

ETSI TS 103 161-9 V1.1.1 (2011-10)



Access, Terminals, Transmission and Multiplexing (ATTM); Integrated Broadband Cable and Television Networks; IPCablecom 1.5; Part 9: Security

[ETSI TS 103 161-9 V1.1.1 \(2011-10\)](https://standards.iteh.ai/catalog/standards/etsi/687b14ac-2011-4636-a7b1-8268cf7f9c2c/etsi-ts-103-161-9-v1-1-1-2011-10)

<https://standards.iteh.ai/catalog/standards/etsi/687b14ac-2011-4636-a7b1-8268cf7f9c2c/etsi-ts-103-161-9-v1-1-1-2011-10>

Reference

DTS/ATTM-003011-9

Keywords

access, broadband, cable, IP, multimedia, PSTN

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

(<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.

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	9
Foreword.....	9
1 Scope and Introduction.....	11
1.1 Scope	11
1.2 Goals	11
1.2.1 Assumptions	11
1.2.2 Requirements	12
2 References	12
2.1 Normative references	12
2.2 Informative references.....	14
3 Definitions and abbreviations.....	14
3.1 Definitions.....	14
3.2 Abbreviations	16
4 Void.....	18
5 Architectural Overview of IPCablecom Security.....	18
5.1 IPCablecom Reference Architecture	18
5.1.1 HFC Network.....	18
5.1.2 Call Management Server	19
5.1.3 Functional Categories	19
5.1.3.1 Device and Service Provisioning	19
5.1.3.2 Dynamic Quality of Service.....	20
5.1.3.3 Billing System Interfaces	20
5.1.3.4 Call Signalling.....	20
5.1.3.5 PSTN Interconnectivity.....	20
5.1.3.6 CODEC Functionality and Media Stream Mapping	20
5.1.3.7 Audio Server Services.....	21
5.1.3.7.1 Media Player Controller (MPC)	21
5.1.3.7.2 Media Player (MP)	21
5.1.3.8 Lawful Interception	21
5.2 Threats.....	21
5.2.1 Theft of Network Services.....	23
5.2.1.1 MTA Clones.....	23
5.2.1.2 Other Clones	23
5.2.1.3 Subscription Fraud	23
5.2.1.4 Non-Payment for Voice Communications Services.....	23
5.2.1.5 Protocol Attacks against an MTA	23
5.2.1.6 Protocol Attacks against Other Network Elements	24
5.2.1.7 Theft of Services Provided by the MTA	24
5.2.1.7.1 Attacks.....	24
5.2.1.8 MTA Moved to Another Network	24
5.2.2 Bearer Channel Information Threats.....	24
5.2.2.1 Attacks	24
5.2.2.1.1 Off-line Cryptanalysis	24
5.2.3 Signalling Channel Information Threats.....	24
5.2.3.1 Attacks	24
5.2.3.1.1 Caller ID	25
5.2.3.1.2 Information with Marketing Value	25
5.2.4 Service Disruption Threats	25
5.2.4.1 Attacks	25
5.2.4.1.1 Remote Interference	25
5.2.5 Repudiation.....	25
5.2.6 Threat Summary	26
5.2.6.1 Primary Threats.....	26

5.2.6.2	Secondary Threats	27
5.3	Security Architecture	27
5.3.1	Overview of Security Interfaces	27
5.3.2	Security Assumptions	30
5.3.2.1	BPI+ CMTS Downstream Messages Are Trusted.....	30
5.3.2.2	Non-Repudiation Not Supported.....	30
5.3.2.3	Root Private Key Compromise Protection	30
5.3.2.4	Limited Prevention of Denial-of-Service Attacks	31
5.3.3	Susceptibility of Network Elements to Attack.....	31
5.3.3.1	Managed IP Network	31
5.3.3.2	MTA.....	31
5.3.3.3	CMTS.....	32
5.3.3.4	Voice Communications Network Servers are Untrusted Network Elements	32
5.3.3.4.1	CMS	32
5.3.3.4.2	RKS	33
5.3.3.4.3	OSS, DHCP and TFTP Servers	33
5.3.3.5	PSTN Gateways	34
5.3.3.5.1	Media Gateway.....	34
5.3.3.5.2	Signalling Gateway	34
6	Security Mechanisms	34
6.1	IPsec	34
6.1.1	Overview	34
6.1.2	IPCablecom Profile for IPsec ESP (Transport Mode)	35
6.1.2.1	IPsec ESP Transform Identifiers	35
6.1.2.2	IPsec ESP Authentication Algorithms	35
6.1.2.3	Replay Protection.....	36
6.1.2.4	Key Management Requirements	36
6.2	Internet Key Exchange (IKE).....	36
6.2.1	Overview	36
6.2.2	IPCablecom Profile for IKE.....	37
6.2.2.1	First IKE Phase	37
6.2.2.1.1	IKE Authentication with Signatures	37
6.2.2.1.2	IKE Authentication with Public-Key Encryption.....	37
6.2.2.1.3	IKE Authentication with Pre-Shared Keys.....	37
6.2.2.2	Second IKE Phase	37
6.2.2.3	Encryption Algorithms for IKE Exchanges	37
6.2.2.4	Diffie-Hellman Groups	38
6.2.2.5	Security Association Renegotiation	38
6.3	SNMPv3	38
6.3.1	SNMPv3 Transform Identifiers	38
6.3.2	SNMPv3 Authentication Algorithms.....	38
6.4	Kerberos / PKINIT	39
6.4.1	Overview	39
6.4.1.1	Kerberos Ticket Storage.....	41
6.4.2	PKINIT Exchange	41
6.4.2.1	PKINIT Profile for IPCablecom	43
6.4.2.1.1	PKINIT Request	43
6.4.2.1.2	PKINIT Reply	45
6.4.2.1.3	Pre-Authenticator for Provisioning Server Location.....	47
6.4.2.2	Profile for the Kerberos AS Request / AS Reply Messages.....	47
6.4.2.3	Profile for Kerberos Tickets.....	48
6.4.3	Symmetric Key AS Request / AS Reply Exchange	48
6.4.3.1	Profile for the Symmetric Key AS Request / AS Reply Exchanges.....	50
6.4.4	Kerberos TGS Request / TGS Reply Exchange.....	51
6.4.4.1	TGS Request Profile	52
6.4.4.2	TGS Reply Profile.....	52
6.4.4.3	Error Reply.....	52
6.4.5	Kerberos Server Locations and Naming Conventions	53
6.4.5.1	Kerberos Realms	53
6.4.5.2	KDC	53
6.4.5.3	CMS	54

6.4.5.4	Provisioning Server	54
6.4.5.5	Names of Other Kerberized Services	55
6.4.6	MTA Principal Names	56
6.4.7	Mapping of MTA MAC Address to MTA FQDN	56
6.4.7.1	MTA FQDN Request	56
6.4.7.2	MTA FQDN Reply	58
6.4.7.3	MTA FQDN Error	59
6.4.8	Server Key Management Time Out Procedure	60
6.4.9	Service Key Versioning	61
6.5	Kerberized Key Management	61
6.5.1	Overview	61
6.5.2	Kerberized Key Management Messages	62
6.5.2.1	Rekey Messages	66
6.5.2.2	IPCablecom Profile for KRB_AP_REQ / KRB_AP_REP Messages	69
6.5.2.3	Error Handling	69
6.5.2.3.1	Error Reply	69
6.5.2.3.2	Clock Skew Error	70
6.5.2.3.3	Handling Ticket Errors After a Wake Up	71
6.5.3	Kerberized IPsec	71
6.5.3.1	Derivation of IPsec Keys	72
6.5.3.2	Periodic Re-establishment of IPsec Security Associations	72
6.5.3.2.1	Periodic Re-establishment of IPsec SAs at the Client	72
6.5.3.2.2	Periodic Re-establishment of IPsec SAs at the Application Server	73
6.5.3.3	Expiration of IPsec SAs	73
6.5.3.4	Initial Establishment of IPsec SAs	73
6.5.3.5	On-demand Establishment of IPsec SAs	74
6.5.3.5.1	Client Loses an Outgoing IPsec SA	74
6.5.3.5.2	Client Loses an Incoming IPsec SA	74
6.5.3.5.3	Application Server Loses an Outgoing IPsec SA	74
6.5.3.5.4	Application Server Loses an Incoming IPsec SA	75
6.5.3.6	IPsec-Specific Errors Returned in KRB_ERROR	75
6.5.4	Kerberized SNMPv3	76
6.5.4.1	Derivation of SNMPv3 Keys	76
6.5.4.2	Periodic Re-establishment of SNMPv3 Keys	77
6.5.4.3	Expiration of SNMPv3 Keys	77
6.5.4.4	Initial Establishment of SNMPv3 Keys	77
6.5.4.5	Error Recovery	77
6.5.4.5.1	SNMP Agent Wishes to Send with Missing SNMPv3 Keys	77
6.5.4.5.2	SNMP Agent Receives with Missing SNMPv3 Keys	77
6.5.4.5.3	SNMP Manager Wishes to Send with Missing SNMPv3 Keys	77
6.5.4.6	SNMPv3-Specific Errors Returned in KRB_ERROR	78
6.6	End-to-End Security for RTP	78
6.7	End-to-End Security for RTCP	79
6.8	BPI+	80
6.9	TLS	81
6.9.1	Overview	81
6.9.2	IPCablecom Profile for TLS with SIP	81
6.9.2.1	TLS Ciphersuites	81
6.9.2.2	IPCablecom TLS Certificates	81
6.9.2.3	Connection Persistence and Re-Use	82
6.9.2.4	Session Caching	82
7	Security Profile	82
7.1	Device and Service Provisioning	83
7.1.1	Device Provisioning	85
7.1.1.1	Security Services	86
7.1.1.1.1	MTA-DHCP Server	86
7.1.1.1.2	MTA-SNMP Manager	86
7.1.1.1.3	MTA-Provisioning Server, via TFTP Server	87
7.1.1.2	Cryptographic Mechanisms	87
7.1.1.2.1	Call Flows MTA-15, 16, 17: MTA-SNMP Manager: SNMP Inform/Get Requests/Responses	87
7.1.1.2.2	Call Flow MTA-18: Provisioning Server-TFTP Server: Create MTA Config File	87

7.1.1.2.3	Call Flows MTA-19, 20 and 21: Establish TFTP Server Location	88
7.1.1.2.4	Call Flows MTA-22, 23: MTA-TFTP Server: TFTP Get/Get Response.....	88
7.1.1.2.5	Security Flows	88
7.1.1.3	Key Management	91
7.1.1.3.1	MTA - SNMP Manager	91
7.1.1.3.2	MTA - TFTP Server	91
7.1.1.4	MTA Embedded Keys.....	91
7.1.1.5	Summary Security Profile Matrix - Device Provisioning	91
7.1.2	Subscriber Enrolment	92
7.2	Quality of Service (QoS) Signalling.....	93
7.2.1	Dynamic Quality of Service (DQoS).....	93
7.2.1.1	Reference architecture for embedded MTAs	93
7.2.1.2	Security Services.....	93
7.2.1.2.1	CM-CMTS DOCSIS® 1.1 QoS Messages	93
7.2.1.2.2	Gate Controller - CMTS COPS Messages.....	93
7.2.1.3	Cryptographic Mechanisms.....	93
7.2.1.3.1	CM-CMTS DOCSIS® 1.1 QoS Messages	93
7.2.1.3.2	Gate Controller - CMTS COPS Messages.....	94
7.2.1.4	Key Management	94
7.2.1.4.1	Gate Controller - CMTS COPS Messages.....	94
7.2.1.4.2	Security Profile Matrix Summary.....	94
7.3	Billing System Interfaces	95
7.3.1	Security Services	95
7.3.1.1	CMS-RKS Interface	95
7.3.1.2	CMTS-RKS Interface.....	95
7.3.1.3	MGC - RKS Interface	95
7.3.2	Cryptographic Mechanisms	95
7.3.2.1	RADIUS Server Chaining.....	95
7.3.3	Key Management	96
7.3.3.1	Key CMS - RKS Interface	96
7.3.3.2	CMTS - RKS Interface.....	96
7.3.3.3	MGC - RKS Interface	96
7.3.4	Billing System Summary Security Profile Matrix	97
7.4	Call Signalling.....	97
7.4.1	Network Call Signalling (NCS).....	97
7.4.1.1	Reference Architecture.....	97
7.4.1.2	Security Services.....	98
7.4.1.3	Cryptographic Mechanisms.....	98
7.4.1.3.1	MTA-CMS Interface	98
7.4.1.3.2	CMS-CMS, CMS-MGC, CMS-SIP Proxy and SIP Proxy - SIP Proxy Interfaces	98
7.4.1.4	Key Management	99
7.4.1.4.1	MTA-CMS Key Management	99
7.4.1.4.2	CMS-CMS, CMS-MGC, CMS-SIP Proxy, SIP Proxy-SIP Proxy Key Management	101
7.4.2	Call Signalling Security Profile Matrix	102
7.5	PSTN Gateway Interface.....	103
7.5.1	Reference Architecture	103
7.5.1.1	Media Gateway Controller.....	103
7.5.1.2	Media Gateway	103
7.5.1.3	Signalling Gateway	103
7.5.2	Security Services	103
7.5.2.1	MGC - MG Interface.....	103
7.5.3	Cryptographic Mechanisms	103
7.5.3.1	MGC - MG Interface.....	103
7.5.4	Key Management	104
7.5.4.1	MGC - MG Interface.....	104
7.5.5	MGC-MG Summary Security Profile Matrix	104
7.6	Media Stream	104
7.6.1	Security Services	104
7.6.1.1	RTP.....	104
7.6.1.2	RTCP.....	105
7.6.2	Cryptographic Mechanisms	105
7.6.2.1	RTP Messages.....	105

7.6.2.1.1	RTP Timestamp	107
7.6.2.1.2	Packet Encoding Requirements	107
7.6.2.1.3	Packet Decoding Requirements	109
7.6.2.2	RTCP Messages	110
7.6.2.2.1	RTCP Format	110
7.6.2.2.2	RTCP Encryption	110
7.6.2.2.3	Sequence Numbers	111
7.6.2.2.4	Block Termination.....	111
7.6.2.2.5	RTCP Message Encoding.....	111
7.6.2.2.6	RTCP Message Decoding.....	111
7.6.2.3	Key Management	112
7.6.2.3.1	Key Management over NCS	112
7.6.2.3.2	Ciphersuite Format	121
7.6.2.3.3	Derivation of End-to-End Keys	121
7.6.2.4	RTP-RTCP Summary Security Profile Matrix.....	122
7.7	Audio Server Services	122
7.7.1	Reference Architecture	122
7.7.2	Security Services	123
7.7.2.1	MTA-CMS NCS Signalling (Ann-1)	123
7.7.2.2	MPC-MP Signalling (Ann-2).....	124
7.7.2.3	MTA-MP (Ann-4).....	124
7.7.3	Cryptographic Mechanisms	124
7.7.3.1	MTA-CMS NCS Signalling (Ann-1)	124
7.7.3.2	MPC-MP Signalling (Ann-2).....	124
7.7.3.3	MTA-MP (Ann-4).....	124
7.7.4	Key Management.....	124
7.7.4.1	MTA-CMS NCS Signalling (Ann-1)	124
7.7.4.2	MPC-MP Signalling (Ann-2).....	124
7.7.4.3	MTA-MP (Ann-4).....	124
7.7.5	MPC-MP Summary Security Profile Matrix	125
7.8	Lawful Interception Interfaces	125
7.8.1	Reference Architecture	125
7.8.2	Security Services	126
7.8.2.1	Event Interfaces CMS-DF, MGC-DF, CMTS-DF and DF-DF	126
7.8.2.2	Call Content Interfaces CMTS-DF, MG-DF, MG-DF and DF-DF	126
7.8.3	Cryptographic Mechanisms	126
7.8.3.1	Interface between CMS and DF	126
7.8.3.2	Interface between CMTS and DF for Event Messages	127
7.8.3.3	Interface between DF and DF for Event Messages	127
7.8.3.4	Interface between MGC and DF	127
7.8.4	Key Management.....	127
7.8.4.1	Interface between CMS and DF	127
7.8.4.2	Interface between CMTS and DF.....	127
7.8.4.3	Interface between DF and DF	127
7.8.4.4	INTERFACE BETWEEN MGC AND DF	128
7.8.5	Lawful Interception Security Profile Matrix.....	128
7.9	CMS Provisioning	129
7.9.1	Reference Architecture	129
7.9.2	Security Services	129
7.9.3	Cryptographic Mechanisms	129
7.9.4	Key Management.....	129
7.9.5	Provisioning Server-CMS Summary Security Profile Matrix.....	129
8	IPCom Certificates.....	130
8.1	Generic Structure.....	130
8.1.1	Version.....	130
8.1.2	Public Key Type	130
8.1.3	Extensions.....	130
8.1.3.1	subjectKeyIdentifier	130
8.1.3.2	authorityKeyIdentifier.....	130
8.1.3.3	KeyUsage	130
8.1.3.4	BasicConstraints.....	130