



***Society of Cable
Telecommunications
Engineers***

**ENGINEERING COMMITTEE
Data Standards Subcommittee**

AMERICAN NATIONAL STANDARD

ANSI/SCTE 24-10 2016

IPCablecom 1.0 Part 10: Security Specification

NOTICE

The Society of Cable Telecommunications Engineers (SCTE) Standards and Operational Practices (hereafter called “documents”) are intended to serve the public interest by providing specifications, test methods and procedures that promote uniformity of product, interchangeability, best practices and ultimately the long term reliability of broadband communications facilities. These documents shall not in any way preclude any member or non-member of SCTE from manufacturing or selling products not conforming to such documents, nor shall the existence of such standards preclude their voluntary use by those other than SCTE members.

SCTE assumes no obligations or liability whatsoever to any party who may adopt the documents. Such adopting party assumes all risks associated with adoption of these documents, and accepts full responsibility for any damage and/or claims arising from the adoption of such documents.

Attention is called to the possibility that implementation of this document may require the use of subject matter covered by patent rights. By publication of this document, no position is taken with respect to the existence or validity of any patent rights in connection therewith. If a patent holder has filed a statement of willingness to grant a license under these rights on reasonable and nondiscriminatory terms and conditions to applicants desiring to obtain such a license, then details may be obtained from the standards developer. SCTE shall not be responsible for identifying patents for which a license may be required or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

Patent holders who believe that they hold patents which are essential to the implementation of this document have been requested to provide information about those patents and any related licensing terms and conditions. Any such declarations made before or after publication of this document are available on the SCTE web site at <http://www.scte.org>.

All Rights Reserved

© Society of Cable Telecommunications Engineers, Inc. 2016
140 Philips Road
Exton, PA 19341

Note: DOCSIS® is a registered trademark of Cable Television Laboratories, Inc., and is used in this document with permission.

Table of Contents

1	SCOPE AND INTRODUCTION	7
1.1	PURPOSE	7
1.2	SCOPE	7
1.2.1	Goals	8
1.2.2	Assumptions	8
1.2.3	Prerequisite	8
1.3	REQUIREMENTS AND CONVENTIONS	8
1.4	DOCUMENT OVERVIEW	9
2	REFERENCES	10
2.1	NORMATIVE REFERENCES	10
2.2	INFORMATIVE REFERENCES	12
3	TERMS AND DEFINITIONS	13
4	ABBREVIATIONS AND ACRONYMS	17
5	ARCHITECTURAL OVERVIEW OF IPCABLECOM SECURITY	24
5.1	IPCABLECOM REFERENCE ARCHITECTURE	24
5.1.1	HFC Network	24
5.1.2	Call Management Server	24
5.1.3	Functional Categories	25
5.2	THREATS	26
5.2.1	Theft of Network Services	28
5.2.2	Bearer Channel Information Threats	29
5.2.3	Signaling Channel Information Threats	29
5.2.4	Service Disruption Threats	30
5.2.5	Repudiation	30
5.2.6	Threat Summary	31
5.3	SECURITY ARCHITECTURE	32
5.3.1	Overview of Security Interfaces	32
5.3.2	Security Assumptions	35
5.3.3	Susceptibility of Network Elements to Attack	36
6	SECURITY MECHANISMS	40
6.1	IPSEC	40
6.1.1	Overview	40
6.1.2	IPCablecom Profile for IPsec ESP (Transport Mode)	40
6.2	INTERNET KEY EXCHANGE (IKE)	42
6.2.1	Overview	42
6.2.2	IPCablecom Profile for IKE	42
6.3	SNMPv3	43
6.3.1	SNMPv3 Transform Identifiers	44
6.3.2	SNMPv3 Authentication Algorithms	44
6.4	KERBEROS / PKINIT	44
6.4.1	Overview	44
6.4.2	PKINIT Exchange	47
6.4.3	Symmetric Key AS Request / AS Reply Exchange	54
6.4.4	Kerberos TGS Request / TGS Reply Exchange	57
6.4.5	Kerberos Server Locations and Naming Conventions	59
6.4.6	MTA Principal Names	62

6.4.7	Mapping of MTA MAC Address to MTA FQDN.....	62
6.4.8	Server Key Management Time Out Procedure.....	66
6.4.9	Service Key Versioning	67
6.4.10	Kerberos Cross-Realm Operation.....	67
6.5	KERBERIZED KEY MANAGEMENT	68
6.5.1	Overview	68
6.5.2	Kerberized Key Management Messages.....	68
6.5.3	Kerberized IPsec	78
6.5.4	Kerberized SNMPv3.....	83
6.6	END-TO-END SECURITY FOR RTP	86
6.7	END-TO-END SECURITY FOR RTCP.....	87
6.8	BPI+	88
7	SECURITY PROFILE.....	89
7.1	DEVICE AND SERVICE PROVISIONING.....	90
7.1.1	Device Provisioning	93
7.1.2	Subscriber Enrollment	99
7.2	QUALITY OF SERVICE (QoS) SIGNALING	100
7.2.1	Dynamic Quality of Service (DQoS)	100
7.3	BILLING SYSTEM INTERFACES.....	102
7.3.1	Security Services.....	102
7.3.2	Cryptographic Mechanisms	102
7.3.3	Key Management.....	103
7.3.4	Billing System Summary Security Profile Matrix	104
7.4	CALL SIGNALING	104
7.4.1	Network Call Signaling (NCS)	104
7.4.2	Call Signaling Security Profile Matrix.....	108
7.5	PSTN GATEWAY INTERFACE	108
7.5.1	Reference Architecture	108
7.5.2	Security Services.....	109
7.5.3	Cryptographic Mechanisms	109
7.5.4	Key Management.....	110
7.5.5	MGC-MG-CMS-SG Summary Security Profile Matrix	110
7.6	MEDIA STREAM.....	110
7.6.1	Security Services.....	110
7.6.2	Cryptographic Mechanisms	111
7.7	AUDIO SERVER SERVICES.....	129
7.8	ELECTRONIC SURVEILLANCE INTERFACES.....	129
7.9	CMS PROVISIONING	129
8	IPCABLECOM CERTIFICATES.....	130
8.1	GENERIC STRUCTURE.....	130
8.1.1	Version	130
8.1.2	Public Key Type	130
8.1.3	Extensions	130
8.1.4	Signature Algorithm.....	130
8.1.5	SubjectName and IssuerName	130
8.1.6	Certificate Profile Notation	131
8.2	CERTIFICATE TRUST HIERARCHY	131
8.2.1	Certificate Validation	131
8.2.2	MTA Device Certificate Hierarchy	132
8.2.3	CableLabs Service Provider Certificate Hierarchy	134
8.2.4	Certificate Revocation.....	139

9	CRYPTOGRAPHIC ALGORITHMS	140
9.1	AES	140
9.2	DES	140
9.2.1	XDESX	140
9.2.2	DES-CBC-PAD	140
9.2.3	3DES-EDE	140
9.3	BLOCK TERMINATION	141
9.4	RSA SIGNATURE	145
9.5	HMAC-SHA1	145
9.6	KEY DERIVATION	146
9.7	THE MMH-MAC	146
9.7.1	The MMH Function	146
9.7.2	The MMH-MAC	148
9.8	RANDOM NUMBER GENERATION	148
10	PHYSICAL SECURITY	149
10.1	PROTECTION FOR MTA KEY STORAGE	149
10.2	MTA KEY ENCAPSULATION	151
11	SECURE SOFTWARE DOWNLOAD	152
APPENDIX I	IPCABLECOM ADMIN GUIDELINES & BEST PRACTICES (INFORMATIVE)	153
I.1	ROUTINE CMS SERVICE KEY REFRESH	153
APPENDIX II	KERBEROS NETWORK AUTHENTICATION SERVICE (NORMATIVE)	154
APPENDIX III	PKINIT SPECIFICATION	247
APPENDIX IV	PKCROSS SPECIFICATION	266
APPENDIX V	EXAMPLE OF MMH ALGORITHM IMPLEMENTATION (INFORMATIVE)	267
APPENDIX VI	OAKLEY GROUPS	272

List of Figures

FIGURE 1.	IPCABLECOM SINGLE ZONE ARCHITECTURE	24
FIGURE 2.	IPCABLECOM SECURED INTERFACES	27
FIGURE 3.	IPCABLECOM SECURITY INTERFACES WITH KEY-MANAGEMENT	33
FIGURE 4.	KERBEROS-BASED KEY MANAGEMENT FOR IPSEC	46
FIGURE 5.	PKINIT EXCHANGE	48
FIGURE 6.	SYMMETRIC-KEY AS REQUEST / AS REPLY EXCHANGE	56
FIGURE 7.	KERBEROS TGS REQUEST / TGS REPLY EXCHANGE	57
FIGURE 8.	KERBEROS AP REQUEST / AP REPLY EXCHANGE	69
FIGURE 9.	REKEY MESSAGE TO ESTABLISH A SECURITY PARAMETER	74
FIGURE 10.	IPCABLECOM PROVISIONING FLOWS	91
FIGURE 11.	QoS SIGNALING INTERFACES IN IPCABLECOM NETWORK	100
FIGURE 12.	NCS REFERENCE ARCHITECTURE	105
FIGURE 13.	KEY MANAGEMENT FOR NCS CLUSTERS	107
FIGURE 14.	RTP PACKET HEADER FORMAT	112
FIGURE 15.	FORMAT OF ENCODED RTP PACKET	112
FIGURE 16.	RTP PACKET PROFILE CHARACTERISTICS	114

FIGURE 17. RTCP PACKET FORMAT	117
FIGURE 18. RTCP ENCRYPTED PACKET FORMAT	117
FIGURE 19. END-END SECRET DISTRIBUTION OVER NCS	120
FIGURE 20. IPCABLECOM CERTIFICATE HIERARCHY	131
FIGURE 21. CBC MODE	141
FIGURE 22. CBC PAD MODE	142
FIGURE 23. DESX-XEX AS BLOCK CIPHER.....	143
FIGURE 24. 3DES-EDE AS BLOCK CIPHER.....	144
FIGURE 25. CBC WITH RESIDUAL BLOCK TERMINATION	145

List of Tables

TABLE 1. IPCABLECOM SECURITY INTERFACES TABLE	34
TABLE 2. IPSEC ESP TRANSFORM IDENTIFIERS	41
TABLE 3. IPSEC AUTHENTICATION ALGORITHMS	41
TABLE 4. SNMPV3 TRANSFORM IDENTIFIERS	44
TABLE 5. SNMPV3 AUTHENTICATION ALGORITHMS	44
TABLE 6. MTA FQDN REQUEST FORMAT.....	63
TABLE 7. KRB_SAFE FORMAT	63
TABLE 8. MTA FQDN FORMAT	64
TABLE 9. KRB_SAFE DATA FORMAT	64
TABLE 10. MAPPING OF KRB_MTAMAP_ERR TO KRB_ERR	66
TABLE 11. SAMPLE IPSEC SECURITY POLICY DATABASE ENTRIES FOR NCS SIGNALING BETWEEN MTA AND CMS	79
TABLE 12. REQUIRED FORMAT FOR DATA IN THE AP REQUEST	83
TABLE 13. REQUIRED FORMAT FOR DATA IN THE AP REPLY	84
TABLE 14. RTP PACKET TRANSFORM IDENTIFIERS.....	86
TABLE 15. RTP IPCABLECOM AUTHENTICATION ALGORITHMS	87
TABLE 16. RTCP PACKET TRANSFORM IDENTIFIERS	87
TABLE 17. RTCP AUTHENTICATION ALGORITHMS.....	87
TABLE 18. RTP – RTCP SECURITY PROFILE MATRIX	89
TABLE 19. KERBEROS KEY MANAGEMENT DURING MTA PROVISIONING.....	92
TABLE 20. POST-MTA PROVISIONING SECURITY FLOWS.....	96
TABLE 21. SECURITY PROFILE MATRIX – MTA DEVICE PROVISIONING	99
TABLE 22. SECURITY PROFILE MATRIX – DQoS.....	102
TABLE 23. SECURITY PROFILE MATRIX – RADIUS	104
TABLE 24. SECURITY PROFILE MATRIX – NETWORK CALL SIGNALING	108
TABLE 25. SECURITY PROFILE MATRIX – TCAP/IP AND TGCP	110
TABLE 26. SECURITY PROFILE MATRIX – RTP & RTCP	129
TABLE 27. MTA ROOT CERTIFICATE.....	132
TABLE 28. MTA MANUFACTURER CERTIFICATE.....	133
TABLE 29. MTA DEVICE CERTIFICATE.....	134
TABLE 30. CABLELABS SERVICE PROVIDER ROOT CERTIFICATE.....	135
TABLE 31. SERVICE PROVIDER CA CERTIFICATE	136
TABLE 32. LOCAL SYSTEM CA CERTIFICATE.....	137
TABLE 33. KEY DISTRIBUTION CENTER CERTIFICATE.....	137
TABLE 34. IPCABLECOM SERVER CERTIFICATES	138

1 SCOPE AND INTRODUCTION

1.1 Purpose

IPCablecom is a project aimed at identifying, qualifying, and supporting packet-based voice and video products over cable systems. These products represent new classes of services utilizing cable-based packet communication networks. New service classes in the near term include voice communications and videoconferencing over cable networks and the Internet.

IPCablecom is a set of protocols and associated element functional requirements developed to provide the capability to deliver Quality-of-Service (QoS) enhanced secure communications services using packetized data transmission technology to a consumer's home over the cable television Hybrid Fiber/Coax (HFC) data network. IPCablecom utilizes a network superstructure that overlays the two-way data-ready cable television network. While the initial service offerings in the IPCablecom product line are anticipated to be Packet Voice and Packet Video, the long-term project vision encompasses a large family of packet-based services.

The purpose of any security technology is to protect items of value, whether a revenue stream, or a purchasable information asset of some type. Threats to this revenue stream exist when a user of the network perceives the value, expends effort and money, and invents a technique to get around the necessary payments. Some network users will go to extreme lengths to steal when they perceive extreme value. The addition of security technology to protect value has an associated cost; the more expended, the more secure one can be. The proper engineering task is to employ a reasonable costing security technology to force any user with the intent to steal or disrupt network services to spend an unreasonable amount of money to circumvent it. Security effectiveness is thus basic economics.

In addition, an IPCablecom network used to offer voice communications must be at least as secure as the Public Switched Telephone Network (PSTN) networks are today. Much of the PSTN security depends on the fact that each telephone is connected to a dedicated line. In order to provide the same level of privacy and resistance to denial-of-service attacks when an IPCablecom IP network is used for voice communications, appropriate cryptography-based security mechanisms have been specified. This secures both voice and signaling data transmitted over a shared HFC network and over a shared IP backbone.

1.2 Scope

The scope of this document is to define the IPCablecom Security architecture, protocols, algorithms, associated functional requirements and any technological requirements that can provide for the security of the system for the IPCablecom network. Authentication, access control, signaling and media content integrity, confidentiality, and non-repudiation security services must be provided as defined herein for each of the network element interfaces.

IPCablecom security spans the entire IPCablecom architecture. The IPCablecom Architecture Technical Report [1] defines the overall IPCablecom architecture, as well as the system elements, interfaces, and functional requirements for the entire IPCablecom network.

From time to time this document refers to the voice communications capabilities of an IPCablecom network in terms of "IP Telephony." The legal/regulatory classification of IP-based voice communications provided over cable networks and otherwise, and the legal/regulatory obligations, if any, borne by providers of such voice communications, are not yet fully defined by appropriate legal and regulatory authorities. Nothing in this specification is addressed to, or intended to affect, those issues.

In particular, while this document uses standard terms such as "call," "call signaling," telephony," etc., it should be recalled that while an IPCablecom network performs activities analogous to these PSTN functions, the manner by which it does so differs considerably from the manner in which they are performed in the PSTN by telecommunications carriers, and that these differences may be significant for legal/regulatory purposes. Moreover, while reference is made here to "IP Telephony," it should be recognized that this term embraces a number of different technologies and network architectures, each with different potential associated legal/regulatory obligations. No particular legal/regulatory consequences are assumed or implied by the use of this term. This specification makes use of existing standards wherever possible. Whenever there is an existing standard used in the definition of any requirement in this specification, the related existing standard will be referenced. When there are

options defined with respect to the existing standards, this specification will explicitly define the options within the existing standard that are supported.

1.2.1 Goals

This standard describes the security relationships between the elements on the IPCablecom network. The general goals of the IPCablecom network security specification and any implementations that encompass the requirements defined herein should be:

- **Secure network communications:** The IPCablecom network security must define a security architecture, methods, algorithms and protocols that meet the stated security service requirement. All media packets and all sensitive signaling communication across the network must be safe from eavesdropping. Unauthorized message modification, insertion, deletion and replays anywhere in the network must be easily detectable and must not affect proper network operation.
- **Reasonable cost:** The IPCablecom network security must define security methods, algorithms and protocols that meet the stated security service requirements such that a reasonable implementation can be manifested with reasonable cost and implementation complexity.
- **Network element interoperability:** All of the security services for any of the IPCablecom network elements must inter-operate with the security services for all of the other IPCablecom network elements. Multiple vendors may implement each of the IPCablecom network elements as well as multiple vendors for a single IPCablecom network element.
- **Extensibility:** The IPCablecom security architecture, methods, algorithms and protocols must provide a framework into which new security methods and algorithms may be incorporated as necessary.

1.2.2 Assumptions

The following assumptions are made relative to the current scope of the IPCablecom Security Specification:

- Embedded Multimedia Terminal Adapters (E-MTAs) and Standalone Multimedia Terminal Adapters (S-MTAs) are within the scope of this specification.
- NCS is the only call signaling method, on the access network, addressed in this specification.
- This version of the IPCablecom Security Specification specifies security for a single administrative domain and the communications between domains.
- Security for chained RADIUS servers is not currently in the scope.
- The IPCablecom Security Specification does not have a requirement for exportability outside the United States; exportability of encryption algorithms is not addressed in this specification.
- This specification also does not include requirements for associated security operational issues (e.g., site security), back-office or inter/intra back-office security, service authorization policies or secure database handling. Record Keeping Servers (RKS), Network Management Systems, File Transfer Protocol (FTP) servers and Dynamic Host Configuration Protocol (DHCP) servers are all considered to be unique to any service provider's implementation and are beyond the scope of this standard.

1.2.3 Prerequisite

The following requirement is made relative to the current scope of the IPCablecom Security Specification:

- All E-MTAs must use DOCSIS 1.1-compliant cable modems and must implement BPI+ [9].

1.3 Requirements and Conventions

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

“MUST”	This word or the adjective “REQUIRED” 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 or the adjective “RECOMMENDED” 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 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.
“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.

The legal/regulatory classification of IP-based voice communications provided over cable networks and otherwise, and the legal/regulatory obligations, if any, borne by providers of such voice communications, are not yet fully defined by appropriate legal and regulatory authorities. Nothing in this specification is addressed to, or intended to affect, those issues. In particular, while this document uses standard terms such as "call," "call signaling," "telephony," etc., it will be evident from this document that while a Packet-Cable network performs activities analogous to these PSTN functions, the manner by which it does so differs considerably from the manner in which they are performed in the PSTN by telecommunications carriers. These differences may be significant for legal/regulatory purposes.

1.4 Document Overview

This standard covers security for the entire IPCablecom architecture. This specification describes the IPCablecom architecture, identifies security risks and specifies mechanisms to secure the architecture. The document is structured as follows:

- Architectural Overview of IPCablecom. The initial section describes the IPCablecom architecture as a point of reference for the remainder of the document. Refer to the IPCablecom 1.0 Architecture [1] and each individual specification for full details.
- Security Threats are described in the context of the reference architecture.
- The overall security architecture and security assumptions are described.
- Security Mechanisms. This section specifies how public domain security mechanisms are to be implemented in IPCablecom including IPsec, Internet Key Exchange (IKE), Kerberos with PKINIT, media stream security, BPI+ and RADIUS.
- Security Profile. This section profiles the security for each major area of the IPCablecom architecture. The profile includes a description of the security requirements as well as the specifications for securing at-risk interfaces. Refer to the individual specifications for details about each IPCablecom interface.
- IPCablecom X.509 Certificate Profile and Management. X.509 Certificates are specified for a number of devices and functions within the IPCablecom architecture. This section describes the format of the Certificates as well as the trust hierarchy for Certificate management within IPCablecom.
- Cryptographic Algorithms. This section specifies the details of cryptographic algorithms specified in the IPCablecom security architecture.
- Physical Security. This section documents assumptions about the physical security of the MTA keys.
- Secure Software Download. This section specifies the secure loading and upgrading of software to the MTAs.

2 REFERENCES

The following documents contain provisions which, through reference in this text, constitute provisions of this standard. At the time of Subcommittee approval, the editions indicated were valid. All documents are subject to revision, and while parties to agreement based on this standard are encouraged to investigate the possibility of applying the most recent editions of the documents listed below, they are reminded that newer editions of those documents might not be compatible with the referenced version.

2.1 Normative References

All references are subject to revision, and users of this document are encouraged to investigate the possibility of applying the most recent editions of the documents listed below.

- [1] ANSI/SCTE 24-01 2016, IPCablecom 1.0 Part 1: Architecture Framework for the Delivery of Time-Critical Services over Cable Television Networks Using Cable Modems.
- [2] ANSI/SCTE 24-03 2016, IPCablecom 1.0 Part 3: Network Call Signaling Protocol for the Delivery of Time-Critical Services over Cable Television Using Data Modems.
- [3] ANSI/SCTE 24-04 2016, IPCablecom 1.0 Part 4: Dynamic Quality of Service for the Provision of Real-Time Services over Cable Television Networks Using Data Modem.
- [4] ANSI/SCTE 24-05 2016, IPCablecom 1.0 Part 5: Media Terminal Adapter (MTA) Device Provisioning Requirements for the Delivery of Real-Time Services over Cable Television Using Cable Modems.
- [5] ANSI/SCTE 24-12 2016, IPCablecom 1.0 Part 12: Trunking Gateway Control Protocol (TGCP).
- [6] ANSI/SCTE 24-09 2016, IPCablecom 1.0 Part 9: Event Message Requirements.
- [7] ANSI/SCTE 24-02 2016, IPCablecom 1.0 Part 2: Audio Codec Requirements for the Provision of Bi-directional Audio Service over Cable Television Networks Using Cable Modems.
- [8] ANSI/SCTE 23-01 2010, DOCSIS 1.1 Part 1: Radio Frequency Interface.
- [9] ANSI/SCTE 23-02 2012, DOCSIS 1.1 Part 2: Baseline Privacy Plus Interface.
- [10] RTP: A Transport Protocol for Real-Time Applications, IETF (H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson), Internet Proposed Standard, RFC 1889, January, 1996.
- [11] HMAC: Keyed-Hashing for Message Authentication, IETF (Krawczyk, Bellare, and Canetti), Internet Proposed Standard, RFC 2104, February 1997.
- [12] Cryptographic Message Syntax, IETF (R. Housley), Internet Proposed Standard, RFC 2630, June 1999.
- [13] RADIUS Accounting, IETF (C. Rigney), Internet Proposed Standard, RFC 2139, April 1997.
- [14] SDP: Session Description Protocol, IETF (M. Handley, V. Jacobson), Internet Proposed Standard, RFC 2327, April 1998.
- [15] Secure Hash Algorithm, Department of Commerce, NIST, FIPS 180-1, April, 1995.
- [16] PKCS#1: RSA Cryptography Specifications Version 2.0, IETF (B. Kaliski, J. Staddon), Internet Informational Standard, RFC 2437, October 1998.
- [17] The TLS Protocol Version 1.0, IETF (T. Dierks, C. Allen), Internet Proposed Standard, RFC 2246, January 1999.
- [18] S. Halevi and H. Krawczyk, "MMH: Software Message Authentication in Gbit/sec Rates," Proceedings of the 4th Workshop on Fast Software Encryption, (1997) vol. 1267 Springer-Verlag, pp. 172-189.
- [19] Security Architecture for the Internet Protocol, IETF (S. Kent, R. Atkinson), Internet Proposed Standard, RFC 2401, November 1998.
- [20] IP Encapsulating Security Payload (ESP), IETF (D. Piper), Internet Proposed Standard, RFC 2406, November 1998.

- [21] The Internet IP Security Domain of Interpretation for ISAKMP, IETF (S. Kent, R. Atkinson), Internet Proposed Standard, RFC 2407, November 1998.
- [22] The ESP CBC-Mode Cipher Algorithms, IETF (R. Pereira, R. Adams), Internet Proposed Standard, RFC 2451, November 1998.
- [23] The Use of HMAC-SHA-1-96 within ESP and AH, IETF (C. Madson, R. Glenn), Internet Proposed Standard, RFC 2404, November 1998.
- [24] The Internet Key Exchange (IKE), IETF (D. Harkins, D. Carrel), Internet Proposed Standard, RFC 2409, November 1998.
- [25] ANSI/SCTE 24-07 2016, IPCablecom 1.0 Part 7: Media Terminal Adapter (MTA) Management Information Base (MIB) Requirements.
- [26] ANSI/SCTE 24-08 2016, IPCablecom 1.0 Part 8: Network Call Signaling Management Information Base (MIB) Requirements.
- [27] User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3), IETF (U. Blumenthal, B. Wijnen), Internet Proposed Standard, RFC 2574, April 1999.
- [28] PF_KEY Key Management API, Version 2, IETF (D. McDonald, C. Metz, B. Phan), Internet Proposed Standard, RFC 2367, July 1998.
- [29] FIPS-81, Federal Information Processing Standards Publication (FIPS PUB) 81, DES Modes of Operation, December 1980.
- [30] RSVP Cryptographic Authentication, IETF (F. Baker, B. Lindell and M. Talwar), Internet Proposed Standard, RFC 2747, January 2000.
- [31] ITU-T Recommendation X.509 (1997 E): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997.
- [32] Internet X.509 Public Key Infrastructure Certificate and CRL Profile, IETF (.R. Housley, W. Ford, W. Polk, D. Solo) Internet Proposed Standard, RFC2459, January 1999.
- [33] FIPS197 Advanced Encryption Standard (AES), Department of Commerce, NIST FIPS197, November 26, 2001.
- [34] ITU-T Recommendation X.690: Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER), December, 1997.
- [35] The Use of HMAC-MD5-96 within ESP and AH, IETF (C. Madson, R. Glenn), Internet Proposed Standard, RFC 2403, November, 1998.
- [36] RFC 2669 DOCSIS Cable Device MIB Cable Device Management Information Base for DOCSIS compliant Cable Modems and Cable Modem Termination Systems, August 1999
- [37] RFC 4131, Management Information Base for DOCSIS Cable Modems and Cable Modem Termination Systems for Baseline Privacy Plus, September 2005, Cable Television Laboratories, Inc.
- [38] RSA Laboratories, PKCS #7, Cryptographic Message Syntax Standard, An RSA Laboratories Technical Note, Version 1.5, Revised November 1, 1993.
- [39] FIPS186-2 Digital Signature Standard, Department of Commerce, NIST FIPS186-2, January 27, 2000.
- [40] Message Processing and Dispatching for the Simple Network Management Protocol (SNMP), IETF (J. Case, D. Harrington, R. Presuhn, B. Wijnen), Internet Proposed Standard, RFC 2572, April 1999.
- [41] Domain Names, Implementation and Specification, IETF (P. Mockapetris), IETF STD13, RFC1035, November 1987.
- [42] A DNS RR for specifying the location of services (DNS SRV), IETF (A. Gulbrandsen, P. Vixie, L. Esibov), Internet Proposed Standard, RFC2782, February 2000.

2.2 Informative References

The following documents may provide valuable information to the reader but are not required when complying with this standard.

- [43] B. Schneier, "Applied Cryptography," John Wiley & Sons Inc, second edition, 1996.
- [44] Randomness Recommendations for Security, Informational RFC (Donald Eastlake, Stephen Crocker and Jeff Schiller) RFC 1750, December 1994.
- [45] How to Protect DES Against Exhaustive Key Search, J. Killian, P. Rogaway, (Edited version presented at Proceedings of Crypto '96), July 1997.
- [46] ReSource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification, IETF (R. Braden, L. Zhang, S. Berson, S. Herzog, S. Jamin), Internet Proposed Standard, RFC 2205, September, 1997.
- [47] FIPS 140-2, Federal Information Processing Standards Publication (FIPS PUB) 140-2, Security Requirements for Cryptographic Modules, May 2000.

3 TERMS AND DEFINITIONS

This standard uses the following terms:

Access Control	Limiting the flow of information from the resources of a system only to authorized persons, programs, processes, or other system resources on a network.
Active	A service flow is said to be "active" when it is permitted to forward data packets. A service flow must first be admitted before it is active.
Admitted	A service flow is said to be "admitted" when the CMTS has reserved resources (e.g., bandwidth) for it on the DOCSIS network.
A-link	A-Links are SS7 links that interconnect STPs and either SSPs or SCPs. 'A' stands for "Access."
Asymmetric Key	An encryption key or a decryption key used in public key cryptography, where encryption and decryption keys are always distinct.
Audio Server	An Audio Server plays informational announcements in IPCablecom network. Media announcements are needed for communications that do not complete and to provide enhanced information services to the user. The component parts of Audio Server services are Media Players and Media Player Controllers.
Authentication	The process of verifying the claimed identity of an entity to another entity.
Authenticity	The ability to ensure that the given information is without modification or forgery and was in fact produced by the entity that claims to have given the information.
Authorization	The act of giving access to a service or device if one has permission to have the access.
Cipher	An algorithm that transforms data between plaintext and ciphertext.
Ciphersuite	A set which must contain both an encryption algorithm and a message authentication algorithm (e.g., a MAC or an HMAC). In general, it may also contain a key-management algorithm, which does not apply in the context of IPCablecom.
Ciphertext	The (encrypted) message output from a cryptographic algorithm that is in a format that is unintelligible.
Cleartext	The original (unencrypted) state of a message or data. Also called plaintext.
Confidentiality	A way to ensure that information is not disclosed to anyone other than the intended parties. Information is encrypted to provide confidentiality. Also known as privacy.
Cryptanalysis	The process of recovering the plaintext of a message or the encryption key without access to the key.
Cryptographic algorithm	An algorithm used to transfer text between plaintext and ciphertext.
Decipherment	A procedure applied to ciphertext to translate it into plaintext.
Decryption	A procedure applied to ciphertext to translate it into plaintext.
Decryption key	The key in the cryptographic algorithm to translate the ciphertext to plaintext.
Digital certificate	A binding between an entity's public key and one or more attributes relating to its identity, also known as a public key certificate.
Digital signature	A data value generated by a public-key algorithm based on the contents of a block of data and a private key, yielding an individualized cryptographic checksum.
Downstream	The direction from the headend toward the subscriber location.
Encipherment	A method used to translate plaintext into ciphertext.
Encryption	A method used to translate plaintext into ciphertext.
Encryption Key	The key used in a cryptographic algorithm to translate the plaintext to ciphertext.
Endpoint	A Terminal, Gateway or Multipoint Conference Unit (MCU).

Errored Second	Any 1-second interval containing at least one bit error.
Event Message	A message capturing a single portion of a connection.
F-link	F-Links are SS7 links that directly connect two SS7 end points, such as two SSPs. 'F' stands for "Fully Associated."
Flow [DOCSIS Flow]	(a.k.a. DOCSIS-QoS "service flow") A unidirectional sequence of packets associated with a Service ID (SID) and a QoS. Multiple multimedia streams may be carried in a single DOCSIS Flow.
Flow [IP Flow]	A unidirectional sequence of packets identified by OSI Layer 3 and Layer 4 header information. This information includes source/destination IP addresses, source/destination port numbers, protocol ID. Multiple multimedia streams may be carried in a single IP Flow.
Gateway	Devices bridging between the IPCablecom IP Voice Communication world and the PSTN. Examples are the Media Gateway, which provides the bearer circuit interfaces to the PSTN and transcodes the media stream, and the Signaling Gateway, which sends and receives circuit switched network signaling to the edge of the IPCablecom network.
H.323	An ITU-T recommendation for transmitting and controlling audio and video information. The H.323 recommendation requires the use of the ITU-T H.225 and ITU-T H.245 protocol for communication control between a "gateway" audio/video endpoint and a "gatekeeper" function.
Header	Protocol control information located at the beginning of a protocol data unit.
Integrity	A way to ensure that information is not modified except by those who are authorized to do so.
IntraLATA	Within a Local Access Transport Area.
Jitter	Variability in the delay of a stream of incoming packets making up a flow such as a voice communication.
Kerberos	A secret-key network authentication protocol that uses a choice of cryptographic algorithms for encryption and a centralized key database for authentication.
Key	A mathematical value input into the selected cryptographic algorithm.
Key Exchange	The swapping of public keys between entities to be used to encrypt communication between the entities.
Key Management	The process of distributing shared symmetric keys needed to run a security protocol.
Key Pair	An associated public and private key where the correspondence between the two are mathematically related, but it is computationally infeasible to derive the private key from the public key.
Keying Material	A set of cryptographic keys and their associated parameters, normally associated with a particular run of a security protocol.
Keyspace	The range of all possible values of the key for a particular cryptographic algorithm.
Latency	The time, expressed in quantity of symbols, taken for a signal element to pass through a device.
Link Encryption	Cryptography applied to data as it travels on data links between the network devices.
Network Layer	Layer 3 in the Open System Interconnection (OSI) architecture that provides network information that is independent from the lower layers.
Network Management	The functions related to the management of data across the network.
Network Management OSS	The functions related to the management of data link layer and physical layer resources and their stations across the data network supported by the hybrid fiber/coax system.

Nonce	A random value used only once that is sent in a communications protocol exchange to prevent replay attacks.
Non-Repudiation	The ability to prevent a sender from denying later that he or she sent a message or performed an action.
Off-Net Call	A communication connecting an IPCablecom subscriber out to a user on the PSTN.
On-Net Call	A communication placed by one customer to another customer entirely on the IPCablecom Network.
One-way Hash	A hash function that has an insignificant number of collisions upon output.
Plaintext	The original (unencrypted) state of a message or data. Also called cleartext.
Pre-shared Key	A shared secret key passed to both parties in a communication flow, using an unspecified manual or out-of-band mechanism.
Privacy	A way to ensure that information is not disclosed to any one other than the intended parties. Information is usually encrypted to provide confidentiality. Also known as confidentiality.
Private Key	The key used in public key cryptography that belongs to an individual entity and must be kept secret.
Proxy	A facility that indirectly provides some service or acts as a representative in delivering information, thereby eliminating the need for a host to support the service.
Public Key	The key used in public key cryptography that belongs to an individual entity and is distributed publicly. Other entities use this key to encrypt data to be sent to the owner of the key.
Public Key Certificate	A binding between an entity's public key and one or more attributes relating to its identity, also known as a digital certificate.
Public Key Cryptography	A procedure that uses a pair of keys, a public key and a private key, for encryption and decryption, also known as an asymmetric algorithm. A user's public key is publicly available for others to use to send a message to the owner of the key. A user's private key is kept secret and is the only key that can decrypt messages sent encrypted by the user's public key.
Root Private Key	The private signing key of the highest-level Certification Authority. It is normally used to sign public key certificates for lower-level Certification Authorities or other entities.
Root Public Key	The public key of the highest level Certification Authority, normally used to verify digital signatures generated with the corresponding root private key.
Secret Key	The cryptographic key used in a symmetric key algorithm, which results in the secrecy of the encrypted data depending solely upon keeping the key a secret, also known as a symmetric key.
Session Key	A cryptographic key intended to encrypt data for a limited period of time, typically between a pair of entities.
Signed and Sealed	An "envelope" of information which has been signed with a digital signature and sealed using encryption.
Subflow	A unidirectional flow of IP packets characterized by a single source and destination IP address and single source and destination UDP/TCP port.
Symmetric Key	The cryptographic key used in a symmetric key algorithm, which results in the secrecy of the encrypted data depending solely upon keeping the key a secret, also known as a secret key.
Systems Management	Functions in the application layer related to the management of various Open Systems Interconnection (OSI) resources and their status across all layers of the OSI architecture.

Transit Delays	The time difference between the instant at which the first bit of a Protocol Data Unit (PDU) crosses one designated boundary, and the instant at which the last bit of the same PDU crosses a second designated boundary.
Trunk	An analog or digital connection from a circuit switch that carries user media content and may carry voice signaling (M_F , R_2 , etc.).
Tunnel Mode	An IPsec (ESP or AH) mode that is applied to an IP tunnel, where an outer IP packet header (of an intermediate destination) is added on top of the original, inner IP header. In this case, the ESP or AH transform treats the inner IP header as if it were part of the packet payload. When the packet reaches the intermediate destination, the tunnel terminates and both the outer IP packet header and the IPsec ESP or AH transform are taken out.
Upstream	The direction from the subscriber location toward the headend.
X.509 certificate	A public key certificate specification developed as part of the ITU-T X.500 standards directory.

4 ABBREVIATIONS AND ACRONYMS

This standard uses the following abbreviations and acronyms:

AAA	Authentication, Authorization and Accounting.
AES	Advanced Encryption Standard. A block cipher, used to encrypt the media traffic in IPCablecom.
AF	Assured Forwarding. This is a DiffServ Per Hop Behavior.
AH	Authentication header. An IPsec security protocol that provides message integrity for complete IP packets, including the IP header.
AMA	Automated Message Accounting. A standard form of call detail records (CDRs) developed and administered by Bellcore (now Telcordia Technologies).
ASD	Application-Specific Data. A field in some Kerberos key management messages that carries information specific to the security protocol for which the keys are being negotiated.
AT	Access Tandem.
ATM	Asynchronous Transfer Mode. A protocol for the transmission of a variety of digital signals using uniform 53-byte cells.
BAF	Bellcore AMA Format, also known as AMA.
BCID	Billing Correlation ID.
BPI+	Baseline Privacy Plus Interface Specification. The security portion of the DOCSIS 1.1 standard that runs on the MAC layer.
CA	Certification Authority. A trusted organization that accepts certificate applications from entities, authenticates applications, issues certificates and maintains status information about certificates.
CA	Call Agent. The part of the CMS that maintains the communication state, and controls the line side of the communication.
CBC	Cipher Block Chaining mode. An option in block ciphers that combines (XORs) the previous block of ciphertext with the current block of plaintext before encrypting that block of the message.
CBR	Constant Bit Rate.
CDR	Call Detail Record. A single CDR is generated at the end of each billable activity. A single billable activity may also generate multiple CDRs.
CIC	Circuit Identification Code. In ANSI SS7, a two-octet number that uniquely identifies a DSO circuit within the scope of a single SS7 Point Code.
CID	Circuit ID (Pronounced "kid"). This uniquely identifies an ISUP DS0 circuit on a Media Gateway. It is a combination of the circuit's SS7 gateway point code and Circuit Identification Code (CIC). The SS7 DPC is associated with the Signaling Gateway that has domain over the circuit in question.
CIF	Common Intermediate Format.
CIR	Committed Information Rate.
CM	DOCSIS Cable Modem.
CMS	Cryptographic Message Syntax.
CMS	Call Management Server. Controls the audio connections. Also called a Call Agent in MGCP/SGCP terminology. This is one example of an Application Server.
CMTS	Cable Modem Termination System. The device at a cable headend which implements the DOCSIS RFI MAC protocol and connects to CMs over an HFC network.
Codec	COder-DECoder.

COPS	Common Open Policy Service. Defined in RFC 2748.
CoS	Class of Service. The type 4 tuple of a DOCSIS configuration file.
CRCX	Create Connection.
CSR	Customer Service Representative.
DA	Directory Assistance.
DE	Default. This is a DiffServ Per Hop Behavior.
DES	Data Encryption Standard.
DF	Delivery Function.
DHCP	Dynamic Host Configuration Protocol.
DHCP-D	DHCP Default. Network Provider DHCP Server.
DNS	Domain Name Service.
DOCSIS®	Data-Over-Cable Service Interface Specifications.
DPC	Destination Point Code. In ANSI SS7, a 3-octet number which uniquely identifies an SS7 Signaling Point, either an SSP, STP, or SCP.
DQoS	Dynamic Quality-of-Service. Assigned on the fly for each communication depending on the QoS requested.
DSA	Dynamic Service Add.
DSC	Dynamic Service Change.
DSCP	DiffServ Code Point. A field in every IP packet that identifies the DiffServ Per Hop Behavior. In IP version 4, the TOS byte is redefined to be the DSCP. In IP version 6, the Traffic Class octet is used as the DSCP.
DTMF	Dual-tone Multi Frequency (tones).
EF	Expedited Forwarding. A DiffServ Per Hop Behavior.
E-MTA	Embedded MTA. A single node that contains both an MTA and a cable modem.
EO	End Office.
ESP	IPsec Encapsulating Security Payload. Protocol that provides both IP packet encryption and optional message integrity, not covering the IP packet header.
ETSI	European Telecommunications Standards Institute.
F-link	F-Links are SS7 links that directly connect two SS7 end points, such as two SSPs. 'F' stands for "Fully Associated."
FEID	Financial Entity ID.
FGD	Feature Group D signaling.
FQDN	Fully Qualified Domain Name. Refer to IETF RFC 2821 for details.
GC	Gate Controller.
GTT	Global Title Translation.
HFC	Hybrid Fiber/Coaxial. An HFC system is a broadband bi-directional shared media transmission system using fiber trunks between the headend and the fiber nodes, and coaxial distribution from the fiber nodes to the customer locations.
HMAC	Hashed Message Authentication Code. A message authentication algorithm, based on either SHA-1 or MD5 hash and defined in IETF RFC 2104.
HTTP	Hypertext Transfer Protocol. Refer to IETF RFC 1945 and RFC 2068.
IANA	Internet Assigned Numbered Authority. See www.ietf.org for details.
IC	Inter-exchange Carrier.

IETF	Internet Engineering Task Force. A body responsible, among other things, for developing standards used on the Internet. See www.ietf.org for details.
IKE	Internet Key Exchange. A key-management mechanism used to negotiate and derive keys for SAs in IPsec.
IKE–	A notation defined to refer to the use of IKE with pre-shared keys for authentication.
IKE+	A notation defined to refer to the use of IKE with X.509 certificates for authentication.
IP	Internet Protocol. An Internet network-layer protocol.
IPsec	Internet Protocol Security. A collection of Internet standards for protecting IP packets with encryption and authentication.
ISDN	Integrated Services Digital Network.
ISTP	Internet Signaling Transport Protocol.
ISUP	ISDN User Part. A protocol within the SS7 suite of protocols that is used for call signaling within an SS7 network.
ITU	International Telecommunication Union.
ITU-T	International Telecommunication Union–Telecommunication Standardization Sector.
IV	Initialization Vector
IVR	Interactive Voice Response system.
KDC	Key Distribution Center.
LATA	Local Access and Transport Area.
LD	Long Distance.
LIDB	Line Information Database. Contains customer information required for real-time access such as calling card personal identification numbers (PINs) for real-time validation.
LLC	Logical Link Control. The Ethernet Packet header and optional 802.1P tag which may encapsulate an IP packet. A sublayer of the Data Link Layer.
LNP	Local Number Portability. Allows a customer to retain the same number when switching from one local service provider to another.
LSSGR	LATA Switching Systems Generic Requirements.
MAC	Message Authentication Code. A fixed-length data item that is sent together with a message to ensure integrity, also known as a MIC.
MAC	Media Access Control. It is a sublayer of the Data Link Layer. It normally runs directly over the physical layer.
MC	Multipoint Controller.
MCU	Multipoint Conferencing Unit.
MD5	Message Digest 5. A one-way hash algorithm that maps variable length plaintext into fixed-length (16 byte) ciphertext.
MDCP	Media Device Control Protocol. A media gateway control specification submitted to IETF by Lucent. Now called SCTP.
MDCX	Modify Connection.
MDU	Multi-Dwelling Unit. Multiple units within the same physical building. The term is usually associated with high-rise buildings.
MEGACO	Media Gateway Control IETF working group. See www.ietf.org for details.
MF	Multi-Frequency.
MG	Media Gateway. Provides the bearer circuit interfaces to the PSTN and transcodes the media stream.

MGC	Media Gateway Controller. The overall controller function of the PSTN gateway. Receives, controls and mediates call-signaling information between the IPCablecom and PSTN.
MGCP	Media Gateway Control Protocol. Protocol follow-on to SGCP. Refer to IETF 2705.
MIB	Management Information Base.
MIC	Message Integrity Code. A fixed-length data item that is sent together with a message to ensure integrity, also known as a Message Authentication Code (MAC).
MMC	Multi-Point Mixing Controller. A conferencing device for mixing media streams of multiple connections.
MSB	Most Significant Bit.
MSO	Multi-System Operator. A cable company that operates many headend locations in several cities.
MSU	Message Signal Unit.
MTA	Multimedia Terminal Adapter. Contains the interface to a physical voice device, a network interface, CODECs, and all signaling and encapsulation functions required for VoIP transport, class features signaling, and QoS signaling.
MTP	The Message Transfer Part. A set of two protocols (MTP 2, MTP 3) within the SS7 suite of protocols that are used to implement physical, data link, and network-level transport facilities within an SS7 network.
MWD	Maximum Waiting Delay.
NANP	North American Numbering Plan.
NANPNAT	North American Numbering Plan Network Address Translation.
NAT Network Layer	Network Address Translation. Layer 3 in the Open System Interconnection (OSI) architecture. This layer provides services to establish a path between open systems.
NCS	Network Call Signaling.
NPA-NXX	Numbering Plan Area (more commonly known as area code) NXX (sometimes called exchange) represents the next three numbers of a traditional phone number. The N can be any number from 2-9 and the Xs can be any number. The combination of a phone number's NPA-NXX will usually indicate the physical location of the call device. The exceptions include toll-free numbers and ported number (see LNP).
NTP	Network Time Protocol. An internet standard used for synchronizing clocks of elements distributed on an IP network.
NTSC	National Television Standards Committee. Defines the analog color television broadcast standard used today in North America.
OID	Object Identification.
OSP	Operator Service Provider.
OSS	Operations Systems Support. The back-office software used for configuration, performance, fault, accounting, and security management.
OSS-D	OSS Default. Network Provider Provisioning Server.
PAL	Phase Alternate Line. The European color television format that evolved from the American NTSC standard.
PCES	IPCablecom Electronic Surveillance.
PCM	Pulse Code Modulation. A commonly employed algorithm to digitize an analog signal (such as a human voice) into a digital bit stream using simple analog-to-digital conversion techniques.
PDU	Protocol Data Unit.

PHS	Payload Header Suppression. A DOCSIS technique for compressing the Ethernet, IP, and UDP headers of RTP packets.
PKCS	Public-Key Cryptography Standards. Published by RSA Data Security Inc. These Standards describe how to use public key cryptography in a reliable, secure and interoperable way.
PKI	Public-Key Infrastructure. A process for issuing public key certificates, which includes standards, Certification Authorities, communication between authorities and protocols for managing certification processes.
PKINIT	Public-Key Cryptography for Initial Authentication. The extension to the Kerberos protocol that provides a method for using public-key cryptography during initial authentication.
PSC	Payload Service Class Table, a MIB table that maps RTP payload Type to a Service Class Name.
PSFR	Provisioned Service Flow Reference. An SFR that appears in the DOCSIS configuration file.
PSTN	Public Switched Telephone Network.
QCIF	Quarter Common Intermediate Format.
QoS	Quality of Service. Guarantees network bandwidth and availability for applications.
RADIUS	Remote Authentication Dial-In User Service. An internet protocol (IETF RFC 2865 and RFC 2866) originally designed for allowing users dial-in access to the internet through remote servers. Its flexible design has allowed it to be extended well beyond its original intended use.
RAS	Registration, Admissions and Status. RAS Channel is an unreliable channel used to convey the RAS messages and bandwidth changes between two H.323 entities.
RFC	Request for Comments. Technical policy documents approved by the IETF which are available on the World Wide Web at http://www.ietf.cnri.reston.va.us/rfc.html .
RFI	The DOCSIS Radio Frequency Interface specification.
RJ-11	Registered Jack-11. A standard 4-pin modular connector commonly used in the United States for connecting a phone unit into a wall jack.
RKS	Record Keeping Server. The device, which collects and correlates the various Event Messages.
RSA	A public-key, or asymmetric, cryptographic algorithm used to provide authentication and encryption services. RSA stands for the three inventors of the algorithm; Rivest, Shamir, Adleman.
RSA Key Pair	A public/private key pair created for use with the RSA cryptographic algorithm.
RSVP	Resource Reservation Protocol.
RTCP	Real-Time Control Protocol.
RTO	Retransmission Timeout.
RTP	Real-time Transport Protocol. A protocol for encapsulating encoded voice and video streams. Refer to IETF RFC 1889.
SA	Security Association. A one-way relationship between sender and receiver offering security services on the communication flow.
SAID	Security Association Identifier. Uniquely identifies SAs in the DOCSIS Baseline Privacy Plus Interface (BPI+) security protocol.
SCCP	Signaling Connection Control Part. A protocol within the SS7 suite of protocols that provides two functions in addition to those provided within MTP. The first function is the ability to address applications within a signaling point. The second function is Global Title Translation.
SCP	Service Control Point. A Signaling Point within the SS7 network, identifiable by a Destination Point Code that provides database services to the network.
SCTP	Stream Control Transmission Protocol.

SDP	Session Description Protocol.
SDU	Service Data Unit. Information delivered as a unit between peer service access points.
SF	Service Flow. A unidirectional flow of packets on the RF interface of a DOCSIS system.
SFID	Service Flow ID. A 32-bit integer assigned by the CMTS to each DOCSIS Service Flow defined within a DOCSIS RF MAC domain. SFIDs are considered to be in either the upstream direction (USFID) or downstream direction (DSFID). Upstream Service Flow IDs and Downstream Service Flow IDs are allocated from the same SFID number space.
SFR	Service Flow Reference. A 16-bit message element used within the DOCSIS TLV parameters of Configuration Files and Dynamic Service messages to temporarily identify a defined Service Flow. The CMTS assigns a permanent SFID to each SFR of a message.
SG	Signaling Gateway. An SG is a signaling agent that receives/sends SCN native signaling at the edge of the IP network. In particular, the SS7 SG function translates variants ISUP and TCAP in an SS7-Internet Gateway to a common version of ISUP and TCAP.
SGCP	Simple Gateway Control Protocol. Earlier draft of MGCP.
SHA – 1	Secure Hash Algorithm 1. A one-way hash algorithm.
SID	Service ID. A 14-bit number assigned by a CMTS to identify an upstream virtual circuit. Each SID separately requests and is granted the right to use upstream bandwidth.
S-MTA	Standalone MTA. A single node that contains an MTA and a non-DOCSIS MAC (e.g., ethernet).
SNMP	Simple Network Management Protocol.
SOHO	Small Office/Home Office.
SS7	Signaling System number 7. An architecture and set of protocols for performing out-of-band call signaling with a telephone network.
SSP	Service Switching Point. SSPs are points within the SS7 network that terminate SS7 signaling links and also originate, terminate, or tandem switch calls.
STP	Signal Transfer Point. A node within an SS7 network that routes signaling messages based on their destination address. This is essentially a packet switch for SS7. It may also perform additional routing services such as Global Title Translation.
TCAP	Transaction Capabilities Application Protocol. A protocol within the SS7 stack that is used for performing remote database transactions with a Signaling Control Point.
TCP	Transmission Control Protocol.
TD	Timeout for Disconnect.
TFTP	Trivial File Transfer Protocol.
TFTP-D	Default – Trivial File Transfer Protocol.
TGS	Ticket Granting Server. A sub-system of the KDC used to grant Kerberos tickets.
TGW	Telephony Gateway.
TIPHON	Telecommunications and Internet Protocol Harmonization Over Network.
TLV	Type-Length-Value. A tuple within a DOCSIS configuration file.
TN	Telephone Number.
ToD	Time-of-Day Server.
TOS	Type of Service. An 8-bit field of every IP version 4 packet. In a DiffServ domain, the TOS byte is treated as the DiffServ Code Point, or DSCP.
TSG	Trunk Subgroup.
UDP	User Datagram Protocol. A connectionless protocol built upon Internet Protocol (IP).
VAD	Voice Activity Detection.

VBR Variable Bit Rate.
VoIP Voice-over-IP.

5 ARCHITECTURAL OVERVIEW OF IPCABLECOM SECURITY

5.1 IPCablecom Reference Architecture

Security requirements have been defined for every signaling and media link within the IPCablecom IP network. In order to understand the security requirements and specifications for IPCablecom, one must first understand the overall architecture. This section presents a brief overview of the IPCablecom architecture. For a more detailed specification, refer to the IPCablecom Architecture Technical Report [1].

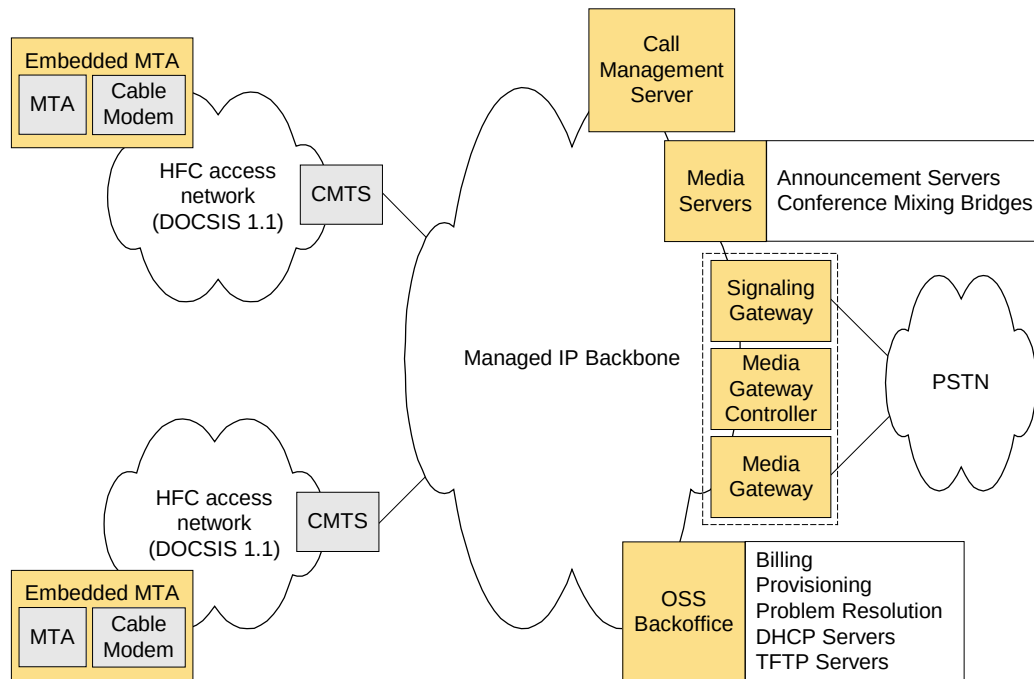


Figure 1. IPCablecom Single Zone Architecture

5.1.1 HFC Network

In Figure 1, the MTAs and the CMTS is an HFC network, which employs DOCSIS 1.1 physical layer and MAC layer protocols [8]. DOCSIS BPI+ [9] and QoS protocols are enabled over this link.

5.1.2 Call Management Server

In the context of voice communications applications, a central component of the system is the Call Management Server (CMS). It is involved in both call signaling and the establishment of Dynamic Quality of Service (DQoS). The CMS also performs queries at the PSTN Gateway for LNP (Local Number Portability) and other services necessary for voice communications, including interfacing with the PSTN.

As described in the IPCablecom Architecture Framework [1], the CMS is divided into the following functional components:

- Call Agent (CA) - The Call Agent maintains network intelligence and call state and controls the media gateway. Most of the time Call Agent is synonymous for Call Management Server.
- Gate Controller (GC) - The Gate Controller is a logical QoS management component that is typically part of the CMS. The GC coordinates all quality of service authorization and control on behalf of the application service - e.g., voice communications.

- Media Player Controller (MPC) – The MPC initiates and manages all announcement services provided by the Media Player. The MPC accepts requests from the CMS and arranges for the MP to provide the announcement in the appropriate stream so that the user hears the announcement.
- Media Gateway Controller (MGC) – The Media Gateway Controller maintains the gateway’s portion of call state for communications traversing the Gateway.

A particular CMS can contain any subset of the above listed functional components.

5.1.3 Functional Categories

The IPCablecom Architecture Framework identifies the following functional categories within the architecture:

- MTA device provisioning
- Quality of Service (HFC access network and managed IP backbone)
- Billing interface security
- Security (specified herein)
- Network call signaling (NCS)
- PSTN interconnectivity
- CODEC functionality and media stream mapping

In most cases, each functional category corresponds to a particular IPCablecom specification document.

5.1.3.1 Device and Service Provisioning

During MTA provisioning, the MTA gets its configuration with the help of the DHCP and TFTP servers, as well as the OSS.

Provisioning interfaces need to be secured and have to configure the MTA with the appropriate security parameters (e.g., customer X.509 certificate signed by the Service Provider). This document specifies the steps in MTA provisioning, but provides detailed specifications only for the security parameters. Refer to [4] for a full specification on MTA provisioning and customer enrollment.

5.1.3.2 Dynamic Quality of Service

IPCablecom provides guaranteed Quality of Service (QoS) for each voice communication within a single zone with Dynamic QoS (DQoS) [3].

DQoS is controlled by the Gate Controller function within the CMS and can guarantee Quality of Service within a single administrative domain. The Gate Controller utilizes the COPS protocol to download QoS policy into the CMTS. After that, the QoS reservation is established via DOCSIS 1.1 QoS messaging between the MTA and the CMTS on both sides of the connection.

5.1.3.3 Billing System Interfaces

The CMS, CMTS and the PSTN Gateway are all required to send out billing event messages to the Record Keeping Server (RKS). This interface is currently specified to be RADIUS. Billing information should be checked for integrity and authenticity as well as kept private. This document defines security requirements and specifications for the communication with RKS.

5.1.3.4 Call Signaling

The call signaling architecture defined within IPCablecom is Network Based Call Signaling (NCS). The CMS is used to control call setup, termination and most other call signaling functions. In the NCS architecture [2], the Call Agent function within the CMS is used in call signaling and utilizes the MGCP protocol.

5.1.3.5 PSTN Interconnectivity

The PSTN interface to the voice communications capabilities of the IPCablecom network is through the Signaling and Media Gateways (SG and MG). Both of these gateways are controlled with the MGC (Media Gateway Controller). The MGC may be standalone or combined with a CMS. For further detail on PSTN Gateways, refer to [5].

All communications between the MGC and the SG and MG may be over the same-shared IP network and is subject to similar threats (e.g., privacy, masquerade, denial-of-service) that are encountered in other links in the same network. This document defines the security requirements and specifications for the PSTN Gateway links.

When communications from an MTA to a PSTN phone are made, bearer channel traffic is passed directly between an MTA and an MG. The protocols used in this case are RTP and RTCP, as in the MTA-to-MTA case. Both security requirements and specifications are very similar to the MTA-to-MTA bearer requirements and are fully defined in this document. After a voice communication enters the PSTN, the security requirements as well as specifications are based on existing PSTN standards and are out of the scope of this document.

5.1.3.6 CODEC Functionality and Media Stream Mapping

The media stream between two MTAs or between an MTA and a PSTN Gateway utilizes the RTP protocol. Although BPI+ provides privacy over the HFC network, the potential threats within the rest of the voice communications network require that the RTP packets be encrypted end-to-end.¹

In addition to RTP, there is an accompanying RTCP protocol, primarily used for reporting of RTCP statistics. In addition, RTCP packets may carry CNAME – a unique identifier of the sender of RTP packets. RTCP also defines a BYE message² that can be used to terminate an RTP session. These two additional RTCP functions raise privacy and denial-of-service threats. Due to these threats, RTCP security requirements are the same as the requirements for all other end-to-end signaling and are addressed in the same manner.

In addition to MTAs and PSTN Gateways, Media Servers may also participate in the media stream flows. Media Servers are network-based components that operate on media flows to support various voice communications service options. Media servers perform audio bridging, play terminating announcements, provide interactive voice response services, and so on. Both media stream and signaling interfaces to a Media Server are the same as the interfaces to an MTA. For more information on Codec functionality, see [7].

5.1.3.7 Audio Server Services

The text in this section has been removed because it is not within the scope of IPCablecom 1.0.

5.1.3.8 Electronic Surveillance

The text in this section has been removed because it is not within the scope of IPCablecom 1.0.

5.2 Threats

Figure 2 below contains the interfaces that were analyzed for security.

There are additional interfaces identified in IPCablecom but for which protocols are not specified. In those cases, the corresponding security protocols are also not specified, and those interfaces are not listed in the Figure 2 below.

As well, the interfaces for which security is not required in IPCablecom are not listed.

¹ In general, it is possible for an MTA-to-MTA or MTA-to-PSTN connection to cross the networks of several different Service Providers. In the process, this path may cross a PSTN network. This is an exception to the rule, where all RTP packets are encrypted end-to-end. The media traffic inside a PSTN network does not utilize RTP and has its own security requirements. Thus, in this case the encryption would not be end-to-end and would terminate at the PSTN Gateway on both sides of the intermediate PSTN network.

² The RTCP BYE message should not be confused with the SIP+ BYE message that is also used to indicate the end of a voice communication within the network.

IPCablecom Security Interfaces

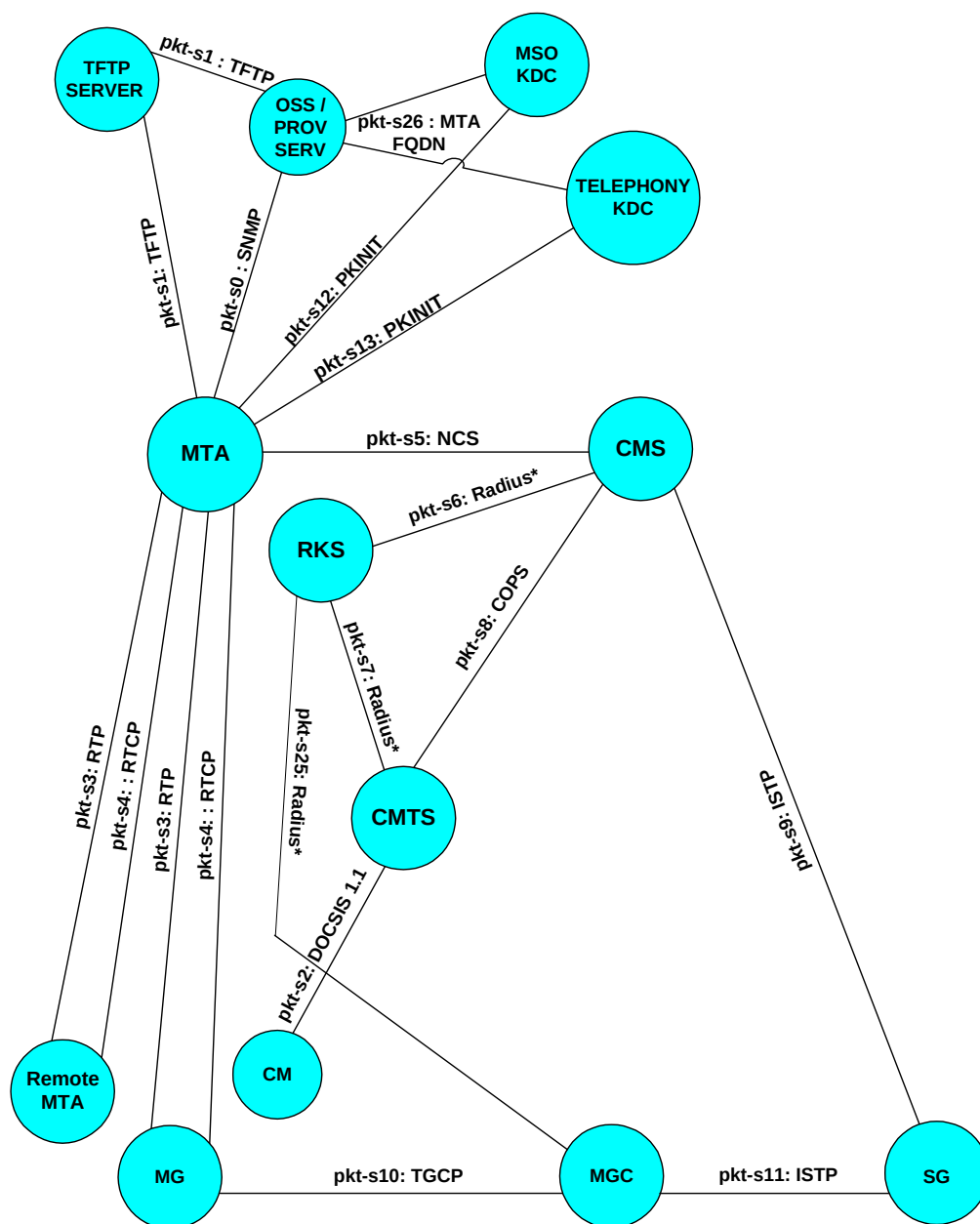


Figure 2. IPCablecom Secured Interfaces

The interfaces marked "RADIUS*" carry event messages, which use the RADIUS format as defined by [13].

Following is a summary of general threats and the corresponding attacks that are relevant in the context of IP voice communications. This list of threats is not based on the knowledge of the specific protocols or security mechanisms employed in the network. A more specific summary of threats that are based on the functionality of each network element is listed in section 5.2.6.

Some of the outlined threats cannot be addressed purely by cryptographic means – physical security and/or fraud management should also be used. These threats may be important, but cannot be fully addressed within the scope of IPCablecom. How vendors and MSOs implement fraud management and physical security will differ and in this case a standard is not required for interoperability.

5.2.1 Theft of Network Services

In the context of voice communications, the main services that may be stolen are:

- Long distance service
- Local (subscription) voice communications service
- Video conferencing
- Network-based three-way calling
- Quality of Service

5.2.1.1 MTA Clones

One or more MTAs can masquerade as another MTA by duplicating its permanent identity and keys. The secret cryptographic keys may be obtained by either breaking the physical security of the MTA or by employing cryptanalysis.

When an MTA is broken into the perpetrator can steal voice communications service and charge it all to the original owner. The feasibility of such an attack depends on where an MTA is located. This attack must be seriously considered in the cases when an MTA is located in an office or apartment building, or on a street corner.

An owner might break into his or her own MTA in at least one instance – after a false account with the MSO providing the voice communications service had been setup. The customer name, address, Social Security Number may all be invalid or belong to someone else. The provided Credit Card Number may be stolen. In that case, the owner of the MTA would not mind giving out the MTA cryptographic identity to others – he or she would not have to pay for service anyway.

In addition to cloning of the permanent cryptographic keys, temporary (usually symmetric) keys may also be cloned. Such an attack is more complex, since the temporary keys expire more often and have to be frequently redistributed. The only reason why someone would attempt this attack is if the permanent cryptographic keys are protected much better than the temporary ones, or if the temporary keys are particularly easy to steal or discover with cryptanalysis.

5.2.1.2 Other Clones

It is conceivable that the cryptographic identity of another network element, such as a CMTS or a CMS, may be cloned. Such an attack is most likely to be mounted by an insider such as a corrupt or disgruntled employee.

5.2.1.3 Subscription Fraud

A customer sets up an account under false information.

5.2.1.4 Non-Payment for Voice Communications Services

A customer stops paying his or her bill, but continues to use the MTA for voice communications service. This can happen if the network does not have an automated method to revoke the customer's access to the network.

5.2.1.5 Protocol Attacks against an MTA

A weakness in the protocol can be manipulated to allow an MTA to authenticate to a network server with a false identity or hijack an existing voice communication. This includes replay and man-in-the-middle attacks.

5.2.1.6 Protocol Attacks against Other Network Elements

A perpetrator might employ similar protocol attacks to masquerade as a different Network Element, such as a CMTS or a CMS. Such an attack may be used in collaboration with cooperating MTAs to steal service.

5.2.1.7 Theft of Services Provided by the MTA

Services such as the support for multiple MTA ports, 3-way calling and call waiting may be implemented entirely in the MTA, without any required interaction with the network.

5.2.1.7.1 Attacks

MTA code to support these services may be downloaded illegally by an MTA clone, in which case the clone has to interact with the network to get the download. In that case, this threat is no different from the network service theft described in the previous section.

Alternatively, downloading an illegal code image using some illegal out-of-band means can also enable these services. Such service theft is much harder to prevent (a secure software environment within the MTA may be required). On the other hand, in order for an adversary to go through this trouble, the price for these MTA-based services has to make the theft worthwhile.

An implication of this threat is that valuable services cannot be implemented entirely inside the MTA without a secure software environment in addition to tamperproof protection for the cryptographic keys. (While a secure software environment within an MTA adds significant complexity, it is an achievable task.)

5.2.1.8 MTA Moved to Another Network

A leased MTA may be reconfigured and registered with another network, contrary to the intent and property rights of the leasing company.

5.2.2 Bearer Channel Information Threats

This class of threats is concerned with the breaking of privacy of voice communications over the IP bearer channel. Threats against non-VoIP communications are not considered here and assumed to require additional security at the application layer.

5.2.2.1 Attacks

Clones of MTAs and other Network Elements, as well as protocol manipulation attacks, also apply in the case of Bearer Channel Information threats. These attacks are already described under the Service Theft threats.

MTA cloning attacks mounted by the actual owner of the MTA are less likely in this case, but not inconceivable. An owner of an MTA may distribute clones to unsuspecting victims, so that he or she can later spy on them.

5.2.2.1.1 Off-line Cryptanalysis

Bearer channel information may be recorded and then analyzed over a period of time, until the encryption keys are discovered through cryptanalysis. The discovered information may be of value even after a relatively long time has passed.

5.2.3 Signaling Channel Information Threats

Signaling information, such as the caller identity and the services to which each customer subscribes may be collected for marketing purposes. The caller identity may also be used illegally to locate a customer that wishes to keep his or her location private.

5.2.3.1 Attacks

Clones of MTAs and other Network Elements, as well as protocol manipulation attacks, also apply in the case of the Signaling Channel Information threats. These attacks were already described under the Service Theft threats.

MTA cloning attacks mounted by the actual owner of the MTA is theoretically possible in this case. An owner of an MTA may distribute clones to the unsuspecting victims, so that he or she can monitor their signaling messages (e.g., for information with marketing value). The potential benefits of such an attack seem unjustified, however.

5.2.3.1.1 *Caller ID*

A number of a party initiating a voice communication is revealed, even though a number is not generally available (i.e., is "unlisted") and the owner of that number enabled ID blocking.

5.2.3.1.2 *Information with Marketing Value*

Dialed numbers and the type of service customers use may be gathered for marketing purposes by other corporations.

5.2.4 Service Disruption Threats

This class of threats is aimed at disrupting the normal operation of voice communications. The motives for denial-of-service attacks may be malicious intent against a particular individual or against the service provider. Or, perhaps a competitor wishes to degrade the performance of another service provider and use the resulting problems in an advertising campaign.

5.2.4.1 *Attacks*

5.2.4.1.1 *Remote Interference*

A perpetrator is able to manipulate the protocol to close down ongoing voice communications. This might be achieved by masquerading as an MTA involved in such an ongoing communication. The same effect may be achieved if the perpetrator impersonates another Network Element, such as a Gate Controller or an Edge Router during either call setup or voice packet routing.

Depending on the signaling protocol security, it might be possible for the perpetrator to mount this attack from the MTA, in the privacy of his or her own home.

Clones of MTAs and other Network Elements, as well as protocol manipulation attacks, also apply in the case of the Service Disruption threats. These attacks are described under Service Theft threats.

MTA cloning attacks mounted by the actual owner of the MTA can theoretically be used in service disruption against unsuspecting clone owners. However, since there are so many other ways to cause service disruption, such an attack cannot be taken seriously in this context.

5.2.5 Repudiation

In a network where masquerading (using the above-mentioned cloning and protocol manipulation techniques) is common or easily achievable, a customer may repudiate a particular communication (and, thus deny responsibility for paying for it) on that basis.

In addition, unless public key-based digital signatures are employed on each message, the source of each message cannot be absolutely proven. If a signature over a message that originated at an MTA is based on a symmetric key that is shared between that MTA and a network server (e.g., the CMS), it is unclear if the owner of the MTA can claim that the Service Provider somehow falsified the message.

However, even if each message were to carry a public key-based digital signature and if each MTA were to employ stringent physical security, the customer can still claim in court that someone else initiated that communication without his or her knowledge, just as a customer of a telecommunications carrier on the PSTN can claim, e.g., that particular long distance calls made from the customer's telephone were not authorized by the customer. Such telecommunications carriers commonly address this situation by establishing contractual and/or tariffed relationships with customers in which customers assume liability for unauthorized use of the customer's service. These same contractual principles are typically implemented in service contracts between information services providers such as ISPs and their subscribers. For these reasons, the benefits of non-repudiation seem dubious at best and do not appear to justify the performance penalty of carrying a public key-based digital signature on every message.

5.2.6 Threat Summary

This section provides a summary of the above of threats and attacks and a brief assessment of their relative importance.

5.2.6.1 Primary Threats

5.2.6.1.1 Theft of Service

Attacks are:

- **Subscription Fraud.** This attack is prevalent in today's telephony systems (i.e., the PSTN) and requires little economic investment. It can only be addressed with a Fraud Management system.
- **Non-payment for services.** Within the PSTN, telecommunications carriers usually do not prosecute the offenders, but simply shut down their accounts. Because prosecution is expensive and not always successful, it is a poor counter to this attack. Methods such as debit-based billing and device authorization (pay as you play), increasingly common in the wireless sector of the PSTN, might be a possible solution for this attack in the IPCablecom context. This threat can also be minimized with effective Fraud Management systems.
- **MTA clones.** This threat requires more technical knowledge than the previous two threats. A technically-knowledgeable adversary or underground organization might offer cloning services for profit. This threat is most effective when combined with subscription fraud, where an MTA registered under a fraudulent account is cloned. This threat can be addressed with both Fraud Management and physical security inside the MTA, or a combination of both.
- **Impersonate a network server.** With proper cryptographic mechanisms, authorization and procedural security in place, this attack is unlikely, but has the potential for great damage.
- **Protocol manipulation.** Can occur only when security protocols are flawed or when not enough cryptographic strength is in place.

5.2.6.1.2 Bearer Channel Information Disclosure

Attacks are:

- **Simple Snooping.** This would happen if voice packets were sent in the clear over some segment of the network. Even if that segment appears to be protected, an insider may still compromise it. This is the only major attack on privacy. The bearer channel privacy attacks listed below are possible but are all of secondary importance.
- **MTA clones.** Again, this threat requires more technical knowledge but can be offered as a service by an underground organization. A most likely variation of this attack is when a publicly accessible MTA (e.g., in an office or apartment building) is cloned.
- **Protocol manipulation.** A flawed protocol may somehow be exploited to discover bearer channel encryption keys.
- **Off-line cryptanalysis.** Even when media packets are protected with encryption, they can be stored and analyzed for long periods of time, until the decryption key is finally discovered. Such an attack is not likely to be prevalent, since it is justified only for particularly valuable customer-provided information (IPCablecom security is not required to protect data). This attack is more difficult to perform on voice packets (as opposed to data). Still, customers are very sensitive to this threat and it can serve as the basis for a negative publicity campaign by competitors.

5.2.6.1.3 Signaling Information Disclosure

This threat is listed as primary only due to potential for bad publicity and customer sensitivity to keeping their numbers and location private. All of the attacks listed below are similar to those for bearer channel privacy and are not described here:

- Simple snooping

- MTA clones
- Protocol manipulation
- Off-line cryptanalysis
- Service disruption

5.2.6.2 *Secondary Threats*

- **Theft of MTA-based Services.** Based on the voice communications services that are planned for the near future, this threat does not appear to have potential for significant economic damage. This could possibly change with the introduction of new value-added services in the future.
- **Illegally Registering a Leased MTA with a Different Service Provider.** Leased MTAs can normally be tracked. Most likely, this threat is combined with the actual theft of a leased MTA. Thus, this threat does not appear to have potential for widespread damage.

5.3 Security Architecture

5.3.1 Overview of Security Interfaces

Figure 3 summarizes all of the IPCablecom security interfaces, including key management.

IPCablecom Security Interfaces with Key Management

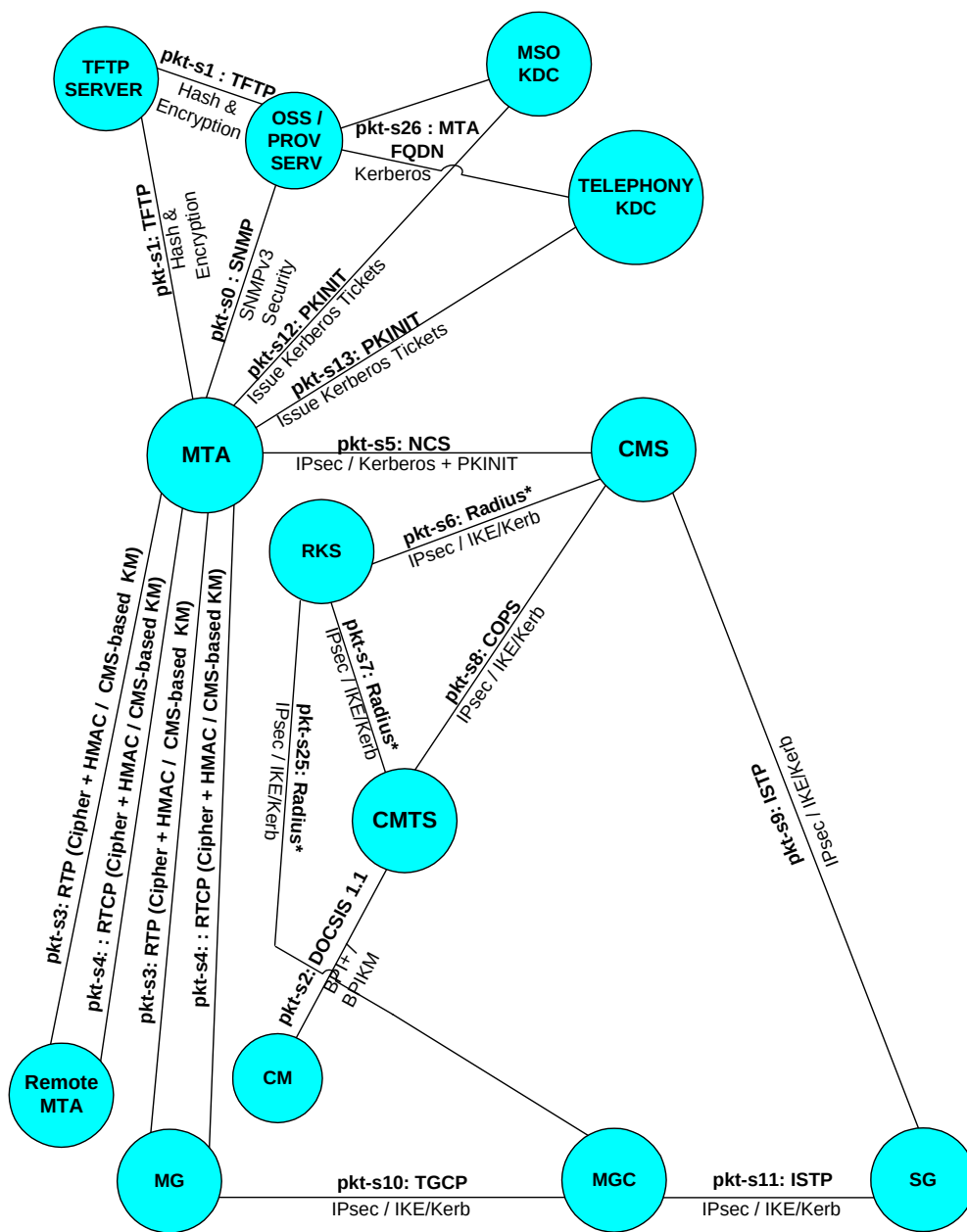


Figure 3. IPCablecom Security Interfaces with Key-Management

In Figure 3, each interface label is of the form:

<label>: <protocol> { <security protocol> / <key management protocol> }

If the key management protocol is missing, it is not needed for that interface. IPCablecom interfaces that do not require security are not shown on this diagram.

The following abbreviations are used in Figure 3:

IKE/Kerb	IKE (with pre-shared keys or X.509 certificates) or Kerberos
IKE+	IKE with X.509 certificates
CMS-based KM	Keys randomly generated and exchanged inside signaling messages
RADIUS*	Event messages, which use the RADIUS format as defined by [13].

Table 1 briefly describes each of the interfaces shown in the above diagram.

Table 1. IPCablecom Security Interfaces Table

Interface	Components	Description
pkt-s0	MTA – PS/OSS	Immediately after the DHCP sequence in the Secure Provisioning Flow, the MTA performs Kerberos-based key management with the Provisioning Server to establish SNMPv3 keys. The MTA bypasses Kerberized SNMPv3 and uses SNMPv2c in the Basic and Hybrid Flows.
pkt-s1	MTA – TFTP	MTA Configuration file download. When the Provisioning Server in the Secure Provisioning Flow sends an SNMP Set command to the MTA, it includes both the configuration name and the hash of the file. Later, when the MTA downloads the file, it authenticates the configuration file using the hash value. The configuration file may be optionally encrypted.
pkt-s2	CM – CMTS	DOCSIS 1.1: This interface should be secured with BPI+ using BPI Key Management. BPI+ privacy is provided on the HFC link.
pkt-s3	MTA – MTA MTA – MG	RTP: End-to-end media packets between two MTAs, or between MTA and MG. RTP packets are encrypted directly with the chosen cipher. Message integrity is optionally provided by an MMH MAC. Keys are randomly generated, and exchanged by the two endpoints inside the signaling messages via the CMS or other application server.
pkt-s4	MTA – MTA MTA – MG	RTCP: RTCP control protocol for RTP. Message integrity and encryption by selected cipher. The RTCP keys are derived using the same secret negotiated during the RTP key management. No additional key management messages are needed or utilized.
pkt-s5	MTA – CMS	NCS: Message integrity and privacy via IPsec. Key management is with Kerberos with PKINIT (public key initial authentication) extension.
pkt-s6	RKS – CMS	RADIUS: RADIUS billing events sent by the CMS to the RKS. RADIUS authentication keys are hardcoded to 0. IPsec is used for message integrity, as well as privacy. Key management is Ike or Kerberos.
pkt-s7	RKS – CMTS	RADIUS: RADIUS events sent by the CMTS to the RKS. RADIUS authentication keys are hardcoded to 0. IPsec is used for message integrity, as well as privacy. Key management is Ike or Kerberos.
pkt-s8	CMS – CMTS	COPS: COPS protocol between the GC and the CMTS, used to download QoS authorization to the CMTS. IPsec is used for message integrity, as well as privacy. Key management is IKE or Kerberos.

Interface	Components	Description
pkt-s9	CMS – SG	ISTP: CMS queries the PSTN Gateway for LNP (Local Number Portability) and other voice communications services. IPsec is used for message integrity, as well as privacy. Key-Management is IKE or Kerberos.
pkt-s10	MGC – MG	TGCP: IPCablecom interface to the PSTN Media Gateway. IPsec is used for both message integrity and privacy. Key management is IKE or Kerberos.
pkt-s11	MGC – SG	ISTP: IPCablecom interface to the PSTN Signaling Gateway. IPsec is used for both message integrity and privacy. Key management is IKE or Kerberos.
pkt-s12	MTA – MSO KDC	PKINIT: An AS-REQ message is sent to the KDC with public-key cryptography used for authentication. The KDC verifies the certificate and issues either a service ticket or a ticket granting ticket (TGT), depending on the contents of the AS Request. The AS Reply returned by the KDC contains a certificate chain and a digital signature that are used by the MTA to authenticate this message. In the case that the KDC returns a TGT, the MTA then sends a TGS Request to the KDC to which the KDC replies with a TGS Reply containing a service ticket. The TGS Request/Reply messages are authenticated using a symmetric session key inside the TGT.
pkt-s13	MTA – Telephony KDC	PKINIT: See pkt-s12 above.
pkt-s25	RKS – MGC	RADIUS: RADIUS events sent by the MGC to the RKS. RADIUS authentication keys are hardcoded to 0. IPsec is used for message integrity, as well as privacy. Key management is IKE or Kerberos.
pkt-s26	OSS/Prov Serv – MSO KDC OSS/Prov Serv – Telephony KDC	The KDC uses Kerberos to map the MTA's MAC address to its FQDN and optionally the MTA's IP address for the purpose of authenticating the MTA before issuing it a ticket.

5.3.2 Security Assumptions

5.3.2.1 BPI+ CMTS Downstream Messages Are Trusted

As mentioned previously, it is assumed that CMTS downstream messages cannot be easily modified in transit and a CMTS can be impersonated only at great expense.

Most messages secured in this specification either move over the shared IP network in addition to the DOCSIS path, or do not go over DOCSIS at all.

In one case – the case of DOCSIS QoS messages exchanged between the CMTS and the CM – this assumption does not apply. Although DOCSIS QoS messages (both upstream and downstream) include an integrity check, the corresponding (BPI+) key management does not authenticate the identity of the CMTS. The CM is unable to cryptographically know that the network element it has connected to is the true CMTS for that network. However, even if a CMTS could be impersonated, it would allow only limited denial-of-service attacks. This vulnerability is not considered to be worth the effort and the expense of impersonating a CMTS.

5.3.2.2 Non-Repudiation Not Supported

Non-repudiation, in this specification, means that an originator of a message cannot deny that he or she sent that message. In this voice communications architecture, non-repudiation is not supported for most messages, with the exception of the top key management layer. This decision was based on the performance penalty incurred with each

public key operation. The most important use for non-repudiation would have been during communications setup – to prove that a particular party had initiated that particular communication. However, due to very strict requirements on the setup time, it is not possible to perform public key operations for each communication.

5.3.2.3 Root Private Key Compromise Protection

The cryptographic mechanisms defined in this document are based on a Public Key Infrastructure (PKI). As is the case with most other architectures that are based on a PKI, there is no automated recovery path from a compromise of a Root Private Key. However, with proper safeguards, the probability of this happening is very low, to the point that the risk of a root private key compromise occurring is outweighed by the benefits of this architecture.

The corresponding Root Public Key is stored as a read-only parameter in many components of this architecture. Once the Root Private Key has been compromised, each manufacturer's certificate would have to be manually reconfigured.

Due to this limitation of a PKI, the Root Private Key must be very carefully guarded with procedural and physical security. And, it must be sufficiently long so that its value cannot be discovered with cryptographic attacks within the expected lifetime of the system.

5.3.2.4 Limited Prevention of Denial-of-Service Attacks

This document does not attempt to address all or even most denial-of-service attacks. The cryptographic mechanisms defined in this specification prevent some denial-of-service attacks that are particularly easy to mount and are hard to detect. For example, they will prevent a compromised MTA from masquerading as other MTAs in the same upstream HFC segment and interrupting ongoing communications with illicit HANGUP messages.

This specification will also prevent more serious denial-of-service attacks, such as an MTA masquerading as a CMS in a different network domain that causes all communications setup requests to fail.

On the other hand, denial-of-service attacks where a router is taken out of service or is bombarded with bad IP packets are not addressed. In general, denial-of-service attacks that are based on damaging one of the network components can only be solved with procedural and physical security, which is out of the scope of this specification.

Denial-of-service attacks where network traffic is overburdened with bad packets cannot be prevented in a large network (although procedural and physical security helps), but can usually be detected. Detection of such an attack and of its cause is out of scope of this specification.

For example, denial-of-service attacks where a router is taken out of order or is bombarded with bogus IP packets cannot be prevented.

5.3.3 Susceptibility of Network Elements to Attack

This section describes the amount and the type of trust that can be assumed for each element of the voice communications network. It also describes the specific threats that are possible if each network component is compromised. These threats are based on the functionality specified for each component. The general categories of threats are described in section 5.2.

Both the trust and the specific threats are described with the assumption that no cryptographic or physical security has been employed in the system, with the exception of the BPI+ security that is assumed on the HFC DOCSIS links. The goal of this security specification is to address threats that are relevant to this voice communications system.

5.3.3.1 Managed IP Network

It is assumed that the same IP network may be shared between multiple, possibly competing service providers. It is also assumed that the service provider may provide multiple services on the same IP network, e.g., Internet connectivity. No assumptions can be made about the physical security of each link in this IP network. An intruder can pop up at any location with the ability to monitor traffic, perform message modification and to reroute messages.

5.3.3.2 MTA

The MTA is considered to be an untrusted network element. It is operating inside customer premises, considered to be a hostile environment. It is assumed that a hostile adversary has the ability to open up the MTA and make software and even hardware modifications to fit his or her needs. This would be done in the privacy of the customer's home.

The MTA communicates with the CMTS over the shared DOCSIS path and has access to downstream and upstream messages from other MTAs within the same HFC segment.

An MTA is responsible for:

- Initiating and receiving communications to/from another MTA or the PSTN
- Negotiating QoS

A compromise of an MTA can result in:

- MTA clones that are capable of:
 - Accessing basic service and any enhanced features in the name of another user's account
 - Violating privacy of the owner of the compromised MTA that doesn't know that the keys were stolen
 - Identity fraud
- An MTA running a bad code image that disrupts communications made by other MTAs or degrades network performance.

5.3.3.3 CMTS

The CMTS communicates both over the DOCSIS path and over the shared IP network. When the CMTS sends downstream messages over the DOCSIS path, it is assumed that a perpetrator cannot modify them or impersonate the CMTS. BPI+ over that path provides privacy.

However, when the CMTS is communicating over the shared IP network (e.g., with the CMS or another CMTS), no such assumptions can be made.

While the CMTS, as well as voice communications network servers are more trusted than the MTAs, they cannot be trusted completely. There is always a possibility of an insider attack.

Insider attacks at the CMTS should be addressed by cryptographic authentication and authorization of the CMTS operators, as well as by physical and procedural security, which are all out of the scope of the IPCablecom specifications.

A CMTS is responsible for:

- Reporting billing-related statistics to the RKS
- QoS allocation for MTAs over the DOCSIS path
- Implementation of BPI+ (MAC layer security) and corresponding key management

A compromise of a CMTS may result in:

- Service theft by reporting invalid information to the RKS
- Unauthorized levels of QoS
- Loss of privacy, since the CMTS holds BPI+ keys. This may not happen if additional encryption is provided above the MAC layer
- Degraded performance of some or all MTAs in that HFC segment
- Some or all of the MTAs in one HFC segment completely taken out of service

5.3.3.4 Voice Communications Network Servers are Untrusted Network Elements

Application servers used for voice communications (e.g., CMS, RKS, Provisioning, OSS, DHCP and TFTP Servers) reside on the network and can potentially be impersonated or subjected to insider attacks. The main difference would be in the damage that can be incurred in the case a particular server is impersonated or compromised.

Threats that are associated with each network element are discussed in the following subsections. To summarize those threats, a compromise or impersonation of each of these servers can result in a wide-scale service theft, loss of privacy, and in highly damaging denial-of-service attacks.

In addition to authentication of all messages to and from these servers (specified in this document), care should be taken to minimize the likelihood of insider attacks. They should be addressed by cryptographic authentication and authorization of the operators, as well as by stringent physical and procedural security, which are all out of scope of the IPCablecom specifications.

5.3.3.4.1 CMS

The Call Management Server is responsible for:

- Authorizing individual voice communications by subscribers
- QoS allocation
- Initializing the billing information in the CMTS
- Distributing per communication keys for MTA-MTA signaling, bearer channel, and DQoS messages on the MTA-CMTS and CMTS-CMTS links
- Interface to PTSN gateway

A compromised CMS can result in:

- Free voice communications service to all of the MTAs that are located in the same network domain (up to 100,000). This may be accomplished by:
 - Allowing unauthorized MTAs to create communications
 - Uploading invalid or wrong billing information to the CMTS
 - Combination of both of the above
- Loss of privacy, since the CMS distributes bearer channel keys
- Unauthorized allocation of QoS
- Unauthorized disclosure of customer identity, location (e.g., IP address), communication patterns, and a list of services to which the customer subscribes

5.3.3.4.2 RKS

The RKS is responsible for collecting billing events and reporting them to the billing system. A compromised RKS may result in:

- Free or reduced-rate service due to improper reporting of statistics
- Billing to a wrong account
- Billing customers for communications that were never made, i.e., fabricating communications
- Unauthorized disclosure of customer identity, personal information, service usage patterns, and a list of services to which the customer subscribes.

5.3.3.4.3 *OSS, DHCP & TFTP Servers*

The OSS system is responsible for:

- MTA and service provisioning
- MTA code downloads and upgrades
- Handling service change requests and dynamic reconfiguration of MTAs

A compromise of the OSS, DHCP, or TFTP server can result in:

- MTAs running illegal code, which may:
 - Intentionally introduce bugs or render the MTA completely inoperable
 - Degrade voice communications performance on the IPCablecom or HFC network
 - Configure the MTA with features to which the customer is not entitled
- MTAs configured with an identity and keys of another customer
- MTAs configured with service options for which the customer did not pay
- MTAs provisioned with a bad set of parameters that would make them perform badly or not perform at all

5.3.3.5 *PSTN Gateways*

5.3.3.5.1 *Media Gateway*

The MG is responsible for:

- Passing media packets between the IPCablecom network and the PSTN
- Reporting statistics to the RKS

A compromise of the MG may result in:

- Service theft by reporting invalid information to the RKS
- Loss of privacy on communications to/from the PSTN

5.3.3.5.2 *Signaling Gateway*

The SG is responsible for translating call signaling between the IPCablecom network and the PSTN.

A compromise of the SG may result in:

- Incorrect MTA identity reported to the PSTN
- Unauthorized services enabled within the PSTN
- Loss of PSTN connectivity
- Unauthorized disclosure of customer identity, location (e.g., IP address), usage patterns and a list of services to which the customer subscribes

6 SECURITY MECHANISMS

Unless explicitly stated otherwise, the following requirements apply to messages described by this document:

- ASN.1 encoded messages and objects **MUST** conform to the Distinguished Encoding Rules [34].
- FQDNs used as components of principal names and principal identifiers **MUST** be rendered in lower case.
- FQDNs **MUST NOT** include the root domain (i.e., they **MUST NOT** include a trailing dot).
- All Kerberos messages in IPCablecom **MUST** utilize only UDP/IP.

6.1 IPsec

6.1.1 Overview

IPsec provides network-layer security that runs immediately above the IP layer in the protocol stack. It provides security for the TCP or UDP layer and above. It consists of two protocols, IPsec ESP and IPsec AH, as specified in [19].

IPsec ESP provides confidentiality and message integrity, IP header not included. IPsec AH provides only message integrity, but that includes most of the IP header (with the exception of some IP header parameters that can change with each hop). IPCablecom utilizes only the IPsec ESP protocol [20], since authentication of the IP header does not significantly improve security within the IPCablecom architecture.

Each protocol supports two modes of use: transport mode and tunnel mode. IPCablecom only utilizes IPsec ESP transport mode. For more detail on IPsec and these two modes, refer to [19]. Note that in [19], all implementations of ESP are required to support the concept of Security Associations (SAs). The IETF RFC, [19], also provides a general model for processing IP traffic relative to SAs.

Although particular IPsec implementations need not follow the details of this general model, the external behavior of any IPsec implementation must match the external behavior of the general model. This ensures that components do not accept traffic from unknown addresses and do not send or accept traffic without security (when security is required). IPCablecom components that implement IPsec are expected to provide behavior that matches the general model described in [19].

6.1.2 IPCablecom Profile for IPsec ESP (Transport Mode)

6.1.2.1 IPsec ESP Transform Identifiers

IPsec Transform Identifier (1 byte) is used by IKE to negotiate an encryption algorithm that is used by IPsec. A list of available IPsec Transform Identifiers is specified in [21]. Within IPCablecom, the same Transform Identifiers are used by all IPsec key management protocols: IKE, Kerberos, and application layer (embedded in IP signaling messages).

The following table describes the IPsec Transform Identifiers (all of which use the CBC mode specified in [22]) supported by IPCablecom.

Table 2. IPsec ESP Transform Identifiers

Transform ID	Value (Hex)	Key Size (in bits)	MUST Support	Description
ESP_3DES	0x03	192	yes	3-DES in CBC mode.
ESP_RC5	0x04	128	no	RC5 in CBC mode
ESP_IDEA	0x05	128	no	IDEA in CBC mode
ESP_CAST	0x06	128	no	CAST in CBC mode
ESP_BLOWFISH	0x07	128	no	BLOWFISH in CBC mode
ESP_NULL	0x0B	0	yes	Encryption turned off
ESP_AES	0x0C	128	no	AES-128 in CBC mode with 128-bit block size

The ESP_3DES and ESP_NULL Transform IDs **MUST** be supported. ESP_AES is included as an optional encryption algorithm. For all of the above transforms, the CBC Initialization Vector (IV) is carried in the clear inside each ESP packet payload [22]. AES-128 [33] **MUST** be used in CBC mode with a 128-bit block size and a randomly generated Initialization Vector (IV). AES-128 requires 10 rounds of cryptographic operations [33].

IKE allows negotiation of the encryption key size. Other IPsec Key Management protocols used by IPCablecom do not allow key size negotiation, and so for consistency a single key size is listed for each Transform ID. If in the future it is desired to increase the key size for one of the above algorithms, IKE will use the built-in key-size negotiation, while other key management protocols will utilize a new Transform ID for the larger key size.

6.1.2.2 IPsec ESP Authentication Algorithms

The IPsec Authentication Algorithm (1-byte) is used by IKE to negotiate a packet-authentication algorithm that is used by IPsec. A list of available IPsec Authentication Algorithms is specified in [21]. Within IPCablecom, the same Authentication Algorithms are used by all IPsec key management protocols: IKE, Kerberos and application layer (embedded in IP signaling messages).

IPCablecom supports the IPsec authentication algorithms listed in Table 3.

Table 3. IPsec Authentication Algorithms

Authentication Algorithm	Value (Hex)	Key Size (in bits)	MUST Support	Description
HMAC-MD5-96	0x01	128	yes (also required by [21])	First 12 bytes of the HMAC-MD5 as described in [35]
HMAC-SHA-1-96	0x02	160	yes	First 12 bytes of the HMAC-SHA1 as described in [23]

The HMAC-MD5-96 and HMAC-SHA-1-96 authentication algorithms **MUST** be supported.

6.1.2.3 Replay Protection

In general, IPsec provides an optional replay-protection service (anti-replay service). An IPsec sequence number outside of the current anti-replay window is flagged as a replay and the packet is rejected. When the anti-replay service is turned on, an IPsec sequence number cannot overflow and roll over to 0. Before that happens, a new Security Association must be created as specified in [20].

Within IPCablecom Security Specification, the IPsec anti-replay service **MUST** be turned on at all times. This is regardless of which key-management mechanism is used with the particular IPsec interface.

6.1.2.4 Key Management Requirements

Within IPCablecom, IPsec is used on a number of different interfaces with different security and performance requirements. Because of this, several different key management protocols have been chosen for different IPCablecom interfaces. On some interfaces it is IKE (see section 6.2), on other interfaces it is Kerberos/PKINIT (see section 6.4).

When IKE is not used for key management, an alternative key management protocol needs an interface to the IPsec layer in order to create/update/delete IPsec Security Associations (SAs). IPsec Security Associations **MUST** be automatically established or re-established as required. This implies that the IPsec layer also needs a way to signal a key management application when a new Security Association needs to be set up (e.g., the old SA is about to expire or there is no SA on a particular interface).

In addition, some network elements are required to run multiple key management protocols. In particular, the Application Server (such as a CMS) and the MTA must support multiple key management protocols. The MTA **MUST** support Kerberos/PKINIT on the MTA-CMS signaling interface. IKE **MUST** be supported on the CMS-CMTS and CMS-RKS interfaces.

The PF_KEY interface (see [28]) **SHOULD** be used for IPsec key management within IPCablecom and would satisfy the above listed requirements. For example, PF_KEY permits multiple key management applications to register for rekeying events. When the IPsec layer detects a missing Security Association, it signals the event to all registered key-management applications. Based on the Identity Extension associated with that Security Association, each key-management application decides if it should handle the event.

6.2 Internet Key Exchange (IKE)

6.2.1 Overview

IPCablecom utilizes IKE as one of the key management protocols for IPsec [24]. It is utilized on interfaces where:

- There are not a very large number of connections
- The endpoints on each connection know about each other's identity in advance

Within IPCablecom, IKE key management is completely asynchronous to call signaling messages and does not contribute to any delays during communications setup. The only exception would be some unexpected error, where Security Association is unexpectedly lost by one of the endpoints.

IKE is a peer-to-peer key management protocol. It consists of 2 phases. In the first phase, a shared secret is negotiated via a Diffie-Hellman key exchange. It is then used to authenticate the second IKE phase. The second phase negotiates another secret, used to derive keys for the IPsec ESP protocol.

6.2.2 IPCablecom Profile for IKE

6.2.2.1 First IKE Phase

There are several modes defined for authentication during the first IKE phase.

6.2.2.1.1 IKE Authentication with Signatures

In this mode, both peers **MUST** be authenticated with X.509 certificates and digital signatures. IPCablecom utilizes this IKE authentication mode on some IPsec interfaces. Whenever this mode is utilized, both sides **MUST** exchange X.509 certificates (although this is optional in [24]).

6.2.2.1.2 IKE Authentication with Public-Key Encryption

IPCablecom **MUST NOT** utilize this IKE authentication with public key encryption. In order to perform this mode of IKE authentication, the initiator must already have the responder's public key, which is not supported by IPCablecom.

6.2.2.1.3 *IKE Authentication with Pre-Shared Keys*

A key derived by some out-of-band (e.g., manual) mechanism is used to authenticate the exchange. IPCablecom utilizes this IKE authentication mode on some IPsec interfaces. IPCablecom does not specify the out-of-band method for deriving pre-shared keys.

When using pre-shared keys, the strength of the system is dependent upon the strength of the shared secret. The goal is to keep the shared secret from being the weak link in the chain of security. This implies that the shared secret needs to contain as much entropy (randomness) as the cipher being used. In other words, the shared secret should have at least 128-160 bits of entropy. This means if the shared secret is just a string of random 8-bit bytes, then of the key can be 16-20 bytes. If the shared secret is derived from a passphrase that is a string of random alpha- numerics (a-zA-Z0-9/+), then it should be at least 22-27 characters. This is because there are only 64 characters (6 bits) instead of 256 characters (8 bits) per 8-bit byte, which implies an expansion of 4/3 the length for the same amount of entropy.

Both random 8-bit bytes and random 6-bit bytes assume truly random numbers. If there is any structure in the password/passphrase, like deriving from English, then even longer passphrases are necessary. A passphrase composed of English would need on the order of 60-100 characters, depending on mixing of case. Using English passphrases (or any language, for that matter) creates the problem that, if an attacker knows the language of the passphrase then they have less space to search. It is less random. This implies fewer bits of entropy per character, so a longer passphrase is required to maintain the same level of entropy.

6.2.2.2 *Second IKE Phase*

In the second IKE phase, an IPsec ESP SA is established, including the IPsec ESP keys and ciphersuites. It is possible to establish multiple Security Associations with a single second-phase IKE exchange.

First, a shared second phase secret is established, and then all the IPsec keying material is derived from it using the one-way function specified in [24].

The second-phase secret is built from encrypted nonces that are exchanged by the two parties. Another Diffie-Hellman exchange may be used in addition to the encrypted nonces. Within IPCablecom, IKE MUST NOT perform a Diffie-Hellman exchange in the second IKE phase in order to avoid the associated performance penalties.

The second IKE phase is authenticated using a shared secret that was established in the first phase. Supported authentication algorithms are the same as those specified for IPsec in section 6.1.2.2.

6.2.2.3 *Encryption Algorithms for IKE Exchanges*

Both phase 1 and phase 2 IKE exchanges include some symmetrically-encrypted messages. The encryption algorithms supported as part of the IPCablecom Profile for IKE MUST be the same algorithms identified in the IPCablecom profile for IPsec ESP in Table 2 of section 6.1.2.1.

6.2.2.4 *Diffie-Hellman Groups*

IKE defines specific sets of Diffie-Hellman parameters (i.e., prime and generator) that may be used for the phase 1 IKE exchanges. These are called groups in [24]. The use of Diffie-Hellman groups within IPCablecom IKE is identical to that specified in [24]: the first group MUST be supported and the remaining groups SHOULD be supported. Note that this is different from the requirements pertaining to the IPCablecom use of groups in PKINIT described in section 6.4.2.1.1. Appendix VI provides details of the first and second Oakley groups.

6.3 *SNMPv3*

Any mention of SNMP in this specification without a specific reference to the SNMP protocol version must be interpreted as SNMPv3.

IPCablecom supports use of SNMPv2c coexistence for network management operations for devices provisioned under the Basic Flow or the Hybrid Flow. It also supports the SNMPv3/v2c coexistence for network management operations when the device is provisioned under the Secure Flow. Refer to the provisioning specification [4] for the use of SNMP coexistence in IPCablecom.

For any interface within the IPCablecom architecture utilizing SNMPv3, SNMPv3 authentication **MUST** be turned on at all times and SNMPv3 privacy **MAY** also be utilized.

In order to establish SNMPv3 keys, all IPCablecom SNMP interfaces **SHOULD** utilize Kerberized SNMPv3 key management (as specified in section 6.5.4). In addition, SNMPv3 key management techniques specified in [27] **MAY** also be used.

6.3.1 SNMPv3 Transform Identifiers

The SNMPv3 Transform Identifier (1 byte) is used by Kerberized key management to negotiate an encryption algorithm for use by SNMPv3.

For IPCablecom, the following SNMPv3 Transform Identifiers are supported:

Table 4. SNMPv3 Transform Identifiers

Transform ID	Value (Hex)	Key Size (in bits)	MUST be Supported	Description
SNMPv3_DES	0x21	128	yes	DES in CBC mode. The first 64 bits are used as the DES Key and the remaining 64 are used as the pre-IV as described in [27].
SNMPv3_NULL	0x20	0	yes	Encryption turned off

The SNMPv3_DES and the SNMPv3_NULL Transform IDs **MUST** be supported. The DES encryption transform for SNMPv3 is specified in [27]. Note that DES encryption does not provide strong privacy but is currently the only encryption algorithm specified by the SNMPv3 standard.

6.3.2 SNMPv3 Authentication Algorithms

SNMPv3 Authentication Algorithm (1 byte) is used by Kerberized key management to negotiate an SNMPv3 message authentication algorithm.

For IPCablecom, the following SNMPv3 Authentication Algorithms are supported (both of which are specified in [27]):

Table 5. SNMPv3 Authentication Algorithms

Authentication Algorithm	Value (Hex)	Key Size (in bits)	MUST be supported	Description
SNMPv3_HMAC-MD5	0x21	128	yes (also required by [27])	MD5 HMAC
SNMPv3_HMAC-SHA-1	0x22	160	no (SHOULD be supported)	SHA-1 HMAC

The SNMPv3_HMAC-MD5 Authentication Algorithm **MUST** be supported. The SNMPv3_HMAC-SHA-1 Authentication Algorithm **SHOULD** be supported.

6.4 Kerberos / PKINIT

6.4.1 Overview

IPCablecom utilizes the concept of Kerberized IPsec for signaling between an Application Server, such as the CMS, and the MTA. This refers to the ability to create IPsec Security Associations using keys derived from the subkeys exchanged using the Kerberos AP Request/AP Reply messages. On this interface, Kerberos (Appendix II) is utilized with the PKINIT public key extension (also see Appendix III).

Kerberized IPsec consists of three distinct phases:

1. A client SHOULD obtain a TGT (Ticket Granting Ticket) from the KDC (Key Distribution Center). Once the client obtains the TGT, it MUST use the TGT in the subsequent phase to authenticate to the KDC and obtain a ticket for the specific Application Server, e.g., a CMS.

In Kerberos, tickets are symmetric authentication tokens encrypted with a particular server's key. (For a TGT, the server is the KDC.) Tickets are used to authenticate a client to a server. A PKI equivalent of a ticket would be an X.509 certificate. In addition to authentication, a ticket is used to establish a session key between a client and a server, where the session key is contained in the ticket.

The logical function within the KDC that is responsible for issuing TGTs is referred to as an Authentication Server or AS.

2. A client obtains a ticket from the KDC for a specific Application Server. In this phase, a client can authenticate with a TGT obtained in the previous phase. A client can also authenticate to the KDC directly using a digital certificate or a password-derived key, bypassing phase 1.

The logical function within the KDC that is responsible for issuing Application Server tickets based on a TGT is referred to as the Ticket Granting Server – TGS. When the TGT is bypassed, it is the Authentication Server that issues the Application Server tickets.

3. A client utilizes the ticket obtained in the previous phase to establish a pair of Security Parameters (one to send and one to receive) with the server. This is the only key management phase that is not already specified in an IETF standard. The previous two phases are part of standard Kerberos, while this phase defines new messages that tie together Kerberos key management and IPsec.

Figure 4 illustrates the three phases of Kerberos-based key management for IPsec:

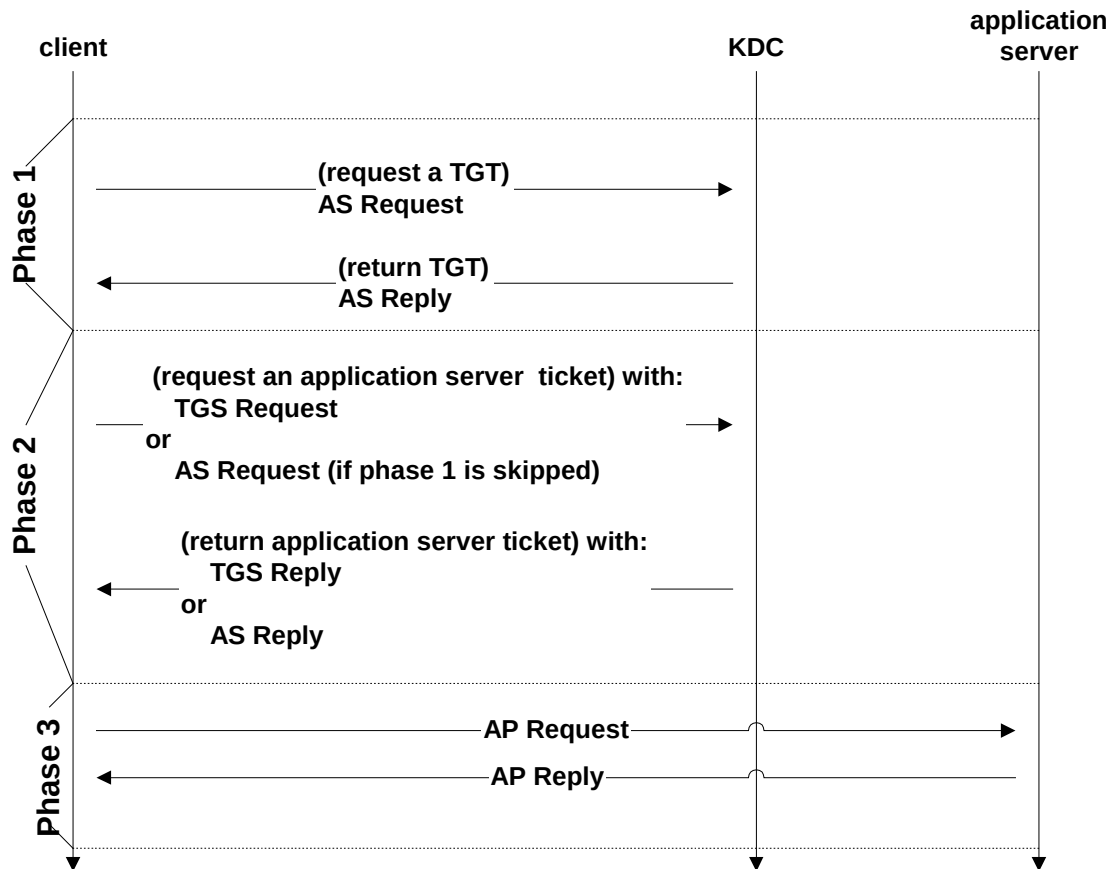


Figure 4. Kerberos-Based Key Management for IPsec

During the AS Request / AS Reply exchange (that can occur in either phase 1 or phase 2), the client and the KDC perform mutual authentication. In standard Kerberos, a client key that is shared with the KDC is used for this authentication (see section 6.4.4). The same AS Request / AS Reply exchange may also be authenticated with digital signatures and certificates when the PKINIT public key extension is used (see section 6.4.2). Both the TGT and the Application Server tickets used within IPCablecom have a relatively long lifetime (days or weeks). This is acceptable as 3-DES, a reasonably strong symmetric algorithm, is required by IPCablecom.

IPCablecom utilizes the concept of a TGT (Ticket Granting Ticket), used to authenticate subsequent requests for Application Server tickets. The use of a TGT has two main advantages:

- It limits the exposure of the relatively long-term client key (that is in some cases reused as the service key). This consideration does not apply to clients that use PKINIT.
- It reduces the number of public key operations that are required for PKINIT clients.

The Application Server ticket contains a symmetric session key, which **MUST** be used in phase 3 to establish a set of keys for the IPsec ESP protocol. The keys used by IPsec **MUST** expire after a configurable time-out period (e.g., 10 minutes). This section provides specifications for how to automatically establish a new IPsec SA right before the expiration of the old one and how to establish IPsec SAs on-demand, when a signaling message needs to be sent.

Normally, the same Application Server ticket **SHOULD** be used to automatically establish a new IPsec SA. However, there are instances where it is desirable to drop IPsec sessions after a Security Association time out and establish them on-demand later. This allows for improved system scalability, since an application server (e.g., CMS)

does not need to maintain a SA for every client (e.g., MTA) that it controls. It is also possible that a group of application servers (e.g., CMS cluster) may control the same subset of clients (e.g., MTAs) for load balancing. In this case, the MTA is not required to maintain a SA with each CMS in that group.

IPCablecom also utilizes the Kerberos protocol to establish SNMPv3 keys between the MTAs and the Provisioning Server. Kerberized SNMPv3 key management is very similar to the Kerberized IPsec key management and consists of the same phases that were explained above for Kerberized IPsec. Each MTA again utilizes the PKINIT extension to Kerberos to authenticate itself to the KDC with X.509 certificates.

Once an MTA obtains its service ticket for the Provisioning Server, it utilizes the same protocol that is used for Kerberized IPsec to authenticate itself to the Provisioning Server and to generate SNMPv3 keys. The key management protocol is specified to allow application-specific data that has different profiles for SNMPv3 and IPsec. The only exception is the Rekey exchange that is specified for IPsec in order to optimize the MTA hand-off between the members of a CMS cluster. The Rekey exchange is not utilized for SNMPv3 key management.

A recipient of any Kerberos message that doesn't fully comply with the IPCablecom requirements **MUST** reject the message.

6.4.1.1 Kerberos Ticket Storage

Kerberos clients that store tickets in persistent storage will be able to re-use the same Kerberos ticket after a reboot. In the event that PKINIT is used, this avoids the need to perform public key operations.

A Kerberos client **MUST NOT** obtain a new TGT upon reboot if it possesses a valid service ticket.

An MTA **MUST** store the Provisioning Server service ticket in persistent storage. An MTA **MUST** be capable of storing a minimum of $\text{pkcMtaDevEndPntCount}+1$ CMS service tickets in persistent storage, where $\text{pkcMtaDevEndPntCount}$ is the MIB object specifying the number of physical endpoints on the MTA. An MTA **MUST** store all CMS service tickets that correspond to active endpoints. This means that an MTA that reaches the maximum number of CMS service tickets that can be stored in persistent storage will not over-write CMS service tickets that correspond to active endpoints.

Kerberos clients other than MTAs **SHOULD** retain service tickets in persistent storage.

Note that Kerberos clients will need to store additional information in order to use and validate the ticket, such as the session key information, the client IP address, and the ticket validity period. Refer to section 7.1 for additional information on reusing stored tickets.

6.4.2 PKINIT Exchange

The diagram below illustrates how a client may use PKINIT to either obtain a TGT (phase 1) or a Kerberos ticket for an Application Server (phase 2).

The PKINIT Request is carried as a Kerberos pre-authenticator field inside an AS Request and the PKINIT Reply is a pre-authenticator inside the AS Reply. The syntax of the Kerberos AS Request / Reply messages and how pre-authenticators plug in is specified in Appendix II.

In this section, the PKINIT client is referred to as an MTA, as it is currently the only IPCablecom element that authenticates itself to the KDC with the PKINIT protocol. If in the future other IPCablecom elements will also utilize the PKINIT protocol, the same specifications will apply. IPCablecom use of the AS Request / AS Reply exchange without PKINIT is covered in section 6.4.3.

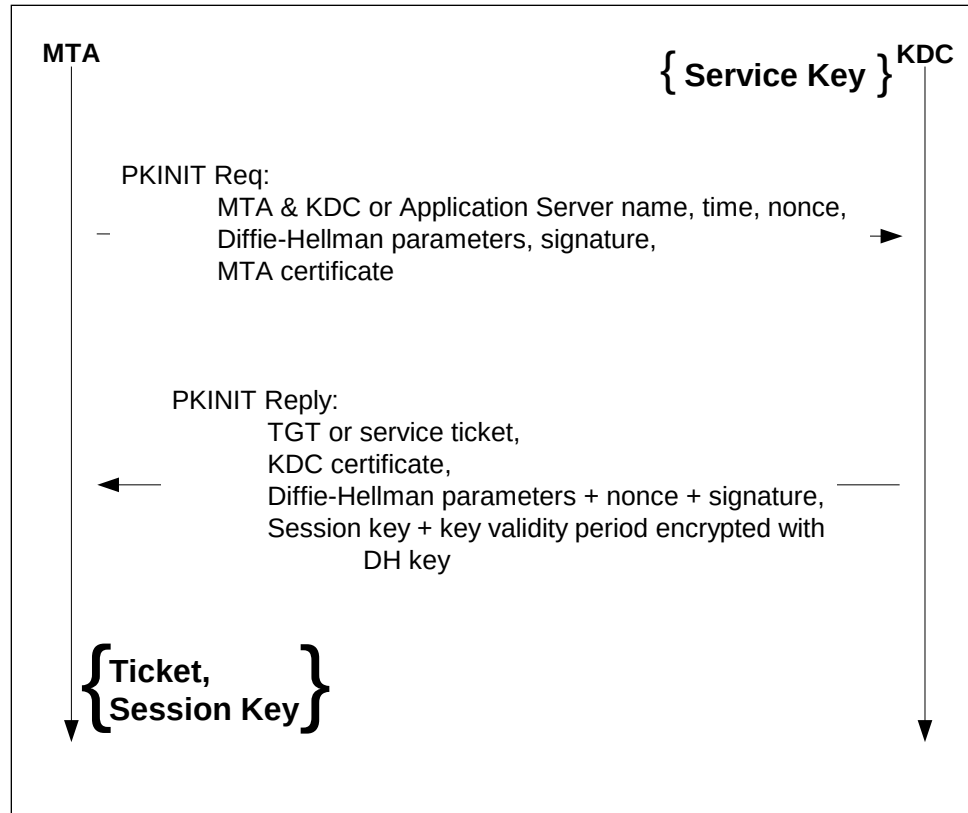


Figure 5. PKINIT Exchange

The above diagram lists several important parameters in the PKINIT Request and Reply messages. These parameters are:

PKINIT Request

- MTA (Kerberos principal) name – found in the KDC-REQ-BODY Kerberos structure (see Appendix II). For the format used in IPCablecom, see section 6.4.7.
- KDC or Application Server (Kerberos principal) name – found in the KDC-REQ-BODY Kerberos structure (see Appendix II). For the format used in IPCablecom, see section 6.4.6.
- Time – found in the PKAuthenticator structure, specified by PKINIT (Appendix III).
- Nonce – found in the PKAuthenticator structure, specified by PKINIT (Appendix III). There is also a second nonce in the KDC-REQ-BODY Kerberos structure.
- Diffie-Hellman parameters, signature and MTA certificate – these are all specified by PKINIT (Appendix III) and their use in IPCablecom is specified in section 6.4.2.1.1. Appendix VI provides details of the first and second Oakley groups.

PKINIT Reply

- TGT or Application Server Ticket – found in the KDC-REP Kerberos structure (see Appendix II).
- KDC Certificate, Diffie-Hellman parameters, signature – these are all specified by PKINIT (see Appendix III) and their use in IPCablecom is specified in section 6.4.2.1.2. Appendix VI provides details of the first and second Oakley groups.
- Nonce – found in the KdcDHKeyInfo structure, specified by PKINIT (Appendix III). This nonce must be the same as the one found in the PKAuthenticator structure of the PKINIT Request. There is another nonce in

EncKDCRepPart Kerberos structure (see Appendix II). This nonce must be the same as the one found in the KDC-REQ-BODY of the PKINIT Request.

- Session key, key validity period – found in the EncKDCRepPart Kerberos structure (see Appendix II).

In this diagram, the PKINIT exchange is performed at long intervals, in order to obtain an (intermediate) symmetric session key. This session key is shared between the MTA and the server via the server's ticket, where the application server may be the KDC (in which case the ticket is the TGT).

6.4.2.1 PKINIT Profile for IPCablecom

A particular MTA implementation **MUST** utilize the PKINIT exchange to either obtain Application Server tickets directly, or obtain a TGT first and then use the TGT to obtain Application Server tickets. An MTA implementation **MAY** also support both uses of PKINIT, where the decision to get a TGT first or not is local to the MTA and is dependent on a particular MTA implementation. On the other hand, the KDC **MUST** be capable of processing PKINIT requests for both a TGT and for Application Server tickets.

The PKINIT exchange occurs independent of the signaling protocol, based on the current Ticket Expiration Time (Ticket_{EXP}) and on the PKINIT Grace Period (PKINIT_{GP}). If the PKINIT client is an MTA and the ticket it currently possesses corresponds to the Provisioning Server in the MIB, a KDC for a REALM that currently exists in the REALM table, or a CMS that currently exists in the CMS table, the MTA **MUST** initiate the PKINIT exchange at the time: Ticket_{EXP} - PKINIT_{GP}.

If the PKINIT client is an MTA and the ticket it currently possesses does not correspond to the Provisioning Server in the MIB, a KDC for a REALM that currently exists in the REALM table, or a CMS that currently exists in the CMS table, the MTA **MUST NOT** initiate a PKINIT exchange. On the interfaces where PKINIT_{GP} is not defined, the MTA **SHOULD** perform PKINIT exchanges on-demand.

In the case where PKINIT is used to obtain an Application Server ticket directly, the use of the grace period accounts for a possible clock skew between the MTA and the CMS or other application server. If the MTA is late with the PKINIT exchange, it still has until Ticket_{EXP} before the Application Server starts rejecting the ticket. Similarly, if PKINIT is used to obtain a TGT the grace period accounts for a possible clock skew between the MTA and the KDC.

The PKINIT exchange stops after the MTA obtains a new ticket, and therefore does not affect existing security parameters between the MTA and the CMS or other application server. Synchronizing the PKINIT exchange with the AP Request/Reply exchange is not required as long as the AS Request/Reply exchange results in a valid, non-expired Kerberos ticket.

The PKINIT Request/Reply messages contain public key certificates, which make them longer than a normal size of a UDP packet. In this case, large UDP packets **MUST** be sent using IP fragmentation.

A KDC server should be implemented on a separate host, independent of the Application Server. This would mean, that frequent PKINIT operations from some MTAs will not affect the performance of any of the application servers or the performance of those MTAs that do not require frequent PKINIT exchanges.

Kerberos Tickets **MUST NOT** be issued for a period of time that is longer than 7 days. The MTA clock **MUST NOT** drift more than 2.5 minutes within that period (7 days). The PKINIT Grace Period PKINIT_{GP} **MUST** be at least 15 minutes.

6.4.2.1.1 PKINIT Request

The PKINIT Request message (PA-PK-AS-REQ) in Appendix III is defined as:

```
PA-PK-AS-REQ ::= SEQUENCE {
    signedAuthPack    [0] ContentInfo,
    trustedCertifiers [1] SEQUENCE OF TrustedCas OPTIONAL,
    kdcCert            [2] IssuerAndSerialNumber OPTIONAL,
    encryptionCert    [3] IssuerAndSerialNumber OPTIONAL
}
```

The following fields MUST be present in PA-PK-AS-REQ for IPCablecom (and all other fields MUST NOT be present):

- signedAuthPack – a signed authenticator field, needed to authenticate the client. It is defined in Cryptographic Message Syntax, identified by the SignedData OID:{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs7(7) 2}. SignedData is defined as:

```
SignedData ::= SEQUENCE {
    version          CMSVersion,
    digestAlgorithms DigestAlgorithmIdentifiers,
    encapContentInfo EncapsulatedContentInfo,
    certificates      [0] IMPLICIT CertificateSet OPTIONAL,
    crls              [1] IMPLICIT CertificateRevocationLists
                     OPTIONAL,
    signerInfos       SignerInfos
}
```

- digestAlgorithms - for now MUST contain an algorithm identifier for SHA-1. Other digest algorithms may optionally be supported in the future.
- encapContentInfo – is of type EncapsulatedContentInfo that is defined by Cryptographic Message Syntax as:

```
EncapsulatedContentInfo ::= SEQUENCE {
    eContentType      ContentType,
    eContent           [0] EXPLICIT OCTET STRING OPTIONAL
}
```

The pachecksum field MUST use the Kerberos checksum type rsa-md5, a plain MD5 checksum over the KDC-REQ-BODY.

The nonce field MUST be non-zero, indicating that the client does not support the caching of Diffie-Hellman values and their expiration.

- certificates - required by IPCablecom. This field MUST contain an MTA Device Certificate and an MTA Manufacturer Certificate. This field MUST NOT contain any other certificates. All IPCablecom certificates are X.509 certificates for RSA Public keys as specified in section 8.
- crls – MUST NOT be filled in by the MTA.
- signerInfos – MUST be a set with exactly one member that holds the MTA signature. This signature is a part of a SignerInfo data structure defined within the Cryptographic Message Syntax. All optional fields in this data structure MUST NOT be used in IPCablecom. The digestAlgorithm MUST be set to SHA-1:

```
{iso(1) identified-organization(3) oiw(14) secsig(3) algorithm(2) 26}
```

and the signatureAlgorithm MUST be set to rsaEncryption:

```
{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
```

PKINIT allows an Ephemeral-Ephemeral Diffie-Hellman exchange as part of the PKINIT Request/Reply sequence. (Ephemeral-Ephemeral means that both parties during each exchange randomly generate the Diffie-Hellman private exponents.) The Kerberos session key is returned to the MTA in the PKINIT Reply, encrypted with a secret that is derived from the Diffie-Hellman exchange. Within IPCablecom, the Ephemeral-Ephemeral Diffie-Hellman MUST be supported.

The IKE specification in [24] defines Diffie-Hellman parameters as Oakley groups. Within the IPCablecom PKINIT profile the second Oakley group MUST be supported and the first Oakley group MAY also be supported. Appendix VI provides details of the first and second Oakley groups.

When generating Diffie-Hellman private keys, a device MUST generate a key of length at least 144 bits when the first Oakley group is used and MUST generate a key of length at least 164 bits when the second Oakley group is used.

For further details of PKINIT, refer to Appendix III.