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	Dıgıtal	Certificate	Authorization	\mathcal{C}	("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").								
Manuf	acturer O	rganization Nan	ne (Full Legal Name	e of Entity executin	this Agreement):				
Main (Corporate	Headquarters A	ddress:		Phone:				
		ce, postal code, cou			Thone.				

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)	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 2 nd 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 2 nd 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, <u>INCLUDING THOSE TERMS CONTAINED ON THE FOLLOWING PAGES HEREOF.</u>

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 <u>Definitions</u>

- 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 <u>Digital Certificate Authorization</u>

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 <u>Use of Digital Certificates and Request/Receipt of Certificates</u>

- 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 <u>MUST</u> be the legally registered business name.
- 4) Use of special characters such as () & * \% \$ # (a)! + = \^ 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:	
	e Authentication process. If you do not know your company's D. Note: The Legal Company Name and Corporate Address listed I-S Database.
MANUFACTURER'S CORPORATE CONTACT:	
This person must work for the organization requesting this	s service and is responsible for the device manufacturing system. Thing administrators who will request Certificates from CableLabs. The ents 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 cer	tificates.
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.

certificates.	
First Name*:	Last Name*:
Title*:	E-mail*:
Phone*:	
Address*:	City and State*:
Zip/Postal Code*:	Country*:
MANUFACTURER'S TECHNICAL CONTINUES IN A technical contact, typically in development with CableLabs.	ΓΑCT ment engineering, authorized to discuss technical issues related to the D
First Name*:	Last Name*:
Title*:	E-mail*:
Phone*:	
MANUFACTURER'S LEGAL CONTACT This person will receive a copy of any contractual re	
First Name*:	Last Name*:
First Name*: Title*:	Last Name*: E-mail*:
Title*:	
Title*: Phone*:	E-mail*:
Title*: Phone*: Address*: Zip/Postal Code*: MANUFACTURER'S BILLING CONTACTOR of the person responsible for payment and notice.	E-mail*: City and State*: Country*:
Title*: Phone*: Address*: Zip/Postal Code*: MANUFACTURER'S BILLING CONTACTORS is the person responsible for payment and notification.	E-mail*: City and State*: Country*: T: Ifying CableLabs of any billing changes, for example an accounts payable
Title*: Phone*: Address*: Zip/Postal Code*: MANUFACTURER'S BILLING CONTACT In the person responsible for payment and notice presentative. Please list any special instructions for the person responsible for payment and notice presentative.	E-mail*: City and State*: Country*: T: Ifying CableLabs of any billing changes, for example an accounts payable for billing (e.g. require purchase order, submit invoice to portal)
Title*: Phone*: Address*: Zip/Postal Code*: MANUFACTURER'S BILLING CONTACTORIST IS IN THE PROPRIED OF THE PRO	E-mail*: City and State*: Country*: T: Ifying CableLabs of any billing changes, for example an accounts payable for billing (e.g. require purchase order, submit invoice to portal) Last Name*:
Title*: Phone*: Address*: Zip/Postal Code*: MANUFACTURER'S BILLING CONTACTOR In the person responsible for payment and not representative. Please list any special instructions for the person responsible for payment and not representative. Please list any special instructions for the person responsible for payment and not representative. Please list any special instructions for the person responsible for payment and not representative. Please list any special instructions for the person responsible for payment and not representative. Please list any special instructions for the person responsible for payment and not representative. Please list any special instructions for the person responsible for payment and not representative. Please list any special instructions for the person responsible for payment and not representative. Please list any special instructions for the person responsible for payment and not representative. Please list any special instructions for the person responsible for payment and not representative. Please list any special instructions for the person responsible for payment and not representative. Please list any special instructions for the person responsible for payment and not represent the person responsible for payment and person responsible for payment a	E-mail*: City and State*: Country*: T: Ifying CableLabs of any billing changes, for example an accounts payable for billing (e.g. require purchase order, submit invoice to portal) Last Name*:

EXHIBIT D1 -

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

Please complete the <u>Requestor Information</u> section and the Subject DN of the <u>Certificate Format</u>.

Requestor Information	1:				
Organization Name:					
Contact Name:				Phone:	
Contact E-mail:					
Certificate Format (To	be comple	eted by Ma	anufacture	er)	
Subject DN		c=			
		o=			
		ou=			
		cn = < (MA)	AC Address	s (to be entered via the account requesting portal)>	
Other Certificate Con	tents (For (CableLab	s and CA u	ise only):	
Version	tents (1 or	v3	, una cri u	see only).	
Serial number		Unique Po	sitive Integer	r 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)			
•		1024-bits			
Parameters	_	NULL			
Standard Extensions	OID	Required	Criticality	Value	
	{id-ce 15}	YES	FALSE	n/a	
				Set	
keyEncipherment				Set	
, ,		YES	FALSE	Calculated per Method 1	
keyIdentifier				<pre><same as="" ca="" certificate="" in="" subjectkeyidentifier=""></same></pre>	
authorityKeyIdentifier keyIdentifier	{id-ce 15} {id-ce 35}	NULL Required Criticality Value YES FALSE n/a Set Set YES FALSE Calculated per Method 1			
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 <u>Requestor Information</u> section and the Subject DN of the <u>Certificate Format</u>.

Requestor Information	1:					
Organization Name:						
Contact Name:				Phone:		
Contact E-mail:						
Certificate Format (To	be compl	eted by Ma	anufacture	er)		
Base Certificate						
Subject DN		c=				
		0=				
		ou=				
		cn = < (MA	AC Address	(to be entered via the account requesting portal)>		
Other Certificate Con	tents (For (CableLabs	and CA u	se only):		
Version	`	v3		• • • • • • • • • • • • • • • • • • • •		
Serial number		Unique Pos	sitive Intege	r assigned by the CA		
Issuer DN		c=US				
		o=CableLabs				
		ou=DOCSIS				
		ou=D CA00004 V2 EXT				
_		cn=CableLabs Cable Modem Certificate Authority				
notBefore			` •	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	T	NULL				
Standard Extensions	OID	-	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="" ca="" certificate="" in="" subjectkeyidentifier=""></same>			
	nt, you here	by authoriz	ze CableLa	bs to set your Device Certificates extensions as noted above		
Signature:	Date:					

EXHIBIT D3 PACKETCABLE DEVICE CERTIFICATE NAMING APPLICATION (Sectigo CA)

			8 /	
:				
			Phone:	
Be Complet	ted by M	anufacturer):	
	c=			
	o=			
	st=			
	1=			
	ou=Pack	etCable		
	ou=			
	ou=			
	cn=<(MAC Address (to be entered via the account requesting portal)>			
ents (For Ca	1	and CA use	e only):	
	Unique Positive Integer assigned by the CA			
	cn = CableLabs, Inc. PacketCable CA			
	yymmdd000000Z (Key Ceremony Date)			
	yymmdd235959Z (20 years)			
	RSA (1 2 840 113549 1 1)			
	Sha1WithRSAEncryption (1 2 840 113549 1 1 5)			
	1024-bits			
	NULL			
OID	Include	Criticality	Value	
{id-ce 15}	YES	TRUE	n/a	
			Set	
			Set	
{id-ce 35}	YES	FALSE	Calculated per Method 1	
	ents (For Ca	C= O= St= I= Ou=Pack Ou= Ou= Cn=< (M.) Ents (For CableLabs V3 Unique P C = US O = Cable Ou=Pack Ou=Pack	Be Completed by Manufacturer c= o= st= l= ou=PacketCable ou= cn=<(MAC Address (ents (For CableLabs and CA use v3 Unique Positive Integer c = US o = CableLabs, Inc. ou=PacketCable ou= PC CA00001 - G3 cn = CableLabs, Inc. Pa yymmdd000000Z (Key yymmdd235959Z (20 y RSA (1 2 840 113549 1 Sha1WithRSAEncrypti 1024-bits NULL OID Include Criticality {id-ce 15} YES TRUE	

By signing this document, you hereby authorized	orize 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	n:				
Organization Name:					
Contact Name:			Phone:		
Contact E-mail:				<u> </u>	
Certificate Format (Te	o be comp	oleted by Ma	nufacturer) :	
Subject DN		c=			
		o=			
		ou=			
		cn= <(M.	AC Address	(to be entered via the account requesting portal)>	
Other Certificate Con	tents (For	· CableLabs	and CA us	e only):	
Issuer DN	(1 01	c=US		o on ji	
		o=CableLabs			
		ou=CA00008			
		cn=CableLab	s Device Cer	tification Authority	
Not Before		<issuing dat<="" td=""><td></td><td></td></issuing>			
Not After		<issuing date<="" td=""><td>e > + Up to 20</td><td>) yrs [*]</td></issuing>	e > + Up to 20) yrs [*]	
Public Key Algorithm		RSA (1 2 840			
Signature Algorithm		Sha256WithRSAEncryption (1 2 840 113549 1 1 11)			
Keysize		RSA: 2048-bits			
Parameters	OID	NULL			
	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 bit="" hash="" of="" string<="" td="" the="" value=""></sha-1>	
				subjectPublicKey (excluding the tag, length, and number of	
/*@* / To 1* *	(* 1 22)	VEC	EALGE	unused bits)>)	
certificatePolicies	{id-ce 32}	YES	FALSE	S.+ (<1.2 (1.4.1.4401.2021.1.5)	
certPolicyId				Set (<1.3.6.1.4.1.4491.2021.1.5>)	
policyQualifiers	(id no 1)	YES	EALCE	Not Set	
authorityInfoAccess	{id-pe 1}	ILS	FALSE	Set (<http authoritative="" ocsp="" of="" responder="" the="" uri="">)</http>	
ocsp	{id-ad 1} {id-ad 2}			1 /	
calssuers	{id-ad 2} {id-ce 31}	VEC	FAICE	Set (<http ca="" certificate="" der="" format="" in="" issuing="" of="" the="" uri="">)</http>	
	{1 u-ce 3 1}	1 L S	FALSE	Set (<http crl="" der="" for="" format="" in="" relevant="" uri="">)</http>	
crlDistributionPoints distributionPoint					

Signatura	Detail

EXHIBIT D5 -

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

Organization Name:							
Contact Name:				Phone:			
Contact E-mail:							
Certificate Format (To	o be comple	ted by N	Ianufactu r	rer):			
Subject DN	c=						
	o=						
		ou=					
		cn= <()	MAC Addro	ess (to be entered via the account requesting portal)>			
Other Contificate Con	40m40 (E0m (Tablat al	ha and CA	use autole			
Other Certificate Con Version	v3	os and CA	use only):				
Serial number			Positive Inte	eger assigned by the CA			
Issuer DN		c=US	Unique Positive Integer assigned by the CA				
issuer DN		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			

Signature:				Date:	
By signing this document,	you hereby authorize	CableLabs to set	your Device C	ertificates extensions	as noted abov

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 Name. Contact E-mail:				r none.			
	. h	tod by Mor	···fo otumow).				
Certificate Format (To	b be comple		iuiacturer):				
Subject DN		c=					
		0=					
		ou=	C 4 11 /				
		cn= <(MA	C Address (to be entered via the account requesting portal)>			
Other Certificate Con	tents (For C	CableLabs a	nd CA use	only):			
Version	v3		•				
Serial number		Unique Pos	itive Integer a	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	1	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			

DOCSIS Digit:	al Certificate Aı	ithorization /	Agreement —	Fxhihit — ˈ	RPHY Device	e Rev 2024-12

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

Requestor Information:	Rec	uestor	Inform	ation
------------------------	-----	--------	--------	-------

Company Name:						
Contact Name:			Phone:			
Contact E-mail:						
Certificate Format (To	Be Compl	eted by Manu	facturer):			
Subject DN	, 20 соптр.	c=				
		0=				
		ou= DOCSIS	4.0 CM Certifi	cate		
		cn = < (MAC A	Address (to be e	entered via the account requesting portal)>		
Other Certificate Con	tents (For (ableLabs and	l CA use only)):		
Version	ients (1 01 C	v3 (0x02)	erruse omy	,		
Serial number			e Integer assigne	ed by the CA		
Issuer DN		c=US		•		
		o=CableLabs				
		ou=Device CA	05			
			Device Certifica	ation Authority		
Not Before		<issuing date=""></issuing>				
Not After	After <issuing date=""> + 20 years</issuing>					
Public Key Algorithm		RSA (1 2 840 1	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 bit="" hash="" of="" string<="" td="" the="" value=""></sha-1>		
				subjectPublicKey (excluding the tag, length, and		
certificatePolicies	(cd as 22)	YES	FALSE	number of unused bits)>)		
certPolicyId	{id-ce 32}	ILS	FALSE	Sat (<1.2 6.1.4.1.4401.2021.1.5\)		
policyQualifiers				Set (<1.3.6.1.4.1.4491.2021.1.5>) Not Set		
	(cd. so 21)	VEC	EALCE	Not Set		
crlDistributionPoints distributionPoint	{id-ce 31}	YES	FALSE	Set (ZITTD LIDI for Delevent CDL in DED formet)		
	(d = 1)	VEC	EALCE	Set (<http crl="" der="" for="" format="" in="" relevant="" uri="">)</http>		
authorityInfoAccess	{id-pe 1}	YES	FALSE	G + (AUTTR LIBT C.1		
ocsp	{id-ad 1}			Set (<http authoritative="" ocsp="" of="" responder="" the="" uri="">)</http>		
caIssuers	{id-ad 2}			Set (<http ca="" certificate="" der="" format="" in="" issuing="" of="" the="" uri="">)</http>		
Ry signing this docume	nt. vou here	ov authorize Ca	ableLabs to set	your Device Certificates extensions as noted above		

DOCSIS Digital Certificate Authorization Agreement – Exhibit – D4.0 Device - Rev 2024-12

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

Contact Name:				Phone:	
Contact E-mail:				·	
ertificate Format (T	o Be Comp	leted by Ma	nufacturei	r):	
ubject DN		c=			
		o=			
		ou=			
		cn = < (MA)	C Address (to be entered via the account requesting portal)>	
ther Certificate Con	tents (For	CableLabs a	and CA use	e only):	
Version		v3 (0x02)			
Serial number			tive Integer	assigned by the CA	
ssuer DN		c=US			
		o=CableLab			
		ou=Device (
AL AD C				ertification Authority	
Not Before		<issuing da<="" td=""><td></td><td>20 543</td></issuing>		20 543	
Not After			te > + Up to 2		
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	0.4(1)	
digitalSignature				Set (1)	
keyEncipherment	(:1 27)	VEC	EALCE	Set (1)	
extendedKeyUsage	{id-ce 37}	YES	FALSE	G + (<1.2 (1.4.1.4401.2021.2.1.45)	
svcONU	+			Set (<1.3.6.1.4.1.4491.2021.2.1.4>)	
clientAuth				Set (id-kp-clientAuth)	
serverAuth	(:1 25)	VEC	EALCE	Set (id-kp-serverAuth)	
nuthorityKeyIdentifier	{id-ce 35}	YES	FALSE	Set (SIIA 1 heek of the value of the DIT STRING	
keyIdentifier				Set (<sha-1 (excluding="" and="" bit="" hash="" length,="" number="" o<="" of="" string="" subjectpublickey="" tag,="" td="" the="" value=""></sha-1>	
				unused bits)>)	
certificatePolicies	{id-ce 32}	YES	FALSE	unused ons)	
certPolicyId	(10.0032)	125	TILOL	Set (<1.3.6.1.4.1.4491.2021.1.5>)	
policyQualifiers				Not Set	
authorityInfoAccess	{id-pe 1}	YES	FALSE		
ocsp	{id-ad 1}	1 Lo	TTESE	Set (<http authoritative="" ocsp="" of="" responder="" the="" uri="">)</http>	
calssuers	{id-ad 1}			Set (<hr/> HTTP URI of the Issuing CA certificate in DER	
	(10 00 2)			format>)	
erlDistributionPoints	{id-ce 31}	YES	FALSE		
distributionPoint	()			Set (<http crl="" der="" for="" format="" in="" relevant="" uri="">)</http>	
	1			(

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

questor Informatio	:								
ompany Name:									
ontact Name:			Phone:						
ontact E-mail:									
rtificate Format (T	be compl	leted by Manufacturer)							
ıbject DN		c=							
-		0=							
		ou=DOCSIS							
		cn=Code Verification Certificate							
her Certificate Con	ents (For	CableLabs and CA use only):							
rsion		2							
rial Number		Integer							
uer DN		c=US o=Data Over Cable Services Interface Specifications ou=Cable Modems (DigiCert) cn=DOCSIS Cable Modem Root Certificate Authority (DigiCert)							
tBefore		yymmdd000000Z (Key Ceremony Date)							
tAfter		yymmdd235959Z (10 years)							
blic Key Algorithm		RSA (1 2 840 113549 1 1)							
nature Algorithm		sha1withRSAEncryption (1 2 840 113549 1 1 5)							
eysize		2048-bits							
rameters		NULL							
andard Extensions	OID	Include	Criticality	Value					
tendedKeyUsage	(id-ce 37)	X	TRUE	n/a					
kp-codeSigning				1.3.6.1.5.5.7.3.3					
tificate.		name must match the company is the c							
	t, you here	eby authorize CableLabs to set your	Device C	_					

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

Requestor Information	1:							
Company Name:								
Contact Name: Phone:								
Contact E-mail:								
Certificate Format (To	be comple	eted by Ma	nufacturer	•)				
Subject DN	(c=						
	(0=						
		ou=DPoE						
	(cn=Code Ve	erification (Certificate				
Other Certificate Cont	ents (For (CahleI ahs	and CA us	e only).				
Version	ciits (1 01 V	v3	and CII us	c only).				
Serial number		_	sitive Integ	er assigned by the CA				
Issuer DN		c=US		and an				
Issuel Div		o=CableLa	ıhs					
		ou=CVC CA (DigiCert)						
			Labs CVC (
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				
certificate.				e company name in the manufacturer's CM device s 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)

Requestor Information	1:							
Company Name:								
Contact Name:				Phone:				
Contact E-mail:								
Certificate Format (To	be comple	eted by Ma	nufacturer	•)				
Subject DN	(2=						
	(0=						
	(ou=DOCSI	S					
	(en=Code V	erification C	Certificate				
Other Certificate Cont	ents (For C	CableLabs	and CA us	e only):				
Version		v3						
Serial number		Unique Po	sitive Intege	er assigned by the CA				
Issuer DN		c=US						
		o=CableLa	ıbs					
			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 c	company n	ame must	match the	company name in the manufacturer's CM device				
By signing this documer	nt, you here	by authoriz	e CableLab	s to set your Device Certificates extensions as noted above.				
Signature:				Date:				

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

Requestor Information	ı:						
Company Name:							
Contact Name:				Phone:			
Contact E-mail:				<u> </u>			
Certificate Format (To	be comple	eted by Ma	nufacturer				
Subject DN	C) =					
	O)=					
ou=DOCSIS							
cn=Code Verification Certificate							
Other Certificate Cont	ents (For C	CableLabs	and CA us	e only):			
Version		v3					
Serial number		Unique Pos	sitive Intege	er assigned by the CA			
Issuer DN		c=US					
		o=CableLa					
			CA01 (Cabl				
AD C		cn= Cablel	_abs CVC (Certification Authority			
notBefore				ide 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		• •	` *	to 10 years)			
Public Key Algorithm			40 113549 1				
Signaure Algorithm			thRSAEncr	yption (1 2 840 113549 1 1 11)			
Keysize		2048-bits					
Parameters	1	NULL	1				
Standard Extensions	OID		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)			
	{id-ce 31}	NO	FALSE				
distributionPoint		770		Set (<http crl="" der="" for="" format="" in="" relevant="" uri="">)</http>			
	{id-ce 32}	NO	FALSE				
certPolicyId				Set (<docsis certificate="" oid="" pki="" policy="">)</docsis>			
policyQualifiers		310	EALGE	Not Set			
•	{id-pe 1}	NO	FALSE				
ocsp	{id-ad 1}			Set (<http authoritative="" ocsp="" of="" responder="" the="" uri="">)</http>			
calssuers	{id-ad 2}			Set (<http ca="" certificate="" der<="" in="" issuing="" of="" td="" the="" uri=""></http>			
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 complete	ed by Manuf	acturer)					
Subject DN	c=	•	,					
	0=							
	cn=							
subjectAltName	dnsNam	e(s)=						
Other Certificate Conto	ents (For Ca		l CA use onl	y):				
Version		v3						
Serial number		•	tive Integer a	assigned by the CA				
Issuer DN		c=US						
		o=CableLab						
				.01 (CableLabs)				
				rovider Certification Authority				
notBefore				Ceremony Date)				
notAfter		1	yymmdd235959Z (25 years)					
Public Key Algorithm		RSA (1 2 840						
Signature Algorithm			RSAEncrypt	ion (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 documen	t, you hereby	authorize Ca	ableLabs to s	et your Device Certificates extensions as noted above.				
				•				
Signature:				Date				
NUMBER				Date				

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

equestor Information	:								
Company Name:									
Contact Name:				Phone:					
Contact E-mail:				<u>, </u>					
ertificate Format (To	Be Compl	eted by Manuf	acturer):						
Subject DN		c=	•						
		0=							
		ou= <manufacturing location=""> (optional)</manufacturing>							
		cn= <device identifier=""></device>							
subjectAltName (optior	nal)	dnsName(s)=							
ther Certificate Conte	ents (For C	CableLabs and	CA use only)	:					
Version		v3 (0x02)	•						
Serial number		Unique Positive	Integer assigne	ed by the CA					
Issuer DN		c=US							
		o=CableLabs							
		ou=Device CA0							
		cn=CableLabs D	Device Certifica	ation Authority					
Not Before		<issuing date=""></issuing>							
Not After		<issuing date=""></issuing>	•						
Public Key Algorithm		RSA (1 2 840 113549 1 1)							
Signature Algorithm			AEncryption (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}	·							
1 71				Set (<sha-1 bit="" hash="" of="" string<="" td="" the="" value=""></sha-1>					
keyIdentifier				subjectPublicKey (excluding the tag, length, and number					
keyldentifier				of unused bits)>)					
	(1) (5)	NO	T	of unused bits)>)					
subjectAltName dNSName	{id-ce 17}	NO	FALSE	of unused bits)>) Set (FQDN)					

Signature:	Data
Signature.	Date:

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

Company Name:	_								
Contact Name:				Phone:					
Contact E-mail:				<u> </u>					
ertificate Format (To	Be Comple	eted by Manuf	acturer):						
Subject DN		c=							
		o=							
		ou= <manufact< td=""><td colspan="7">u=<manufacturing location=""> (optional)</manufacturing></td></manufact<>	u= <manufacturing location=""> (optional)</manufacturing>						
		cn= <device ide<="" td=""><td>entifier></td><td></td></device>	entifier>						
subjectAltName (option	nal)	dnsName(s)=							
` 1									
ther Certificate Conte	ents (For C	CableLabs and	CA use only)	<u>:</u>					
Version	71105 (2 01 0	v3 (0x02)	011 0150 01113)	•					
Serial number		Unique Positive	Integer assigne	ed by the CA					
Issuer DN		c=US		y					
		o=CableLabs							
		ou=Device CA()5						
		cn=CableLabs I	Device Certifica	tion Authority					
Not Before		<issuing date=""></issuing>		•					
Not After		<issuing date=""></issuing>	+ 5 years*						
Public Key Algorithm		RSA (1 2 840 1							
Signature Algorithm		_		2 840 113549 1 1 11)					
Key size		2048-bits	71	,					
Parameters		NULL							
C. LIE.	OID	Required	Critical	Value					
Standard Extensions	OID								
Standard Extensions keyUsage		YES	TRUE						
keyUsage	{id-ce 15}	_	TRUE	Set (1)					
keyUsage digitalSignature		_	TRUE	Set (1) Set (1)					
keyUsage digitalSignature keyEncipherment	{id-ce 15}	YES		Set (1) Set (1)					
keyUsage digitalSignature keyEncipherment extendedKeyUsage		_	TRUE FALSE	Set (1)					
keyUsage digitalSignature keyEncipherment	{id-ce 15}	YES		Set (1) Set (id-cl-pki-ext-eku-CMTS)					
digitalSignature keyEncipherment extendedKeyUsage svcCMTS clientAuth	{id-ce 15}	YES		Set (1) Set (id-cl-pki-ext-eku-CMTS) Set (id-kp-clientAuth)					
digitalSignature keyEncipherment extendedKeyUsage svcCMTS clientAuth serverAuth	{id-ce 15}	YES		Set (1) Set (id-cl-pki-ext-eku-CMTS)					
keyUsage digitalSignature keyEncipherment extendedKeyUsage svcCMTS clientAuth serverAuth authorityKeyIdentifier	{id-ce 15}	YES	FALSE	Set (1) Set (id-cl-pki-ext-eku-CMTS) Set (id-kp-clientAuth) Set (id-kp-serverAuth)					
digitalSignature keyEncipherment extendedKeyUsage svcCMTS clientAuth serverAuth	{id-ce 15}	YES	FALSE	Set (1) Set (id-cl-pki-ext-eku-CMTS) Set (id-kp-clientAuth) Set (id-kp-serverAuth) Set (<sha-1 bit="" hash="" of="" string)<="" td="" the="" value=""></sha-1>					
keyUsage digitalSignature keyEncipherment extendedKeyUsage svcCMTS clientAuth serverAuth authorityKeyIdentifier	{id-ce 15}	YES	FALSE	Set (id-cl-pki-ext-eku-CMTS) Set (id-kp-clientAuth) Set (id-kp-serverAuth) Set (<sha-1 (excluding="" and="" bit="" hash="" length,="" number<="" of="" string="" subjectpublickey="" tag,="" td="" the="" value=""></sha-1>					
keyUsage digitalSignature keyEncipherment extendedKeyUsage svcCMTS clientAuth serverAuth authorityKeyIdentifier keyIdentifier	{id-ce 15} {id-ce 37} {id-ce 35}	YES YES YES	FALSE	Set (1) Set (id-cl-pki-ext-eku-CMTS) Set (id-kp-clientAuth) Set (id-kp-serverAuth) Set (<sha-1 bit="" hash="" of="" string)<="" td="" the="" value=""></sha-1>					
digitalSignature keyEncipherment extendedKeyUsage svcCMTS clientAuth serverAuth authorityKeyIdentifier keyIdentifier certificatePolicies	{id-ce 15}	YES	FALSE	Set (1) Set (id-cl-pki-ext-eku-CMTS) Set (id-kp-clientAuth) Set (id-kp-serverAuth) Set (<sha-1 (excluding="" and="" bit="" bits)="" hash="" length,="" numbe="" of="" string="" subjectpublickey="" tag,="" the="" unused="" value="">)</sha-1>					
digitalSignature keyEncipherment extendedKeyUsage svcCMTS clientAuth serverAuth authorityKeyIdentifier keyIdentifier certificatePolicies certPolicyId	{id-ce 15} {id-ce 37} {id-ce 35}	YES YES YES	FALSE	Set (1) Set (id-cl-pki-ext-eku-CMTS) Set (id-kp-clientAuth) Set (id-kp-serverAuth) Set (<sha-1 (excluding="" and="" bit="" bits)="" hash="" length,="" numbe="" of="" string="" subjectpublickey="" tag,="" the="" unused="" value="">) Set (<1.3.6.1.4.1.4491.2021.1.5>)</sha-1>					
digitalSignature keyEncipherment extendedKeyUsage svcCMTS clientAuth serverAuth authorityKeyIdentifier keyIdentifier certificatePolicies certPolicyId policyQualifiers	{id-ce 15} {id-ce 37} {id-ce 35} {id-ce 32}	YES YES YES	FALSE FALSE	Set (1) Set (id-cl-pki-ext-eku-CMTS) Set (id-kp-clientAuth) Set (id-kp-serverAuth) Set (<sha-1 (excluding="" and="" bit="" bits)="" hash="" length,="" numbe="" of="" string="" subjectpublickey="" tag,="" the="" unused="" value="">)</sha-1>					
digitalSignature keyEncipherment extendedKeyUsage svcCMTS clientAuth serverAuth authorityKeyIdentifier keyIdentifier certificatePolicies certPolicyId policyQualifiers authorityInfoAccess	{id-ce 15} {id-ce 37} {id-ce 35} {id-ce 32}	YES YES YES	FALSE	Set (1) Set (id-cl-pki-ext-eku-CMTS) Set (id-kp-clientAuth) Set (id-kp-serverAuth) Set (<sha-1 (excluding="" and="" bit="" bits)="" hash="" length,="" numbe="" of="" string="" subjectpublickey="" tag,="" the="" unused="" value="">) Set (<1.3.6.1.4.1.4491.2021.1.5>) Not Set</sha-1>					
digitalSignature keyEncipherment extendedKeyUsage svcCMTS clientAuth serverAuth authorityKeyIdentifier keyIdentifier certificatePolicies certPolicyId policyQualifiers authorityInfoAccess ocsp	{id-ce 37} {id-ce 37} {id-ce 35} {id-ce 32} {id-pe 1} {id-ad 1}	YES YES YES	FALSE FALSE	Set (1) Set (id-cl-pki-ext-eku-CMTS) Set (id-kp-clientAuth) Set (id-kp-serverAuth) Set (<sha-1 (excluding="" and="" bit="" bits)="" hash="" length,="" number="" of="" string="" subjectpublickey="" tag,="" the="" unused="" value="">) Set (<1.3.6.1.4.1.4491.2021.1.5>) Not Set Set (<http authoritative="" ocsp="" of="" responder="" uri="">)</http></sha-1>					
digitalSignature keyEncipherment extendedKeyUsage svcCMTS clientAuth serverAuth authorityKeyIdentifier keyIdentifier certificatePolicies certPolicyId policyQualifiers authorityInfoAccess ocsp calSsuers	{id-ce 37} {id-ce 37} {id-ce 35} {id-ce 32} {id-pe 1} {id-ad 1} {id-ad 2}	YES YES YES YES	FALSE FALSE FALSE	Set (1) Set (id-cl-pki-ext-eku-CMTS) Set (id-kp-clientAuth) Set (id-kp-serverAuth) Set (<sha-1 (excluding="" and="" bit="" bits)="" hash="" length,="" numbe="" of="" string="" subjectpublickey="" tag,="" the="" unused="" value="">) Set (<1.3.6.1.4.1.4491.2021.1.5>) Not Set</sha-1>					
digitalSignature keyEncipherment extendedKeyUsage svcCMTS clientAuth serverAuth authorityKeyIdentifier keyIdentifier certificatePolicies certPolicyId policyQualifiers authorityInfoAccess ocsp caIssuers crIDistributionPoints	{id-ce 37} {id-ce 37} {id-ce 35} {id-ce 32} {id-pe 1} {id-ad 1}	YES YES YES	FALSE FALSE	Set (id-cl-pki-ext-eku-CMTS) Set (id-kp-clientAuth) Set (id-kp-serverAuth) Set (<sha-1 (excluding="" and="" bit="" bits)="" hash="" length,="" number="" of="" string="" subjectpublickey="" tag,="" the="" unused="" value="">) Set (<1.3.6.1.4.1.4491.2021.1.5>) Not Set Set (<http authoritative="" ocsp="" of="" responder="" uri="">) Set (<http ca="" der="" format="" in="" issuing="" of="" uri="">)</http></http></sha-1>					
digitalSignature keyEncipherment extendedKeyUsage svcCMTS clientAuth serverAuth authorityKeyIdentifier keyIdentifier certificatePolicies certPolicyId policyQualifiers authorityInfoAccess ocsp calssuers crlDistributionPoints distributionPoint	{id-ce 37} {id-ce 37} {id-ce 35} {id-ce 32} {id-pe 1} {id-ad 1} {id-ad 2} {id-ce 31}	YES YES YES YES NO	FALSE FALSE FALSE FALSE	Set (1) Set (id-cl-pki-ext-eku-CMTS) Set (id-kp-clientAuth) Set (id-kp-serverAuth) Set (<sha-1 (excluding="" and="" bit="" bits)="" hash="" length,="" number="" of="" string="" subjectpublickey="" tag,="" the="" unused="" value="">) Set (<1.3.6.1.4.1.4491.2021.1.5>) Not Set Set (<http authoritative="" ocsp="" of="" responder="" uri="">)</http></sha-1>					
digitalSignature keyEncipherment extendedKeyUsage svcCMTS clientAuth serverAuth authorityKeyIdentifier keyIdentifier certificatePolicies certPolicyId policyQualifiers authorityInfoAccess ocsp caIssuers crIDistributionPoints	{id-ce 37} {id-ce 37} {id-ce 35} {id-ce 32} {id-pe 1} {id-ad 1} {id-ad 2}	YES YES YES YES	FALSE FALSE FALSE	Set (id-cl-pki-ext-eku-CMTS) Set (id-kp-clientAuth) Set (id-kp-serverAuth) Set (<sha-1 (excluding="" and="" bit="" bits)="" hash="" length,="" number="" of="" string="" subjectpublickey="" tag,="" the="" unused="" value="">) Set (<1.3.6.1.4.1.4491.2021.1.5>) Not Set Set (<http authoritative="" ocsp="" of="" responder="" uri="">) Set (<http ca="" der="" format="" in="" issuing="" of="" uri="">)</http></http></sha-1>					

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

Version	Requestor Information	•							
Contact E-mail: Certificate Format (To Be Completed by Manufacturer): Subject DN Completed Dy Manufacturing Location Coptional	Company Name:								
Certificate Format (To Be Completed by Manufacturer): Subject DN C= O= O= O= O= O= O= O= O= O=	Contact Name:				Phone:				
Subject DN c= o= o= o= o= o= o= o=	Contact E-mail:								
Subject DN C= on=		.							
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 o=CableLabs ou=Device CA05 cn=CableLabs ou=Device Crtification Authority Not Before slssuing Date> Not After slssuing Date> (slssuing Date> Not After slssuing Date> + 25 years Public Key Algorithm Sha256WithRSAEncryption (1 2 840 113549 1 11) Key size 2048-bits Parameters NULL Standard Extensions OID Required Critical ReyUsage fid-ce 15} VES TRUE digitalSignature keyEusighement extendedKeyUsage svcCAP svcCMTS clientAuth serverAuth surhorityKeyIdentifier keyIdentifier KeyIdentifier KeyIdentifier KeyIdentifier keyIdentifier FALSE certPolicyId policyQualifiers subjectAltName dNSName Set (FQDN) FALSE Set (FQDN)</device></manufacturing>		Be Compl		facturer):					
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 slssuing Date> v3 (12 840 113549 1 1) Signature Algorithm Sha256WithRSAEncryption (12 840 113549 1 11) Signature Algorithm Sha256WithRSAEncryption (12 840 113549 1 11) Signature Algorithm Key size 2048-bits Parameters NULL Standard Extensions (id-ee 15) YES TRUE digitalSignature keyUsage (id-ee 15) YES TRUE digitalSignature keyEncipherment Set (1) extendedKeyUsage (id-ee 37) svcCAP sv</device></manufacturing>	Subject DN								
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 Vissuing Date> Not After Vissuing Date> + 25 years Public Key Algorithm Sha (1 2 840 113549 1 1 1) Signature Algorithm Key size 2048-bits Parameters NULL Standard Extensions OID Required Critical digitalSignature keyUsage did-ce 15} VES TRUE digitalSignature extendedKeyUsage svcCAP svcCCAP svcCCAP svcCMTS clientAuth serverAuth authorityKeyIdentifier keyIdentifier keyIdentifier keyIdentifier Set (id-kp-serverAuth) authorityKeyIdentifier keyIdentifier subjectPublicKey (excluding the tag, length, and numbe of certificatePolicies certPolicyId policyQualifiers subjectAlName did-ce 17} NO FALSE divide Control set (GODN)</device>			•	uring Location	o (ontional)				
SubjectAltName (optional) InsName(s)=									
Other Certificate Contents (For CableLabs and CA use only):	gubiact Alt Nama (antior	va1)		ienunei>					
Version	subject Amname (opnor	iai)	ulisivallie(s)–						
Version	Other Certificate Cont	ents (For (ableLabs and	(CA use only)	•				
Serial number Unique Positive Integer assigned by the CA		ents (1 or v		cri use omy)	•				
C=US			_ ` /	e Integer assigne	ed by the CA				
Not Before Classing Date			•						
Cn=CableLabs Device Certification Authority									
Not After <issuing date=""> 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) Set (1) keyEncipherment Set (1) Set (1) extendedKeyUsage {id-ce 37} YES FALSE svcCCAP Set (id-cl-pki-ext-eku-CCAP) svcCMTS Set (id-cl-pki-ext-eku-CCAP) scilientAuth 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>) Not Set policyQualifiers Not Set</issuing>			ou=Device CA	05					
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 Image: TRUE TRUE Image: TRUE			cn=CableLabs	Device Certifica	tion Authority				
RSA (1 2 840 113549 1 1)	Not Before		<issuing date=""></issuing>						
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) Set (1) keyEncipherment Set (id-ce 37) YES extendedKeyUsage Set (id-ce 37) Set (id-cl-pki-ext-eku-CCAP) svcCCAP Set (id-cl-pki-ext-eku-CMTS) clientAuth Set (id-kp-clientAuth) serverAuth Set (id-kp-clientAuth) serverAuth Set (id-kp-serverAuth) authorityKeyIdentifier Set (SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and numbe of unused bits)>) certificatePolicies {id-ce 32} YES FALSE certifloicyId Set (<1.3.6.1.4.1.4491.2021.1.5>) policyQualifiers Not Set subjectAltName {id-ce 17} NO dNSName Set (FQDN)	11001111001			•					
Rey size 2048-bits NULL	· U								
Parameters				AEncryption (1	2 840 113549 1 1 11)				
Standard Extensions OID Required Critical Value									
keyUsage{id-ce 15}YESTRUEdigitalSignatureSet (1)keyEnciphermentSet (1)extendedKeyUsage{id-ce 37}YESsvcCCAPSet (id-cl-pki-ext-eku-CCAP)svcCMTSSet (id-cl-pki-ext-eku-CMTS)clientAuthSet (id-kp-clientAuth)serverAuthSet (id-kp-serverAuth)authorityKeyIdentifierFALSEkeyIdentifierSet (<sha-1 (excluding="" and="" bit="" bits)="" hash="" length,="" numbe="" of="" string="" subjectpublickey="" tag,="" the="" unused="" value="">)certificatePolicies{id-ce 32}YEScertPolicyIdSet (<1.3.6.1.4.1.4491.2021.1.5>)policyQualifiersNot SetsubjectAltName{id-ce 17}NOdNSNameSet (FQDN)</sha-1>		_							
digitalSignature keyEncipherment sextendedKeyUsage svcCCAP svcCMTS clientAuth serverAuth authorityKeyIdentifier keyIdentifier keyIdentifier certificatePolicies certPolicyId policyQualifiers subjectAltName dNSName Set (1) Set (2) Set (3) Set (4) Set (5)					Value				
keyEncipherment 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} keyIdentifier Set (<sha-1 (excluding="" and="" bit="" bits)="" hash="" length,="" number="" of="" string="" subjectpublickey="" tag,="" the="" unused="" value="">) certificatePolicies {id-ce 32} certPolicyId Set (<1.3.6.1.4.1.4491.2021.1.5>) policyQualifiers Not Set subjectAltName {id-ce 17} NO dNSName Set (FQDN)</sha-1>	• •	{id-ce 15}	YES	TRUE	G . (1)				
extendedKeyUsage svcCCAP svcCCAP svcCMTS clientAuth serverAuth authorityKeyIdentifier keyIdentifier certificatePolicies certPolicyId policyQualifiers svcCAP Set (id-cl-pki-ext-eku-CCAP) Set (id-cl-pki-ext-eku-CMTS) Set (id-kp-clientAuth) Set (id-kp-serverAuth) Set (id-kp-serverAuth) Set (id-kp-serverAuth) Set (SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits)>) FALSE Set (<1.3.6.1.4.1.4491.2021.1.5>) Not Set SubjectAltName {id-ce 17} NO FALSE Set (FQDN)									
svcCCAP svcCMTS clientAuth serverAuth authorityKeyIdentifier keyIdentifier certificatePolicies certPolicyId policyQualifiers subjectAltName dNSName Set (id-cl-pki-ext-eku-CCAP) Set (id-cl-pki-ext-eku-CMTS) Set (id-kp-clientAuth) Set (id-kp-serverAuth) Set (id-kp-serverAuth) FALSE Set (<sha-1 (excluding="" and="" bit="" bits)="" hash="" length,="" number="" of="" string="" subjectpublickey="" tag,="" the="" unused="" value="">) Set (<1.3.6.1.4.1.4491.2021.1.5>) Not Set Set (<1.3.6.1.4.1.4491.2021.1.5>) Set (<1.3.6.1.4.1.4491.2021.1.5>) Set (FQDN)</sha-1>		C.1 27)	VEC	EALCE	Set (1)				
svcCMTS clientAuth serverAuth serverAuth set (id-cl-pki-ext-eku-CMTS) Set (id-kp-clientAuth) Set (id-kp-serverAuth) Set (id-kp-clientAuth) Set (id-k	· U	{1d-ce 3/}	YES	FALSE	Cat (id al relai ant alon CCAD)				
clientAuth serverAuth authorityKeyIdentifier {id-ce 35} YES keyIdentifier keyIdentifier certificatePolicies {id-ce 32} YES certPolicyId policyQualifiers dNSName Set (id-kp-clientAuth) Set (id-kp-serverAuth) Set (id-kp-serverAuth) Set (id-kp-serverAuth) Set (id-kp-clientAuth) Set (id-kp-serverAuth) Set (SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits)>) Not Set (<1.3.6.1.4.1.4491.2021.1.5>) Set (FQDN)									
serverAuth authorityKeyIdentifier {id-ce 35} YES keyIdentifier keyIdentifier Set (<sha-1 (excluding="" and="" bit="" bits)="" hash="" length,="" number="" of="" string="" subjectpublickey="" tag,="" the="" unused="" value="">) certificatePolicies {id-ce 32} YES certPolicyId policyQualifiers policyQualifiers subjectAltName {id-ce 17} NO FALSE dNSName Set (<1.3.6.1.4.1.4491.2021.1.5>) Not Set Set (FQDN)</sha-1>					` 1				
authorityKeyIdentifier {id-ce 35} YES FALSE keyIdentifier Set (<sha-1 (excluding="" and="" bit="" bits)="" hash="" length,="" number="" of="" string="" subjectpublickey="" tag,="" the="" unused="" value="">) 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 dNSName Set (FQDN)</sha-1>					1				
keyIdentifier Set (<sha-1 (excluding="" and="" bit="" bits)="" hash="" length,="" number="" of="" string="" subjectpublickey="" tag,="" the="" unused="" value="">) 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)</sha-1>		(id-ce 35)	VES	FALSE	Set (Id-kp-set vet Autil)				
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)		\langle \langl	IES	FALSE	Set (<sha-1 bit="" hash="" of="" string<="" td="" the="" value=""></sha-1>				
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 dNSName Set (FQDN)	Regidentifier								
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 dNSName Set (FQDN)									
certPolicyId Set (<1.3.6.1.4.1.4491.2021.1.5>) policyQualifiers Not Set subjectAltName {id-ce 17} NO dNSName Set (FQDN)	certificatePolicies	{id-ce 32}	YES	FALSE	, ,				
subjectAltName {id-ce 17} NO FALSE dNSName Set (FQDN)	certPolicyId								
dNSName Set (FQDN)	policyQualifiers				Not Set				
	subjectAltName	{id-ce 17}	NO	FALSE					
[*] The expiration shall not exceed the issuing CA's one	dNSName				Set (FQDN)				
	[*] The expiration shall not	exceed the iss	suing CA's one						
	Samatana.				Deter				

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=
	0=
	ou= <manufacturing location=""> (optional)</manufacturing>
	cn= <device identifier=""></device>
subjectAltName (optional)	dnsName(s)=

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

Other Certificate Conte	ents (For C	CableLabs and Ca	A 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 Dev	vice Certifica	tion Authority			
Not Before		<issuing date=""></issuing>					
Not After		<issuing date=""> + 2</issuing>	25 years				
Public Key Algorithm		RSA (1 2 840 113:	549 1 1)				
Signature Algorithm		Sha256WithRSAE	Encryption (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 bit="" hash="" of="" string<="" td="" the="" value=""></sha-1>			
				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 crl="" der="" for="" format="" in="" relevant="" uri="">)</http>					
authorityInfoAccess	{id-pe 1}	NO FALSE					
ocsp	{id-ad 1}			Set (<http authoritative="" ocsp="" of="" responder="" the="" uri="">)</http>			
caIssuers {id-ad 2}				Set (<http ca="" certificate="" der<="" in="" issuing="" of="" td="" the="" uri=""></http>			
				format>)			
subjectAltName	NO	FALSE					
dNSName				Set (FQDN)			

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

By signing this document, y	you hereby author	orize CableLabs to	set your	Device (Certificates	extensions	as noted above.
Signature:					Date:		