embedding or otherwise using such Digital Certificate(s) in any or all affected Device(s). Manufacturer shall keep secret or destroy any unused or revoked Digital Certificates and any associated private keys, and take such other action as is reasonably directed by CableLabs. Notwithstanding any termination of this Agreement, un-revoked Digital Certificate(s) used in Device(s) that are no longer under the control of Manufacturer shall be valid until the expiration of their validity period as stated in the DOCSIS or Remote PHY specifications.

5.0 Fees

5.1. **Fees**. Manufacturer shall pay to CableLabs in advance. (Please contact CableLabs at pkiops@CableLabs.com for fee information). CableLabs may, upon thirty (30) days' prior notice, modify the Fees.

5.2. **Applicable Taxes**. CableLabs is exempt from income tax in the United States under Section 501(c)(6) of the Internal Revenue Code. The Fees paid by Manufacturer hereunder are exclusive of, and Manufacturer shall pay, all sales, use, value added, excise, income tax, withholding tax, and any and all other taxes (other than income taxes) or other costs or fees that may be levied upon either party by taxing authorities other than the United States in connection with this Agreement (except for taxes based on CableLabs' employees) and shall pay all income taxes that may be levied upon Manufacturer.

6.0 Warranty, Indemnity, Limitation of Liability

6.1. **Indemnification**. Manufacturer shall indemnify and hold harmless CableLabs, its members, directors, employees, and agents (including the entity that holds the Root Certificates and the CA Certificates that issue the CVCs and Device Certificates), for any claim arising from or related to Manufacturer's use and implementation of the Digital Certificates, including, without limitation, Wrongful Use. Such indemnification obligations shall be subject to: (i) CableLabs notifying Manufacturer, in writing of any such claim and (ii) Manufacturer having the sole control of the defense and all negotiations for any settlement or compromise of such claim, provided, however, that CableLabs may participate in such defense using counsel of its own choice and at its sole expense.

6.2. **Disclaimer of Warranties. TO THE MAXIMUM EXTENT PERMITTED BY LAW:** THE DIGITAL CERTIFICATES, USE OF WHICH IS AUTHORIZED HEREUNDER, ARE PROVIDED "AS IS" AND CABLELABS DISCLAIMS ALL REPRESENTATIONS AND WARRANTIES, FOR THE DIGITAL CERTIFICATES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, QUIET ENJOYMENT, ACCURACY, SECURITY, OR NON-INFRINGEMENT.

6.3. **Limitation of Liability**. **TO THE MAXIMUM EXTENT PERMITTED BY LAW**: WITH THE EXCEPTION OF MANUFACTURER'S "WRONGFUL USE", IN NO EVENT WILL EITHER PARTY BE LIABLE UNDER THIS AGREEMENT FOR ANY SPECIAL, INDIRECT, CONSEQUENTIAL, OR PUNITIVE DAMAGES INCLUDING, WITHOUT LIMITATION, DAMAGES WHICH REFLECT LOST BUSINESS, PROFITS OR REVENUE OBTAINED OR LOST, OR THE COSTS OF RECONSTRUCTING DATA OR REBUILDING DEVICES, WHETHER DAMAGES OF THIS NATURE WERE FORESEEABLE OR NOT, AND EVEN IF THAT PARTY HAD BEEN ADVISED THAT DAMAGES OF THIS NATURE WERE POSSIBLE. IN NO EVENT SHALL EITHER PARTY BE LIABLE UNDER THIS AGREEMENT TO THE OTHER PARTY FOR ANY AMOUNT EXCEEDING THE FEES ACTUALLY RECEIVED BY CABLELABS FROM MANUFACTURER.

6.4. **Manufacturer Liability for Manufacturer Supplied Information**. Manufacturer is solely liable for the resulting Digital Certificates created from the information Manufacturer provides in the exhibits attached hereto and incorporated by this reference. **Failure to completely and correctly complete the attached exhibits will result in incorrect Digital Certificates.**

7.0 General

7.1. **Notices**. Any notices, required or permitted to be made or given to either party pursuant to this Agreement shall be in writing and shall be delivered to the address set forth on the first page, or to such other address as the receiving party may have designated by written notice given to the other party. Legal notices shall be sent to the person listed as the Legal Contact. Technical notices shall be sent to the name listed as the Technical Contact.

7.2. **Export**. Manufacturer shall not export or re-export (directly or, knowingly indirectly) any Digital Certificates, documentation, or other technical data without complying with the U.S. Export Administration Act and the associated regulations.

7.3. **Audit**. CableLabs or its duly authorized representatives shall be permitted, upon reasonable notice, and subject to appropriate non-disclosure terms, to inspect all records pertaining to the Digital Certificates, including, without limitation, records related or pertaining to the security, usage, and distribution of the Digital Certificates. The inspections may be made notwithstanding termination of this Agreement while any outstanding claim remains unsettled in the view of either party. In the event CableLabs needs to conduct an audit due to a discrepancy discovered in a prior audit, CableLabs may charge Manufacturer for reasonable airfare, meals and lodging for such subsequent audit.

7.4. **Irreparable Harm**. Manufacturer acknowledges and agrees that due to the unique and sensitive nature of the use of the Digital Certificates authorized hereunder, including any private keys therein, there can

be no adequate remedy at law for breach of Manufacturer's obligations hereunder, that such breach or unauthorized use or release of the Digital Certificates will cause material damage and result in irreparable harm. Therefore, upon any such breach or any threat thereof, CableLabs shall be entitled to appropriate equitable relief in addition to whatever remedies it might have at law.

7.5. **Amendments**. No amendment or modification hereof shall be valid or binding upon the parties unless made in writing and signed by both parties hereto.

7.6. **Waiver**. Any waiver by either party hereto of any breach of this Agreement shall not constitute a waiver of any subsequent or other breach.

7.7. **Survival**. Sections 1, 3.1, 3.2, 3.3,4.4, 4.5, 6, 7.3, 7.7, 7.9, 7.10, and 7.11 shall survive any termination of the Agreement.

7.8. **Assignment**. Manufacturer may not assign this Agreement without the express, prior written approval of CableLabs.

7.9. **Entire Agreement.** This Agreement embodies the entire understanding of the parties with respect to the subject matter hereof and merges all prior discussions between them, and neither of the parties shall be bound by any conditions, definitions, warranties, understandings or representations with respect to the subject matter hereof other than as expressly provided herein.

7.10. **Severability.** If any provision of this Agreement shall be held to be invalid, illegal or unenforceable, the validity, legality and enforceability of the remaining provisions shall not be in any way affected or impaired thereby.

7.11. **Governing Law; Forum.** This Agreement shall be construed in accordance with the law of the state of Colorado, without regard to its conflict of laws rules. The parties here by agree to exclusive jurisdiction and venue in the federal/**state courts located in the city and county of Denver, Colorado.**

EXHIBIT A –
COMPANY INFORMATION

PLEASE COMPLETE ALL FIELDS ACCURATELY WITH THE APPROPRIATE INFORMATION

Notes:

1) Fields marked with (*) are compulsory for the specified section.
2) When entering phone numbers, ensure that you **include country and area codes.**
3) **Organization name** is a compulsory field and **MUST** be the **legally registered business name**.
4) Use of special characters such as () & * % $ # @ ! + = ^ is not permitted in the **Organization name**.

CORPORATE INFORMATION:

Manufacturer Organization Name*: (Full Legal Name or Registered Trade Name)
Legal Headquarters Address*: (city, state or province, postal code, country)
D-U-N-S Number: Providing Your DUNS number in advance can assist in the Authentication process. If you do not know your company's D-U-N-S number, you can look it up at http://www.dnb.com. Note: The Legal Company Name and Corporate Address listed above must match the information that is listed in the D-U-N-S Database.

MANUFACTURER'S CORPORATE CONTACT:

This person must work for the organization requesting this service and is responsible for the device manufacturing system. This individual will authorize the other account contacts including administrators who will request Certificates from CableLabs. This person may periodically receive emails regarding issues or events occurring with this service.

First Name*:	Last Name*:
Title*:	E-mail*:
Phone*:	

PRIMARY ADMINISTRATOR CONTACT:

This is the person who is authorized to request and receive certificates.

Same as the Corporate Contact? ☐ YES ☑ NO

First Name*:	Last Name*:
Title*:	E-mail*:
Phone*:	
Address*:	City and State*:
Zip/Postal Code*:	Country*:

SECOND ADMINISTRATOR CONTACT:

This person is authorized to back-up the primary administrator contact. This person is also authorized to request and receive certificates.

First Name*:	Last Name*:
Title*:	E-mail*:
Phone*:	
Address*:	City and State*:
Zip/Postal Code*:	Country*:

MANUFACTURER'S TECHNICAL CONTACT

This is a technical contact, typically in development engineering, authorized to discuss technical issues related to the DOCSIS PKI with CableLabs.

First Name*:	Last Name*:
Title*:	E-mail*:
Phone*:	

MANUFACTURER'S LEGAL CONTACT

This person will receive a copy of any contractual related notices.

First Name*:	Last Name*:
Title*:	E-mail*:
Phone*:	
Address*:	City and State*:
Zip/Postal Code*:	Country*:

MANUFACTURER'S BILLING CONTACT:

This is the person responsible for payment and notifying CableLabs of any billing changes, for example an accounts payable representative. Please list any special instructions for billing (e.g. require purchase order, submit invoice to portal)

First Name*:	Last Name*:
Title*:	E-mail*:
Phone*:	
Special Instructions:	
Bill To Address:	Ship To Address:

EXHIBIT D1 -
DOCSIS® CABLE MODEM DEVICE CERTIFICATE - NAMING APPLICATION
(for use with DOCSIS 3.0 and earlier devices – Sectigo CA)

Please complete the Requestor Information section and the Subject DN of the Certificate Format.

Requestor Information:

Organization Name:	
Contact Name:	Phone:
Contact E-mail:	

Certificate Format (To be completed by Manufacturer)

Subject DN	c=
	o=
	ou=
	cn= <(MAC Address (to be entered via the account requesting portal)>

Other Certificate Contents (For CableLabs and CA use only):

Version		v3		
Serial number		Unique Positive Integer assigned by the CA		
Issuer DN		c=US o=CableLabs ou=DOCSIS ou=D CA00004 cn=CableLabs Cable Modem Certificate Authority		
notBefore		yymmdd000000Z (Key Ceremony Date)		
notAfter		yymmdd235959Z (20 years*)		
Public Key Algorithm		RSA (1 2 840 113549 1 1)		
Signature Algorithm		sha1withRSAEncryption (1 2 840 113549 1 1 5)		
Keysize		1024-bits		
Parameters		NULL		
Standard Extensions	**OID**	**Required**	**Criticality**	**Value**
keyUsage	**{id-ce 15}**	**YES**	**FALSE**	**n/a**
digitalSignature				Set
keyEncipherment				Set
authorityKeyIdentifier	**{id-ce 35}**	**YES**	**FALSE**	**Calculated per Method 1**
keyIdentifier				<same as subjectKeyIdentifier in CA certificate>

By signing this document, you hereby authorize CableLabs to set your Device Certificates extensions as noted above.

Signature: _____ Date: _____

EXHIBIT D2 -
EXTENDED DOCSIS® CABLE MODEM DEVICE CERTIFICATE - NAMING APPLICATION (for use with DOCSIS 3.0 and earlier devices – Sectigo Extended CA)

Please complete the Requestor Information section and the Subject DN of the Certificate Format.

Requestor Information:

Organization Name:	
Contact Name:	Phone:
Contact E-mail:	

Certificate Format (To be completed by Manufacturer)

Base Certificate	
Subject DN	c=
	o=
	ou=
	cn= <(MAC Address (to be entered via the account requesting portal)>

Other Certificate Contents (For CableLabs and CA use only):

Version		v3		
Serial number		Unique Positive Integer assigned by the CA		
Issuer DN		c=US o=CableLabs ou=DOCSIS ou=D CA00004 V2 EXT cn=CableLabs Cable Modem Certificate Authority		
notBefore		yymmdd000000Z (Key Ceremony Date)		
notAfter		yymmdd235959Z (20 years*)		
Public Key Algorithm		RSA (1 2 840 113549 1 1)		
Signature Algorithm		sha1withRSAEncryption (1 2 840 113549 1 1 5)		
Keysize		1024-bits		
Parameters		NULL		
Standard Extensions	**OID**	**Required**	**Criticality**	**Value**
keyUsage	**{id-ce 15}**	**YES**	**FALSE**	**n/a**
digitalSignature				Set
keyEncipherment				Set
authorityKeyIdentifier	**{id-ce 35}**	**YES**	**FALSE**	**Calculated per Method 1**
keyIdentifier				<same as subjectKeyIdentifier in CA certificate>

By signing this document, you hereby authorize CableLabs to set your Device Certificates extensions as noted above.

Signature: _____ Date: _____

EXHIBIT D3 -
PACKETCABLE DEVICE CERTIFICATE NAMING APPLICATION
(Sectigo CA)

Requestor Information:

Organization Name:	
Contact Name:	Phone:
Contact E-mail:	

Certificate Format (To Be Completed by Manufacturer):

Subject DN	c=
	o=
	st=
	l=
	ou=PacketCable
	ou=
	ou=
	cn=<(MAC Address (to be entered via the account requesting portal)>

Other Certificate Contents (For CableLabs and CA use only):

Version		v3		
Serial number		Unique Positive Integer assigned by the CA		
Issuer DN		c = US o = CableLabs, Inc. ou=PacketCable ou= PC CA00001 – G3 cn = CableLabs, Inc. PacketCable CA		
notBefore		yymmdd000000Z (Key Ceremony Date)		
notAfter		yymmdd235959Z (20 years)		
Public Key Algorithm		RSA (1 2 840 113549 1 1)		
Signature Algorithm		Sha1WithRSAEncryption (1 2 840 113549 1 1 5)		
Keysize		1024-bits		
Parameters		NULL		
Standard Extensions	**OID**	**Include**	**Criticality**	**Value**
keyUsage	**{id-ce 15}**	**YES**	**TRUE**	**n/a**
digitalSignature				Set
keyEncipherment				Set
authorityKeyIdentifier	**{id-ce 35}**	**YES**	**FALSE**	**Calculated per Method 1**
keyIdentifier				<same as subjectKeyIdentifier in CA certificate>

By signing this document, you hereby authorize CableLabs to set your Device Certificates extensions as noted above.

Signature: _____ Date: _____

EXHIBIT D4 -
DPoE ONU DEVICE CERTIFICATE NAMING APPLICATION
(for use with DPoE ONU devices – DigiCert CA)

Requestor Information:

Organization Name:	
Contact Name:	Phone:
Contact E-mail:	

Certificate Format (To be completed by Manufacturer):

Subject DN	c=
	o=
	ou=
	cn= <(MAC Address (to be entered via the account requesting portal)>

Other Certificate Contents (For CableLabs and CA use only):

Issuer DN		c=US o=CableLabs ou=CA00008 – G2 cn=CableLabs Device Certification Authority		
Not Before		**<Issuing Date>**		
Not After		<Issuing Date> + Up to 20 yrs [*]		
Public Key Algorithm		RSA (1 2 840 113549 1 1)		
Signature Algorithm		Sha256WithRSAEncryption (1 2 840 113549 1 1 11)		
Keysize		RSA: 2048-bits		
Parameters		NULL		
Standard Extensions	**OID**	**Required**	**Critical**	**Value**
keyUsage	**{id-ce 15}**	**YES**	**TRUE**	
digitalSignature				Set (1)
keyEncipherment				Set (1)
extendedKeyUsage	**{id-ce 37}**	**YES**	**FALSE**	
svcONU				Set (<1.3.6.1.4.1.4491.2021.2.1.4>)
clientAuth				Set (id-kp-clientAuth)
serverAuth				Set (id-kp-serverAuth)
authorityKeyIdentifier	**{id-ce 35}**	**YES**	**FALSE**	
keyIdentifier				Set (<SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits)>)
certificatePolicies	**{id-ce 32}**	**YES**	**FALSE**	
certPolicyId				Set (<1.3.6.1.4.1.4491.2021.1.5>)
policyQualifiers				Not Set
authorityInfoAccess	**{id-pe 1}**	**YES**	**FALSE**	
ocsp	{id-ad 1}			Set (<HTTP URI of the authoritative OCSP responder>)
caIssuers	{id-ad 2}			Set (<HTTP URI of the Issuing CA certificate in DER format>)
crlDistributionPoints	**{id-ce 31}**	**YES**	**FALSE**	
distributionPoint				Set (<HTTP URI for Relevant CRL in DER format>)

By signing this document, you hereby authorize CableLabs to set your Device Certificates extensions as noted above.

Signature: _____ Date: _____

EXHIBIT D5 -
DOCSIS® CABLE MODEM DEVICE CERTIFICATE - NAMING APPLICATION
(for use with DOCSIS 3.1 devices – Sectigo CA)

Requestor Information:

Organization Name:	
Contact Name:	Phone:
Contact E-mail:	

Certificate Format (To be completed by Manufacturer):

Subject DN	c=
	o=
	ou=
	cn= <(MAC Address (to be entered via the account requesting portal)>

Other Certificate Contents (For CableLabs and CA use only):

Version		v3		
Serial number		Unique Positive Integer assigned by the CA		
Issuer DN		c=US o=CableLabs ou = Device CA04 cn=CableLabs Device Certificate Authority		
notBefore		yymmdd000000Z (Key Ceremony Date)		
notAfter		yymmdd235959Z (20 years**)		
Public Key Algorithm		RSA (1 2 840 113549 1 1)		
Signature Algorithm		Sha256withRSAEncryption (1 2 840 113549 1 1 11)		
Keysize		2048-bits		
Parameters		NULL		
Standard Extensions	**OID**	**Includ**	**Criticality**	**Value**
keyUsage	**{id-ce 15}**	**YES**	**TRUE**	
digitalSignature				Set (1)
keyEncipherment				Set (1)
authorityKeyIdentifier	**{id-ce 35}**	**YES**	**FALSE**	
keyIdentifier				Calculated per Method 1

By signing this document, you hereby authorize CableLabs to set your Device Certificates extensions as noted above.

Signature: _____ Date: _____

EXHIBIT D6 -
REMOTE PHY (R-PHY) DEVICE CERTIFICATE - NAMING APPLICATION
(for use with Remote PHY devices – Sectigo CA)

Requestor Information:

Organization Name:	
Contact Name:	Phone:
Contact E-mail:	

Certificate Format (To be completed by Manufacturer):

Subject DN	c=
	o=
	ou=
	cn= <(MAC Address (to be entered via the account requesting portal)>

Other Certificate Contents (For CableLabs and CA use only):

Version		v3		
Serial number		Unique Positive Integer assigned by the CA		
Issuer DN		c=US o=CableLabs ou = Device CA04 cn=CableLabs Device Certificate Authority		
notBefore		yymmdd000000Z (Key Ceremony Date)		
notAfter		yymmdd235959Z (20 years**)		
Public Key Algorithm		RSA (1 2 840 113549 1 1)		
Signature Algorithm		Sha256withRSAEncryption (1 2 840 113549 1 1 11)		
Keysize		2048-bits		
Parameters		NULL		
Standard Extensions	**OID**	**Required**	**Criticality**	**Value**
keyUsage	**{id-ce 15}**	**YES**	**TRUE**	
digitalSignature				Set (1)
keyEncipherment				Set (1)
authorityKeyIdentifier	**{id-ce 35}**	**YES**	**FALSE**	
keyIdentifier				Calculated per Method 1

By signing this document, you hereby authorize CableLabs to set your Device Certificates extensions as noted above.

Signature: _____ Date: _____

EXHIBIT D7 -
DOCSIS® CABLE MODEM DEVICE CERTIFICATE - NAMING APPLICATION
(for DOCSIS 4.0 devices – Sectigo CA)

Requestor Information:

Company Name:	
Contact Name:	Phone:
Contact E-mail:	

Certificate Format (To Be Completed by Manufacturer):

Subject DN	c=
	o=
	ou= DOCSIS 4.0 CM Certificate
	cn= <(MAC Address (to be entered via the account requesting portal)>

Other Certificate Contents (For CableLabs and CA use only):

Version		v3 (0x02)		
Serial number		Unique Positive Integer assigned by the CA		
Issuer DN		c=US o=CableLabs ou=Device CA05 cn=CableLabs Device Certification Authority		
Not Before		<Issuing Date>		
Not After		<Issuing Date> + 20 years		
Public Key Algorithm		RSA (1 2 840 113549 1 1)		
Signature Algorithm		Sha256WithRSAEncryption (1 2 840 113549 1 1 11)		
Keysize		RSA: 2048-bits		
Parameters		NULL		
Standard Extensions	**OID**	**Required**	**Critical**	**Value**
keyUsage	**{id-ce 15}**	**YES**	**TRUE**	
digitalSignature				Set (1)
keyEncipherment				Set (1)
extendedKeyUsage	**{id-ce 37}**	**YES**	**FALSE**	
svcCM				Set (<1.3.6.1.4.1.4491.2021.2.1.2>)
clientAuth				Set (id-kp-clientAuth)
serverAuth				Set (id-kp-serverAuth)
authorityKeyIdentifier	**{id-ce 35}**	**YES**	**FALSE**	
keyIdentifier				Set (<SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits)>)
certificatePolicies	**{id-ce 32}**	**YES**	**FALSE**	
certPolicyId				Set (<1.3.6.1.4.1.4491.2021.1.5>)
policyQualifiers				Not Set
crlDistributionPoints	**{id-ce 31}**	**YES**	**FALSE**	
distributionPoint				Set (<HTTP URI for Relevant CRL in DER format>)
authorityInfoAccess	**{id-pe 1}**	**YES**	**FALSE**	
ocsp	{id-ad 1}			Set (<HTTP URI of the authoritative OCSP responder>)
caIssuers	{id-ad 2}			Set (<HTTP URI of the Issuing CA certificate in DER format>)

By signing this document, you hereby authorize CableLabs to set your Device Certificates extensions as noted above.

Signature: _____ Date: _____

EXHIBIT D8 -
DPoE 2.0 ONU DEVICE CERTIFICATE NAMING APPLICATION
(for use with DPoE ONU devices – Sectigo CA)

Requestor Information:

Company Name:	
Contact Name:	Phone:
Contact E-mail:	

Certificate Format (To Be Completed by Manufacturer):

Subject DN	c=
	o=
	ou=
	cn= <(MAC Address (to be entered via the account requesting portal)>

Other Certificate Contents (For CableLabs and CA use only):

Version		v3 (0x02)		
Serial number		Unique Positive Integer assigned by the CA		
Issuer DN		c=US o=CableLabs ou=Device CA04 cn=CableLabs Device Certification Authority		
Not Before		<Issuing Date>		
Not After		<Issuing Date> + Up to 20 yrs [*]		
Public Key Algorithm		RSA (1 2 840 113549 1 1)		
Signature Algorithm		Sha256WithRSAEncryption (1 2 840 113549 1 1 11)		
Keysize		RSA: 2048-bits		
Parameters		NULL		
Standard Extensions	OID	Required	Critical	Value
keyUsage	{id-ce 15}	YES	TRUE	
digitalSignature				Set (1)
keyEncipherment				Set (1)
extendedKeyUsage	{id-ce 37}	YES	FALSE	
svcONU				Set (<1.3.6.1.4.1.4491.2021.2.1.4>)
clientAuth				Set (id-kp-clientAuth)
serverAuth				Set (id-kp-serverAuth)
authorityKeyIdentifier	{id-ce 35}	YES	FALSE	
keyIdentifier				Set (<SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits)>)
certificatePolicies	{id-ce 32}	YES	FALSE	
certPolicyId				Set (<1.3.6.1.4.1.4491.2021.1.5>)
policyQualifiers				Not Set
authorityInfoAccess	{id-pe 1}	YES	FALSE	
ocsp	{id-ad 1}			Set (<HTTP URI of the authoritative OCSP responder>)
caIssuers	{id-ad 2}			Set (<HTTP URI of the Issuing CA certificate in DER format>)
crlDistributionPoints	{id-ce 31}	YES	FALSE	
distributionPoint				Set (<HTTP URI for Relevant CRL in DER format>)

By signing this document, you hereby authorize CableLabs to set your Device Certificates extensions as noted above.

Signature: _____ Date: _____

EXHIBIT C1 -
DOCSIS® MANUFACTURER (SIGNER) CVC - NAMING APPLICATION
(for use with DOCSIS 3.0 and earlier devices)

Important! Please include your CSR (PKCS# 10) file when returning form to pkiops@cablelabs.com.

Requestor Information:

Company Name:	
Contact Name:	Phone:
Contact E-mail:	

Certificate Format (To be completed by Manufacturer)

Subject DN	c=
	o=
	ou=DOCSIS
	cn=Code Verification Certificate

Other Certificate Contents (For CableLabs and CA use only):

Version		2		
Serial Number		Integer		
Issuer DN		c=US o=Data Over Cable Services Interface Specifications ou=Cable Modems (DigiCert) cn=DOCSIS Cable Modem Root Certificate Authority (DigiCert)		
notBefore		yymmdd000000Z (Key Ceremony Date)		
notAfter		yymmdd235959Z (10 years)		
Public Key Algorithm		RSA (1 2 840 113549 1 1)		
Signature Algorithm		sha1withRSAEncryption (1 2 840 113549 1 1 5)		
Keysize		2048-bits		
Parameters		NULL		
Standard Extensions	**OID**	**Include**	**Criticality**	**Value**
extendedKeyUsage	{id-ce 37}	X	TRUE	n/a
id-kp-codeSigning				1.3.6.1.5.5.7.3.3

***The manufacturer's company name must match the company name in the manufacturer's CM device certificate.**

By signing this document, you hereby authorize CableLabs to set your Device Certificates extensions as noted above.

Signature: _____ Date: _____

EXHIBIT C2 -
DPoE MANUFACTURER (SIGNER) CVC - NAMING APPLICATION

Important! Please include your CSR (PKCS# 10) file when returning form to pkiops@cablelabs.com.

Requestor Information:

Company Name:	
Contact Name:	Phone:
Contact E-mail:	

Certificate Format (To be completed by Manufacturer)

Subject DN	c=
	o=
	ou=DPoE
	cn=Code Verification Certificate

Other Certificate Contents (For CableLabs and CA use only):

Version		v3		
Serial number		Unique Positive Integer assigned by the CA		
Issuer DN		c=US o=CableLabs ou=CVC CA (DigiCert) cn= CableLabs CVC Certification Authority		
notBefore		If needed, please provide the desired start date for the certificate's validity period (format: YYMMDD000000Z) If no date is provided, the signing date and time will be used (Key Ceremony Date)		
notAfter		yymmdd235959Z (up to 10 years)		
Public Key Algorithm		RSA (1 2 840 113549 1 1)		
Signature Algorithm		Sha256WithRSAEncryption (1 2 840 113549 1 1 11)		
Keysize		2048-bits		
Parameters		NULL		
Standard Extensions	**OID**	**Required**	**Criticality**	**Value**
extKeyUsage	**{id-ce 37}**	**YES**	**TRUE**	
codeSigning				Set
authorityKeyIdentifie	**{id-ce 35}**	**YES**	**FALSE**	
keyIdentifier				Calculated per Method 1

***The manufacturer's company name must match the company name in the manufacturer's CM device certificate.**

By signing this document, you hereby authorize CableLabs to set your Device Certificates extensions as noted above.

Signature: _____ Date: _____

EXHIBIT C3 -
DOCSIS® MANUFACTURER (SIGNER) CVC NAMING APPLICATION
(for DOCSIS 3.1 and Remote PHY devices)

Important! Please include your CSR (PKCS# 10) file when returning form to pkiops@cablelabs.com.

Requestor Information:

Company Name:	
Contact Name:	Phone:
Contact E-mail:	

Certificate Format (To be completed by Manufacturer)

Subject DN	c=
	o=
	ou=DOCSIS
	cn=Code Verification Certificate

Other Certificate Contents (For CableLabs and CA use only):

Version		v3		
Serial number		Unique Positive Integer assigned by the CA		
Issuer DN		c=US o=CableLabs ou=CVC CA01 (CableLabs) cn=CableLabs CVCV Certification Authority		
notBefore		If needed, please provide the desired start date for the certificate's validity period (format: YYMMDD000000Z) If no date is provided, the signing date and time will be used (Key Ceremony Date)		
notAfter		yymmdd235959Z (up to 10 years)		
Public Key Algorithm		RSA (1 2 840 113549 1 1)		
Signature Algorithm		Sha256WithRSAEncryption (1 2 840 113549 1 1 11)		
Keysize		2048-bits		
Parameters		NULL		
Standard Extensions	**OID**	**Required**	**Criticality**	**Value**
extKeyUsage	**{id-ce 37}**	**YES**	**TRUE**	
codeSigning				Set
authorityKeyIdentifie	**{id-ce 35}**	**YES**	**FALSE**	
keyIdentifier				Calculated per Method 1

***The manufacturer's company name must match the company name in the manufacturer's CM device certificate.**

By signing this document, you hereby authorize CableLabs to set your Device Certificates extensions as noted above.

Signature: _____ Date: _____

EXHIBIT C4 -
DOCSIS® MANUFACTURER (SIGNER) CVC NAMING APPLICATION
(for DOCSIS 4.0)

Important! Please include your CSR (PKCS# 10) file when returning form to pkiops@cablelabs.com.

Requestor Information:

Company Name:	
Contact Name:	Phone:
Contact E-mail:	

Certificate Format (To be completed by Manufacturer)

Subject DN	c=
	o=
	ou=DOCSIS
	cn=Code Verification Certificate

Other Certificate Contents (For CableLabs and CA use only):

Version		v3		
Serial number		Unique Positive Integer assigned by the CA		
Issuer DN		c=US o=CableLabs ou= CVC CA01 (CableLabs) cn= CableLabs CVC Certification Authority		
notBefore		If needed, please provide the desired start date for the certificate's validity period (format: YYMMDD000000Z) If no date is provided, the signing date and time will be used (Key Ceremony Date)		
notAfter		yymmdd235959Z (up to 10 years)		
Public Key Algorithm		RSA (1 2 840 113549 1 1)		
Signaure Algorithm		Sha256WithRSAEncryption (1 2 840 113549 1 1 11)		
Keysize		2048-bits		
Parameters		NULL		
Standard Extensions	**OID**	**Required**	**Criticality**	**Value**
extKeyUsage	**{id-ce 37}**	**YES**	**TRUE**	
codeSigning				Set
authorityKeyIdentifie	**{id-ce 35}**	**YES**	**FALSE**	
keyIdentifier				Calculated per Method 1
keyUsage	**{id-ce 15}**	**NO**	**TRUE**	
digitalSignature				Set (1)
crlDistributionPoints	**{id-ce 31}**	**NO**	**FALSE**	
distributionPoint				Set (<HTTP URI for Relevant CRL in DER format>)
certificatePolicies	**{id-ce 32}**	**NO**	**FALSE**	
certPolicyId				Set (<DOCSIS PKI Certificate Policy OID>)
policyQualifiers				Not Set
authorityInfoAccess	**{id-pe 1}**	**NO**	**FALSE**	
ocsp	{id-ad 1}			Set (<HTTP URI of the authoritative OCSP responder>)
caIssuers	{id-ad 2}			Set (<HTTP URI of the Issuing CA certificate in DER

By signing this document, you hereby authorize CableLabs to set your Device Certificates extensions as noted above.

Signature: _____ Date: _____

EXHIBIT S1 -
REMOTE PHY SERVER/AAA CERTIFICATE NAMING APPLICATION

Requestor Information:

Company Name:	
Contact Name:	Phone:
Contact E-mail:	

Certificate Format (To be completed by Manufacturer)

Subject DN	c=
	o=
	cn=
subjectAltName	dnsName(s)=

Other Certificate Contents (For CableLabs and CA use only):

Version		v3		
Serial number		Unique Positive Integer assigned by the CA		
Issuer DN		c=US o=CableLabs ou= Service Provider CA01 (CableLabs) cn= CableLabs Service Provider Certification Authority		
notBefore		yymmdd000000Z (Key Ceremony Date)		
notAfter		yymmdd235959Z (25 years)		
Public Key Algorithm		RSA (1 2 840 113549 1 1)		
Signature Algorithm		Sha256WithRSAEncryption (1 2 840 113549 1 1 11)		
Keysize		2048-bits		
Parameters		NULL		
Standard Extensions	**OID**	**Required**	**Criticality**	**Value**
keyUsage	**{id-ce 15}**	**YES**	**TRUE**	
digitalSignature				Set
keyEncipherment				Set
authorityKeyIdentifier	**{id-ce 35}**	**YES**	**FALSE**	
keyIdentifier				Calculated per Method 1
subjectAltName	**{id-ce 17}**	**YES**	**FALSE**	
dNSName				
extendedKeyUsage	**{id-ce 37}**	**NO**	**FALSE**	
serverAuth	{id-kp 1}			Set (id-kp-serverAuth), or Not Set
clientAuth	{id-kp 2}			Set (id-kp-clientAuth), or Not Set

By signing this document, you hereby authorize CableLabs to set your Device Certificates extensions as noted above.

Signature: _____ Date: _____

EXHIBIT S2 -
DOCSIS 4.0 CMTS NO REVOCATION INFORMATION (NRI) – NAMING APPLICATION (Sectigo CA)

Requestor Information:

Company Name:	
Contact Name:	Phone:
Contact E-mail:	

Certificate Format (To Be Completed by Manufacturer):

Subject DN	c=
	o=
	ou=<Manufacturing Location> (optional)
	cn=<Device Identifier>
subjectAltName (optional)	dnsName(s)=

Other Certificate Contents (For CableLabs and CA use only):

Version		v3 (0x02)		
Serial number		Unique Positive Integer assigned by the CA		
Issuer DN		c=US o=CableLabs ou=Device CA05 cn=CableLabs Device Certification Authority		
Not Before		<Issuing Date>		
Not After		<Issuing Date> + 5 years*		
Public Key Algorithm		RSA (1 2 840 113549 1 1)		
Signature Algorithm		Sha256WithRSAEncryption (1 2 840 113549 1 1 11)		
Key size		2048-bits		
Parameters		NULL		
Standard Extensions	**OID**	**Required**	**Critical**	**Value**
keyUsage	**{id-ce 15}**	**YES**	**TRUE**	
digitalSignature				Set (1)
keyEncipherment				Set (1)
extendedKeyUsage	**{id-ce 37}**	**YES**	**FALSE**	
svcCMTS				Set (id-cl-pki-ext-eku-CMTS)
clientAuth				Set (id-kp-clientAuth)
serverAuth				Set (id-kp-serverAuth)
certificatePolicies	**{id-ce 32}**	**YES**	**FALSE**	
certPolicyId				Set (<1.3.6.1.4.1.4491.2021.1.5>)
policyQualifiers				Not Set
authorityKeyIdentifier	**{id-ce 35}**	**YES**	**FALSE**	
keyIdentifier				Set (<SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits)>)
authorityInfoAccess	**{id-pe 1}**	**NO**	**FALSE**	
caIssuers	{id-ad 2}			Set (<HTTP URI of the Issuing CA in DER format>)
subjectAltName	**{id-ce 17}**	**NO**	**FALSE**	
dNSName				Set (FQDN)

[*] The expiration date shall not exceed the issuing CA's expiration date

By signing this document, you hereby authorize CableLabs to set your Device Certificates extensions as noted above.

Signature: _____ Date: _____

EXHIBIT S3 -
DOCSIS 4.0 CMTS FULL – NAMING APPLICATION (Sectigo CA)

Requestor Information:

Company Name:	
Contact Name:	Phone:
Contact E-mail:	

Certificate Format (To Be Completed by Manufacturer):

Subject DN	c=
	o=
	ou=<Manufacturing Location> (optional)
	cn=<Device Identifier>
subjectAltName (optional)	dnsName(s)=

Other Certificate Contents (For CableLabs and CA use only):

Version		v3 (0x02)		
Serial number		Unique Positive Integer assigned by the CA		
Issuer DN		c=US o=CableLabs ou=Device CA05 cn=CableLabs Device Certification Authority		
Not Before		<Issuing Date>		
Not After		<Issuing Date> + 5 years*		
Public Key Algorithm		RSA (1 2 840 113549 1 1)		
Signature Algorithm		Sha256WithRSAEncryption (1 2 840 113549 1 1 11)		
Key size		2048-bits		
Parameters		NULL		
Standard Extensions	**OID**	**Required**	**Critical**	**Value**
keyUsage	**{id-ce 15}**	**YES**	**TRUE**	
digitalSignature				Set (1)
keyEncipherment				Set (1)
extendedKeyUsage	**{id-ce 37}**	**YES**	**FALSE**	
svcCMTS				Set (id-cl-pki-ext-eku-CMTS)
clientAuth				Set (id-kp-clientAuth)
serverAuth				Set (id-kp-serverAuth)
authorityKeyIdentifier	**{id-ce 35}**	**YES**	**FALSE**	
keyIdentifier				Set (<SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits)>)
certificatePolicies	**{id-ce 32}**	**YES**	**FALSE**	
certPolicyId				Set (<1.3.6.1.4.1.4491.2021.1.5>)
policyQualifiers				Not Set
authorityInfoAccess	**{id-pe 1}**	**YES**	**FALSE**	
ocsp	{id-ad 1}			Set (<HTTP URI of authoritative OCSP responder>)
caIssuers	{id-ad 2}			Set (<HTTP URI of Issuing CA in DER format>)
crlDistributionPoints	**{id-ce 31}**	**NO**	**FALSE**	
distributionPoint				Set (<HTTP URI for Relevant CRL in DER format>)
subjectAltName	**{id-ce 17}**	**NO**	**FALSE**	
dNSName				Set (FQDN)

[*] The expiration shall not exceed the issuing CA's one

By signing this document, you hereby authorize CableLabs to set your Device Certificates extensions as noted above.

Signature: _____ Date: _____

EXHIBIT S4 -
CCAP CORE NO-REVOCATION INFORMATION (NRI) – NAMING APP (Sectigo CA)

Requestor Information:

Company Name:	
Contact Name:	Phone:
Contact E-mail:	

Certificate Format (To Be Completed by Manufacturer):

Subject DN	c=
	o=
	ou=<Manufacturing Location> (optional)
	cn=<Device Identifier>
subjectAltName (optional)	dnsName(s)=

Other Certificate Contents (For CableLabs and CA use only):

Version		v3 (0x02)		
Serial number		Unique Positive Integer assigned by the CA		
Issuer DN		c=US o=CableLabs ou=Device CA05 cn=CableLabs Device Certification Authority		
Not Before		<Issuing Date>		
Not After		<Issuing Date> + 25 years		
Public Key Algorithm		RSA (1 2 840 113549 1 1)		
Signature Algorithm		Sha256WithRSAEncryption (1 2 840 113549 1 1 11)		
Key size		2048-bits		
Parameters		NULL		
Standard Extensions	**OID**	**Required**	**Critical**	**Value**
keyUsage	**{id-ce 15}**	**YES**	**TRUE**	
digitalSignature				Set (1)
keyEncipherment				Set (1)
extendedKeyUsage	**{id-ce 37}**	**YES**	**FALSE**	
svcCCAP				Set (id-cl-pki-ext-eku-CCAP)
svcCMTS				Set (id-cl-pki-ext-eku-CMTS)
clientAuth				Set (id-kp-clientAuth)
serverAuth				Set (id-kp-serverAuth)
authorityKeyIdentifier	**{id-ce 35}**	**YES**	**FALSE**	
keyIdentifier				Set (<SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits)>)
certificatePolicies	**{id-ce 32}**	**YES**	**FALSE**	
certPolicyId				Set (<1.3.6.1.4.1.4491.2021.1.5>)
policyQualifiers				Not Set
subjectAltName	**{id-ce 17}**	**NO**	**FALSE**	
dNSName				Set (FQDN)

[*] The expiration shall not exceed the issuing CA's one

By signing this document, you hereby authorize CableLabs to set your Device Certificates extensions as noted above.

Signature: _____ Date: _____

EXHIBIT S5 -
CCAP CORE FULL – NAMING APPLICATION (Sectigo CA) Requestor Information:

Company Name:	
Contact Name:	Phone:
Contact E-mail:	

Certificate Format (To Be Completed by Manufacturer):

Subject DN	c=
	o=
	ou=<Manufacturing Location> (optional)
	cn=<Device Identifier>
subjectAltName (optional)	dnsName(s)=

Other Certificate Contents (For CableLabs and CA use only):

Version		v3 (0x02)		
Serial number		Unique Positive Integer assigned by the CA		
Issuer DN		c=US o=CableLabs ou=Device CA05 cn=CableLabs Device Certification Authority		
Not Before		<Issuing Date>		
Not After		<Issuing Date> + 25 years		
Public Key Algorithm		RSA (1 2 840 113549 1 1)		
Signature Algorithm		Sha256WithRSAEncryption (1 2 840 113549 1 1 11)		
Key size		2048-bits		
Parameters		NULL		
Standard Extensions	**OID**	**Required**	**Critical**	**Value**
keyUsage	**{id-ce 15}**	**YES**	**TRUE**	
digitalSignature				Set (1)
keyEncipherment				Set (1)
extendedKeyUsage	**{id-ce 37}**	**YES**	**FALSE**	
svcCCAP				Set (id-cl-pki-ext-eku-CCAP)
svcCMTS				Set (id-cl-pki-ext-eku-CMTS)
clientAuth				Set (id-kp-clientAuth)
serverAuth				Set (id-kp-serverAuth)
authorityKeyIdentifier	**{id-ce 35}**	**YES**	**FALSE**	
keyIdentifier				Set (<SHA-1 hash of the value of the BIT STRING subjectPublicKey>)
certificatePolicies	**{id-ce 32}**	**YES**	**FALSE**	
certPolicyId				Set (<1.3.6.1.4.1.4491.2021.1.5>)
policyQualifiers				Not Set
crlDistributionPoints	**{id-ce 31}**	**NO**	**FALSE**	
distributionPoint				Set (<HTTP URI for Relevant CRL in DER format>)
authorityInfoAccess	**{id-pe 1}**	**NO**	**FALSE**	
ocsp	{id-ad 1}			Set (<HTTP URI of the authoritative OCSP responder>)
caIssuers	{id-ad 2}			Set (<HTTP URI of the Issuing CA certificate in DER format>)
subjectAltName	**{id-ce 17}**	**NO**	**FALSE**	
dNSName				Set (FQDN)

[*] The expiration shall not exceed the issuing CA's one

By signing this document, you hereby authorize CableLabs to set your Device Certificates extensions as noted above.

Signature: _____ Date: _____