



SLOVENSKI STANDARD
SIST EN 302 878-5 V1.1.1:2012

01-februar-2012

Dostop, priključki, prenos in multipleksiranje (ATTM) - Tretja generacija prenosnih sistemov za storitve interaktivne kabelske televizije - IP-kabelski modemi - 5. del: Varnostne storitve - DOCSIS 3.0

Access, Terminals, Transmission and Multiplexing (ATTM) - Third Generation Transmission Systems for Interactive Cable Television Services - IP Cable Modems - Part 5: Security Services - DOCSIS 3.0

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[SIST EN 302 878-5 V1.1.1:2012
https://standards.iteh.ai/catalog/standards/sist/2174b9d8-7613-42f5-80b7-e38b123abb28/sist-en-302-878-5-v1-1-1-2012](https://standards.iteh.ai/catalog/standards/sist/2174b9d8-7613-42f5-80b7-e38b123abb28/sist-en-302-878-5-v1-1-1-2012)

Ta slovenski standard je istoveten z: EN 302 878-5 Version 1.1.1

ICS:

35.180	Terminalska in druga periferna oprema IT	IT Terminal and other peripheral equipment
--------	---	---

SIST EN 302 878-5 V1.1.1:2012 **en**

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN 302 878-5 V1.1.1:2012

<https://standards.iteh.ai/catalog/standards/sist/2174b9d8-7613-42f5-80b7-e38b123abb28/sist-en-302-878-5-v1-1-1-2012>

ETSI EN 302 878-5 V1.1.1 (2011-11)



**Access, Terminals, Transmission and Multiplexing (ATTM);
Third Generation Transmission Systems for
Interactive Cable Television Services - IP Cable Modems;
Part 5: Security Services;**

DOCSIS 3.0

<https://standards.iteh.ai/catalog/standards/sist/302-878-5-v1-1-1-2012>
e38b123abb28/sist-en-302-878-5-v1-1-1-2012

Reference

DEN/ATTM-003006-5

Keywords

access, broadband, cable, data, IP, IPCable,
modem

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN 302 878-5 V1.1.1:2012

<https://standards.iteh.ai/catalog/standards/sist/2174b9d8-7613-42f5-80b7-e38b123ab728/etsi-en-302-878-5-v1-1-1-2012>

Important notice

Individual copies of the present document can be downloaded from:

<http://www.etsi.org>

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at

<http://portal.etsi.org/tb/status/status.asp>

If you find errors in the present document, please send your comment to one of the following services:

http://portal.etsi.org/chaicor/ETSI_support.asp

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2011.
All rights reserved.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPP™ and **LTE™** are Trade Marks of ETSI registered for the benefit of its Members and
of the 3GPP Organizational Partners.
GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

Contents

Intellectual Property Rights	10
Foreword.....	10
1 Scope	11
1.1 Introduction and Purpose.....	11
1.2 Requirements.....	11
1.3 Conventions.....	11
2 References	11
2.1 Normative references	12
2.2 Informative references.....	13
3 Definitions and abbreviations.....	14
3.1 Definitions.....	14
3.2 Abbreviations	14
4 Void.....	16
5 Overview	16
5.1 New DOCSIS 3.0 Security Features.....	16
5.2 Technical Overview	17
5.2.1 BPI+ Architecture.....	17
5.2.1.1 Packet Data Encryption.....	17
5.2.1.2 Key Management Protocol.....	17
5.2.1.3 DOCSIS Security Associations.....	18
5.2.1.4 QoS SIDs and DOCSIS SAIDs.....	19
5.2.1.5 BPI+ Enforce.....	19
5.2.2 Secure Provisioning	20
5.3 Operation.....	20
5.3.1 Cable Modem Initialization.....	20
5.3.1.1 Network Admission Control.....	21
5.3.1.2 EAE and Authentication Reuse.....	21
5.3.1.3 Configuration Registration Enforcement	21
5.3.2 Cable Modem Key Update Mechanism.....	22
5.3.3 Cable Modem Secure Software Download.....	22
6 Encrypted DOCSIS MAC Frame Formats	22
6.1 CM Requirements.....	22
6.2 CMTS Requirements.....	22
6.3 Variable-Length PDU MAC Frame Format.....	23
6.3.1 Baseline Privacy Extended Header Formats	24
6.4 Fragmentation MAC Frame Format	25
6.5 Registration Request (REG-REQ-MP) MAC Management Messages.....	26
6.6 Use of the Baseline Privacy Extended Header in the MAC Header.....	28
7 Baseline Privacy Key Management (BPKM) Protocol	28
7.1 State Models.....	28
7.1.1 Introduction.....	28
7.1.1.1 Authorization State Machine Overview.....	28
7.1.1.2 TEK State Machine Overview	30
7.1.2 Encrypted Multicast.....	31
7.1.2.1 Signaling of Dynamic and Static Multicast Session SAs when MDF is Disabled	32
7.1.2.2 Signaling of Dynamic and Static Multicast Session SAs when MDF is Enabled	32
7.1.2.2.1 Requirements Specific to the Signaling of Dynamic SAs for Dynamic Multicast Sessions	32
7.1.2.2.2 Requirements Specific to the Signaling of Dynamic SAs for Static Multicast Sessions	33
7.1.3 Selecting Cryptographic Suites.....	33
7.1.4 Authorization State Machine	34
7.1.4.1 Brief Description of States	35
7.1.4.1.1 [Start].....	35

7.1.4.1.2	[Auth Wait].....	35
7.1.4.1.3	[Authorized]	35
7.1.4.1.4	[Reauth Wait]	35
7.1.4.1.5	[Auth Reject Wait]	35
7.1.4.1.6	[Silent]	36
7.1.4.2	Brief Description of Messages	36
7.1.4.2.1	Authorization Request (Auth Request).....	36
7.1.4.2.2	Authorization Reply (Auth Reply)	36
7.1.4.2.3	Authorization Reject (Auth Reject).....	36
7.1.4.2.4	Authorization Invalid (Auth Invalid).....	36
7.1.4.2.5	Authentication Information (Auth Info)	36
7.1.4.3	Brief Description of Events.....	37
7.1.4.3.1	{Initiate Authentication}	37
7.1.4.3.2	{Timeout}	37
7.1.4.3.3	{Auth Grace Timeout}	37
7.1.4.3.4	{Reauth}	37
7.1.4.3.5	{Auth Invalid}	37
7.1.4.3.6	{Perm Auth Reject}	37
7.1.4.3.7	{Auth Reject}	37
7.1.4.3.8	{EAE Disabled Auth Reject}	37
7.1.4.4	Events sent to TEK State Machine.....	37
7.1.4.4.1	{TEK Stop}	38
7.1.4.4.2	{TEK Authorized}	38
7.1.4.4.3	{Auth Pend}	38
7.1.4.4.4	{Auth Comp}	38
7.1.4.5	Brief Description of Timing Parameters	38
7.1.4.5.1	Authorize Wait Timeout (Auth Wait Timeout)	38
7.1.4.5.2	Reauthorize Wait Timeout (Reauth Wait Timeout).....	38
7.1.4.5.3	Authorization Grace Time (Auth Grace Timeout).....	38
7.1.4.5.4	Authorize Reject Wait Timeout (Auth Reject Wait Timeout).....	38
7.1.4.6	Timers	38
7.1.4.6.1	Authorization Request	38
7.1.4.6.2	Authorization Reject	38
7.1.4.6.3	Authorization Grace	38
7.1.4.7	Actions	39
7.1.5	TEK State Machine.....	41
7.1.5.1	Brief Description of States	42
7.1.5.1.1	[Start].....	42
7.1.5.1.2	[Op Wait].....	42
7.1.5.1.3	[Op Reauth Wait]	42
7.1.5.1.4	[Op]	42
7.1.5.1.5	[Rekey Wait]	42
7.1.5.1.6	[Rekey Reauth Wait]	42
7.1.5.2	Brief Description of Messages	42
7.1.5.2.1	Key Request	42
7.1.5.2.2	Key Reply.....	43
7.1.5.2.3	Key Reject	43
7.1.5.2.4	TEK Invalid	43
7.1.5.3	Brief Description of Events.....	43
7.1.5.3.1	{Stop}.....	43
7.1.5.3.2	{Authorized}	43
7.1.5.3.3	{Auth Pend}	43
7.1.5.3.4	{Auth Comp}	43
7.1.5.3.5	{TEK Invalid}	43
7.1.5.3.6	{Timeout}.....	43
7.1.5.3.7	{TEK Refresh Timeout}.....	43
7.1.5.4	Brief Description of Timing Parameters	43
7.1.5.4.1	Operational Wait Timeout	44
7.1.5.4.2	Rekey Wait Timeout.....	44
7.1.5.4.3	TEK Grace Time	44
7.1.5.5	Timers	44
7.1.5.5.1	Key Request Retry.....	44

7.1.5.5.2	TEK Refresh.....	44
7.1.5.6	Actions	44
7.2	Key Management Message Formats.....	46
7.2.1	Packet Formats.....	46
7.2.1.1	Authorization Request (Auth Request)	48
7.2.1.2	Authorization Reply (Auth Reply).....	48
7.2.1.3	Authorization Reject (Auth Reject).....	49
7.2.1.4	Key Request	49
7.2.1.5	Key Reply	50
7.2.1.6	Key Reject.....	50
7.2.1.7	Authorization Invalid	51
7.2.1.8	TEK Invalid.....	51
7.2.1.9	Authentication Information (Auth Info).....	51
7.2.1.10	SA Map Request (MAP Request)	52
7.2.1.11	SA Map Reply (Map Reply)	52
7.2.1.12	SA Map Reject (Map Reject).....	52
7.2.2	BPKM Attributes	53
7.2.2.1	Serial-Number	54
7.2.2.2	Manufacturer-ID	54
7.2.2.3	MAC-Address	55
7.2.2.4	RSA-Public-Key	55
7.2.2.5	CM-Identification.....	55
7.2.2.6	Display-String	56
7.2.2.7	Auth-Key.....	56
7.2.2.8	TEK.....	56
7.2.2.9	Key-Lifetime.....	56
7.2.2.10	Key-Sequence-Number.....	57
7.2.2.11	HMAC-Digest.....	57
7.2.2.12	SAID	57
7.2.2.13	TEK-Parameters	57
7.2.2.14	CBC-IV	58
7.2.2.15	Error-Code	58
7.2.2.16	Vendor-Defined	59
7.2.2.17	CA-Certificate	59
7.2.2.18	CM-Certificate	60
7.2.2.19	Security-Capabilities	60
7.2.2.20	Cryptographic-Suite	60
7.2.2.21	Cryptographic-Suite-List.....	61
7.2.2.22	BPI-Version	61
7.2.2.23	SA-Descriptor	61
7.2.2.24	SA-Type.....	62
7.2.2.25	SA-Query	62
7.2.2.26	SA-Query-Type.....	63
7.2.2.27	IPv4-Address.....	63
7.2.2.28	Download-Parameters	63
7.2.2.29	CVC-Root-CA-Certificate	63
7.2.2.30	CVC-CA-Certificate	64
8	Early Authentication and Encryption (EAE).....	64
8.1	Introduction	64
8.2	EAE Signaling	64
8.3	EAE Encryption	66
8.4	EAE Enforcement.....	66
8.4.1	CMTS and CM behaviours when EAE is Enabled	66
8.4.2	EAE enforcement determination.....	67
8.4.2.1	Ranging-Based EAE Enforcement.....	67
8.4.2.2	Capability-Based EAE Enforcement.....	67
8.4.2.3	Total EAE Enforcement	67
8.4.3	EAE Enforcement of DHCP Traffic	67
8.4.4	CMTS and CM Behaviour when EAE is Disabled.....	67
8.4.5	EAE Exclusion List	67
8.4.6	Interoperability issues	68

8.5	Authentication Reuse	68
8.6	BPI+ Control by Configuration File	68
8.6.1	EAE Enabled	68
8.6.2	EAE Disabled	69
9	Secure Provisioning.....	69
9.1	Introduction	69
9.2	Encryption of Provisioning Messages	69
9.3	Securing DHCP	69
9.3.1	Securing DHCP on the Cable Network Link	69
9.3.2	DHCPv6.....	69
9.4	TFTP Configuration File Security.....	70
9.4.1	Introduction.....	70
9.4.2	CMTS Security Features for Configuration File Download	70
9.4.2.1	TFTP Proxy.....	70
9.4.2.2	Protecting TFTP Server Addresses	70
9.4.2.3	Configuration File Name Authorization.....	70
9.4.2.4	Configuration File Learning.....	71
9.4.2.5	TFTP Options for CM's MAC and IP Address	71
9.5	Securing REG-REQ-MP Messages	71
9.6	Source Address Verification.....	71
9.7	Address Resolution Security Considerations	73
10	Using Cryptographic Keys	74
10.1	CMTS	74
10.2	Cable Modem	76
10.3	Authentication of Dynamic Service Requests	77
10.3.1	CM.....	77
10.3.2	CMTS	77
11	Cryptographic Methods.....	77
11.1	Packet Data Encryption	77
11.2	Encryption of the TEK	78
11.3	HMAC-Digest Algorithms.....	79
11.4	TEKs, KEKs and Message Authentication Keys	79
11.5	Public-Key Encryption of Authorization Key	79
11.6	Digital Signatures	80
11.7	The MMH-MIC	80
11.7.1	The MMH Function	80
11.7.1.1	MMH[16, σ , 1].....	80
11.7.1.2	MMH[16, σ , n].....	82
11.7.1.3	MMH[16, σ , 4].....	82
11.7.1.4	Handling Variable-Size Data	82
11.7.2	Definition of MMH-MAC	82
11.7.3	Calculating the DOCSIS MMH-MAC.....	83
11.7.4	MMH Key Derivation for CMTS Extended MIC.....	84
11.7.5	Shared Secret Recommendations.....	85
11.7.6	Key Generation Function.....	85
12	Physical Protection of Keys in the CM	85
13	BPI+ X.509 Certificate Profile and Management	86
13.1	BPI+ Certificate Management Architecture Overview	86
13.2	Cable Modem Certificate Storage and Management in the CM.....	88
13.3	Certificate Processing and Management in the CMTS.....	89
13.3.1	CMTS Certificate Management Model.....	89
13.3.2	Certificate Validation.....	89
13.4	Certificate Revocation	90
13.4.1	Certificate Revocation Lists.....	90
13.4.1.1	CMTS CRL Support	91
13.4.2	Online Certificate Status Protocol	91
14	Secure Software Download	92
14.1	Introduction	92

iTech STANDARD PREVIEW
(standards.itech.ai)

14.2	Overview	92
14.3	Software Code Upgrade Requirements	94
14.3.1	Code File Processing Requirements	94
14.3.2	Code File Access Controls.....	95
14.3.2.1	Subject Organization Names	95
14.3.2.2	Time Varying Controls	95
14.3.3	Cable Modem Code Upgrade Initialization	95
14.3.3.1	Manufacturer Initialization.....	96
14.3.3.2	Network Initialization	96
14.3.3.2.1	Processing the Configuration File CVC	97
14.3.3.2.2	Processing the SNMP CVC.....	97
14.3.4	Code Signing Guidelines	98
14.3.5	Code Verification Requirements.....	98
14.3.5.1	Cable Modem Code Verification Steps.....	98
14.3.6	DOCSIS Interoperability	99
14.3.7	Error Codes.....	99
14.4	Security Considerations (Informative)	100
Annex A (normative): TFTP Configuration File Extensions		102
A.1	Encodings	102
A.1.1	Baseline Privacy Configuration Setting	102
A.1.1.1	Internal Baseline Privacy Encodings	102
A.1.1.1.1	Authorize Wait Timeout	102
A.1.1.1.2	Reauthorize Wait Timeout	102
A.1.1.1.3	Authorization Grace Time.....	103
A.1.1.1.4	Operational Wait Timeout.....	103
A.1.1.1.5	Rekey Wait Timeout	103
A.1.1.1.6	TEK Grace Time	103
A.1.1.1.7	Authorize Reject Wait Timeout	103
A.1.1.1.8	SA Map Wait Timeout	103
A.1.1.1.9	SA Map Max Retries.....	103
A.2	Parameter Guidelines	104
Annex B (normative): TFTP Options.....		105
Annex C (normative): DOCSIS 1.1/2.0 Dynamic Security Associations.....		113
C.1	Introduction	113
C.2	Theory of Operation	113
C.3	SA Mapping State Model	114
C.3.1	Brief Description of States	115
C.3.1.1	[Start].....	115
C.3.1.2	[Map Wait].....	115
C.3.1.3	[Mapped]	115
C.3.2	Brief Description of Messages	115
C.3.2.1	Map Request	115
C.3.2.2	Map Reply	116
C.3.2.3	Map Reject.....	116
C.3.3	Brief Description of Events	116
C.3.3.1	{Map}	116
C.3.3.2	{Unmap}.....	116
C.3.3.3	{Map Reply}.....	116
C.3.3.4	{Map Reject}	116
C.3.3.5	{Timeout}	116
C.3.3.6	{Max Retries}	116
C.3.3.7	Brief Description of Parameters.....	116
C.3.3.8	SA Map Wait Timeout.....	116
C.3.3.9	SA Map Max Retries	116
C.3.4	Actions	117

Annex D (normative):	BPI/BPI+ Interoperability	118
D.1	DOCSIS BPI/BPI+ Interoperability Requirements	118
D.2	BPI 40-bit DES Export Mode Considerations.....	119
D.3	System Operation	120
D.3.1	CMTS with BPI Capability	120
D.3.2	CMTS with BPI+ Capability.....	120
Annex E (informative):	Example Messages, Certificates, PDUs and Code File	121
E.1	Notation.....	121
E.2	Authentication Info.....	121
E.2.1	CA Certificate details	122
E.3	Authorization Request.....	123
E.3.1	CM Certificate details	124
E.4	Authorization Reply	126
E.4.1	RSA encryption details.....	126
E.4.2	RSA decryption details.....	128
E.4.3	Hashing details	129
E.4.3.1	KEK.....	129
E.4.3.2	Message authentication keys.....	129
E.4.3.3	Mask-generation function.....	130
E.5	Key Request	130
E.5.1	HMAC digest details.....	131
E.6	Key Reply.....	132
E.6.1	TEK encryption details.....	133
E.6.2	HMAC details	134
E.7	Packet PDU encryption (DES).....	134
E.7.1	CBC only.....	135
E.7.2	CBC with residual block processing.....	135
E.7.3	Runt frame.....	136
E.7.4	40-bit key.....	137
E.8	Encryption of PDU with Payload Header Suppression (DES).....	138
E.8.1	Downstream	138
E.8.2	Upstream	139
E.9	Fragmented packet encryption (DES)	140
E.10	Packet PDU encryption (AES).....	141
E.10.1	CBC only.....	141
E.10.2	CBC with residual block processing	142
E.10.3	Runt frame.....	143
E.11	Encryption of PDU with Payload Header Suppression (AES).....	144
E.11.1	Downstream	144
E.11.2	Upstream	144
E.12	Fragmented packet encryption (AES)	145
E.13	Secure Software Download CM Code File	147
Annex F (informative):	Example of Multilinear Modular Hash (MMH) Algorithm Implementation	163
Annex G (informative):	Certificate Authority and Provisioning Guidelines	171
G.1	Certificate Format and Extensions	171
G.1.1	tbsCertificate.validity.notBefore and tbsCertificate.validity.notAfter.....	171
G.1.2	tbsCertificate.serialNumber	171

G.1.3	tbsCertificate.signature and signatureAlgorithm	172
G.1.4	tbsCertificate.issuer and tbsCertificate.subject	172
G.1.4.1	DOCSIS Root CA Certificate	172
G.1.4.2	Centralized Mfg CA Certificate	172
G.1.4.3	Manufacturer CA Certificate	172
G.1.4.4	CM Device Certificate	173
G.1.5	tbsCertificate.issuerUniqueID and tbsCertificate.subjectUniqueID	174
G.1.6	tbsCertificate.extensions	174
G.1.6.1	CM Device Certificates	174
G.1.6.2	Manufacturer CA Certificates	174
G.1.6.3	Centralized Mfg CA Certificate	174
G.1.6.4	DOCSIS Root CA Certificate	174
G.1.7	Code Verification Certificate Format	175
G.1.8	signatureValue	175
G.2	Certificate Provisioning	176
G.2.1	DOCSIS Root CA	176
G.2.2	Digital Certificate Validity Period and Re-issuance	176
G.2.2.1	DOCSIS Root CA Certificate	176
G.2.2.2	Void	176
G.2.2.3	Code Verification Certificate	176
G.2.3	CM Code File Signing Policy	177
G.2.3.1	Manufacturer CM Code File Signing Policy	177
G.2.3.2	Operator CM Code File Signing Policy	177
G.2.4	CM Code File Format	177
G.2.4.1	DOCSIS PKCS#7 Signed Data	178
G.2.4.1.1	Code Signing Keys	179
G.2.4.1.2	Code Verification Certificate Format	179
G.2.4.1.3	Code Verification Certificate Revocation	180
G.2.4.2	Signed Content	180
Annex H (informative):	Bibliography	181
History	https://standards.iteh.ai/catalog/standards/sist/2174b9d8-7613-42f5-80b7-e38b123abb28/sist-en-302-878-5-v1-1-1-2012	185

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: "*Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards*", which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (<http://ipr.etsi.org>).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This European Standard (EN) has been produced by ETSI Technical Committee Access, Terminals, Transmission and Multiplexing (ATTM).

The present document is part 5 of a multi-part deliverable. Full details of the entire series can be found in part 1 [i.9].

National transposition dates	
Date of adoption of this EN:	14 November 2011
Date of latest announcement of this EN (doa):	29 February 2012
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	31 August 2012
Date of withdrawal of any conflicting National Standard (dow):	31 August 2012

iTech STANDARD PREVIEW
(standards.iteh.ai)
SIST EN 302 878-5 V1.1.1:2012
<https://standards.iteh.ai/catalog/standards/sist/2174b9d8-7613-4215-80b7-e38b123abb28/sist-en-302-878-5-v1-1-1-2012>

1 Scope

1.1 Introduction and Purpose

The present document is part of a series of specifications that define the third generation of high-speed data-over-cable systems. This series was developed for the benefit of the cable industry, and includes contributions by operators and vendors from North America, Europe, and other regions.

The present document defines the Base Line Privacy Plus (BPI+) architecture which covers CM authentication, key exchange, and establishing encrypted traffic sessions between the CM and CMTS. Early Authentication and Encryption (EAE) applies BPI+, earlier in the provisioning process (see clause 8). This specification also defines security features for the CM provisioning process, which includes Secure Software Download (SSD).

1.2 Requirements

Throughout the present 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.
"SHOULD NOT"	This phrase means that there may exist valid reasons in particular circumstances when the listed behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.
"MAY"	This word 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.

The present 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 must comply with all mandatory (MUST and MUST NOT) requirements to be considered compliant with the present document. Support of non-mandatory features and parameter values is optional.

1.3 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.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at <http://docbox.etsi.org/Reference>.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

- [1] Cable Television Laboratories, Inc. CM-SP-OSSIV3.0-I12-100611 (June 2010): "Data-Over-Cable Service Interface Specifications - DOCSIS 3.0 - Operations Support System Interface Specification".
- [2] ETSI EN 302 878-4: "Access, Terminals, Transmission and Multiplexing (ATTM); Third Generation Transmission Systems for Interactive Cable Television Services - IP Cable Modems; Part 4: MAC and Upper Layer Protocols; DOCSIS 3.0".
- [3] ETSI ES 201 488-3 (V1.2.2): "Access and Terminals (AT); Data Over Cable Systems; Part 3: Baseline Privacy Plus Interface Specification".
- [4] FIPS PUB 46-3 (October 1999): "Data Encryption Standard (DES)".
- [5] FIPS PUB 140-2 (May 2001): "Security Requirements for Cryptographic Modules".
- [6] FIPS PUB 180-2 (August 2002): "Secure Hash Standard".
- [7] FIPS PUB 197 (November 2001): "Advanced Encryption Standard (AES)".
- [8] ISO/IEC 8859-1:1998: "Information technology -- 8-bit single-byte coded graphic character sets -- Part 1: Latin alphabet No. 1".
- [9] Proceedings of the 4th Workshop on Fast Software Encryption, LNCS vol. 1267, Springer, 1997. Pages 172-189: "MMH: Software Message Authentication in the Gbit/second Rates", S. Halevi and H. Krawczyk.
- [10] NIST-800-38A (2001): "Recommendation for Block Cipher Modes of Operation, Methods and Techniques", Morris Dworkin.
- [11] RSA Laboratories, PKCS #7 (Version 1.5, Revised November 1, 1993): "Cryptographic Message Syntax Standard", an RSA Laboratories Technical Note.
- [12] IETF RFC 826/STD0037 (1982): "Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware".
- [13] IETF RFC 1350/STD0033 (1992): "The TFTP Protocol (Revision 2)".
- [14] IETF RFC 2104 (1997): "HMAC: Keyed-Hashing for Message Authentication".
- [15] IETF RFC 2347 (1998): "TFTP Option Extension".
- [16] IETF RFC 2348 (1998): "TFTP Blocksize Option".
- [17] IETF RFC 2349 (1998): "TFTP Timeout Interval and Transfer Size Options".
- [18] IETF RFC 4861 (2007): "Neighbor Discovery for IP version 6 (IPv6)".
- [19] IETF RFC 2560 (1999): "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".
- [20] IETF RFC 2616 (1999): "Hypertext Transfer Protocol -- HTTP/1.1".
- [21] IETF RFC 5280 (2008): "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".
- [22] IETF RFC 3376 (2002): "Internet Group Management Protocol, Version 3".
- [23] IETF RFC 4131 (2005): "Management Information Base for Data Over Cable Service Interface Specification (DOCSIS) Cable Modems and Cable Modem Termination Systems for Baseline Privacy Plus".
- [24] RSA Laboratories PKCS #1 (Version 1.5 - November 1993): "RSA Encryption Standard".

- [25] RSA Laboratories PKCS #1 (Version 2.0 - October 1999): "RSA Cryptography Standard".
- [26] ANSI/SCTE 22-2 (2007): "Data-Over-Cable Service Interface Specification DOCSIS 1.0 Baseline Privacy Interface (BPI)".
- [27] ANSI/SCTE 52 (2008): "Data Encryption Standard - Cipher Block Chaining Packet Encryption Specification".
- [28] ITU-T Recommendation X.509 (2008): "Information technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks".
- [29] ITU-T Recommendation X.690 (2008) | 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)".
- [30] IETF RFC 4388: "Dynamic Host Configuration Protocol (DHCP) Leasequery".
- [31] IETF RFC 5007: "DHCPv6 Leasequery".
- [32] IETF RFC 4994: "DHCPv6 Relay Agent Echo Request Option".

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

- [i.1] Cable Television Laboratories, Inc. CM-SP-CMCIv3.0-I01-080320 (March 2008): "Data-Over-Cable Service Interface Specifications, Cable Modem to Customer Premise Equipment, Interface Specification".
- [i.2] ISO 3166-1: "Codes for the representation of names of countries and their subdivisions -- Part 1: Country codes".
- [i.3] IETF RFC 1750 (December 1994): "Randomness Recommendations for Security", D. Eastlake 3rd, S. Crocker, J. Schiller.
- [i.4] IETF RFC 2202 (September 1997): "Test Cases for HMAC-MD5 and HMAC-SHA-1", P. Cheng, R. Glenn.
- [i.5] IETF RFC 3550/STD0064 (July 2003): "RTP: A Transport Protocol for Real-Time Applications", H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson.
- [i.6] RSA Laboratories (November 1993): "Some Examples of the PKCS Standards", RSA Data Security, Inc., Bedford, MA.
- [i.7] Secure Electronic Transaction (SET) Specification Book 2 (Version 1.0 - May 1997): "Programmer's Guide".
- [i.8] ITU-T Recommendation X.680 (July 2002): "Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation".
- [i.9] ETSI EN 302 878-1: "Access, Terminals, Transmission and Multiplexing (ATTM); Third Generation Transmission Systems for Interactive Cable Television Services - IP Cable Modems; Part 1: General; DOCSIS 3.0".
- [i.10] IEEE 802.3: "Ethernet Working Group".