

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

[ETSI EN 302 878-5 V1.1.1 \(2011-11\)](https://standards.iteh.ai/catalog/standards/etsi/17056ac2-4992-4496-be35-e9cfb4cb9bd8/etsi-en-302-878-5-v1-1-1-2011-11)

<https://standards.iteh.ai/catalog/standards/etsi/17056ac2-4992-4496-be35-e9cfb4cb9bd8/etsi-en-302-878-5-v1-1-1-2011-11>

Reference

DEN/ATTM-003006-5

Keywordsaccess, 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 Standards
(<https://standards.iteh.ai>)
Document Preview

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.

DECTTM, PLUGTESTSTM, UMTSTM and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPPTM and LTETM 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 Algorithm	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

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 Extensions102

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