CableLabs PKI

Trust Infrastructure Document
(Certificate Templates)

C-PKI-TI-V1.2

3/14/2022

DISCLAIMER

This document is furnished on an "AS IS" basis and neither CableLabs nor its members provide any representation or warranty, express or implied, regarding the accuracy, completeness, noninfringement, or fitness for a particular purpose of this document, or any document referenced herein. Any use or reliance on the information or opinion in this document is at the risk of the user, and CableLabs and its members must not be liable for any damage or injury incurred by any person arising out of the completeness, accuracy, or utility of any information or opinion contained in this document.

CableLabs reserves the right to revise this document for any reason including, but not limited to, changes in laws, regulations, or standards promulgated by various entities, technology advances, or changes in equipment design, manufacturing techniques, or operating procedures described, or referred to, herein.

Contents

Figures

Tables

1 SCOPE

1.1 Introduction and Purpose

This specification is part of the DOCSIS® family of specifications developed by Cable Television Laboratories (CableLabs). In particular, this specification is part of a series of specifications that define the trust infrastructure and its configuration to provide secure authentication credentials for the broadband industry all around the world (e.g., North and South America, Europe, Asia, and Africa).

1.2 Background

Trust Infrastructure (TI) related specifications are listed in Table 1.

Table 1 – Trust Infrastructure (TI) Related Specifications

Designation	Title
CM-SP-SECv3.1	DOCSIS 3.1 Security Specification
CM-SP-SECv4.0	DOCSIS 4.0 Security Specification
CM-SP-R-PHY	Remote PHY Specification
DPoE-SP-SECv2.0	DPoE Specification
CM-SP-FMA-SYS	Flexible MAC Architecture Specification

1.3 Requirements

Throughout this document, the words that are used to define the significance of particular requirements are capitalized. These words are:

"MUST"	This word means that the item is an absolute requirement of this specification.
"MUST NOT"	This phrase means that the item is an absolute prohibition of this specification.
"SHOULD"	This word means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood, and the case carefully weighed before choosing a different course.
“SHALL”	This word has the same meaning as “SHOULD” and can be used equivalently throughout this document.
"SHOULD NOT"	This phrase means that there may exist valid reasons in particular circumstances when the listed behavior is acceptable or even useful, but the full implications should be understood, and the case carefully weighed before implementing any behavior described with this label.
“SHALL NOT”	This phrase has the same meaning as “SHOULD NOT” and can be used equivalently throughout this document.
"MAY"	This word or the adjective "OPTIONAL" means that this item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because it enhances the product, for example; another vendor may omit the same item.

This document defines many features and parameters, and a valid range for each parameter is usually specified. Equipment (CM and CMTS) requirements are always explicitly stated. Equipment is to comply with all mandatory (MUST and MUST NOT) requirements to be considered compliant with this specification. Support of non-mandatory features and parameter values is optional.

1.4 Conventions

In this specification, the following convention applies any time a bit field is displayed in a figure. The bit field should be interpreted by reading the figure from left to right, then from top to bottom, with the MSB being the first bit so read and the LSB being the last bit so read.

```
MIB syntax and XML Schema syntax is represented by this code sample font.
```

Notices and/or Warnings are identified by this style font and label.

2 REFERENCES

2.1 Normative References

In order to claim compliance with this specification, it is necessary to conform to the following standards and other works as indicated, in addition to the other requirements of this specification. Intellectual property rights may be required to implement these references.

[DOCSIS SECv4.0]	DOCSIS 3.1 Security Specification, CM-SP-SECv4.0-I02-201202, Dec 2, 2020, Cable Television Laboratories, Inc.
[DOCSIS SECv3.1]	DOCSIS 3.1 Security Specification, CM-SP-SECv3.1-I09-200407, Apr 7, 2020, Cable Television Laboratories, Inc.
[DPoE SECv2.0]	DOCSIS Provisioning of EPON Specifications. DPoE Security and Certificate Specification. DPoE-SP-SECv2.0-I06-180228. February 28, 2018, Cable Television Laboratories, Inc.
[FIPS 140-2]	Federal Information Processing Standards Publication (FIPS PUB) 140-2, Security Requirements for Cryptographic Modules, June 2001.
[FIPS 180-4]	Federal Information Processing Standards Publication (FIPS PUB) 180-2, Secure Hash Standard, May 2014.
[PKCS#7]	RSA Laboratories, PKCS #7: Cryptographic Message Syntax Standard, An RSA Laboratories Technical Note, Version 1.5, Revised November 1, 1993.
[RFC 5280]	IETF RFC 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk, May 2008.
[RFC 6960]	IETF RFC 6960, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, S. Santesson, M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams, June 2013.
[X.509]	ITU-T Recommendation X.509 (10/12): Information Technology - Open Systems Interconnection - The Directory: Public key and attribute certificate frameworks.
[X.690]	ITU-T Recommendation X.690 (11/08) | ISO/IEC 8825-1:2002, Information Technology - ASN.1 Encoding Rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).

2.2 Informative References

This specification uses the following informative references.

[ISO 3166]	ISO 3166-1, Codes for the representation of names of countries and their subdivisions -- Part 1: Country codes.
[NIST SP800-63B]	NIST Special Publication 800-63B, Digital Identity Guidelines Authentication and Lifecycle Management, National Institute of Standards and Technology, June 2017.
[NIST SP800-90A]	NIST Special Publication 800-90A, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Revision 1, National Institute of Standards and Technology, June 2015.
[RSA2]	RSA Laboratories, Some Examples of the PKCS Standards, RSA Data Security, Inc., Bedford, MA, November 1, 1993.

2.3 Reference Acquisition

- Cable Television Laboratories, Inc., 858 Coal Creek Circle, Louisville, CO 80027; Phone +1-303-661-9100; Fax +1-303-661-9199. http://www.cablemodem.com.
- Federal Information Processing Standards: 100 Bureau Drive, Mail Stop 3200, Gaithersburg, MD 20899-3200. Phone +1-301-975-4054; Fax +1-301-926-8091. http://csrc.nist.gov/publications/fips/.
- IETF Secretariat, c/o Corporation for National Research Initiatives, 1895 Preston White Drive, Suite 100, Reston, VA 20191-5434 Phone +1-703-620-8990; Fax +1-703-620-9071. http://www.ietf.org.

- ITU Recommendations: Place des Nations, CH-1211, Geneva 20, Switzerland. Phone +41-22-730-51-11; Fax +41-22-733-7256. http://www.itu.int.
- Public Key Cryptography Standards: RSA Security Inc. 174 Middlesex Turnpike, Bedford, MA 01730. Phone +1-781-515-5000; Fax 781-515-5010. http://www.rsasecurity.com/rsalabs/.
- SCTE, Society of Cable Telecommunications Engineers, 140 Philips Road, Exton, PA 19341-1318, Phone +1-800-542-5040; Fax+1-610-363-5898, http://www.scte.org/default.aspx/.

3 TERMS AND DEFINITIONS

This specification uses the following terms.

DER Encoded	A value which is encoded using the ASN.1 Distinguished Encoding Rules [X.690].
Hardware	Includes software and CPU and instructions and data that are permanently embedded in such device or component in a form that cannot be modified or updated using *widely available tools* and can only be modified or updated using *professional tools* with *difficulty*.
Software	An implementation that includes but is not limited to DOCSIS 4.0 functions through a CPU executing computer program code consisting of instructions or data, other than such instructions or data that are included in *hardware*, where such instructions or data can be modified by download or by any manner of update. *Hardware* is a physical device, including a component that implements any part of the DOCSIS 4.0 requirements.
Trust Anchor	An authoritative entity for which trust is assumed and not derived. In DOCSIS 4.0, the root certificate acts as the trust anchor from which the chain of trust is derived.

4 ABBREVIATIONS AND ACRONYMS

This specification uses the following abbreviations and acronyms.

AES	Advanced Encryption Standard
ASN.1	Abstract Syntax Notation 1
CA	Certificate Authority
CCAP	Converged Cable Access Platform
CM	Cable Modem
CMS	Cryptographic Message Structure
CMTS	Cable Modem Termination System
CRL	Certificate Revocation List
CVC	Code Verification Certificate
CVS	Code Verification Signature
DER	Distinguished Encoding Rules
DPoE	DOCSIS® Provisioning of EPON
DOCSIS	Data-Over-Cable Service Interface Specifications
EAE	Early Authentication and Encryption
ECDSA	Elliptic Curve Digital Signature Algorithm
FIPS	Federal Information Processing Standards
FQDN	Fully Qualified Domain Name
HFC	Hybrid Fiber/Coax
IP	Internet Protocol
IPR	Intellectual Property Rights
IPv4	Version 4 of the Internet Protocol
IPv6	Version 6 of the Internet Protocol
ISO	International Organization for Standards
ITU-T	Telecommunication Standardization Sector of the International Telecommunications Union
LAN	Local Area Network
MAC	Media Access Control
MSO	Multiple Systems Operator
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
RFC	Request For Comments
RSA	Rivest, Shamir, Adleman (a public key cryptographic algorithm)
SHA-1	Secure Hash Algorithm 1
SSD	Secure Software Download

SSH	Secure Shell
TLS	Transport Layer Security
TLV	Type/Length/Value
UTC	Coordinated Universal Time

5 OVERVIEW

5.1 The Broadband Trust Infrastructure

This section describes the certificate format and extensions used by CableLabs certification authorities (CA) and summarizes the fields of [X.509] version 3 certificates. The CableLabs certificate PKI hierarchy is shown in Figure 1.

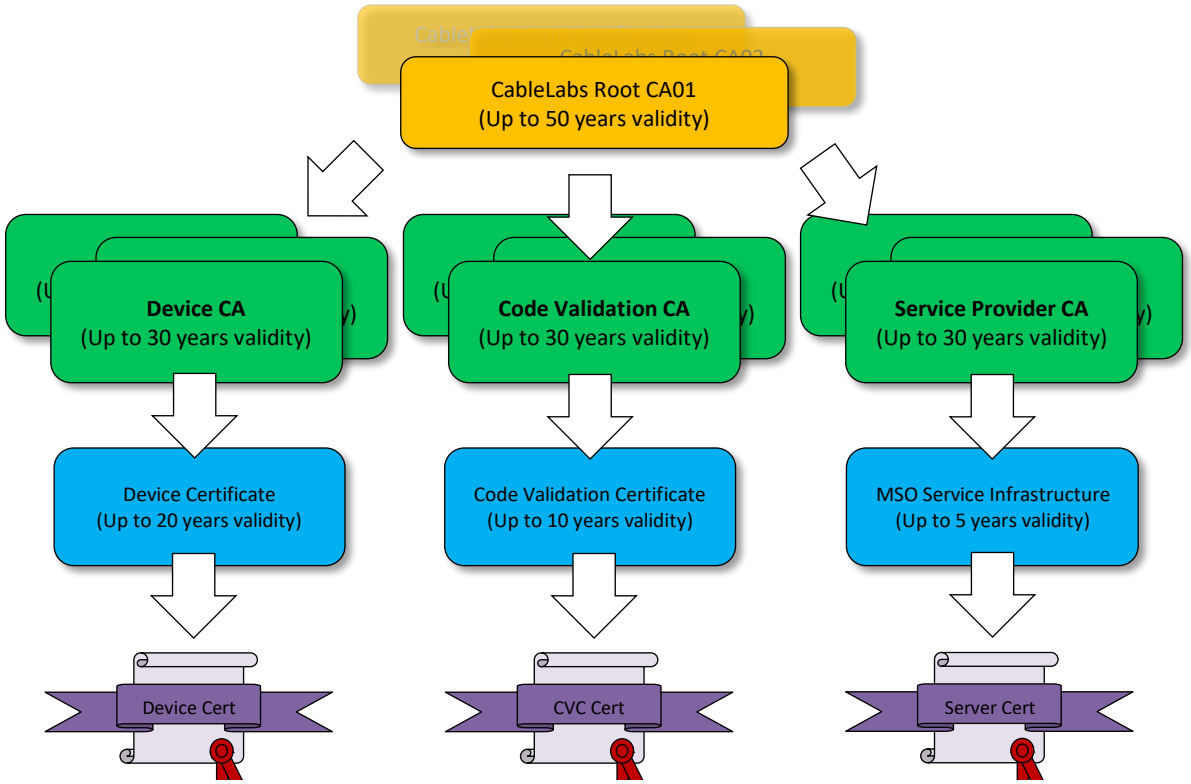

Figure 1 - DOCSIS PKI Hierarchy (D3.1+)

All certificates and CRLs described in this specification are signed with the RSA signature algorithm, using SHA-2 as the hash function (i.e., SHA-256, SHA-384, or SHA-512). The RSA signature algorithm is described in PKCS #1 **Error! Reference source not found.**; SHA-256 is described in [FIPS 180-4].

5.2 Names Encoding

Names in [X.509] are SEQUENCEs of `RelativeDistinguishedNames`, which are in turn SETs of `AttributeTypeAndValue`. `AttributeTypeAndValue` is a SEQUENCE of an `AttributeType` (an OBJECT IDENTIFIER) and an `AttributeValue`. The value of the `countryName` attribute is a 2-character `PrintableString`, chosen from [ISO 3166]; all other `AttributeValues` are encoded as either `UTF8String` or `PrintableString` character strings. The `PrintableString` encoding is used if the character string contains only characters from the `PrintableString` set, specifically:

abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ
0123456789
'()+,-./:=? and space.

The `UTF8String` type is used if the character string contains characters not in the `PrintableString` set.

The DER-encoded `tbsCertificate.issuer` field of a valid DOCSIS certificate is an exact binary match to the DER-encoded `tbsCertificate.subject` field of its issuer certificate.

5.3 CableLabs OID Arc Management

The CableLabs OID (1.3.6.1.4.1.4491) is the base OID for the definition of identifiers used in CableLabs protocols. The CableLabs OID arc is organized as follows:

```
CableLabs OID ::= { 1.3.6.1.4.1.4491}
  |
  +-> id-cl-docsis-pki ::= {cl-id 2021}
      |
      +-> id-cl-docsis-pki-cp ::= {id-cl-docsis-pki 1}
      |
      +-> id-cl-docsis-pki-ext ::= {id-cl-docsis-pki 2}
          |
          +-> id-cl-docsis-pki-ext-eku ::= {id-cl-docsis-pki-ext 1}
```

Where values under the `id-cl-docsis-pki-ext` arc identify available functionality (e.g., CM or ONU). In order to request changes in the CableLabs OID arc, please contact the Policy Authority and follow the associated procedures.

5.3.1 Service OIDs for Extended Key Usage Values

The DOCSIS PKI defines several different values under the CableLabs' DOCSIS PKI extensions arc `id-cl-docsis-pki-ext-eku (1.3.6.1.4.1.4491.2021.2.1)`. Specifically, Table 2 provides the details of the different values and associated usage.

Table 2 - Object Identifiers for EKU enabled functionalities

Short Name	Name	Value	Description
svcCMTS	id-cl-pki-eku-CMTS	{id-cl-docsis-pki-ext-eku 1}	CMTS functionalities
svcCM	id-cl-pki-eku-CM	{id-cl-docsis-pki-ext-eku 2}	CM functionalities
svcRPD	id-cl-pki-eku-RPD	{id-cl-docsis-pki-ext-eku 3}	RPD functionalities
svcONU	id-cl-pki-eku-ONU	{id-cl-docsis-pki-ext-eku 4}	ONU functionalities
svcOLT	id-cl-pki-eku-OLT	{id-cl-docsis-pki-ext-eku 5}	OLT functionalities
svcMACNE	id-cl-pki-eku-MACNE	{id-cl-docsis-pki-ext-eku 6}	MACNE functionalities
svcMGMT	id-cl-pki-eku-MGMT	{id-cl-docsis-pki-ext-eku 7}	Management functionalities
svcCCAP	id-cl-pki-eku-CCAP	{id-cl-docsis-pki-ext-eku 8}	CCAP functionalities

5.3.1.1 Service OIDs Examples

The values in the table are all relative to the `id-cl-pki-ext-eku` base OID. For example, the `id-cl-pki-eku-CMTS` and `id-cl-pki-eku-CM` that are used in CMTS and CM certificates respectively have the following dotted representation:

```
id-cl-pki-eku-CMTS ::= { id-cl-pki-ext-eku 1 }
   --- Value: 1.3.6.1.4.1.4491.2021.2.1.1

id-cl-pki-eku-CM ::= { id-cl-pki-ext-eku 2 }

   --- Value: 1.3.6.1.4.1.4491.2021.2.1.2
```

Refer to the Policy Authority for how to submit changes to this table.

6 CERTIFICATE VALIDATION

Relying parties that want to validate certificates issued under the 2nd Gen DOCSIS® PKI, unless specified differently in the relevant protocol specifications, must follow standard procedures described in RFC5280.

Specifically, relying parties must be able to correctly build the path to the trusted Root CA, via the path building process, and then perform the identified procedures for path validation process.

In case of errors during the path building or path validation processes, the relying party must reject the presented certificate and certificate chain unless otherwise specified in the relevant protocol specifications.

6.1 Name Validation

Relying parties that want to validate names contained in certificates issued under the 2nd Gen DOCSIS® PKI, unless specified differently in the relevant protocol specifications, must follow standard procedures described in RFC5280.

Specifically, unless specifically instructed to do so by the relevant specifications and protocols, relying party must not apply additional checks on data types or order of relative distinguished names components.

6.2 Processing Certificates Extensions

The use of extensions in certificates is aimed at maintaining the infrastructure updated and to allow relying parties to leverage enhanced services from the participating Certification Authorities and Partners.

When validating certificates and certificate chains, relying party must ignore extensions that are present in the certificate(s) and are not used in the protocol or not supported by the device unless they are marked as critical.

6.2.1 Optional Certificate Extensions

The profiles described in this document may contain extensions that are marked optional (i.e., Required = No). The optionality of these extension depends on the certificate provider's capability to either embed the extension in certificates or provide the associated service.

The Policy Authority works with the participating providers to enable or disable the use of these optional extensions to make sure that their deployment is well supported and coordinated across the entire DOCSIS Ecosystem.

For example, for providers that are not capable of setting the proper value for the `cRLDistributionPoints` in issued certificates, the Policy Authority will configure the profiles to not include the extension (since it is an optional one). For providers that do not incur into these limitations (and provide support the associated service, if required), the Policy Authority works with them to enable the use of the optional extensions as necessary.

7 TRUST STORE STORAGE REQUIREMENTS

The DOCSIS® PKI is already in its second generation where the cryptographic parameters like key sizes and hashing algorithms have been updated to align with current best practices.

Devices and Applications that participate in the DOCSIS® Ecosystem should provide enough secure storage space (or provide a secure extensible storage space) to accommodate for the size of current cryptographic parameters and plan for the next generation cryptography ones. For example, current post-quantum certificates can have sizes of several Kb (e.g., 10-20 Kb) each, thus increasing the order of magnitude of storage space needed for trust anchors storage, especially at higher security levels (e.g., 192 or 256 bits of security).

8 TRIAL CERTIFICATE PROFILES

The DOCSIS® Ecosystem is constantly evolving with new protocols and new requests to support additional profiles for our ecosystem. To accommodate the development and test of new profiles before they can be officially added to the family of supported ones, the Policy Authority works with members of the ecosystem and the certificate providers to be able to issue short-lived (less than 90 days) certificates for test and development purposes.

These certificates must be well identified as test certificates by using the "Test Certificate" text in the subject of the certificate. In particular, test certificates must set the "Manufacturing Facility" value to "Test Certificate" (i.e., "OU=Test Certificate").

Other qualifiers for the specific protocol can be used in the OU as needed, however, at minimum, the "Test" or "Tests" text MUST always be present in the value (case insensitive). Examples of compliant OU values are: "DPoE Test Certificate", "DOCSIS 4.0 Test Certificate", "Louisville Tests", "R-PHY TEST CCAP Core Device".

Test certificates MUST NOT be installed in production environments.

9 ROOT CERTIFICATION AUTHORITIES

9.1 CableLabs RSA Root CA RSA Certificate

The DOCSIS PKI comprises one or more Root Certification Authorities. Root Certification Authorities only issue Intermediate CA certificates (no EE certificates issued from the Root) and OCSP Responder ones. The profile for Root Certificates is defined in Table 3:

Table 3 - CableLabs Root CA RSA Certificate Profile

CableLabs Root CA RSA Certificate Profile				
Version	v3 (0x02)			
Serial number	Unique Positive Integer assigned by the CA			
Issuer DN	c=US o=CableLabs ou=Root CA<ID#> cn=CableLabs Root Certification Authority			
Subject DN	c=US o=CableLabs ou=Root CA<ID#> cn=CableLabs Root Certification Authority			
Validity Period				
Not Before	<Issuing Date>			
Not After	<Issuing Date> + Up to 50 yrs			
Public Key Info				
Public Key Data	**Public Key Algorithm:** • RSA 4096 bit (1 2 840 113549 1 1)	**Parameters:** • NONE		
	Public Key Algorithm: • RSA 8092 bit (1 2 840 113549 1 1)	**Parameters:** • NONE		
Signature Algorithm(s)	**Allowed OIDs:** • Sha256WithRSAEncryption (1 2 840 113549 1 1 11), or • Sha384WithRSAEncryption (1 2 840 113549 1 1 11), or • Sha512WithRSAEncryption (1 2 840 113549 1 1 11)			
Extensions				
Standard Extensions	**OID**	**Required**	**Critical**	**Value**
keyUsage	{id-ce 15}	**Yes**	**TRUE**	
keyCertSign				Set (1)
cRLSign				Set (1)
digitalSignature				Set (1), or Not Set (0)
basicConstraints	{id-ce 19}	**Yes**	**TRUE**	
cA				Set (TRUE)
subjectKeyIdentifier	{id-ce 14}	**Yes**	FALSE	
keyIdentifier				Set (<SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits)>)
subjectAltName	{id-ce 17}	No	FALSE	**(Deprecated)**
directoryName				Set by the issuing CA

Values in angle brackets (<>) indicate that appropriate text as indicated below is present:

<ID#>: indicates the ID number of the CA and is populated with the CA certificate is issued (e.g., 01);

10 INTERMEDIATE CERTIFICATION AUTHORITIES

10.1 CableLabs Device CA RSA Certificate

The CableLabs Device Certification Authority is issued by the **Root Certification Authority** and issues certificate for DOCSIS devices.

For example, the Device CA is used to issue certificates for Cable Modems, CMTS, and Remote Phy Devices. The Device CA may also issue OCSP Responder certificates.

Note that in order to support the use of a single certificate for D4.0 devices operating in D3.1 mode, the Device CA certificate must be less than or equal to 1487 bytes in size because of the DOCSIS 3.1 BPKM message limitation that caps the maximum supported size for the Auth Info message to 1490 bytes.

The profile for the Device CA certificate is provided in Table 4:

Table 4 - CableLabs Device CA RSA Certificate Profile

CableLabs Device CA RSA Certificate Profile				
Version	v3 (0x02)			
Serial number	Unique Positive Integer assigned by the CA			
Issuer DN	c=US o=CableLabs ou=Root CA<ID#> cn=CableLabs Root Certification Authority			
Subject DN	c=US o=CableLabs ou=Device CA<ID#> cn=CableLabs Device Certification Authority			
Validity Period				
Not Before	<Issuing Date>			
Not After	<Issuing Date> + Up to 30 yrs [*]			
Public Key Info				
Public Key Data	**Public Key Algorithm:** • RSA 2048 bit (1 2 840 113549 1 1)	**Parameters:** • NONE		
	Public Key Algorithm: • RSA 3072 bit (1 2 840 113549 1 1)	**Parameters:** • NONE		
	Public Key Algorithm: • RSA 4096 bit (1 2 840 113549 1 1)	**Parameters:** • NONE		
Signature Algorithm(s)	**Allowed OIDs:** • Sha256WithRSAEncryption (1 2 840 113549 1 1 11) for RSA, or • Sha384WithRSAEncryption (1 2 840 113549 1 1 12) for RSA, or • Sha512WithRSAEncryption (1 2 840 113549 1 1 13) for RSA			
Extensions				
Standard Extensions	**OID**	**Required**	**Critical**	**Value**
keyUsage	{id-ce 15}	**Yes**	**TRUE**	
keyCertSign				Set (1)
cRLSign				Set (1)
digitalSignature				Set (1), or Not Set (0)
basicConstraints	{id-ce 19}	**Yes**	**TRUE**	
cA				Set (TRUE)

pathLenConstraint				0
subjectKeyIdentifier	{id-ce 14}	**Yes**	FALSE	
keyIdentifier				Set (<SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits)>)
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)>)
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 format>)
subjectAltName	{id-ce 17}	No	FALSE	**(Deprecated)**
directoryName				Set by the issuing CA for online CAs

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

Values in angle brackets (<>) indicate that appropriate text as indicated below is present:

<RootCA Organization Unit>: OU value copied from the issuing CA

<RootCA Name>: CN value copied from the issuing CA

<ID#>: indicates the ID number of the CA and is populated when the CA certificate is issued (e.g., 01);

10.2 CableLabs CVC CA RSA Certificate

The CableLabs CVC CA is issued by the **Root Certification Authority,** and it is used to issue certificates for Code Validation. This type of certificates is used for authenticating Software Images (e.g., for Secure Software Download).

The profile for CVC CA certificates is provided in Table 5:

Table 5 - CableLabs DOCSIS CVC CA RSA Certificate Profile

CableLabs CVC CA RSA Certificate Profile	
Version	v3 (0x02)
Serial number	Unique Positive Integer assigned by the CA
Issuer DN	c=US o=CableLabs ou=Root CA<ID#> cn=CableLabs Root Certification Authority
Subject DN	c=US o=CableLabs ou=CVC CA<ID#> cn=CableLabs CVC Certification Authority
Validity Period	
Not Before	<Issuing Date>
Not After	<Issuing Date> + Up to 30 yrs [*]

Public Key Info		
Public Key Data	**Public Key Algorithm:** • RSA 2048 bit (1 2 840 113549 1 1)	**Parameters:** • NONE
	Public Key Algorithm: • RSA 3072 bit (1 2 840 113549 1 1)	**Parameters:** • NONE
	Public Key Algorithm: • RSA 4096 bit (1 2 840 113549 1 1)	**Parameters:** • NONE
Signature Algorithm(s)	**Allowed OIDs:** • Sha256WithRSAEncryption (1 2 840 113549 1 1 11) for RSA, or • Sha384WithRSAEncryption (1 2 840 113549 1 1 12) for RSA, or • Sha512WithRSAEncryption (1 2 840 113549 1 1 13) for RSA	

Extensions				
Standard Extensions	**OID**	**Required**	**Critical**	**Value**
keyUsage	{id-ce 15}	**Yes**	**TRUE**	
keyCertSign				Set (1)
cRLSign				Set (1)
digitalSignature				Set (1), or Not Set (0)
basicConstraints	{id-ce 19}	**Yes**	**TRUE**	
cA				Set (TRUE)
pathLenConstraint				Set (0)
subjectKeyIdentifier	{id-ce 14}	**Yes**	**FALSE**	
keyIdentifier				Set (<SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits)>)
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)>)
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 format>)
subjectAltName	{id-ce 17}	No	FALSE	**(Deprecated)**
directoryName				Set by the issuing CA for online CAs

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

Values in angle brackets (<>) indicate that appropriate text as indicated below is present:

<Root CA Organization Unit>: OU value copied from the issuing CA

<Root CA Name>: CN copied from the issuing Root CA

<ID#>: indicates the ID number of the CA and is populated when the CA certificate is issued (e.g., 01)

<Country of Manufacturer>: two-letter country code

<Company Name>: name that identifies the company

10.3 CableLabs Service Provider CA RSA Certificate

Service Provider CAs are issued by issued by **Root Certification Authorities** and they are used to issue certificates for the operator's infrastructure. For example, Service Provider CAs issue certificates for operators' network services like AAA servers, etc.

The profile for Service Provider CA Certificates is provided in Table 6:

Table 6 - CableLabs Service Provider CA RSA Certificate Profile

CableLabs Service Provider CA RSA Certificate Profile				
Version	v3 (0x02)			
Serial number	Unique Positive Integer assigned by the CA			
Issuer DN	c=US o=CableLabs ou=Root CA<ID#> cn=CableLabs Root Certification Authority			
Subject DN	c=US o=CableLabs ou=Service Provider CA<ID#> cn=CableLabs Service Provider Certification Authority			
Validity Period				
Not Before	<Issuing Date>			
Not After	<Issuing Date> + Up to 30 years [*]			
Public Key Info				
Public Key Algorithm	**Public Key Algorithm:** • RSA 2048 bit (1 2 840 113549 1 1)	**Parameters:** • NONE		
	Public Key Algorithm: • RSA 3072 bit (1 2 840 113549 1 1)	**Parameters:** • NONE		
	Public Key Algorithm: • RSA 4096 bit (1 2 840 113549 1 1)	**Parameters:** • NONE		
Signature Algorithm	**Allowed OIDs:** • Sha256WithRSAEncryption (1 2 840 113549 1 1 11) for RSA, or • Sha384WithRSAEncryption (1 2 840 113549 1 1 12) for RSA, or • Sha512WithRSAEncryption (1 2 840 113549 1 1 13) for RSA			
Extensions				
Standard Extensions	**OID**	**Required**	**Critical**	**Value**
keyUsage	{id-ce 15}	**Yes**	**TRUE**	
keyCertSign				Set (1)
cRLSign				Set (1)
digitalSignature				Set (1), or Not Set (0)
basicConstraints	{id-ce 19}	**Yes**	**TRUE**	
cA				Set (TRUE)
pathLenConstraint				Set (0)
subjectKeyIdentifier	{id-ce 14}	**Yes**	FALSE	
keyIdentifier				Set (<SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits)>)
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)>)
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 format>)
subjectAltName	{id-ce 17}	No	FALSE	
directoryName				**(Deprecated)** Set by the issuing CA for online CAs

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

Values in angle brackets (<>) indicate that appropriate text as indicated below is present:

<Root CA Organization Unit>: OU value copied from the issuing CA

<Root CA Name>: CN copied from the issuing Root CA

<ID#>: indicates the ID number of the CA and is populated when the CA certificate is issued (e.g., 01)

11 REVOCATION SERVICES

The DOCSIS infrastructure supports the revocation of certificates. This section introduces the requirements around the profiles of certificates and revocation objects via OCSP and CRL.

11.1 OCSP Revocation Services

The OCSP protocol allows for querying the revocation status of individual certificates.

11.1.1 OCSP Responder Certificates

OCSP Responses MUST conform to [RFC6960] and MUST either be:

- signed by the CA that issued the Certificates whose revocation status is being checked, or
- signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate and has the whose revocation status is being checked.

OCSP certificates MUST use the `id-kp-ocspSigning` OID in the Extended Key Usage field (EKU).

OCSP responses MUST use a validity period that does not exceed <731> days.

11.1.2 OCSP Responses Version Number(s)

OCSP responses MUST support use of OCSP version 1 as defined by [RFC6960].

11.1.3 OCSP Responses Extensions

When an OCSP Responder signing certificate is used instead of the CA certificate to sign OCSP responses, the signing certificate MUST contain the extension `id-pkix-ocsp-nocheck` as defined by [RFC6960].

Other non-critical extensions might be used as needed.

11.2 Certificate Revocation Lists (CRL)

CRLs MUST conform to [RFC 5280] and MUST use a validity period that does not exceed <365> days.

11.2.1 Version Number(s)

The CAs SHALL support the issuance of X.509 Version two (2) CRLs. The CRL version number MUST be set to the integer value of "1" for Version 2 as described in Section 5.1.2.1 of [RFC 5280].

11.2.2 CRL Extensions

The CAs SHALL support the use of non-critical extensions in CRLs.

The CAs SHALL issue CRLs version 2 with the `cRLNumber` extension set to a monotonically increasing sequence number for a given CRL scope and issuer.

Other non-critical extensions might be used as needed.

12 EXTENDED INFRASTRUCTURE SERVICES

12.1 Code Verification RSA Certificates (CVC)

Code Verification Certificates (or CVCs) are issued by **CVC Certification Authorities,** and they are used to authenticate software images.

This type of certificate is used to sign Firmware images that are then loaded onto devices (e.g., Cable Modems, RPD Nodes, or ONUs) via the Secure Software Download.

The details about the Code Verification Certificate profile are provided in Table 7:

Table 7 - Code Verification RSA Certificate Profile

CVC Certificate RSA Profile				
Version	v3 (0x02)			
Serial number	Unique Positive Integer assigned by the CA			
Issuer DN	c=US o=CableLabs ou=CVC CA<ID#> cn=CableLabs CVC Certification Authority			
Subject DN	c=<Country of Manufacturer> o=<Company Name> [ou=<Environment>] cn=Code Verification Certificate			
Validity Period				
Not Before	<Issuing Date>			
Not After	<Issuing Date> + Up to 10 yrs [*]			
Public Key Info				
Public Key Data	**Public Key Algorithm:** • RSA 2048 bit (1 2 840 113549 1 1)	**Parameters:** • NONE		
	Public Key Algorithm: • RSA 3072 bit (1 2 840 113549 1 1)	**Parameters:** • NONE		
	Public Key Algorithm: • RSA 4096 bit (1 2 840 113549 1 1)	**Parameters:** • NONE		
Signature Algorithm(s)	**Allowed OIDs:** • Sha256WithRSAEncryption (1 2 840 113549 1 1 11) for RSA, or • Sha384WithRSAEncryption (1 2 840 113549 1 1 12) for RSA, or • Sha512WithRSAEncryption (1 2 840 113549 1 1 13) for RSA			
Extensions				
Standard Extensions	**OID**	**Required**	**Critical**	**Value**
extendedKeyUsage	{id-ce 37}	**Yes**	**TRUE**	
codesigning				Set (id-kp-codeSigning)
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)>)
keyUsage	{id-ce 15}	No	TRUE	
digitalSignature				Set (1), or Not Set (0)
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 format>)

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

Values in angle brackets (<>) indicate that appropriate text as indicated below is present:

<Country of Manufacturer>: two-letter country code;

<Company Name>: name that identifies the company;

<Environment>: optional field to identify a specific environment for the CVC;

Co-signer CVCs will have a unique numeric value for the <Company Name> which is assigned by CableLabs. The value is a printable string of eight hexadecimal digits. Each hexadecimal digit in the name is chosen from the ranges 0x30 to 0x39 or 0x41 to 0x46.

The string 0x3030303030303030 is not assigned.

In addition to the required subject entries for CVC certificates as detailed in the relevant specifications, device manufacturers may choose to include one additional `organizationalUnit` field that carries the ecosystem environment associated with the CVC. When the optional OU is added to the certificate, the allowed values are provided in Table 8:

Table 8 - Allowed Values for <Environment> field.

Value	Description
`DPoE`	Used for DPoE CVCs
`R-Phy`	Used for Remote Phy CVCs
`DOCSIS`	Used for DOCSIS CVCs
`FMA`	Used for MAC NE and Management CVCs

12.2 AAA Server RSA Certificates

AAA Server Certificates are issued by **Service Provider Certification Authorities** and are used to secure credential servers.

The profile for AAA Certificates is provided in Table 9:

Table 9 - CableLabs AAA Server RSA Certificate Profile

CableLabs AAA Server RSA Certificate Profile	
Version	v3 (0x02)
Serial number	Unique Positive Integer assigned by the CA
Issuer DN	c=US o=CableLabs ou=Service Provider CA<ID#> cn=CableLabs Service Provider Certification Authority

CableLabs AAA Server RSA Certificate Profile				
Subject DN	c=<Country Code> o=<Company Name> ou=Service Provider Certificate cn=<Common Name>			
Validity Period				
Not Before	<Issuing Date>			
Not After	<Issuing Date> + Up to 5 yrs [*]			
Public Key Info				
Public Key Data	**Public Key Algorithm:** • RSA 2048 bit (1 2 840 113549 1 1)	**Parameters:** • NONE		
	Public Key Algorithm: • RSA 3072 bit (1 2 840 113549 1 1)	**Parameters:** • NONE		
	Public Key Algorithm: • RSA 4096 bit (1 2 840 113549 1 1)	**Parameters:** • NONE		
Signature Algorithm(s)	**Allowed OIDs:** • Sha256WithRSAEncryption (1 2 840 113549 1 1 11) for RSA, or • Sha384WithRSAEncryption (1 2 840 113549 1 1 12) for RSA, or • Sha512WithRSAEncryption (1 2 840 113549 1 1 13) for RSA			
Extensions				
Standard Extensions	**OID**	**Required**	**Critical**	**Value**
keyUsage	**{id-ce 15}**	**Yes**	**TRUE**	
digitalSignature				Set (1)
keyEncipherment				Set (1)
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)>)
extendedKeyUsage	{id-ce 37}	No	TRUE	
serverAuth	{id-kp 1}			Set (id-kp-serverAuth), or Not Set
clientAuth	{id-kp 2}			Set (id-kp-clientAuth), or Not Set
ocspSigning	{id-kp 9}			Set (id-kp-ocspSigning), or Not Set
timeStamping	{id-kp 8}			Set (id-kp-timeStamping), or Not Set
subjectAltName	{id-ce 17}	No	FALSE	
dNSName				Set (<Server's FQDN>), or Not Set
otherName nai_on_realm	{1.3.6.1.5.5.7.8.8}			Set (<Server's Realm>), or Not Set
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>), or Not Set
caIssuers	{id-ad 2}			Set (<HTTP URI of the Issuing CA certificate in DER format>), or Not Set

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

Values in angle brackets (<>) indicate that appropriate text as indicated below is present:

<ID#>: indicates the ID number of the issuing CA (e.g., 01)

<Country Code>: two-letter country code

<Company Name>: name that identifies the company

<Common Name>: meaningful name or identifier for the service

Other non-critical extensions might be used in Service Provider certificates as requested by operators.

12.3 Service Provider RSA Certificates

Service Provider Certificates are issued by **Service Provider Certification Authorities** and are used to authenticate the MSO's DOCSIS infrastructure.

The DOCSIS credentials can be easily validated by any entity (e.g., a Cable Modem, a CCAP Core, an RPD, etc.) that is participating in the trust infrastructure.

The profile for Service Provider Certificates is provided in Table 10:

Table 10 - CableLabs Service Provider RSA Certificate Profile

CableLabs Service Provider RSA Certificate Profile				
Version	v3 (0x02)			
Serial number	Unique Positive Integer assigned by the CA			
Issuer DN	c=US o=CableLabs ou=Service Provider CA<ID#> cn=CableLabs Service Provider Certification Authority			
Subject DN	c=<Country Code> o=<Company Name> ou=Service Provider Certificate cn=<Common Name>			
Validity Period				
Not Before	<Issuing Date>			
Not After	<Issuing Date> + Up to 5 yrs [*]			
Public Key Info				
Public Key Data	**Public Key Algorithm:** • RSA 2048 bit (1 2 840 113549 1 1)	**Parameters:** • NONE		
	Public Key Algorithm: • RSA 3072 bit (1 2 840 113549 1 1)	**Parameters:** • NONE		
	Public Key Algorithm: • RSA 4096 bit (1 2 840 113549 1 1)	**Parameters:** • NONE		
Signature Algorithm	**Allowed OIDs:** • Sha256WithRSAEncryption (1 2 840 113549 1 1 11) for RSA, or • Sha384WithRSAEncryption (1 2 840 113549 1 1 12) for RSA, or • Sha512WithRSAEncryption (1 2 840 113549 1 1 13) for RSA			
Extensions				
Standard Extensions	**OID**	**Required**	**Critical**	**Value**
keyUsage	**{id-ce 15}**	**Yes**	**TRUE**	
digitalSignature				Set (1)

CableLabs Service Provider RSA Certificate Profile				
keyEncipherment				Set (1)
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)>)
extendedKeyUsage	**{id-ce 37}**	No	TRUE	
serverAuth	{id-kp 1}			Set (id-kp-serverAuth), or Not Set
clientAuth	{id-kp 2}			Set (id-kp-clientAuth), or Not Set
emailProtection	{id-kp 4}			Set (id-kp-emailProtection), or Not Set
timeStamping	{id-kp 8}			Set (id-kp-timeStamping), or Not Set
subjectAltName	{id-ce 17}	No	FALSE	
dNSName				Set (<Server's FQDN>), or Not Set
otherName nai_on_realm	{1.3.6.1.5.5.7.8.8}			Set (<Server's Realm>), or Not Set
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>), or Not Set
caIssuers	{id-ad 2}			Set (<HTTP URI of the Issuing CA certificate in DER format>), or Not Set

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

Values in angle brackets (<>) indicate that appropriate text as indicated below is present:

<ID#>: indicates the ID number of the issuing CA (e.g., 01)

<Country Code>: two-letter country code

<Company Name>: name that identifies the company

<Common Name>: meaningful name or identifier for the service

Other non-critical extensions might be used in Service Provider certificates as requested by operators.

13 PROTOCOL SPECIFIC CERTIFICATE PROFILES

13.1 DOCSIS 4.0 Certificates

This section provides the definition of the certificates issued for DOCSIS 4.0 protocol.

13.1.1 DOCSIS 4.0 CM Device Certificate

Device Certificates are issued by **Device Certification Authorities** to DOCSIS 4.0 certified Cable Modems. Note that in order to support the use of a single certificate for D4.0 devices operating in D3.1 mode, the CM Device certificate must be less than 1650 bytes in size.

The profile for DOCSIS 4.0 CM Device Certificate is provided in Table 11:

Table 11 – CableLabs DOCSIS 4.0 CM Certificate Profile

General Data				
Version	v3 (0x02)			
Serial number	Unique Positive Integer assigned by the CA			
Issuer DN	c=US o=CableLabs ou=Device CA<ID#> cn=CableLabs Device Certification Authority			
Subject DN	c=<Country of Manufacturer> o=<Company Name> ou=<Manufacturing Location> cn=<Device Identifier>			
Validity Period				
Not Before	<Issuing Date>			
Not After	<Issuing Data> + Up to 20 yrs [*]			
Public Key Info				
Public Key Data	**Public Key Algorithm:** • RSA 2048 bit (1 2 840 113549 1 1)	**Parameters:** • NONE		
	Public Key Algorithm: • RSA 3072 bit (1 2 840 113549 1 1)	**Parameters:** • NONE		
	Public Key Algorithm: • RSA 4096 bit (1 2 840 113549 1 1)	**Parameters:** • NONE		
Signature Algorithm	**Allowed OIDs:** • Sha256WithRSAEncryption (1 2 840 113549 1 1 11) for RSA, or • Sha384WithRSAEncryption (1 2 840 113549 1 1 12) for RSA, or • Sha512WithRSAEncryption (1 2 840 113549 1 1 13) for RSA			
Extensions				
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 (id-cl-pki-ext-eku-CM)
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 (<DOCSIS PKI Certificate Policy OID>)
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>), or Not Set
caIssuers	{id-ad 2}			Set (<HTTP URI of the Issuing CA certificate in DER format>), or Not Set

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

Values in angle brackets (<>) indicate that appropriate text as indicated below is present:

<ID#>: indicates the ID number of the issuing CA (e.g., 01);

<Country of Manufacturer>: two-letter country code;

<Company Name>: name that identifies the company;

<Manufacturing Location>: name that identifies the location of manufacturer;

<Device Identifier>: Device Identifier (e.g., MAC address of the CM).

CM Certificates use the device MAC Address as the <Device Identifier>. When MAC Addresses are used as <Device Identifier>, the value must be expressed as six pairs of hexadecimal digits separated by single colons (e.g., 00:60:21:A5:0A:23). Hexadecimal digits greater than 9 are expressed as uppercase letters.

Other non-critical extensions might be used in Device Certificates as needed.

13.1.2 DOCSIS 4.0 CMTS Certificate

Device Certificates are issued by **Device Certification Authorities** to DOCSIS 4.0 Cable Modem Termination Systems or CMTS.

The profile for DOCSIS 4.0 CMTS Certificates is provided in Table 12:

Table 12 - CableLabs DOCSIS 4.0 CMTS Certificate Profile

DOCSIS 4.0 CMTS Certificate Profile	
Version	v3 (0x02)
Serial number	Unique Positive Integer assigned by the CA
Issuer DN	c=US o=CableLabs ou=Device CA<ID#> cn=CableLabs Device Certification Authority
Subject DN	c=<Country of Manufacturer> o=<Company Name> ou=<Manufacturing Location> cn=<Device Identifier>
Validity Period	
Not Before	<Issuing Date>
Not After	<Issuing Date> + Up to 5 years [*]
Public Key Info	

Public Key Data	**Public Key Algorithm:** RSA 2048 bit (1 2 840 113549 1 1)	**Parameters:** • NONE
	Public Key Algorithm: • RSA 3072 bit (1 2 840 113549 1 1)	**Parameters:** • NONE
	Public Key Algorithm: • RSA 4096 bit (1 2 840 113549 1 1)	**Parameters:** • NONE
Signature Algorithm	**Allowed OIDs:** • Sha256WithRSAEncryption (1 2 840 113549 1 1 11) for RSA, or • Sha384WithRSAEncryption (1 2 840 113549 1 1 12) for RSA, or • Sha512WithRSAEncryption (1 2 840 113549 1 1 13) for RSA	

Extensions

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 (<DOCSIS PKI Certificate Policy OID>)
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>), or Not Set
caIssuers	{id-ad 2}			Set (<HTTP URI of the Issuing CA certificate in DER format>), or Not Set
subjectAltName	{id-ce 17}	No	FALSE	
dNSName				Set (<FQDN>), or Not Set

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

Values in angle brackets (<>) indicate that appropriate text as indicated below is present:

<ID#>: indicates the ID number of the issuing CA (e.g., 01);

<Country of Manufacturer>: two-letter country code;

<Company Name>: name that identifies the company;

<Manufacturing Location>: name that identifies the location of manufacture;

<Device Identifier>: Meaningful identifier for the device (e.g., FQDN or Device MAC address).

When a MAC Address is used for the <Device Identifier>, the value of the MAC Address is expressed as six pairs of hexadecimal digits separated by single colons (e.g., 00:60:21:A5:0A:23). Hexadecimal digits greater than 9 are expressed as uppercase letters.

13.2 DOCSIS 3.1 Certificates

This section provides the definition of the certificates issued for use with the DOCSIS 3.1 protocol.

13.2.1 DOCSIS 3.1 CM Device RSA Certificate

Device Certificates are issued by **Device Certification Authorities** to DOCSIS 3.1 certified Cable Modems.

The profile for DOCSIS 3.1 CM Device Certificate is provided in Table 13:

Table 13 – CableLabs DOCSIS 3.1 CM Device RSA Certificate Profile

DOCSIS 3.1 CM Device RSA Certificate Profile				
Version	v3 (0x02)			
Serial number	Unique Positive Integer assigned by the CA			
Issuer DN	c=US o=CableLabs ou=Device CA<ID#> cn=CableLabs Device Certification Authority			
Subject DN	c=<Country of Manufacturer> o=<Company Name> ou=<Manufacturing Location> cn=<MAC Address>			
Validity Period				
Not Before	<Issuing Date>			
Not After	<Issuing Date> + Up to 20 yrs [*]			
Public Key Info				
Public Key Data	**Public Key Algorithm:** • RSA 2048 bit (1 2 840 113549 1 1)	**Parameters:** • NONE		
Signature Algorithm(s)	**Allowed OIDs:** • Sha256WithRSAEncryption (1 2 840 113549 1 1 11)			
Extensions				
Standard Extensions	**OID**	**Required**	**Critical**	**Value**
keyUsage	**{id-ce 15}**	**Yes**	**TRUE**	
digitalSignature				Set (1)
keyEncipherment				Set (1)
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)>)

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

Values in angle brackets (<>) indicate that appropriate text as indicated below is present:

<ID#>: indicates the ID number of the issuing CA (e.g., 01);

<Country of Manufacturer>: two-letter country code;

<Company Name>: name that identifies the company;

<Manufacturing Location>: name that identifies the location of manufacture;

<MAC Address>: MAC address of the CM.

The MAC address in the CM Certificate will be the same as the MAC address in the BPKM Attributes field.

The MAC Address is expressed as six pairs of hexadecimal digits separated by single colons (☺, e.g., 00:60:21:A5:0A:23. Hexadecimal digits greater than 9 are expressed as uppercase letters.

Other non-critical extensions might be used in Device Certificates as needed.

13.3 Remote PHY Certificates

This section provides the definition of the certificates issued for use with CCAP, Remote PHY Devices (RPD) and servers.

13.3.1 CCAP RSA Certificate

CCAP Certificates are issued by **Device Certification Authorities** to CCAP systems to establish security associations with devices such as CMs or RPDs and other Management functions.

The profile for CCAP Certificates is provided in Table 10:

Table 14 – Remote PHY CCAP RSA Certificate Profile

Remote PHY CCAP Certificate Profile		
Version	v3 (0x02)	
Serial number	Unique Positive Integer assigned by the CA	
Issuer DN	c=US o=CableLabs ou=Device CA<ID#> cn=CableLabs Device Certification Authority	
Subject DN	c=<Country of Manufacturer> o=<Company Name> ou=<Manufacturing Location> cn=<Device Identifier>	
Validity Period		
Not Before	<Issuing Date>	
Not After	<Issuing Date> + Up to 5 years [*]	
Public Key Info		
Public Key Data	**Public Key Algorithm:** • RSA 2048 bit (1 2 840 113549 1 1)	**Parameters:** • NONE
	Public Key Algorithm: • RSA 3072 bit (1 2 840 113549 1 1)	**Parameters:** • NONE
	Public Key Algorithm: • RSA 4096 bit (1 2 840 113549 1 1)	**Parameters:** • NONE
Signature Algorithm	**Allowed OIDs:** • Sha256WithRSAEncryption (1 2 840 113549 1 1 11) for RSA, or • Sha384WithRSAEncryption (1 2 840 113549 1 1 12) for RSA, or • Sha512WithRSAEncryption (1 2 840 113549 1 1 13) for RSA	

Extensions				
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 (<DOCSIS PKI Certificate Policy OID>)
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>), or Not Set
caIssuers	{id-ad 2}			Set (<HTTP URI of the Issuing CA certificate in DER format>), or Not Set
subjectAltName	{id-ce 17}	No	FALSE	
dNSName				Set (<FQDN>), or Not Set

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

Values in angle brackets (<>) indicate that appropriate text as indicated below is present:

<ID#>: indicates the ID number of the issuing CA (e.g., 01);

<Country of Manufacturer>: two-letter country code;

<Company Name>: name that identifies the company;

<Manufacturing Location>: name that identifies the location of manufacture;

<Device Identifier>: Meaningful identifier for the device (e.g., FQDN, Device MAC address, Unique CCAP ID, or UUID).

When a MAC Address is used for the <Device Identifier>, the value of the MAC Address is expressed as six pairs of hexadecimal digits separated by single colons (e.g., 00:60:21:A5:0A:23). Hexadecimal digits greater than 9 are expressed as uppercase letters.

13.3.2 Remote PHY Device RSA Certificates

RPD Certificates are issued by **Device Certification Authorities** to RPD devices for secure connectivity to management and backhaul to hubs or headend equipment.

The profile for RPD Device Certificate is provided in Table 15:

Table 15 – Remote Phy Device RSA Certificate Profile

R-PHY Device RSA Certificate Profile	
Version	v3 (0x02)
Serial number	Unique Positive Integer assigned by the CA
Issuer DN	c=US o=CableLabs ou=Device CA<ID#> cn=CableLabs Device Certification Authority
Subject DN	c=<Country of Manufacturer> o=<Company Name> ou=<Manufacturing Location> cn=<MAC Address>
Validity Period	
Not Before	<Issuing Date>

Not After	<Issuing Date> + Up to 20 yrs [*]	
Public Key Info		
Public Key Data	**Public Key Algorithm:** • RSA 2048 bit (1 2 840 113549 1 1)	**Parameters:** • NONE
Signature Algorithm(s)	**Allowed OIDs:** • Sha256WithRSAEncryption (1 2 840 113549 1 1 11)	

Extensions				
Standard Extensions	**OID**	**Required**	**Critical**	**Value**
keyUsage	{id-ce 15}	**Yes**	**TRUE**	
digitalSignature				Set (1)
keyEncipherment				Set (1)
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)>)

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

Values in angle brackets (<>) indicate that appropriate text as indicated below is present:

<Country of Manufacturer>: two-letter country code;

<Company Name>: name that identifies the company;

<MAC Address>: MAC address of the RPD.

The MAC Address is expressed as six pairs of hexadecimal digits separated by single colons (:), e.g., `00:60:21:A5:0A:23`. Hexadecimal digits greater than 9 are expressed as uppercase letters.

13.4 DPoE Certificates

The DPoE Network uses device identity and authentication procedures functionally equivalent to DOCSIS. In DPoE, the Optical Line Termination (OLT) terminates the DOCSIS protocol on the server side, while the Optical Network Unit (ONU) assume the role of the cable modem.

13.4.1 Optical Network Unit Device Certificates (ONU)

DPoE ONU Certificates are issued by **Device Certification Authorities** to DPoE ONU compliant devices (e.g., S-ONU, B-ONU, and D-ONU).

The contents of the DPoE ONU Device certificates are shown in Table 15.

Table 16 – DPoE ONU Device Certificate Profile

DPoE ONU Device Certificate Profile				
Version	v3 (0x02)			
Serial number	Unique Positive Integer assigned by the CA			
Issuer DN	c=US o=CableLabs ou=Device CA<ID#> cn=CableLabs Device Certification Authority			
Subject DN	c=<Country of Manufacturer> o=<Company Name> ou=<Manufacturing Location> cn=<MAC Address>			
Validity Period				
Not Before	<Issuing Date>			
Not After	<Issuing Date> + Up to 20 yrs [*]			
Public Key Info				
Public Key Data	**Public Key Algorithm:** • RSA 2048 bit (1 2 840 113549 1 1)	**Parameters:** • NONE		
Signature Algorithm(s)	**Allowed OIDs:** • Sha256WithRSAEncryption (1 2 840 113549 1 1 11)			
Extensions				
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 (id-cl-pki-ext-eku-ONU)
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 (<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 format>) or Not Set.
crlDistributionPoints	{id-ce 31}	No	FALSE	
distributionPoint				Set (<HTTP URI for Relevant CRL in DER format>)

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

Values in angle brackets (<>) indicate that appropriate text as indicated below is present:

<Country of Manufacturer>: two-letter country code;

<Company Name>: name that identifies the company;

<MAC Address>: MAC address of the RPD.

The MAC Address is expressed as six pairs of hexadecimal digits separated by single colons (:), e.g., `00:60:21:A5:0A:23`. Hexadecimal digits greater than 9 are expressed as uppercase letters.

13.5 Flexible MAC Architecture Certificates

This section provides the definition of the certificates issued for systems and devices of the Flexible MAC Architecture (FMA). This includes MSO Backoffice, Management functionalities, and MAC Network Elements (MAC NEs). FMA allows use of RSA and Elliptical Curve (EC) based cryptography and profiles are provided for both in the certificate types profiled.

13.5.1 FMA MSO Backoffice Certificates

FMA MSO Backoffice processes (client and server) use Service Provider Certificates issued by **Service Provider Certification Authorities** as defined in Section 12**Error! Reference source not found.**. FMA MSO Backoffice processes and are used to securely access FMA functional elements.

13.5.1.1 FMA MSO Backoffice RSA Certificates

This section provides the profile for RSA based certificates. The RSA and EC MSO Backoffice Certificate profiles provide the similar functionalities with important differences in the keyUsage and Public Key Algorithm selections.

The profile for FMA MSO Backoffice RSA Certificates is provided in Table 17.

Table 17 - CableLabs FMA MSO Backoffice RSA Certificate Profile

CableLabs FMA MSO Backoffice RSA Certificate Profile				
Version	v3 (0x02)			
Serial number	Unique Positive Integer assigned by the CA			
Issuer DN	c=US o=CableLabs ou=Service Provider CA<ID#> cn=CableLabs Service Provider Certification Authority			
Subject DN	c=<Country of Manufacture> o=<Company Name> ou=FMA Infrastructure Certificate cn=<Common Name>			
Validity Period				
Not Before	<Issuing Date>			
Not After	<Issuing Date> + Up to 5 years [*]			
Public Key Info				
Public Key Data	**Public Key Algorithm:** • RSA 2048 bit (1 2 840 113549 1 1)	**Parameters:** • NONE		
	Public Key Algorithm: • RSA 3072 bit (1 2 840 113549 1 1)	**Parameters:** • NONE		
	Public Key Algorithm: • RSA 4096 bit (1 2 840 113549 1 1)	**Parameters:** • NONE		
Signature Algorithm(s)	**Allowed OIDs:** • Sha256WithRSAEncryption (1 2 840 113549 1 1 11), or • Sha384WithRSAEncryption (1 2 840 113549 1 1 12), or • Sha512WithRSAEncryption (1 2 840 113549 1 1 13)			
Extensions				
Standard Extensions	**OID**	**Required**	**Critical**	**Value**
keyUsage	**{id-ce 15}**	**Yes**	**TRUE**	
digitalSignature				Set (1)
keyEncipherment				Set (1)
authorityKeyIdentifier	**{id-ce 35}**	**Yes**	**FALSE**	

CableLabs FMA MSO Backoffice RSA Certificate Profile				
keyIdentifier				Set (<SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits)>)
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
subjectAltName	{id-ce 17}	No	FALSE	
dNSName				Set (<Server's FQDN>), or Not Set
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>), or Not Set
caIssuers	{id-ad 2}			Set (<HTTP URI of the Issuing CA certificate in DER format>), or Not Set

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

Values in angle brackets (<>) indicate that appropriate text as indicated below is present:

<ID#>: indicates the ID number of the issuing CA (e.g., 01);

<Country of Manufacturer>: two-letter country code;

<Company Name>: name that identifies the company;

<Manufacturing Location>: name that identifies the location of manufacture;

<Common Name>: meaningful name or identifier for the device (e.g., Device Name, a UUID, etc.)

When a MAC Address is used for the <Common Name>, the value of the MAC Address is expressed as six pairs of hexadecimal digits separated by single colons (e.g., 00:60:21:A5:0A:23). Hexadecimal digits greater than 9 are expressed as uppercase letters.

13.5.1.2 FMA MSO Backoffice Elliptic-Curve Certificates

This section provides the profile for RSA based certificates. The RSA and EC MSO Backoffice Certificate profiles provide the similar functionalities with important differences in the keyUsage and Public Key Algorithm selections.

The profile for FMA MSO Backoffice Elliptic-Curve Certificates is provided in Table 18.

Table 18 - CableLabs FMA MSO Backoffice ECC Certificate Profile

CableLabs FMA MSO Backoffice ECC Certificate Profile	
Version	v3 (0x02)
Serial number	Unique Positive Integer assigned by the CA
Issuer DN	c=US o=CableLabs ou=Service Provider CA<ID#> cn=CableLabs Service Provider Certification Authority
Subject DN	c=<Country Code> o=<Company Name> ou= FMA Infrastructure Certificate cn=<Common Name>

CableLabs FMA MSO Backoffice ECC Certificate Profile				
Validity Period				
Not Before	<Issuing Date>			
Not After	<Issuing Date> + Up to 5 years [*]			
Public Key Info				
Public Key Data	**Public Key Algorithm:** • ecPublicKey (1 2 840 10045 2 1)	**Parameters:** • secp256r1 (1.2.840.10045.3.1.7), or • secp384r1 (1.3.132.0.34), or • secp521r1 (1.3.132.0.35)		
	Public Key Algorithm: • id-Ed25519 (1 3 101 112)	**Parameters:** • id-Ed25519 (1 3 101 112)		
	Public Key Algorithm: • id-Ed448 (1 3 101 113)	**Parameters:** • id-Ed448 (1 3 101 113)		
Signature Algorithm	**Allowed OIDs:** • Sha256WithRSAEncryption (1 2 840 113549 1 1 11), or • Sha384WithRSAEncryption (1 2 840 113549 1 1 12), or • Sha512WithRSAEncryption (1 2 840 113549 1 1 13)			
Extensions				
Standard Extensions	**OID**	**Required**	**Critical**	**Value**
keyUsage	**{id-ce 15}**	**Yes**	**TRUE**	
digitalSignature				Set (1)
keyAgreement				Set (1)
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)>)
extendedKeyUsage	{id-ce 37}	No	TRUE	
serverAuth	{id-kp 1}			Set (id-kp-serverAuth)
clientAuth	{id-kp 2}			Set (id-kp-clientAuth)
subjectAltName	{id-ce 17}	No	FALSE	
dNSName				Set (<Server's FQDN>), or Not Set
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>), or Not Set
caIssuers	{id-ad 2}			Set (<HTTP URI of the Issuing CA certificate in DER format>), or Not Set

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

Values in angle brackets (<>) indicate that appropriate text as indicated below is present:

<ID#>: indicates the ID number of the issuing CA (e.g., 01);

<Country of Manufacturer>: two-letter country code;

<Company Name>: name that identifies the company;

<Manufacturing Location>: name that identifies the location of manufacture;

<Common Name>: meaningful name or identifier for the device (e.g., Device Name, a UUID, etc.)

When a MAC Address is used for the <Common Name>, the value of the MAC Address is expressed as six pairs of hexadecimal digits separated by single colons (e.g., 00:60:21:A5:0A:23). Hexadecimal digits greater than 9 are expressed as uppercase letters.

13.5.2 FMA Management Functionality Certificates

FMA Management Functionality Certificates are issued by **Device Certification Authorities** to support security associations for the management of FMA. This includes Packet Cable Aggregator and MAC Manager systems or devices.

13.5.2.1 FMA Management Functionality RSA Certificates

This section provides the profile for RSA based certificates. The RSA and EC MSO Backoffice Certificate profiles provide the similar functionalities with important differences in the keyUsage and Public Key Algorithm selections.

The profile for FMA Management Functionality RSA Certificates is provided in Table 19.

Table 19 - CableLabs FMA Management Functionality RSA Certificate Profile

FMA Management Functionality RSA Certificate Profile				
Version	v3 (0x02)			
Serial number	Unique Positive Integer assigned by the CA			
Issuer DN	c=US o=CableLabs ou=Device CA<ID#> cn=CableLabs Device Certification Authority			
Subject DN	c=<Country of Manufacturer> o=<Company Name> ou=<Manufacturing Location> cn=<Device Identifier>			
Validity Period				
Not Before	<Issuing Date>			
Not After	<Issuing Date> + Up to 5 years [*]			
Public Key Info				
Public Key Data	**Public Key Algorithm:** • RSA 2048 bit (1 2 840 113549 1 1)	**Parameters:** • NONE		
	Public Key Algorithm: • RSA 3072 bit (1 2 840 113549 1 1)	**Parameters:** • NONE		
	Public Key Algorithm: • RSA 4096 bit (1 2 840 113549 1 1)	**Parameters:** • NONE		
Signature Algorithm	**Allowed OIDs:** • Sha256WithRSAEncryption (1 2 840 113549 1 1 11), or • Sha384WithRSAEncryption (1 2 840 113549 1 1 12), or • Sha512WithRSAEncryption (1 2 840 113549 1 1 13)			
Extensions				
Standard Extensions	**OID**	**Required**	**Critical**	**Value**
keyUsage	{id-ce 15}	**Yes**	**TRUE**	
digitalSignature				Set (1)
keyEncipherment				Set (1)
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)>)
extendedKeyUsage	{id-ce 37}	**Yes**	**FALSE**	
svcMGMT				Set (id-cl-pki-ext-eku-MGMT), or Not Set
svcCCAP				Set (id-cl-pki-ext-eku-CCAP), or Not Set
clientAuth				Set (id-kp-clientAuth)
serverAuth				Set (id-kp-serverAuth)
certificatePolicies	**{id-ce 32}**	**Yes**	**FALSE**	
certPolicyId				Set (<DOCSIS PKI Certificate Policy OID>)
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>), or Not Set
caIssuers	{id-ad 2}			Set (<HTTP URI of the Issuing CA certificate in DER format>), or Not Set
subjectAltName	{id-ce 17}	No	FALSE	
dNSName				Set (<FQDN>), or Not Set

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

Values in angle brackets (<>) indicate that appropriate text as indicated below is present:

<ID#>: indicates the ID number of the issuing CA (e.g., 01);

<Country of Manufacturer>: two-letter country code;

<Company Name>: name that identifies the company;

<Manufacturing Location>: name that identifies the location of manufacture;

<Device Identifier>: Meaningful identifier for the device (e.g., FQDN, MAC address, CCAP ID, Core ID, or UUID).

If used, extendedKeyUsage may include either svcMGMT or svcCCAP service OIDs. MAC Managers may use svcCCAP and all other Management Functionalities may use svcMGMT.

When a MAC Address is used for the <Device Identifier>, the value of the MAC Address is expressed as six pairs of hexadecimal digits separated by single colons (e.g., 00:60:21:A5:0A:23). Hexadecimal digits greater than 9 are expressed as uppercase letters.

13.5.2.2 FMA Management Functionality ECC Certificates

This section provides the profile for EC based certificates. The FMA Management Functionality EC Certificate profiles provide the similar functionalities to the RSA ones with important differences in the keyUsage and Public Key Algorithm selections.

The profile for FMA Management Functionality EC Certificates is provided in Table 20.

Table 20 - CableLabs FMA Management Functionality ECC Certificate Profile

FMA Management Functionality ECC Certificate Profile	
Version	v3 (0x02)
Serial number	Unique Positive Integer assigned by the CA

Issuer DN	c=US o=CableLabs ou=Device CA<ID#> cn=CableLabs Device Certification Authority	
Subject DN	c=<Country of Manufacturer> o=<Company Name> ou=<Manufacturing Location> cn=<Device Identifier>	
Validity Period		
Not Before	<Issuing Date>	
Not After	<Issuing Date> + Up to 5 years [*]	
Public Key Info		
Public Key Data	**Public Key Algorithm:** • ecPublicKey (1 2 840 10045 2 1)	**Parameters:** • secp256r1 (1.2.840.10045.3.1.7), or • secp384r1 (1.3.132.0.34), or • secp521r1 (1.3.132.0.35)
	Public Key Algorithm: • id-Ed25519 (1 3 101 112)	**Parameters:** • id-Ed25519 (1 3 101 112)
	Public Key Algorithm: • id-Ed448 (1 3 101 113)	**Parameters:** • id-Ed448 (1 3 101 113)
Signature Algorithm(s)	**Allowed OIDs:** • Sha256WithRSAEncryption (1 2 840 113549 1 1 11), or • Sha384WithRSAEncryption (1 2 840 113549 1 1 12), or • Sha512WithRSAEncryption (1 2 840 113549 1 1 13)	

Extensions

Standard Extensions	OID	Required	Critical	Value
keyUsage	{id-ce 15}	**Yes**	**TRUE**	
digitalSignature				Set (1)
keyAgreement				Set (1)
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)>)
extendedKeyUsage	{id-ce 37}	**Yes**	**FALSE**	
svcMGMT				Set (id-cl-pki-ext-eku-MGMT), or Not Set
svcCCAP				Set (id-cl-pki-ext-eku-CCAP), or Not Set
clientAuth				Set (id-kp-clientAuth)
serverAuth				Set (id-kp-serverAuth)
certificatePolicies	**{id-ce 32}**	**Yes**	**FALSE**	
certPolicyId				Set (<DOCSIS PKI Certificate Policy OID>)
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>), or Not Set
caIssuers	{id-ad 2}			Set (<HTTP URI of the Issuing CA certificate in DER format>), or Not Set
subjectAltName	{id-ce 17}	No	FALSE	

dNSName				Set (<FQDN>), or Not Set

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

Values in angle brackets (<>) indicate that appropriate text as indicated below is present:

<ID#>: indicates the ID number of the issuing CA (e.g., 01);

<Country of Manufacturer>: two-letter country code;

<Company Name>: name that identifies the company;

<Manufacturing Location>: name that identifies the location of manufacture;

<Device Identifier>: Meaningful identifier for the device (e.g., FQDN, MAC address, CCAP ID, Core ID, or UUID).

If used, extendedKeyUsage may include either svcMGMT or svcCCAP service OIDs. MAC Managers may use svcCCAP and all other Management Functionalities may use svcMGMT.

When a MAC Address is used for the <Device Identifier>, the value of the MAC Address is expressed as six pairs of hexadecimal digits separated by single colons (e.g., 00:60:21:A5:0A:23). Hexadecimal digits greater than 9 are expressed as uppercase letters.

13.5.3 FMA MAC Network Element (MAC-NE) Certificates

FMA MAC Network Element (MAC-NE) Certificates are issued by **Device Certification Authorities** to support security associations for supporting management and data plane functions FMA. This includes Remote MAC Devices (RMDs).

13.5.3.1 FMA MAC Network Element (MAC-NE) RSA Certificates

This section provides the profile for RSA based certificates. The RSA and EC MAC Network Element (MAC-NE) Certificate profiles provide the similar functionalities with important differences in the keyUsage and Public Key Algorithm selections.

The profile for FMA MAC-NE Certificates is provided in Table 21:

Table 21 - CableLabs FMA MAC-NE RSA Certificate Profile

FMA MAC-NE RSA Certificate Profile		
Version	v3 (0x02)	
Serial number	Unique Positive Integer assigned by the CA	
Issuer DN	c=US o=CableLabs ou=Device CA<ID#> cn=CableLabs Device Certification Authority	
Subject DN	c=<Country of Manufacturer> o=<Company Name> ou=<Manufacturing Location> cn=<Device Identifier>	
Validity Period		
Not Before	<Issuing Date>	
Not After	<Issuing Date> + Up to 5 years [*]	
Public Key Info		
Public Key Data	**Public Key Algorithm:** • RSA 2048 bit (1 2 840 113549 1 1)	**Parameters:** • NONE
	Public Key Algorithm: • RSA 3072 bit (1 2 840 113549 1 1)	**Parameters:** • NONE

	Public Key Algorithm: • RSA 4096 bit (1 2 840 113549 1 1)	**Parameters:** • NONE
Signature Algorithm(s)	**Allowed OIDs:** • Sha256WithRSAEncryption (1 2 840 113549 1 1 11), or • Sha384WithRSAEncryption (1 2 840 113549 1 1 12), or • Sha512WithRSAEncryption (1 2 840 113549 1 1 13)	

Extensions

Standard Extensions	OID	Required	Critical	Value
keyUsage	{id-ce 15}	**Yes**	**TRUE**	
digitalSignature				Set (1)
keyEncipherment				Set (1)
extendedKeyUsage	{id-ce 37}	**Yes**	**FALSE**	
svcMACNE				Set (id-cl-pki-ext-eku-MACNE)
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 (<DOCSIS PKI Certificate Policy OID>)
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>), or Not Set
caIssuers	{id-ad 2}			Set (<HTTP URI of the Issuing CA certificate in DER format>), or Not Set
subjectAltName	{id-ce 17}	No	FALSE	
dNSName				Set (<FQDN>), or Not Set

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

Values in angle brackets (<>) indicate that appropriate text as indicated below is present:

<ID#>: indicates the ID number of the issuing CA (e.g., 01);

<Country of Manufacturer>: two-letter country code;

<Company Name>: name that identifies the company;

<Manufacturing Location>: name that identifies the location of manufacture;

<Device Identifier>: Meaningful identifier for the device (e.g., FQDN, Device MAC address, Hostname, MacNeUniqueid, or UUID).

When a MAC Address is used for the <Device Identifier>, the value of the MAC Address is expressed as six pairs of hexadecimal digits separated by single colons (e.g., 00:60:21:A5:0A:23). Hexadecimal digits greater than 9 are expressed as uppercase letters.

13.5.3.2 FMA MAC Network Element ECC Certificates

This section provides the profile for EC based certificates. The FMA MAC Network Element (MAC-NE) ECC Certificate profiles provide the similar functionalities to the RSA ones with important differences in the keyUsage and Public Key Algorithm selections.

The profile for FMA MAC-NE Certificates is provided in Table 22:

Table 22 - CableLabs FMA MAC-NE ECC Certificate Profile

FMA MAC-NE ECC Certificate Profile				
Version	v3 (0x02)			
Serial number	Unique Positive Integer assigned by the CA			
Issuer DN	c=US o=CableLabs ou=Device CA<ID#> cn=CableLabs Device Certification Authority			
Subject DN	c=<Country of Manufacturer> o=<Company Name> ou=<Manufacturing Location> cn=<Device Identifier>			
Validity Period				
Not Before	<Issuing Date>			
Not After	<Issuing Date> + Up to 5 years [*]			
Public Key Info				
Public Key Data	**Public Key Algorithm:** ecPublicKey (1 2 840 10045 2 1)	**Parameters:** • secp256r1 (1.2.840.10045.3.1.7), or • secp384r1 (1.3.132.0.34), or • secp521r1 (1.3.132.0.35)		
	Public Key Algorithm: • id-Ed25519 (1 3 101 112)	**Parameters:** • id-Ed25519 (1 3 101 112)		
	Public Key Algorithm: • id-Ed448 (1 3 101 113)	**Parameters:** • id-Ed448 (1 3 101 113)		
Signature Algorithm(s)	**Allowed OIDs:** • Sha256WithRSAEncryption (1 2 840 113549 1 1 11), or • Sha384WithRSAEncryption (1 2 840 113549 1 1 12), or • Sha512WithRSAEncryption (1 2 840 113549 1 1 13)			
Extensions				
Standard Extensions	**OID**	**Required**	**Critical**	**Value**
keyUsage	{id-ce 15}	**Yes**	**TRUE**	
digitalSignature				Set (1)
keyAgreement				Set (1)
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)>)
extendedKeyUsage	{id-ce 37}	**Yes**	**FALSE**	
svcMACNE				Set (id-cl-pki-ext-eku-MACNE)
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 (<DOCSIS PKI Certificate Policy OID>)
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>), or Not Set
caIssuers	{id-ad 2}			Set (<HTTP URI of the Issuing CA certificate in DER format>), or Not Set
subjectAltName	{id-ce 17}	No	FALSE	
dNSName				Set (<FQDN>), or Not Set

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

Values in angle brackets (<>) indicate that appropriate text as indicated below is present:

<ID#>: indicates the ID number of the issuing CA (e.g., 01);

<Country of Manufacturer>: two-letter country code;

<Company Name>: name that identifies the company;

<Manufacturing Location>: name that identifies the location of manufacture.

<Device Identifier>: Meaningful identifier for the device (e.g., FQDN, Device MAC address, Hostname, MacNeUniqueid, or UUID).

When a MAC Address is used for the <Device Identifier>, the value of the MAC Address is expressed as six pairs of hexadecimal digits separated by single colons (e.g., 00:60:21:A5:0A:23). Hexadecimal digits greater than 9 are expressed as uppercase letters.

Appendix I Acknowledgements (Informative)

On behalf of the cable industry and our member companies, CableLabs would like to thank the following individuals for their contributions to the development of this specification.

Contributor	Company Affiliation
Massimiliano Pala, Steve Goeringer	CableLabs
Jane Keys, Scott Kenny	Kyrio, Inc.

* * *