

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

J.125

(12/2007)

SERIES J: CABLE NETWORKS AND TRANSMISSION
OF TELEVISION, SOUND PROGRAMME AND OTHER
MULTIMEDIA SIGNALS

Interactive systems for digital television distribution

Link privacy for cable modem implementations

ITU-T Recommendation J.125

ITU-T Recommendation J.125

Link privacy for cable modem implementations

Summary

ITU-T Recommendation J.125 was Annex O to ITU-T Recommendation J.112 Annex B. Since it is also applicable to MAC layer privacy services for ITU-T Recommendation J.122, it became a stand-alone Recommendation (J.125). This Recommendation, often referred to as Baseline Privacy Interface Plus or BPI+, has the following two goals:

- provide cable modem users with data privacy across the cable network; and
- provide cable operators with service protection; i.e., prevent unauthorized users from gaining access to the network's RF MAC services.

BPI+ provides a level of data privacy across the shared medium cable network equal to or better than that provided by dedicated line network access services (analog modems or digital subscriber lines).

Source

ITU-T Recommendation J.125 was approved on 14 December 2007 by ITU-T Study Group 9 (2005-2008) under the ITU-T Recommendation A.8 procedure.

... ..

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2008

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

CONTENTS

Page

1	Scope	1
2	References.....	1
2.1	Normative	1
2.2	Informative	2
3	Terms and definitions	2
4	Abbreviations.....	3
5	Baseline privacy plus background and overview	3
5.1	Architectural overview	4
5.2	Operational overview	7
6	DOCSIS MAC frame formats	9
6.1	Variable-length packet data PDU MAC frame format.....	9
6.2	Fragmentation MAC frame format.....	11
6.3	Requirements on usage of BP extended header element	13
7	Baseline privacy key management (BPKM) protocol	13
7.1	State models.....	13
7.2	Key management message formats	29
8	Dynamic SA mapping.....	53
8.1	Introduction	53
8.2	Theory of operation	54
8.3	SA Mapping state model	55
8.4	IP multicast traffic and dynamic SAs	58
9	Key usage	59
9.1	CMTS	59
9.2	Cable modem.....	62
9.3	Authentication of DOCSIS v1.1/2.0 dynamic service requests	62
10	Cryptographic methods.....	63
10.1	Packet data encryption.....	63
10.2	Encryption of TEK	64
10.3	HMAC-Digest algorithm.....	64
10.4	Derivation of TEKs, KEKs and message authentication keys	64
10.5	Public-key encryption of authorization key	65
10.6	Digital signatures.....	65
10.7	Supporting alternative algorithms	65
11	Physical protection of keys in the CM and CMTS	66
12	BPI+ X.509 certificate profile and management	66
12.1	BPI+ certificate management architecture overview	67
12.2	Certificate format.....	68

	Page
12.3 Cable modem certificate storage and management in the CM.....	74
12.4 Certificate processing and management in the CMTS	74
Annex A – TFTP configuration file extensions	78
A.1 Encodings	78
A.2 Parameter guidelines	80
Annex B – Verifying downloaded operational software	82
B.1 Introduction	82
B.2 Overview	82
B.3 Code upgrade requirements	84
B.4 Security considerations (Informative)	97
Annex C – BPI/BPI+ interoperability	99
C.1 DOCSIS v1.0/v1.1/v2.0 interoperability	99
C.2 DOCSIS BPI/BPI+ interoperability requirements.....	99
C.3 BPI 40-bit DES export mode considerations.....	100
C.4 System operation	101
Annex D – Upgrading from BPI to BPI+	102
D.1 Hybrid cable modem with BPI+.....	102
D.2 Upgrading procedure	102
Appendix I – Example messages, certificates and PDUs	103
I.1 Notation	103
I.2 Authentication Info.....	103
I.3 Authorization Request	105
I.4 Authorization Reply	108
I.5 Key Request.....	114
I.6 Key Reply	115
I.7 Packet PDU encryption	118
I.8 Encryption of packet PDU with payload header suppression	122
I.9 Fragmented packet encryption	124
Bibliography.....	126

ITU-T Recommendation J.125

Link privacy for cable modem implementations

1 Scope

This Recommendation provides MAC layer privacy (encryption and authentication) services for DOCSIS CMTS-CM communications. This Recommendation, often referred to as Baseline Privacy Interface Plus or BPI+, has the following two goals:

- provide cable modem users with data privacy across the cable network; and
- provide cable operators with service protection; i.e., prevent unauthorized users from gaining access to the network's RF MAC services.

BPI+ provides a level of data privacy across the shared medium cable network equal to or better than that provided by dedicated line network access services (analog modems or digital subscriber lines).

NOTE – The structure and content of this Recommendation have been organized for ease of use by those familiar with the original source material; as such, the usual style of ITU-T recommendations has not been applied.

2 References

2.1 Normative

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated are valid. All Recommendations and other references are subject to revisions; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

- [ITU-T J.112-B] ITU-T Recommendation J.112 Annex B (2004), *Data-over-cable service interface specifications: Radio-frequency interface specification*.
- [ITU-T J.122] ITU-T Recommendation J.122 (2007), *Second-generation transmission systems for interactive cable television services – IP cable modems*.
- [ITU-T X.509] ITU-T Recommendation X.509 (2000) | ISO/IEC 9594-8:2001, *Information technology – Open Systems Interconnection – The Directory: Public-key attribute certificate frameworks*.
- [FIPS-46-3] Federal Information Processing Standards Publications 46-3 (1999), *Data Encryption Standard (DES)*.
- [FIPS-140-2] Federal Information Processing Standards Publication 140-2 (2001), *Security Requirements for Cryptographic Modules*.
- [FIPS-180-2] Federal Information Processing Standards Publication 180-2 (2002), *Secure Hash Standard (SHS)*.
- [IETF RFC 2104] IETF RFC 2104 (1997), *HMAC: Keyed-Hashing for Message Authentication*.
- [IETF RFC 3083] IETF RFC 3083 (2001), *Baseline Privacy Interface Management Information Base for DOCSIS Compliant Cable Modems and Cable Modem Termination Systems*.

- [IETF RFC 3280] IETF RFC 3280 (2002), *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.
- [PKCS #7] IETF RFC 2315 (1998), *PKCS #7: Cryptographic Message Syntax Version 1.5*.
- [RSA3] *PKCS #1: RSA Cryptography Specifications Version 2.0*, October 1998.
- [SCTE22-2] ANSI/SCTE 22-2 2002, *Data-Over-Cable Service Specification DOCSIS 1.0 Part 2: Baseline Privacy Interface (BPI)*. www.scte.org
- [SCTE23-3] ANSI/SCTE 23-3 2003, *DOCSIS 1.1 Part 3: Operations Support System Interface*. www.scte.org
- [SCTE79-2] ANSI/SCTE 79-2 2002, *DOCS 2.0 Operations Support System Interface*. www.scte.org

2.2 Informative

- [DOCSIS4] *Data-Over-Cable Service Interface Specifications DOCSIS 1.1, Cable Modem to Customer Premise Equipment Interface Specification*, SP-CMCI-I09-030730, July 30, 2003.
- [DOCSIS8] *Management Information Base for DOCSIS Cable Modems and Cable Modem Termination Systems for Baseline Privacy Plus*, draft-ietf-ipcdn-bpiplus-mib-05.txt, May 8, 2001.
- [FIPS-74] Federal Information Processing Standards Publication 74 (1981), *Guidelines for Implementing and Using the NBS Data Encryption Standard*.
- [FIPS-81] Federal Information Processing Standards Publication 81 (1980), *DES Modes of Operation*. (Includes Change Notice, November 1981).
- [FIPS-186-2] Federal Information Processing Standards Publication 186-2 (2000), *Digital Signature Standard (DSS)*.
- [IETF RFC 2868] IETF RFC 2868 (2000), *RADIUS Attributes for Tunnel Protocol Support*.
- [RSA1] RSA Laboratories, *PKCS #1: RSA Encryption Standard, Version 1.5*, RSA Security, Inc., Bedford, MA, November 1993.
- [RSA2] RSA Laboratories, *Some Examples of the PKCS Standards*, RSA Data Security, Inc., Redwood City, CA, November 1993.
- [SCTE22-1] ANSI/SCTE 22-1 2002, *Data-Over-Cable Service Interface Specification DOCSIS 1.0 Part 1: Radio Frequency Interface (RFI)*. www.scte.org
- [SCTE22-3] ANSI/SCTE 22-3 2002, *Data-Over-Cable Service Interface Specification DOCSIS 1.1 Part 3: Operations Support System Interface (OSSI)*. www.scte.org

3 Terms and definitions

This Recommendation defines the following terms:

3.1 DOCSIS: The term for a system or device compliant with any one of the Cable Television Laboratories, Inc. ("CableLabs") series of specifications located at: <http://www.cablemodem.com/specifications/>.

3.2 DOCSIS 1.0: A system or device compliant with the following Data Over Cable Service Interface Specifications [SCTE22-1], [SCTE22-2], [SCTE22-3], [DOCSIS4].

3.3 DOCSIS 1.1: A system or device compliant with the following Data Over Cable Service Interface Specifications: [ITU-T J.112-B], [SCTE23-3], [DOCSIS4] and this Recommendation.

3.4 DOCSIS 2.0: A system or device compliant with the following Data Over Cable Service Interface Specifications [ITU-T J.122], [SCTE79-2], [DOCSIS4] and this Recommendation.

4 Abbreviations

This Recommendation uses the following abbreviations:

BPI+	Baseline Privacy Interface Plus
BPKM	Baseline Privacy Key Management
CBC	Cipher Block Chaining
CM	Cable Modem
CMTS	Cable Modem Termination System
DES	US Data Encryption Standard
HMAC	Keyed-Hashing for Message Authentication
QoS	Quality of Service
RSA	RSA Laboratories
SA	Security Association
SAID	Security Association Identifier
SID	Service Identifier
TEK	Traffic Encryption Key

5 Baseline privacy plus background and overview

Cable operators are interested in deploying high-speed packet-based communications systems on cable television systems that are capable of supporting a wide variety of services. Services under consideration by cable operators include high-speed Internet access, packet telephony service, video conferencing service, T1/frame relay equivalent service and many others.

The intended service will allow transparent bidirectional transfer of Internet Protocol (IP) traffic, between the cable system headend and customer locations, over an all-coaxial or hybrid fibre/coax (HFC) cable television network. This is shown in simplified form in Figure 5-1.

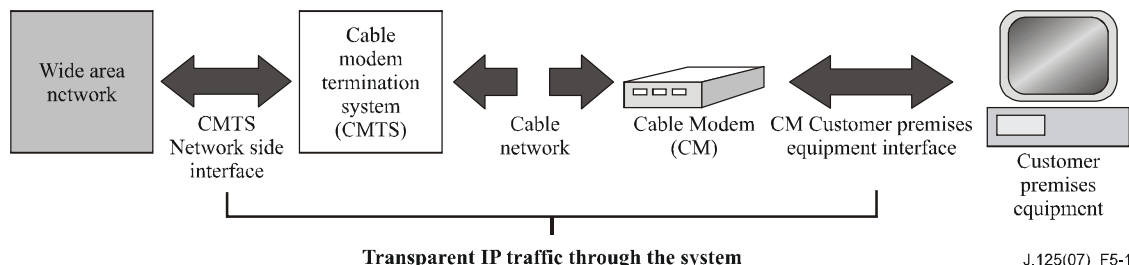


Figure 5-1 – Transparent IP traffic through the data-over-cable system

The transmission path over the cable system is realized at the headend by a CMTS, and at each customer location by a CM. At the headend (or hub), the interface to the data-over-cable system is called the cable modem termination system – network side interface (CMTS-NSI). At the customer

locations, the interface is called the cable-modem-to-customer-premises-equipment interface (CMCI). The intent is for the cable operators to transparently transfer IP traffic between these interfaces, including but not limited to datagrams, DHCP, ICMP, and IP Group addressing (broadcast and multicast).

Baseline privacy (BPI) and baseline privacy plus (BPI+) provide cable modem users with data privacy across the cable network. They do this by encrypting traffic flows between CM and CMTS. Baseline Privacy is the original version of this feature and is detailed in reference [SCTE22-2]. Baseline Privacy Plus is the updated version of this feature and the subject of this Recommendation. See Annex C for a more detailed discussion of the differences between the two versions.

In addition, BPI+ provides cable operators with strong protection from theft of service. The protected DOCSIS MAC data communications services fall into three categories:

- best-effort, high-speed, IP data services;
- QoS (e.g., constant bit rate) data services; and
- IP multicast group services.

Under BPI+, the CMTS protects against unauthorized access to these data transport services by enforcing encryption of the associated traffic flows across the cable network. BPI+ employs an authenticated client/server key management protocol in which the CMTS, the server, controls distribution of keying material to client CMs.

5.1 Architectural overview

Baseline Privacy Plus has two component protocols:

- An encapsulation protocol for encrypting packet data across the cable network. This protocol defines:
 - 1) the frame format for carrying encrypted packet data within DOCSIS MAC frames;
 - 2) a set of supported cryptographic suites, i.e., pairings of data encryption and authentication algorithms; and
 - 3) the rules for applying those algorithms to a DOCSIS MAC frame's packet data.
- A key management protocol (baseline privacy key management, or "BPKM") providing the secure distribution of keying data from CMTS to CMs. Through this key management protocol, CM and CMTS synchronize keying data; in addition, the CMTS uses the protocol to enforce conditional access to network services.

5.1.1 Packet data encryption

BPI+ encryption services are defined as a set of extended services within the DOCSIS MAC sublayer. Packet Header information specific to BPI+ is placed in a Baseline Privacy Extended Header element within the MAC Extended Header.

At the time of this Recommendation's release, BPI+ supports a single packet data encryption algorithm: the cipher block chaining (CBC) mode of the US data encryption standard (DES) algorithm [FIPS-46-3] and [FIPS-81]. BPI+ does not pair DES CBC with any packet data authentication algorithm. Additional data encryption algorithms may be supported in future enhancements to the BPI+ protocol specification, and these algorithms may be paired with data authentication algorithms.

BPI+ encrypts a DOCSIS MAC Frame's packet data; the DOCSIS MAC Frame's Header is not encrypted. DOCSIS MAC management messages MUST be sent in the clear to facilitate registration, ranging, and normal operation of the DOCSIS MAC sublayer.¹

Clause 6 specifies the format of DOCSIS MAC Frames carrying encrypted packet data payloads.

5.1.2 Key management protocol

CMs use the Baseline Privacy Key Management protocol to obtain authorization and traffic keying material from the CMTS, and to support periodic reauthorization and key refresh. The key management protocol uses X.509 digital certificates, a public-key encryption algorithm [RSA3] and two-key triple DES to secure key exchanges between CM and CMTS.

The Baseline Privacy Key Management protocol adheres to a client/server model, where the CM, a BPKM "client", requests keying material, and the CMTS, a BPKM "server", responds to those requests, ensuring individual CM clients only receive keying material they are authorized for. The BPKM protocol uses DOCSIS MAC management messaging.

BPI+ uses public-key cryptography to establish a shared secret (i.e., an Authorization Key) between CM and CMTS. The shared secret is then used to secure subsequent BPKM exchanges of traffic encryption keys. This two-tiered mechanism for key distribution permits refreshing of traffic encryption keys without incurring the overhead of computation-intensive public-key operations.

A CMTS authenticates a client CM during the initial authorization exchange. Each CM carries a unique X.509 digital certificate issued by the CM's manufacturer. The digital certificate contains the CM's Public Key along with other identifying information; i.e., CM MAC address, manufacturer ID and serial number. When requesting an Authorization Key, a CM presents its digital certificate to a CMTS. The CMTS verifies the digital certificate, and then uses the verified Public Key to encrypt an Authorization Key, which the CMTS then sends back to the requesting CM.

The CMTS associates a cable modem's authenticated identity to a paying subscriber, and hence to the data services that subscriber is authorized to access. Thus, with the Authorization Key exchange, the CMTS establishes an authenticated identity of a client CM, and the services (i.e., specific traffic encryption keys) the CM is authorized to access.

Since the CMTS authenticates CMs, it can protect against an attacker employing a *cloned* modem, masquerading as a legitimate subscriber's modem. The use of the X.509 certificates prevents cloned modems from passing fake credentials onto a CMTS.

CMs MUST have factory-installed RSA private/public key pairs or provide an internal algorithm to generate such key pairs dynamically. If a CM relies on an internal algorithm to generate its RSA key pair, the CM MUST generate the key pair prior to its first Baseline Privacy initialization, described in clause 5.2.1. CMs with factory-installed RSA key pairs MUST also have factory-installed X.509 certificates. Cable modems that rely on internal algorithms to generate an RSA key pair MUST support a mechanism for installing a manufacturer-issued X.509 certificate following key generation.

The BPKM protocol is defined in detail in clause 7.

5.1.3 BPI+ security associations

A BPI+ *security association* (SA) is the set of security information a CMTS and one or more of its client CMs share in order to support secure communications across the cable network. BPI+ defines three types of Security Associations: *Primary*, *Static* and *Dynamic*. A Primary Security Association is tied to a single CM, and is established when that CM completes DOCSIS MAC registration.

¹ The DOCSIS MAC headers of Packet Data PDUs and non-BPI+ DOCSIS MAC management messages MAY be encrypted when part of a fragmented concatenated packet [ITU-T J.112-B] or [ITU-T J.122].

Static Security Associations are provisioned within the CMTS. Dynamic Security Associations are established and eliminated, on the fly, in response to the initiation and termination of specific (downstream) traffic flows. Both Static and Dynamic SAs can be shared by multiple CMs.

A Security Association's shared information includes traffic encryption keys and CBC initialization vectors. In order to support, in future BPI+ enhancements, alternative data encryption and data authentication algorithms, BPI+ Security Association parameters include a cryptographic suite identifier, indicating the particular pairing of packet data encryption and packet data authentication algorithms employed by the security association. At the time of release of this Recommendation, 56-bit DES and 40-bit DES are the only packet data encryption algorithms supported, and neither are paired with a packet data authentication algorithm.²

BPI+ identifies Security Associations with a 14-bit *security association identifier (SAID)*.

Each (BPI+ enabled) CM establishes an exclusive Primary Security Association with its CMTS. All of a CM's upstream traffic **MUST** be encrypted under the CM's exclusive, Primary Security Association. The SAID corresponding to a CM's Primary SA **MUST** be equal to the CM's Primary DOCSIS 1.1 or DOCSIS 2.0 Service ID (SID) [ITU-T J.112-B] or [ITU-T J.122]. On the other hand, while typically all downstream unicast traffic directed at CPE device(s) behind the CM are encrypted under the CM's exclusive Primary Security Association, selected downstream unicast traffic flows can be encrypted under Static or Dynamic SAs. That is, downstream traffic **MAY** be encrypted under any of the three types of SAs. A downstream IP multicast data packet, however, is typically intended for multiple CMs and hence is more likely to be encrypted under Static or Dynamic SAs, which multiple CMs can access, as opposed to a Primary SA, which is restricted to a single CM.

The compliant CM **MUST** support a Primary SA, one or more Dynamic SAs, and one or more Static SAs. The compliant CMTS **MUST** support a Primary SA and one or more Dynamic SAs, and **MAY** support one or more Static SAs. BPI+ specification does not specify the number of the Static and Dynamic SAs required for the devices.

Using the BPKM protocol, a CM requests from its CMTS a SA's keying material. The CMTS ensures that each client CM only has access to the Security Associations it is authorized to access.

A SA's keying material (e.g., DES key and CBC Initialization Vector) has a limited lifetime. When the CMTS delivers SA keying material to a CM, it also provides the CM with that material's remaining lifetime. It is the responsibility of the CM to request new keying material from the CMTS before the set of keying material that the CM currently holds expires at the CMTS. The BPKM protocol specifies how CM and CMTS maintain key synchronization.

5.1.4 QoS SIDs and BPI+ SAIDs

The BPI+ Extended Header Element in downstream DOCSIS MAC frames contains the BPI+ SAID under which the downstream frame is encrypted. If the downstream frame is a unicast packet addressed to a CPE device behind a particular CM, the frame will typically be encrypted under the CM's Primary SA, in which case the SAID will be equal to the target CM's Primary SID. If the downstream frame is a multicast packet intended for receipt by multiple CMs, the extended header element will contain the Static or Dynamic SAID mapped to that multicast group. The SAID (Primary, Static or Dynamic), in combination with other data fields in the downstream extended header element, identifies to a receiving modem the particular set of keying material required to decrypt the DOCSIS MAC frame's encrypted Packet Data field.

Since all of a CM's upstream traffic is encrypted under its unique Primary SA, upstream DOCSIS MAC Frames, unlike downstream DOCSIS MAC Frames, need not carry a BPI+ SAID in their

² BPI+ encrypts a Packet PDU's Ethernet/802.3 CRC. While this provides some degree of data authentication, it does not provide cryptographically secure data authentication.

extended headers; instead, the Baseline Privacy EH element MAY contain any valid QoS SID assigned to the CM.

The Baseline Privacy extended header element serves multiple purposes in upstream DOCSIS Packet Data PDU MAC Frames. In addition to identifying the particular set of keying material used to encrypt a Frame's packet data, it also provides a mechanism for issuing piggybacked bandwidth requests, and it can carry fragmentation control data. These latter two functions are tied to a particular QoS SID; for this reason, upstream Baseline Privacy Extended Header Elements contain a QoS SID rather than a BPI+ Primary SAID, which can be inferred from the QoS SID and the logical upstream on which the MAC frame was received.

Unlike SAIDs corresponding to the Primary SA – which are equal to the CM's Primary SID – the SAID associated with a Static or Dynamic SA can be any 14-bit value. So that a modem does not have two different Security Associations with the same SAID, a compliant CMTS MUST NOT assign the same SAID to more than one type of SA within a MAC domain. In other words, if a SAID is being used as a Primary SA, the CMTS cannot use the same SAID for a Static or Dynamic SA within the same MAC domain. Likewise, if a CMTS has assigned a SAID to a Static or Dynamic SA, that value cannot be used as the SAID (and hence, the SID) for any modem within that MAC domain.

5.2 Operational overview

5.2.1 Cable modem initialization

[ITU-T J.112-B] or [ITU-T J.122] divides cable modem initialization into the following sequence of tasks:

- scan for downstream channel and establish synchronization with the CMTS;
- obtain transmit parameters;
- perform ranging;
- establish IP connectivity (DHCP);
- establish time of day;
- transfer operational parameters (download parameter file via TFTP);
- CMTS Registration.

Baseline Privacy establishment follows CMTS registration.

If a CM is to run Baseline Privacy, the Privacy Enable setting (type 29) in the DOCSIS 1.1 or 2.0 style configuration file MUST be explicitly/implicitly set to enable, regardless of the presence of the Baseline Privacy Configuration Settings (type 17). In other words, Baseline Privacy Configuration Settings do not need to be present in the configuration file in order to run Baseline Privacy. These additional configuration settings are defined in Annex A.

Upon completing CMTS registration, the CMTS will have assigned one or more static Service IDs (SIDs) to the registering CM that match the CM's static class-of-service provisioning. The first static SID assigned during the registration process is the Primary SID, and this SID will also serve as the CM's BPI+ Primary SAID. If a CM is configured to run Baseline Privacy, CMTS registration is immediately followed by initialization of the CM's Baseline Privacy security functions.

Baseline Privacy Initialization begins with the CM sending the CMTS an Authentication Information message with the CM's Manufacturer CA Certificate and an Authorization Request with the following information:

- data identifying the CM (e.g., MAC address);
- the CM's RSA public key;

- an X.509 certificate verifying the binding between the CM's identifying data and the CM's public key;
- a list of the CM's security capabilities (i.e., the particular pairings of encryption and authentication algorithms the CM supports); and
- the CM's Primary SAID (i.e., the Primary SID).

If the CMTS determines the requesting CM is authorized for the Authorization Request's Primary SAID, the CMTS responds with an Authorization Reply containing an Authorization Key, from which CM and CMTS derive the keys needed to secure a CM's subsequent requests for traffic encryption keys and the CMTS's responses to these requests. The CMTS encrypts the Authorization Key with the receiving cable modem's public key.

The Authorization Reply also contains a list of security association descriptors, identifying the primary and static SAs the requesting CM is authorized to access. Each SA descriptor consists of a collection of SA parameters, including the SA's SAID, type and cryptography. The list contains at least one entry: a descriptor describing the CM's primary security association. Additional entries are optional, and would describe any static SAs the CM was provisioned to access.

After successfully completing authentication and authorization with the CMTS, the cable modem sends key requests to the CMTS, requesting traffic encryption keys to use with each of its SAIDs. A CM's traffic key requests are authenticated using a keyed hash (the HMAC algorithm [IETF RFC 2104]); the Message Authentication Key is derived from the Authorization Key obtained during the earlier authorization exchange. The CMTS responds with key replies, containing the traffic encryption keys (TEKs); TEKs are triple DES encrypted with a key encryption key derived from the Authorization Key. Like the Key Requests, Key Replies are authenticated with a keyed hash, where the Message Authentication Key is derived from the Authorization Key.

Baseline Privacy Initialization ends when the CMTS sends or CM receives the Key Reply messages associated with all the SAIDs in the Authorization Reply message.

5.2.2 Cable modem key update mechanism

The traffic encryption keys which the CMTS provides to client CMs have a limited lifetime. The CMTS delivers a key's remaining lifetime, along with the key value, in the key replies it sends to its client CMs. The CMTS controls which keys are current by flushing expired keys and generating new keys. It is the responsibility of individual cable modems to ensure the keys they are using match those the CMTS is using. Cable modems do this by tracking when a particular SAID's key is scheduled to expire and issuing a new key request for the latest key prior to that expiration time.

In addition, cable modems are required to periodically reauthorize with the CMTS; as is the case with Traffic Encryption Keys, an Authorization Key has a finite lifetime which the CMTS provides the CM along with the key value. It is the responsibility of each cable modem to reauthorize and obtain a fresh Authorization Key (and an up-to-date list of SA descriptors) before the CMTS expires the CM's current Authorization Key.

Baseline Privacy initialization and key update is implemented within the Baseline Privacy Key Management protocol, defined in detail in clause 7.

6 DOCSIS MAC frame formats

When operating with BPI+ enabled, anytime after the Baseline Privacy Initialization ends, the CMTS and CM MUST encrypt the Data PDU regions of all of the following two types of DOCSIS MAC frames transmitted onto the cable network and MUST NOT forward any of them onto the cable network without encryption unless explicitly allowed by the DOCSIS specification or explicitly provisioned by the operator:

- Variable-length Packet Data PDU MAC Frames;
- Fragmentation MAC Frames.

In each of the two cases, a Baseline Privacy Extended Header Element in the DOCSIS MAC Header identifies the Security Association and accompanying keying material used to encrypt the Data PDU.

6.1 Variable-length packet data PDU MAC frame format

Figure 6-1 depicts the format of a DOCSIS variable-length Packet Data PDU with a Privacy Extended Header (EH) Element and encrypted Packet PDU payload.

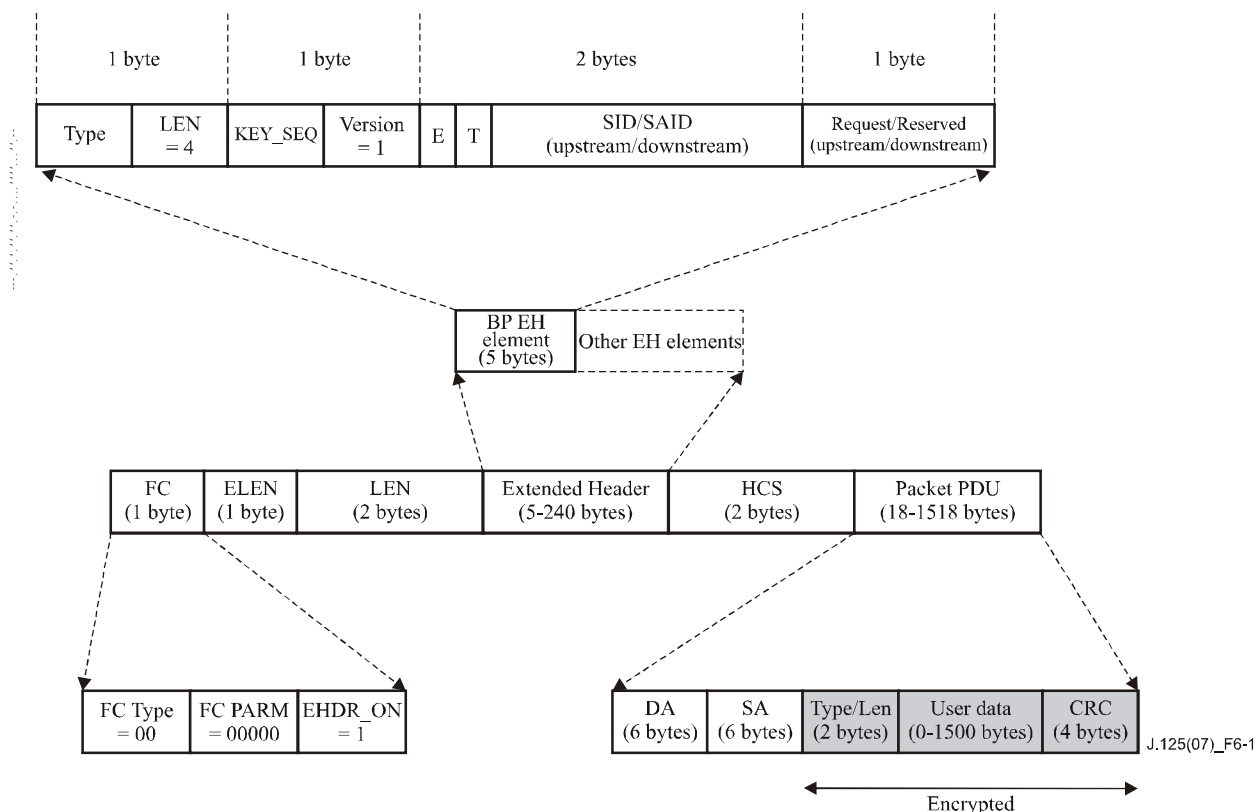


Figure 6-1 – Format of DOCSIS variable-length packet data PDU with privacy EH element

The first 12 octets of the Packet PDU, containing the Ethernet/802.3 destination and source addresses (DA/SA), are not encrypted. The Packet PDU's Ethernet/802.3 CRC is encrypted.

The CMTS includes the Baseline Privacy EH element in all downstream Packet Data PDUs it encrypts under Baseline Privacy Plus. Similarly, a CM includes the Baseline Privacy EH element in all upstream Packet Data PDUs it encrypts under Baseline Privacy Plus. If there are multiple Extended Header elements present in the DOCSIS MAC Header, the Baseline Privacy Extended Header element MUST be the first.

The Privacy Extended Header element employs two EH element type values, BPI_UP and BPI_DOWN, for use with upstream and downstream Packet Data PDUs, respectively. [ITU-T J.112-B] or [ITU-T J.122] defines the specific EH element type values assigned to BPI_UP and BPI_DOWN.

The high-order 4 bits of a BPI+ Extended Header element's value field contains a key sequence number, KEY_SEQ. Recall that the keying material associated with a BPI+ SAID has a limited lifetime, and the CMTS periodically refreshes a SAID's keying material. The CMTS manages a 4-bit key sequence number independently for each SAID and distributes this key sequence number along with the SAID's keying material to client CMs. The CMTS increments the key sequence number with each new generation of keying material. The Privacy EH element includes this sequence number, along with the SAID, to identify the specific generation of that SAID's keying material being used to encrypt the attached Packet Data PDU. Being a 4-bit quantity, the sequence number wraps around to 0 when it reaches 15.

Comparing a received frame's key sequence number with what it believes to be the "current" key sequence number, a CM or CMTS can easily recognize a loss of key synchronization with its peer. A CM MUST maintain the two most recent generations of keying material for each BPI+ SAID. Keeping on-hand the two most recent key generations is necessary for maintaining uninterrupted service during a SAID's key transition.

The 4 bits following KEY_SEQ contain a protocol version number. This protocol version number is set to 1 in DOCSIS Variable-length Packet Data PDU MAC headers.

The next two bytes contain the 2 bits of encryption status and the 14-bit SID/SAID (SID for upstream frames, SAID for downstream frames). The ENABLE encryption status bit indicates whether encryption is enabled or disabled for that PDU. If the ENABLE bit is 0, the Packet Data PDU is not encrypted and the Baseline Privacy EH element MUST be ignored (with the exception of the optional piggybacked bandwidth request – see below). The TOGGLE bit MUST match the state of the least significant bit (LSB) of KEY_SEQ, the Key Sequence Number.

The DOCSIS MAC protocol [ITU-T J.112-B] or [ITU-T J.122] defines a Request EH element for piggybacking a bandwidth request on a data transmission. Baseline Privacy defines an additional mechanism for piggybacking bandwidth requests: the last byte of the Baseline Privacy upstream EH element (EH element type = BPI_UP) carries an optional piggybacked bandwidth allocation request. If there is a piggybacked request, the byte represents the number of requested mini-slots. The 14-bit SID within the upstream Baseline Privacy EH element and the logical upstream on which the MAC frame was received identifies the Service ID the bandwidth request applies to. If there is no piggybacked request within the Baseline Privacy EH element, the request byte is set to zero. A piggybacked request within the Baseline Privacy EH element MUST be processed regardless of the status of the ENABLE bit.

In downstream packets (extender header element type = BPI_DOWN), the fourth and final byte is reserved and set to zero.

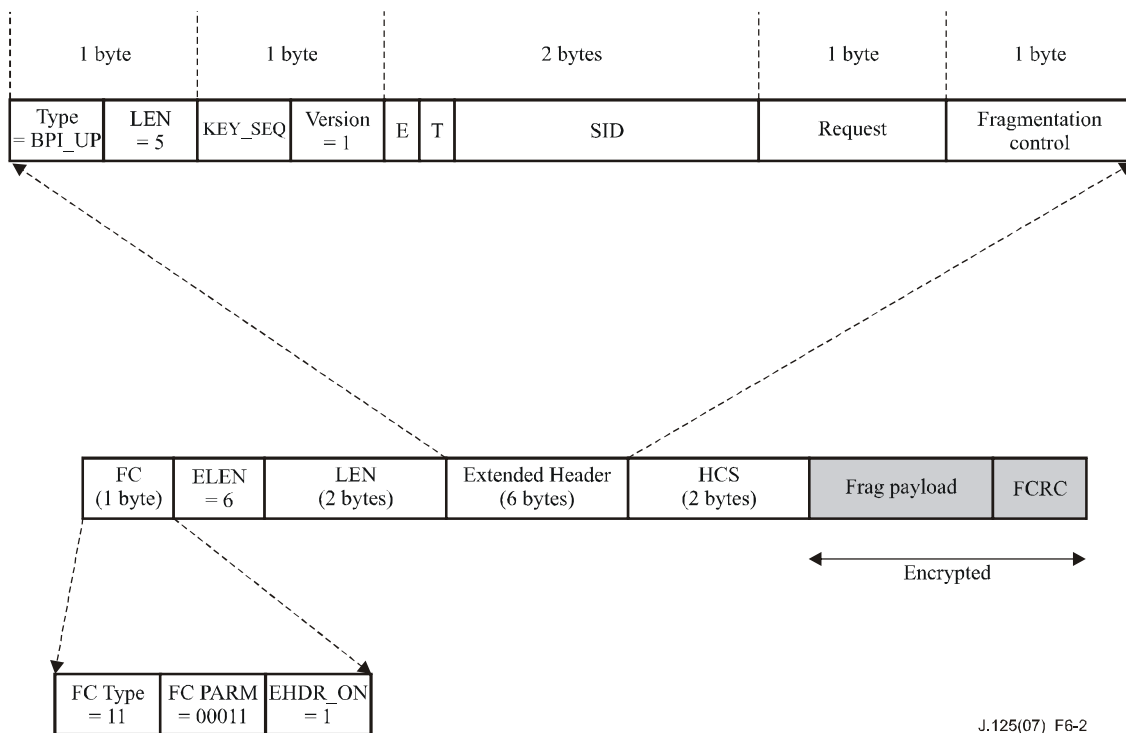
Table 6-1 – Summary of the contents of the two baseline privacy EH elements

EH_TYPE	EH_LEN	EH_VALUE
BPI_UP See [ITU-T J.112-B] or [ITU-T J.122]	4	KEY_SEQ (4 bits), Version (4 bits), SID (2 bytes), Request [piggyback] (1 byte) [CM → CMTS] KEY_SEQ field (4 bits): Key sequence number Version field (4 bits) is defined as: 0x1 SID field is defined as: Bit[15]: ENABLE: 1..Encryption enabled; 0..Encryption Disabled Bit[14]: TOGGLE: 1..Odd Key; 0..Even Key Bit[13:0]: Service ID. Request field contains the number of mini-slots requested for upstream bandwidth.
BPI_DOWN See [ITU-T J.112-B] or [ITU-T J.122]	4	KEY_SEQ (4 bits), Version (4 bits), SID (2 bytes), Reserved (1 byte) [CMTS → CM] KEY_SEQ field (4 bits): Key sequence number Version field (4 bits) is defined as: 0x1 SAID field is defined as: Bit[15]: ENABLE: 1..Encryption enabled; 0..Encryption Disabled Bit[14]: TOGGLE: 1..Odd Key; 0..Even Key Bit[13:0]: Security Association ID. Reserved field is set to 0.

In the case of encrypted Packet Data PDUs transmitted in an upstream data contention interval, the SID in the Baseline Privacy EH element MUST identify the QoS SID; it MUST NOT be set to the Request/Data contention interval's Multicast Service ID.

6.2 Fragmentation MAC frame format

In order to support fragmentation of upstream DOCSIS MAC frames, DOCSIS 1.1 or DOCSIS 2.0 has recast the Baseline Privacy EH element to carry both encryption and fragmentation control fields [ITU-T J.112-B] or [ITU-T J.122]. When functioning in this dual role, the upstream Baseline Privacy EH element (EH element type BPI_UP) is extended by one byte, the final byte serving as the fragmentation control field. Figure 6-2 depicts the format of a DOCSIS Fragmentation MAC Frame with an encrypted fragmentation payload.



J.125(07)_F6-2

Figure 6-2 – Format of a DOCSIS MAC fragmentation frame with an encrypted payload

An FC Type = 11 and FC PARM = 00011 identify a DOCSIS MAC frame as a Fragmentation frame. Unlike Packet Data PDU MAC frames, Fragmentation MAC frames have a fixed-size (six-byte) MAC Extended Header containing the "stretched" Baseline Privacy EH element.

The Fragmentation MAC header is followed by a Fragment Payload and a Fragment CRC. When Baseline Privacy encryption is applied to a Fragmentation MAC frame, the *entire* Fragment Payload is encrypted along with the Fragment CRC. In other words, unlike Baseline Privacy's encryption of Packet Data PDUs, there is no 12-byte offset into the payload before beginning encryption.³

The LEN field of the Baseline Privacy EH element in Fragmentation MAC Frames is 5 rather than 4, accounting for the additional 1-byte fragmentation control field. The KEY_SEQ field, VERSION field, ENABLE and TOGGLE flags, and SID field are what they would be for an upstream Packet Data PDU MAC Frame.

³ For non-fragmented frames, the first 12 bytes are left in the clear to allow pre-decryption DA/SA filtering. For fragmented frames, DA/SA filtering cannot occur before packet reassembly; hence, there is no value in supporting the 12-byte encryption offset in DOCSIS Fragmentation MAC frames.

**Table 6-2 – Summary of the contents of a DOCSIS fragmentation
MAC frame's baseline privacy EH element**

EH_TYPE	EH_LEN	EH_VALUE
BPI_UP See [ITU-T J.112-B] or [ITU-T J.122]	5	KEY_SEQ (4 bits), Version (4 bits), SID (2 bytes), Request [piggyback] (1 byte), Fragmentation Control (1 byte) [CM → CMTS] KEY_SEQ field (4 bits): Key sequence number Version field (4 bits) is defined as: 0x1 SID field is defined as: Bit[15]: ENABLE: 1..Encryption enabled; 0..Encryption Disabled Bit[14]: TOGGLE: 1..Odd Key; 0..Even Key Bit[13:0]: Service ID. Request field contains the number of mini-slots requested for upstream bandwidth. Fragmentation Control field contains fragmentation-specific control information; see [ITU-T J.112-B] or [ITU-T J.122] for details.

The fragmentation operation overrides BPI+ in the sense that the CM must first determine whether or not a packet will be fragmented based on grant size (the number of mini-slots a CMTS grants to a CM in an Upstream Bandwidth Allocation MAP [ITU-T J.112-B] or [ITU-T J.122]). If the packet is to be fragmented, the BPI+ encryption **MUST** occur on a fragment by fragment basis, and not over the PDU as a whole; each fragment will have its own fragmentation header and be encrypted separately. If the packet is not to be fragmented, then it **MUST** be encrypted as a single unit, with a single privacy header.

6.3 Requirements on usage of BP extended header element in MAC header

If BPI+ is not enabled on a particular downstream traffic flow (e.g., a CM's unicast traffic or a particular IP multicast group), the BP Extended Header element **SHOULD NOT** be used.

If BPI+ is not enabled for a CM's unicast traffic, fragmented upstream frames **MUST** still use the BP Extended Header element, but with the Encryption ENABLE bit turned off (0). This way the BP Extended Header can still be used for piggybacked bandwidth requests according to fragmentation rules described in [ITU-T J.112-B] or [ITU-T J.122].

For MAC frames consisting of only a MAC header and optional EHDR, Baseline privacy **MUST** be disabled. A Baseline Privacy EHDR **MAY** be present on these frames, but the enable bit **MUST** be cleared to disable privacy.

7 Baseline privacy key management (BPKM) protocol

7.1 State models

7.1.1 Introduction

The BPKM protocol is specified by two separate, but interdependent, state models: an authorization state model (the Authorization state machine) and an operational service key state model (the Traffic Encryption Key, or *TEK* state machine). This clause defines these two state models. The state models are for explanatory purposes only, and should not be construed as constraining an actual implementation.

Cable modem authorization, controlled by the Authorization state machine, is the process of:

- the CMTS authenticating a client CM's identity;
- the CMTS providing the authenticated CM with an Authorization Key, from which a key encryption key (KEK) and message authentication keys are derived;
- the CMTS providing the authenticated CM with the identities (i.e., the SAIDs) and properties of primary and static security associations the CM is authorized to obtain keying information for.

The KEK is a two-key triple DES encryption key that the CMTS uses to encrypt the traffic encryption keys (TEKs) it sends to the modem. Traffic encryption keys are used for encrypting user data traffic. CM and CMTS use message authentication keys to authenticate, via a keyed message digest, the key requests and responses they exchange.

After achieving initial authorization, a cable modem periodically seeks reauthorization with the CMTS; reauthorization is also managed by the CM's Authorization state machine. A CM **MUST** maintain its authorization status with the CMTS in order to be able to refresh aging Traffic Encryption Keys. TEK state machines manage the refreshing of Traffic Encryption Keys.

A cable modem begins authorization by sending an Authentication Information message to its CMTS. The Authentication Information message contains the cable modem manufacturer's X.509 certificate. The Authentication Information message is strictly informative, i.e., the CMTS may choose to ignore it; however, it does provide a mechanism for a CMTS to learn the manufacturer certificates of its client CMs.

The cable modem sends an Authorization Request message to its CMTS immediately after sending the Authentication Information message. This is a request for an Authorization Key, as well as for the SAIDs identifying any Static Security Associations the CM is authorized to participate in. The Authorization Request includes:

- the cable modem's manufacturer ID and serial number;
- the cable modem's MAC address;
- the cable modem's public key;
- a manufacturer-issued X.509 certificate binding the cable modem's public key to its other identifying information;
- a description of the cryptographic algorithms the requesting cable modem supports; a CM's cryptographic capabilities is presented to the CMTS as a list of cryptographic suite identifiers, each indicating a particular pairing of packet data encryption and packet data authentication algorithms the CM supports;
- the cable modem's Primary SAID, *which is equal to the CM's Primary SID* (the Primary SID is the first static SID the CMTS assigns to a CM during RF MAC registration).

In response to an Authorization Request message, if a CMTS validates the requesting CM's identity and determines the encryption algorithm and protocol support it shares with the CM, the CMTS **MUST** activate an Authorization Key for the CM, encrypt it with the cable modem's public key, and send it back to the CM in an Authorization Reply message. The authorization reply includes:

- an Authorization Key encrypted with the CM's public key;
- a 4-bit key sequence number, used to distinguish between successive generations of Authorization Keys;
- a key lifetime;
- the identities (i.e., the SAIDs) and properties of the single primary and zero or more static security associations the CM is authorized to obtain keying information for.

If the CMTS supports Static SAs, the Authorization Reply to a CM MUST identify Static SAs associated with the CM in addition to the Primary SA whose SAID matches the requesting CM's best-effort SID. The Authorization Reply MUST NOT identify any Dynamic SAs.

The CMTS, in responding to a CM's Authorization Request, will determine whether the re-requesting cable modem, whose identity can be verified via the X.509 digital certificate, is authorized for basic unicast services, and what additional statically provisioned services (i.e., Static SAIDs) the cable modem's user has subscribed for.

NOTE 1 – The protected services a CMTS makes available to a client CM can depend upon the particular cryptographic suites CM and CMTS share support for.

Upon achieving authorization, a CM starts a separate TEK state machine for each of the SAIDs identified in the Authorization Reply message. Each TEK state machine operating within the CM is responsible for managing the keying material associated with its respective SAID. TEK state machines periodically send Key Request messages to the CMTS, requesting a refresh of keying material for their respective SAIDs. A Key Request includes:

- identifying information unique to the cable modem, consisting of the manufacturer ID, serial number, MAC address and RSA Public Key;
- the SAID whose keying material is being requested;
- an HMAC keyed message digest, authenticating the Key Request.

The CMTS MUST respond to a Key Request message with a Key Reply message, containing the CMTS's active keying material for a specific SAID if the CMTS validates the HMAC digest of the Key Request message, the requesting CM's identity and the SAID. This keying material includes:

- the triple-DES-encrypted traffic encryption key;
- CBC initialization vector;
- a key sequence number;
- a key's remaining lifetime;
- an HMAC keyed message, authenticating the Key Reply.

The traffic encryption key (TEK) in the Key Reply is triple DES (encrypt-decrypt-encrypt or EDE mode) encrypted, using a two-key, triple DES key encryption key (KEK) derived from the Authorization Key.

NOTE 2 – At all times the CMTS maintains two active sets of keying material per SAID. The lifetimes of the two generations overlap such that each generation becomes active halfway through the life of its predecessor and expires halfway through the life of its successor. A CMTS includes in its Key Replies *both* of a SAID's active generations of keying material.

The Key Reply provides the requesting CM, in addition to the TEK and CBC initialization vector, the remaining lifetime of each of the two sets of keying material. The receiving CM uses these remaining lifetimes to estimate when the CMTS will invalidate a particular TEK, and therefore when to schedule future Key Requests such that the CM requests and receives new keying material before the CMTS expires the keying material the CM currently holds.

The operation of the TEK state machine's Key Request scheduling algorithm, combined with the CMTS's regimen for updating and using a SAID's keying material (see clause 9), ensures that the CM will be able to continually exchange encrypted traffic with the CMTS.

A CM MUST periodically refresh its Authorization Key by reissuing an Authorization Request to the CMTS. Reauthorization is identical to authorization with the exception that the CM does not send Authentication Information messages during reauthorization cycles. The description of the authorization state machine (see clause 7.1.2) clearly indicates when Authentication Information messages are sent.

To avoid service interruptions during reauthorization, successive generations of the CM's Authorization Keys have overlapping lifetimes. Both CM and CMTS MUST be able to support up to two simultaneously active Authorization Keys during these transition periods. The operation of the Authorization state machine's Authorization Request scheduling algorithm, combined with the CMTS's regimen for updating and using a client CM's Authorization Keys (see clause 9), ensures that CMs will be able to refresh TEK keying information without interruption over the course of the CM's reauthorization periods.

A TEK state machine remains active as long as:

- the CM is authorized to operate in the CMTS's security domain; i.e., it has a valid Authorization Key; and
- the CM is authorized to participate in that particular Security Association; i.e., CMTS continues to provide fresh keying material during re-key cycles.

The parent Authorization state machine stops *all* of its child TEK state machines when the CM receives from the CMTS an Authorization Reject during a reauthorization cycle. Individual TEK state machines can be started or stopped during a reauthorization cycle if a CM's Static SAID authorization changed between successive reauthorizations.

Communication between Authorization and TEK state machines occurs through the passing of events and protocol messaging. The Authorization state machine generates events (i.e., Stop, Authorized, Authorization Pending, and Authorization Complete events) that are targeted at its child TEK state machines. TEK state machines do not target events at their parent Authorization state machine. The TEK state machine affects the Authorization state machine indirectly through the messaging a CMTS sends in response to a modem's requests: a CMTS MAY respond to a TEK machine's Key Requests with a failure response (i.e., Authorization Invalid message) that will be handled by the Authorization state machine.

7.1.1.1 Preliminary comment on dynamic security associations and dynamic SA mapping

Clause 5 introduced Dynamic SAs and mentioned how a CMTS can establish or eliminate a Dynamic SA in response to the initiation or termination of downstream traffic flows (e.g., a particular IP multicast group's traffic). In order for a CM to run a TEK state machine to obtain a Dynamic Security Association's keying material, the CM needs to know the corresponding SAID value. The CMTS, however, does not volunteer to client CMs the existence of Dynamic SAs; instead, it is the responsibility of CMs to request of the CMTS the mapping of traffic flow identifiers (e.g., an IP multicast address) to dynamic SAIDs.

BPI+ defines a messaging exchange by which a CM learns the mapping of a downstream traffic flow to a Dynamic SA (all upstream traffic is encrypted under a CM's Primary SA). A SA Mapping state machine specifies how cable modems manage the transmission of these mapping request messages. Currently only DOCSIS' IP multicast management services utilize this mechanism. In the future, additional services may employ BPI+ Dynamic SAs.

The Authorization state machine controls the establishment and termination of TEK state machines associated with the Primary and any Static SAs; it does not, however, control the establishment and termination of TEK state machines associated with Dynamic SAs. CMs MUST implement the necessary logic to establish and terminate a Dynamic SA's TEK state machine. This interface specification, however, does not specify how CMs should manage their Dynamic SA's TEK state machines.

A full description of the SA Mapping state model is deferred to clause 8.

7.1.1.2 Security capabilities selection

As part of their BPI+ authorization exchange, the CM provides the CMTS with a list of all the cryptographic suites (pairing of data encryption and data authentication algorithms) the CM

supports. The CMTS selects from this list a single cryptographic suite to employ with the requesting CM's primary SA. The Authorization Reply the CMTS sends back to the CM includes a primary SA descriptor which, among other things, identifies the cryptographic suite the CMTS selected to use for the CM's primary SA. A CMTS MUST reject the authorization request if it determines that none of the offered cryptographic suites are satisfactory.

The Authorization Reply also contains an optional list of static SA descriptors; each static SA descriptor identifies the cryptographic suite employed within the SA. The selection of a static SA's cryptographic suite is typically made independent of the requesting CM's cryptographic capabilities. A CMTS MAY include in its Authorization Reply static SA descriptors identifying cryptographic suites the requesting CM does not support; if this is the case, the CM MUST NOT start TEK state machines for static SAs whose cryptographic suites the CM does not support.

The above selection framework was incorporated into BPI+ in order to support future enhancements to DOCSIS hardware and to the BPI+ protocol. At the time of release of this Recommendation, 56-bit DES and 40-bit DES are the only packet data encryption algorithms supported, and neither are paired with a packet data authentication algorithm.

7.1.2 Authorization state machine

The Authorization state machine consists of six states and eight distinct events (including receipt of messages) that can trigger state transitions. The Authorization finite state machine (FSM) is presented below in a graphical format, as a state flow model (Figure 7-1), and in a tabular format, as a state transition matrix (Table 7-1).

The state flow diagram depicts the protocol messages transmitted and internal events generated for each of the model's state transitions; however, the diagram does not indicate additional internal actions, such as the clearing or starting of timers, that accompany the specific state transitions. Accompanying the state transition matrix is a detailed description of the specific actions accompanying each state transition; the state transition matrix MUST be used as the definitive specification of protocol actions associated with each state transition.

The following legend applies to the Authorization State Machine flow diagram in depicted in Figure 7-1.

- ovals are states;
- events are in *italics*;
- messages are in normal font;
- State transitions (i.e., the lines between states) are labelled with <what causes the transition>/<messages and events triggered by the transition>. So "*timeout*/Auth Request" means that the state received a "timeout" event and sent an Authorization Request ("Auth Request") message. If there are multiple events or messages before the slash "/" separated by a comma, *any* of them can cause a transition. If there are multiple events or messages listed after the slash, *all* of the specified actions must accompany the transition.

The Authorization state transition matrix presented in Table 7-1 lists the six Authorization machine states in the top-most row and the eight Authorization machine events (includes message receipts) in the left-most column. Any cell within the matrix represents a specific combination of state and event, with the next state (the state transitioned to) displayed within the cell. For example, cell 4-B represents the receipt of an Authorization Reply (Auth Reply) message when in the Authorize Wait (Auth Wait) state. Within cell 4-B is the name of the next state, "Authorized". Thus, when a CM's Authorization state machine is in the Authorize Wait state and an Authorization Reply message is received, the Authorization state machine will transition to the Authorized state. In conjunction with this state transition, several protocol actions must be taken; these are described in the listing of protocol actions, under the heading 4-B, in clause 7.1.2.5.

A shaded cell within the state transition matrix implies that either the specific event cannot or should not occur within that state, and if the event does occur, the state machine MUST ignore it. For example, if an Authorization Reply message arrives when in the Authorized state, that message should be ignored (cell 4-C). The CM MAY, however, in response to an improper event, log its occurrence, generate an SNMP event, or take some other vendor-defined action. These actions, however, are not specified within the context of the Authorization state machine, which simply ignores improper events.

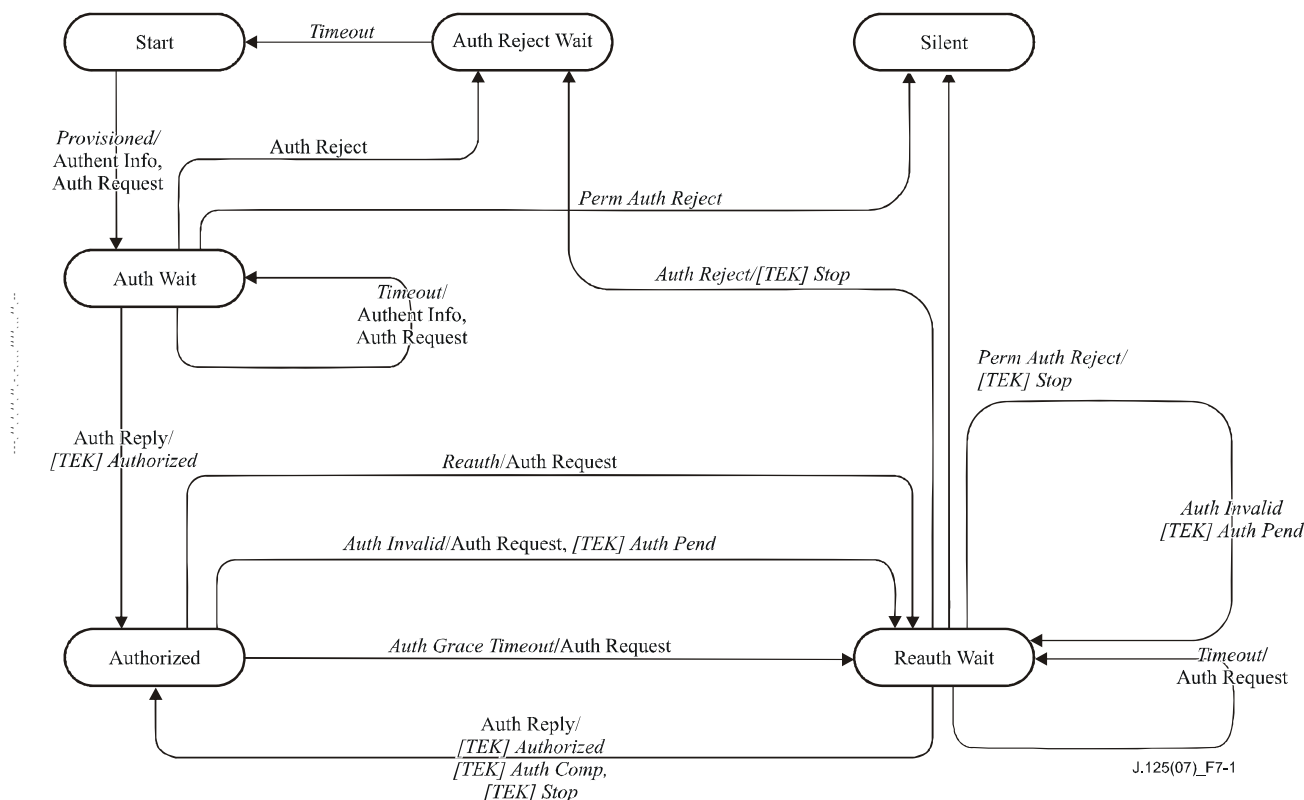


Figure 7-1 – Authorization state machine flow diagram

Table 7-1 – Authorization FSM state transition matrix

State Event or rcvd message	(A) Start	(B) Auth Wait	(C) Authorized	(D) Reauth Wait	(E) Auth Reject Wait	(F) Silent
(1) <i>Provisioned</i>	Auth Wait					
(2) <i>Auth Reject</i>		Auth Reject Wait		Auth Reject Wait		
(3) <i>Perm Auth Reject</i>		Silent		Silent		
(4) <i>Auth Reply</i>		Authorized		Authorized		
(5) <i>Timeout</i>		Auth Wait		Reauth Wait	Start	
(6) <i>Auth Grace Timeout</i>			Reauth Wait			
(7) <i>Auth Invalid</i>			Reauth Wait	Reauth Wait		
(8) <i>Reauth</i>			Reauth Wait			

7.1.2.1 States

7.1.2.1.1 Start

This is the initial state of the FSM. No resources are assigned to or used by the FSM in this state – e.g., all timers are off, and no processing is scheduled.

7.1.2.1.2 Authorize Wait (Auth Wait)

The CM has received the "Provisioned" event indicating that it has completed RF MAC registration with the CMTS. In response to receiving the event, the CM has sent both an Authentication Information and an Authorize Request message to the CMTS and is waiting for the reply.

7.1.2.1.3 Authorized

The CM has received an Authorization Reply message which contains a list of valid SAIDs for this CM. At this point, the modem has a valid Authorization Key and SAID list. Transition into this state triggers the creation of one TEK FSM for each of the CM's privacy-enabled SAIDs.

7.1.2.1.4 Reauthorize Wait (Reauth Wait)

The CM has an outstanding reauthorization request. The CM was either about to time out its current authorization or received an indication (an Authorization Invalid message from the CMTS) that its authorization was no longer valid. The CM has sent an Authorization Request message to the CMTS and is waiting for a response.

7.1.2.1.5 Authorize Reject Wait (Auth Reject Wait)

The CM received an Authorization Reject message in response to its last Authorization Request. The Authorization Reject's error code indicated the error was not of a permanent nature. In response to receiving this reject message, the CM set a timer and transitioned to the Authorize Reject Wait state. The CM remains in this state until the timer expires.

7.1.2.1.6 Silent

The CM received an Authorization Reject message in response to its last Authorization Request. The Authorization Reject's error code indicated the error was of a permanent nature. This triggers a transition to the Silent state. In the Silent state, the CM MUST NOT pass CPE traffic, but MUST be able to respond to SNMP management requests arriving from across the cable network. The CMTS MAY choose to forward data traffic to a CM that is in the silent state unencrypted, or the CMTS MAY block such traffic.

7.1.2.2 Messages

The message formats are defined in detail in clause 7.2.

7.1.2.2.1 Authorization Request (Auth Request)

Request an Authorization Key and list of authorized SAIDs. Sent from CM to CMTS.

7.1.2.2.2 Authorization Reply (Auth Reply)

Receive an Authorization Key and list of authorized, static SAIDs. Sent from CMTS to CM. The Authorization Key is encrypted with the CM's public key.

7.1.2.2.3 Authorization Reject (Auth Reject)

Attempt to authorize was rejected. Sent from the CMTS to the CM.

7.1.2.2.4 Authorization Invalid (Auth Invalid)

The CMTS can send an Authorization Invalid message to a client CM as:

- an unsolicited indication; or

- a response to a message received from that CM.

In either case, the Authorization Invalid message instructs the receiving CM to reauthorize with its CMTS.

The CMTS MUST respond to a Key Request with an Authorization Invalid message if:

- 1) the CMTS does not recognize the CM as being authorized (i.e., no valid Authorization Key associated with cable modem); or
- 2) verification of the Key Request's keyed message digest (in HMAC-Digest Attribute) failed.

NOTE – The Authorization Invalid event, referenced in both the state flow diagram and the state transition matrix, signifies either the receipt of an Authorization Invalid message or an internally generated event.

7.1.2.2.5 Authentication Information (Authent Info)

The Authentication Information message contains the cable modem manufacturer's X.509 Certificate, issued by DOCSIS. The Authent Info message is strictly an informative message the CM sends to the CMTS; with it, a CMTS MAY dynamically learn the manufacturer certificate of client CMs. Alternatively, a CMTS MAY require out-of-band configuration of its list of manufacturer certificates.

7.1.2.3 Events

7.1.2.3.1 Provisioned

The Authorization state machine generates this event upon entering the Start state if the RF MAC has completed initialization, i.e., CMTS registration. If the RF MAC initialization is not complete, the CM sends a Provisioned event to the Authorization FSM upon completing CMTS registration. The Provisioned event triggers the CM to begin the process of getting its Authorization Key and TEKs.

7.1.2.3.2 Timeout

A retransmission or wait timer timed out. Generally a request is resent.

7.1.2.3.3 Authorization Grace Timeout (Auth Grace Timeout)

The Authorization Grace timer timed out. This timer fires a configurable amount of time (the Authorization Grace Time) before the current authorization is supposed to expire, signalling the CM to reauthorize before its authorization actually expires. The Authorization Grace Time is specified in a configuration setting within the TFTP-downloaded parameter file.

7.1.2.3.4 Reauthorize (Reauth)

CM's set of authorized static SAIDs may have changed. Event generated in response to an SNMP set, [DOCSIS8], meant to trigger a reauthorization cycle.

7.1.2.3.5 Authorization Invalid (Auth Invalid)

This event can be internally generated by the CM when there is a failure authenticating a Key Reply, Key Reject, or TEK Invalid message, or externally generated by the receipt of an Authorization Invalid message, sent from the CMTS to the CM. A CMTS responds to a Key Request with an Authorization Invalid if verification of the request's message authentication code fails. Both cases indicate CMTS and CM have lost Authorization Key synchronization.

A CMTS MAY also send a CM an unsolicited Authorization Invalid message to a CM, forcing an Authorization Invalid event.

7.1.2.3.6 Permanent Authorization Reject (Perm Auth Reject)

The CMTS MUST send an Authorization Reject message with the error code 6 (Permanent Authorization Reject) in response to an Authorization Request message in any of the following conditions:

- CM Certificate validation failure per clause 12.4.2 (that is, the CM Certificate is marked Invalid);
- incompatible security capabilities.

BPI+'s associated OSS document [DOCSIS8] provides a description of the particular CMTS MIB objects which control the actions a CMTS takes in the event any of the above error conditions occur.

When a CM receives an Authorization Reject indicating a permanent failure condition, the Authorization State machine moves into a Silent state. CMs MUST issue a DOCSIS Event upon entering the Silent State.

7.1.2.3.7 Authorization Reject (Auth Reject)

The CM receives an Authorization Reject in response to an Authorization Request. The error code in the Authorization Reject does not indicate the failure was due to a permanent error condition. As a result, the CM's Authorization state machine will set a wait timer and transition into the Authorization Reject Wait State. The CM remains in this state until the timer expires, at which time it will reattempt authorization.

NOTE – The following events are sent by an Authorization state machine to the TEK state machine.

7.1.2.3.8 [TEK] Stop

Sent by the Authorization FSM to an active (non-START state) TEK FSM to terminate the FSM and remove the corresponding SAID's keying material from the CM's key table.

7.1.2.3.9 [TEK] Authorized

Sent by the Authorization FSM to a non-active (START state), but valid TEK FSM.

7.1.2.3.10 [TEK] Authorization Pending (Auth Pend)

Sent by the Authorization FSM to a specific TEK FSM to place that TEK FSM in a wait state until the Authorization FSM can complete its reauthorization operation.

7.1.2.3.11 [TEK] Authorization Complete (Auth Comp)

Sent by the Authorization FSM to a TEK FSM in the Operational Reauthorize Wait (Op Reauth Wait) or Rekey Reauthorize Wait (Rekey Reauth Wait) states to clear the wait state begun by a TEK FSM Authorization Pending event.

7.1.2.4 Parameters

All configuration parameter values are specified in the TFTP-downloaded parameter file (see Annex A: TFTP Configuration File Extensions).

7.1.2.4.1 Authorize Wait Timeout (Auth Wait Timeout)

Timeout period between sending Authorization Request messages from Authorize Wait state. See clause A.1.1.1.1.

7.1.2.4.2 Reauthorize Wait Timeout (Reauth Wait Timeout)

Timeout period between sending Authorization Request messages from Reauthorize Wait state. See clause A.1.1.1.2.

7.1.2.4.3 Authorization Grace Time (Auth Grace Timeout)

Amount of time before authorization is scheduled to expire that the CM starts reauthorization. See clause A.1.1.1.3.

7.1.2.4.4 Authorize Reject Wait Timeout (Auth Reject Wait Timeout)

Amount of time a CM's Authorization FSM remains in the Authorize Reject Wait state before transitioning to the Start state. See clause A.1.1.1.7.

7.1.2.5 Actions

Actions taken in association with state transitions are listed by <event/rcvd message> – <state> below:

1-A Start (*Provisioned*) → Auth Wait

- send Authentication Information message to CMTS;
- send Authorization Request message to CMTS;
- set Authorization Request retry timer to Authorize Wait Timeout.

2-B Auth Wait (*Auth Reject*) → Auth Reject Wait

- clear Authorization Request retry timer;
- set a wait timer to Authorize Reject Wait Timeout.

2-D Reauth Wait (*Auth Reject*) → Auth Reject Wait

- clear Authorization Request retry timer;
- generate TEK FSM Stop events for all active TEK state machines;
- set a wait timer to Authorize Reject Wait Timeout.

3-B Auth Wait (*Perm Auth Reject*) → Silent

- clear Authorization Request retry timer;
- disable all forwarding of CPE traffic.

3-D Reauth Wait (*Perm Auth Reject*) → Silent

- clear Authorization Request retry timer;
- generate TEK FSM Stop events for all active TEK state machines;
- disable all forwarding of CPE traffic.

4-B Auth Wait (*Auth Reply*) → Authorized

- clear Authorization Request retry timer;
- decrypt and record Authorization Key delivered with Authorization Reply;
- start TEK FSMs for all SAIDs listed in Authorization Reply (provided the CM supports the cryptographic suite that is associated with a SAID) and issue a TEK FSM Authorized event for each of the new TEK FSMs;
- set the Authorization Grace timer to go off "Authorization Grace Time" seconds prior to the supplied Authorization Key's scheduled expiration.

4-D Reauth Wait (*Auth Reply*) → Authorized

- clear Authorization Request retry timer;
- decrypt and record Authorization Key delivered with Authorization Reply;
- start TEK FSMs for any newly authorized SAIDs listed in Authorization Reply (provided the CM supports the cryptographic suite that is associated with the new SAID) and issue TEK FSM Authorized event for each of the new TEK FSMs;

- generate TEK FSM Authorization Complete events for any currently active TEK FSMs whose corresponding SAIDs were listed in Authorization Reply;
- generate TEK FSM Stop events for any currently active TEK FSMs whose corresponding SAIDs were not listed in Authorization Reply;
- set the Authorization Grace timer to go off "Authorization Grace Time" seconds prior to the supplied Authorization Key's scheduled expiration.

5-B Auth Wait (*Timeout*) → Auth Wait

- send Authentication Information message to CMTS;
- send Authorization Request message to CMTS;
- set Authorization Request retry timer to Authorize Wait Timeout.

5-D Reauth Wait (*Timeout*) → Reauth Wait

- send Authorization Request message to CMTS;
- set Authorization Request retry timer to Reauthorize Wait Timeout.

5-E Auth Reject Wait (*Timeout*) → Start

- no protocol actions associated with state transition.

6-C Authorized (*Auth Grace Timeout*) → Reauth Wait

- send Authorization Request message to CMTS;
- set Authorization Request retry timer to Reauthorize Wait Timeout.

7-C Authorized (*Auth Invalid*) → Reauth Wait

- clear Authorization Grace timer;
- send Authorization Request message to CMTS;
- set Authorization Request retry timer to Reauthorize Wait Timeout;
- if the Authorization Invalid event is associated with a particular TEK FSM, generate a TEK FSM Authorization Pending event for the TEK state machine responsible for the Authorization Invalid event (i.e., the TEK FSM that either generated the event, or sent the Key Request message the CMTS responded to with an Authorization Invalid message).

7-D Reauth Wait (*Auth Invalid*) → Reauth Wait

- if the Authorization Invalid event is associated with a particular TEK FSM, generate a TEK FSM Authorization Pending event for the TEK state machine responsible for the Authorization Invalid event (i.e., the TEK FSM that either generated the event, or sent the Key Request message the CMTS responded to with an Authorization Invalid message).

8-C Authorized (*Reauth*) → Reauth Wait

- clear Authorization grace timer;
- send Authorization Request message to CMTS;
- set Authorization Request retry timer to Reauthorize Wait Timeout.

7.1.3 TEK state machine

The TEK state machine consists of six states and nine events (including receipt of messages) that can trigger state transitions. Like the Authorization state machine, the TEK state machine is presented in both a state flow diagram and a state transition matrix. And as was the case for the Authorization state machine, the state transition matrix **MUST** be used as the definitive specification of protocol actions associated with each state transition.

Shaded states in Figure 7-2 (Operational, Rekey Wait, and Rekey Reauthorize Wait) have valid keying material and encrypted traffic can be passed.

The Authorization state machine starts an independent TEK state machine for each of its authorized SAIDs.

As mentioned previously in clause 7.1.1, the CMTS maintains two active TEKs per SAID. The CMTS includes in its Key Replies both of these TEKs, along with their remaining lifetimes. The CMTS encrypts downstream traffic with the older of its two TEKs and decrypts upstream traffic with either the older or newer TEK, depending upon which of the two keys the CM was using at the time. The CM encrypts upstream traffic with the newer of its two TEKs and decrypts downstream traffic with either the older or newer TEK, depending upon which of the two keys the CMTS was using at the time. See clause 9 for details on CM and CMTS key usage requirements.

Through operation of a TEK state machine, the CM attempts to keep its copies of a SAID's TEKs synchronized with those of its CMTS. A TEK state machine issues Key Requests to refresh copies of its SAID's keying material after the scheduled expiration time of the older of its two TEKs and before the expiration of its newer TEK. To accommodate for CM/CMTS clock skew and other system processing and transmission delays, the CM schedules its Key Requests a configurable number of seconds (i.e., "TEK Grace Time") before the newer TEK's estimated expiration in the CMTS. With the receipt of the Key Reply, the CM MUST always update its records with the TEK Parameters from both TEKs contained in the Key Reply Message. Figure 9-2 illustrates the CM's scheduling of its key refreshes in conjunction with its management of a BPI+ SA's active TEKs.

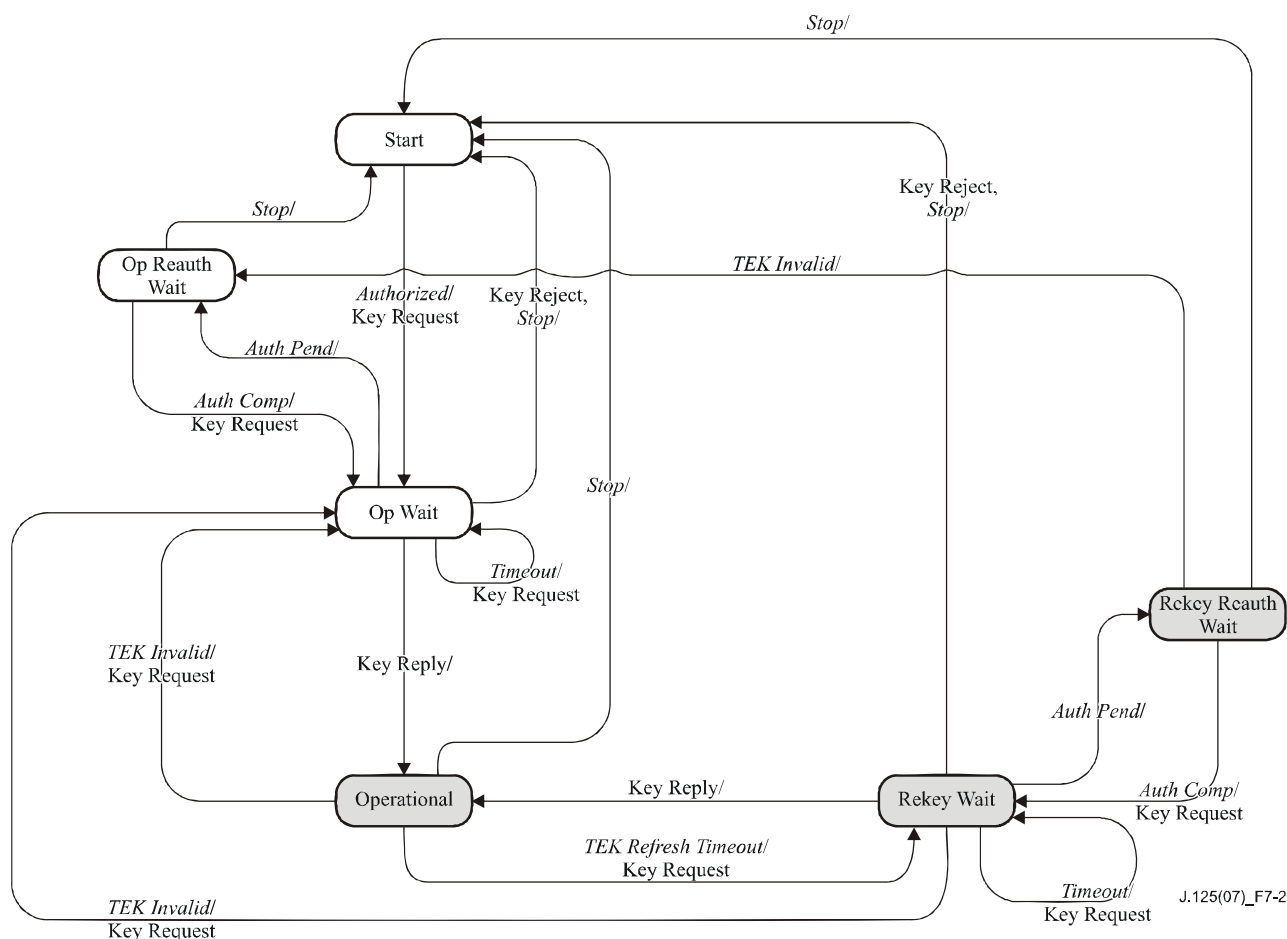


Figure 7-2 – TEK state machine flow diagram

Table 7-2 – TEK FSM state transition matrix

<i>State</i> <i>Event</i> <i>or rcvd</i> <i>message</i>	(A) Start	(B) Op Wait	(C) Op Reauth Wait	(D) Op	(E) Rekey Wait	(F) Rekey Reauth Wait
(1) <i>Stop</i>		Start	Start	Start	Start	Start
(2) <i>Authorized</i>	Op Wait					
(3) <i>Auth Pend</i>		Op Reauth Wait			Rekey Reauth Wait	
(4) <i>Auth Comp</i>			Op Wait			Rekey Wait
(5) <i>TEK Invalid</i>				Op Wait	Op Wait	Op Reauth Wait
(6) <i>Timeout</i>		Op Wait			Rekey Wait	
(7) <i>TEK Refresh Timeout</i>				Rekey Wait		
(8) <i>Key Reply</i>		Operational			Operational	
(9) <i>Key Reject</i>		Start			Start	

7.1.3.1 States

7.1.3.1.1 Start

This is the initial state of the FSM. No resources are assigned to or used by the FSM in this state – e.g., all timers are off, and no processing is scheduled.

7.1.3.1.2 Operational Wait (Op Wait)

The TEK state machine has sent its initial request (Key Request) for its SAID's keying material (traffic encryption key and CBC initialization vector), and is waiting for a reply from the CMTS.

7.1.3.1.3 Operational Reauthorize Wait (Op Reauth Wait)

The wait state the TEK state machine is placed in if it does not have valid keying material while the Authorization state machine is in the middle of a reauthorization cycle.

7.1.3.1.4 Operational

The CM has valid keying material for the associated SAID.

7.1.3.1.5 Rekey Wait

The TEK Refresh Timer has expired and the CM has requested a key update for this SAID.

NOTE – The newer of its two TEKs has not expired and can still be used for both encrypting and decrypting data traffic.

7.1.3.1.6 Rekey Reauthorize Wait (Rekey Reauth Wait)

The wait state the TEK state machine is placed in if the TEK state machine has valid traffic keying material, has an outstanding request for the latest keying material, and the Authorization state machine initiates a reauthorization cycle.

7.1.3.2 Messages

The message formats are defined in detail in clause 7.2.

7.1.3.2.1 Key Request

Request a TEK for this SAID. Sent by the CM to the CMTS and authenticated with keyed message digest. The message authentication key is derived from the Authorization Key.

7.1.3.2.2 Key Reply

Response from the CMTS carrying the two active sets of traffic keying material for this SAID. Sent by the CMTS to the CM, it includes the SAID's traffic encryption keys, triple DES encrypted with a key encryption key derived from the Authorization Key. The Key Reply message is authenticated with a keyed message digest; the authentication key is derived from the Authorization Key.

7.1.3.2.3 Key Reject

The CMTS MUST send a Key Reject message to the CM in response to a Key Request message in order to indicate that no key will be sent if the SAID in the Key Request message is no longer valid. The Key Reject message is authenticated with a keyed message digest; the authentication key is derived from the Authorization Key.

7.1.3.2.4 TEK Invalid

The CMTS MUST send a CM the TEK Invalid message if it determines that the CM encrypted an upstream Packet Data PDU with an invalid TEK; i.e., a SAID's TEK key sequence number, contained within the received packet's Baseline Privacy Extended Header element, is out of the CMTS's range of known, valid sequence numbers for that SAID.

7.1.3.3 Events

7.1.3.3.1 Stop

Sent by the Authorization FSM to an active (non-START state) TEK FSM to terminate TEK FSM and remove the corresponding SAID's keying material from the CM's key table. See clause 7.1.2.3.8.

7.1.3.3.2 Authorized

Sent by the Authorization FSM to a non-active (START state) TEK FSM to notify TEK FSM of successful authorization. See clause 7.1.2.3.9.

7.1.3.3.3 Authorization Pending (Auth Pend)

Sent by the Authorization FSM to TEK FSM to place TEK FSM in a wait state while Authorization FSM completes reauthorization. See clause 7.1.2.3.10.

7.1.3.3.4 Authorization Complete (Auth Comp)

Sent by the Authorization FSM to a TEK FSM in the Operational Reauthorize Wait or Rekey Reauthorize Wait states to clear the wait state begun by the prior Authorization Pending event. See clause 7.1.2.3.11.

7.1.3.3.5 TEK Invalid

This event can be triggered by either a CM's data packet decryption logic, or by the receipt of a TEK Invalid message from the CMTS.

A CM's data packet decryption logic triggers a TEK Invalid event if it recognizes a loss of TEK key synchronization between itself and the encrypting CMTS; i.e., a SAID's TEK key sequence number, contained within the received, downstream packet's Baseline Privacy Extended Header element, is out of the CM's range of known sequence numbers for that SAID.

A CMTS sends a CM a TEK Invalid message, triggering a TEK Invalid event within the CM, if the CMTS's decryption logic recognizes a loss of TEK key synchronization between itself and the CM.

7.1.3.3.6 Timeout

A retry timer timeout. Generally, the particular request is retransmitted.

7.1.3.3.7 TEK refresh timeout

The TEK refresh timer timed out. This timer event signals the TEK state machine to issue a new Key Request in order to refresh its keying material. The refresh timer is set to fire a configurable length of time (*TEK Grace Time*) before the expiration of the newer TEK the CM currently holds. This is configured via the CMTS to occur after the scheduled expiration of the older of the two TEKs.

7.1.3.4 Parameters

All configuration parameter values are specified in TFTP downloaded parameter file (see Annex A).

7.1.3.4.1 Operational Wait Timeout

Timeout period between sending of Key Request messages from the Op Wait state. See clause A.1.1.1.4.

7.1.3.4.2 Rekey Wait Timeout

Timeout period between sending of Key Request messages from the Rekey Wait state. See clause A.1.1.1.5.

7.1.3.4.3 TEK Grace Time

Time interval, in seconds, before the estimated expiration of a TEK that the CM starts rekeying for a new TEK.

TEK Grace Time is specified in a configuration setting within the TFTP-downloaded parameter file, and is the same across all SAIDs. See clause A.1.1.1.6.

7.1.3.5 Actions

1-B Op Wait (*Stop*) → Start

- clear Key Request retry timer;
- terminate TEK FSM.

1-C Op Reauth Wait (*Stop*) → Start

- terminate TEK FSM.

1-D Operational (*Stop*) → Start

- clear TEK refresh timer, which is timer set to go off "*Tek Grace Time*" seconds prior to the TEK's scheduled expiration time;
- terminate TEK FSM;
- remove SAID keying material from key table.

1-E Rekey Wait (*Stop*) → Start

- clear Key Request retry timer;
- terminate TEK FSM;
- remove SAID keying material from key table.

1-F Rekey Reauth Wait (*Stop*) → Start

- terminate TEK FSM;
- remove SAID keying material from key table.

- 2-A Start (*Authorized*) → Op Wait
- send Key Request Message to CMTS;
 - set Key Request retry timer to Operational Wait Timeout.
- 3-B Op Wait (*Auth Pend*) → Op Reauth Wait
- clear Key Request retry timer.
- 3-E Rekey Wait (*Auth Pend*) → Rekey Reauth Wait
- clear Key Request retry timer.
- 4-C Op Reauth Wait (*Auth Comp*) → Op Wait
- send Key Request message to CMTS;
 - set Key Request retry timer to Operational Wait Timeout.
- 4-F Rekey Reauth Wait (*Auth Comp*) → Rekey Wait
- send Key Request message to CMTS;
 - set Key Request retry timer to Rekey Wait Timeout.
- 5-D Operational (*TEK Invalid*) → Op Wait
- clear TEK refresh timer;
 - send Key Request message to CMTS;
 - set Key Request retry timer to Operational Wait Timeout;
 - remove SAID keying material from key table.
- 5-E Rekey Wait (*TEK Invalid*) → Op Wait
- clear Key Request retry timer;
 - send Key Request message to CMTS;
 - set Key Request retry timer to Operational Wait Timeout;
 - remove SAID keying material from key table.
- 5-F Rekey Reauth Wait (*TEK Invalid*) → Op Reauth Wait
- remove SAID keying material from key table.
- 6-B Op Wait (*Timeout*) → Op Wait
- send Key Request message to CMTS;
 - set Key Request retry timer to Operational Wait Timeout.
- 6-E Rekey Wait (*Timeout*) → Rekey Wait
- send Key Request message to CMTS;
 - set Key Request retry timer to Rekey Wait Timeout.
- 7-D Operational (*TEK Grace Timeout*) → Rekey Wait
- send Key Request message to CMTS;
 - set Key Request retry timer to Rekey Wait Timeout.
- 8-B Op Wait (Key Reply) → Operational

NOTE 1 – Key Reply passed message authentication.

- clear Key Request retry timer;
- process contents of Key Reply message and incorporate new keying material into key database;

- set the TEK refresh timer to go off "TEK Grace Time" seconds prior to the key's scheduled expiration.

8-E Rekey Wait (Key Reply) → Operational

NOTE 2 – Key Reply passed message authentication.

- clear Key Request retry timer;
- process contents of Key Reply message and incorporate new keying material into key database;
- set the TEK refresh timer to go off "TEK Grace Time" seconds prior to the key's scheduled expiration.

9-B Op Wait (Key Reject) → Start

NOTE 3 – Key Reject passed message authentication.

- clear Key Request retry timer;
- terminate TEK FSM.

9-E Rekey Wait (Key Reject) → Start

- clear Key Request retry timer;
- terminate TEK FSM;
- remove SAID keying material from key table.

7.2 Key management message formats⁴

Baseline Privacy Key Management employs two MAC message types: BPKM-REQ and BPKM-RSP. [ITU-T J.112-B] and [ITU-T J.122] define the specific type values assigned to them.

Table 7-3 – Baseline privacy key management MAC messages

Type value	Message name	Message description
See [ITU-T J.112-B] or [ITU-T J.122]	BPKM-REQ	Privacy Key Management Request [CM → CMTS]
See [ITU-T J.112-B] or [ITU-T J.122]	BPKM-RSP	Privacy Key Management Response [CMTS → CM]

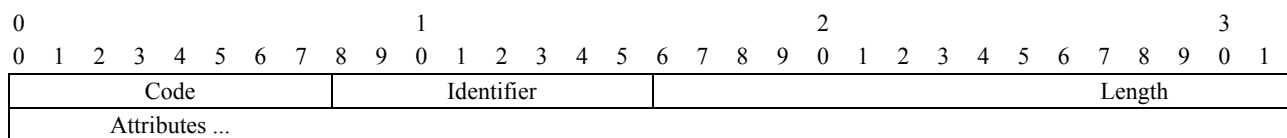
While these two MAC management message types distinguish between BPKM requests (CM to CMTS) and responses (CMTS to CM), more detailed information about message contents is encoded in the BPKM messages themselves. This maintains a clean separation between privacy management functions and RF MAC upstream bandwidth allocation, timing and synchronization (RF MAC management's principal responsibilities).

7.2.1 Packet formats

Exactly one BPKM message is encapsulated in the Management Message Payload field of a MAC management message.

A summary of the BPKM message format is shown below. The fields are transmitted from left to right.

⁴ Message formats for the Baseline Privacy Key Management protocol are modelled after those of the Remote Authentication Dial In User Service (RADIUS) protocol, defined in [IETF RFC 2868], and an Internet standards track protocol. BPKM, like RADIUS, adheres to a client/server model. Unlike RADIUS, BPKM will not run over UDP/IP. BPKM messages are encapsulated within RF MAC management messages.



Code

The Code field is one octet, and identifies the type of BPKM packet. When a packet is received with an invalid Code field, it SHOULD be silently discarded.

BPKM Codes (decimal) are assigned as follows:

Table 7-4 – Baseline privacy key management message codes

Code	BPKM message type	MAC management message name
0-3	Reserved	–
4	Auth Request	BPKM-REQ
5	Auth Reply	BPKM-RSP
6	Auth Reject	BPKM-RSP
7	Key Request	BPKM-REQ
8	Key Reply	BPKM-RSP
9	Key Reject	BPKM-RSP
10	Auth Invalid	BPKM-RSP
11	TEK Invalid	BPKM-RSP
12	Authent Info	BPKM-REQ
13	Map Request	BPKM-REQ
14	Map Reply	BPKM-RSP
15	Map Reject	BPKM-RSP
16-255	Reserved	–

Identifier

The Identifier field is one octet. A CM uses the identifier to match the CMTS's responses to the CM's requests.

The CM MUST change (e.g., increment, wrapping around to 0 after reaching 255) the Identifier field whenever it issues a new BPKM message. A "new" message is an Authorization Request, Key Request or SA Map Request that is not a retransmission being sent in response to a Timeout event. For retransmissions, the Identifier field MUST remain unchanged.

The Identifier field in Authentication Information messages, which are informative and do not effect any response messaging, MAY be set to zero.

The Identifier field in a CMTS's BPKM response message MUST match the Identifier field of the BPKM Request message the CMTS is responding to. The Identifier field in TEK Invalid messages, which are not sent in response to BPKM requests, MUST be set to zero. The Identifier field in unsolicited Authorization Invalid messages MUST be set to zero.

On reception of a BPKM response message, the CM associates the message with a particular state machine (the Authorization state machine in the case of Authorization Replies, Authorization Rejects, and Authorization Invalids; a particular TEK state machine in the case of Key Replies, Key Rejects and TEK Invalids; a particular SA Mapping state machine in the case of SA Map Replies and SA Map Rejects).

A CM MAY keep track of the Identifier of its latest, pending Authorization Request. The CM MAY silently discard Authorization Replies and Authorization Rejects whose Identifier fields do not match those of the pending requests.

A CM MAY keep track of the Identifier of its latest, pending Key Request. The CM MAY silently discard Key Replies and Key Rejects whose Identifier fields do not match those of the pending requests.

A CM MAY keep track of the Identifier of its latest, pending SA Map Request. The CM MAY silently discard SA Map Replies and SA Map Rejects whose Identifier fields do not match those of the pending requests.

Length

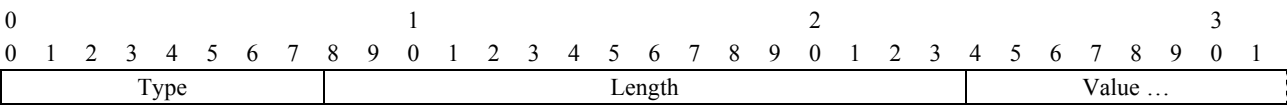
The Length field is two octets. It indicates the length of the Attribute fields in octets. The length field does not include the Code, Identifier and Length fields. Octets outside the range of the Length field MUST be treated as padding and ignored on reception. If the packet is shorter than the Length field indicates, it SHOULD be silently discarded. The minimum length is 0 and maximum length is 1490.

Attributes

BPKM Attributes carry the specific authentication, authorization and key management data exchanged between client and server. Each BPKM packet type has its own set of required and optional Attributes. Unless explicitly stated, there are no requirements on the ordering of attributes within a BPKM message.

The end of the list of Attributes is indicated by the Length of the BPKM packet.

Attributes are type/length/value (TLV) encoded, as shown below. The fields are transmitted from left to right.



Packet formats for each of the BPKM messages are described below. The descriptions list the BPKM attributes contained within each BPKM message type. The Attributes themselves are described in clause 7.2.2. Unknown attributes MUST be ignored on receipt, and skipped over while scanning for recognized attributes.

The CMTS MUST silently discard all requests that do not contain ALL required attributes. The CM MUST silently discard all responses that do not contain ALL required attributes.

7.2.1.1 Authorization Request (Auth Request)

Code: 4

Attributes:

Table 7-5 – Authorization Request attributes

Attribute	Contents
CM-Identification	Contains information used to identify cable modem to CMTS
CM-Certificate	Contains the CM's X.509 user certificate
Security-Capabilities	Describes requesting CM's security capabilities
SAID	CM's primary SAID equal to the Primary SID

The CM-Identification attribute contains a set of data that identifies the requesting cable modem to the CMTS.

NOTE – The CMTS is in all likelihood using only a single item in the CM-Identification attribute (e.g., CM MAC address) as a CM handle. While a specific item could be selected for inclusion in the Authorization Request message, including the entire CM-Identification attribute for client identification provides vendors with greater flexibility in the headend's system design.

The CM-Certificate attribute contains an X.509 CM certificate issued by the CM's manufacturer. The CM's X.509 certificate is a public-key certificate which binds the CM's identifying information to its RSA public key in a verifiable manner. The X.509 certificate is digitally signed by the CM's manufacturer, and that signature can be verified by a CMTS that knows the manufacturer's public key. The manufacturer's public key is placed in an X.509 certification authority (CA) certificate, which in turn is signed by a higher level certification authority.

The Security-Capabilities attribute is a compound attribute describing the requesting cable modem's security capabilities. This includes the packet data encryption algorithm(s) a CM supports and the packet data authentication algorithm(s) supported (of which there are currently none) and the version of the Baseline Privacy Protocol supported (of which there is currently one: version 1 for BPI+).

A SAID attribute contains a Baseline Privacy security association identifier, or SAID. In this case, the provided SAID is the CM's BPI+ primary SAID, which is equal to the Primary SID assigned to the cable modem during RF MAC registration.

7.2.1.2 Authorization Reply (Auth Reply)

Sent by the CMTS to a client CM in response to an Authorization Request, the Authorization Reply message contains an Authorization Key, the key's lifetime, the key's sequence number, and a list of SA-Descriptors identifying the Primary and Static Security Associations the requesting cable modem is authorized to access and their particular properties (e.g., type, cryptographic suite). The Authorization Key MUST be encrypted with the CM's public key. The SA-Descriptor list MUST include a descriptor for the primary BPI+ SAID reported to the CMTS in the corresponding Authorization Request. The SA-Descriptor list MAY include descriptors of Static SAIDs the CM is authorized to access.

Code field: 5

Attributes:

Table 7-6 – Authorization Reply attributes

Attribute	Contents
AUTH-Key	Authorization (AUTH) Key, encrypted with the target client CM's public key
Key-Lifetime	Authorization key lifetime
Key-Sequence-Number	Authorization key sequence number
(One or more) SA-Descriptor	Each SA-Descriptor compound Attribute specifies a SAID and additional properties of the SA

7.2.1.3 Authorization Reject (Auth Reject)

CMTS responds to a CM's authorization request with an Authorization Reject message if the CMTS rejects the CM's authorization request.

Code field: 6

Attributes:

Table 7-7 – Auth Rej attributes

Attribute	Contents
Error-Code	Error code identifying reason for rejection of authorization request
Display-String (optional)	Display String providing reason for rejection of authorization request

The Error-Code and Display-String attributes describe to the requesting CM the reason for the authorization failure.

7.2.1.4 Key Request

Code: 7

Attributes:

Table 7-8 – Key Request attributes

Attribute	Contents
CM-Identification	Contains information used to identify cable modem to CMTS
Key-Sequence-Number	Authorization key sequence number
SAID	Security Association ID
HMAC-Digest	Keyed SHA message digest

The HMAC-Digest Attribute is a keyed message digest. The HMAC-Digest Attribute MUST be the final Attribute in the Key Request's Attribute list. The message digest is performed over the packet header and all of the Key Request's Attributes, other than the HMAC-Digest, in the order in which they appear within the packet.

Inclusion of the keyed digest allows the CMTS to authenticate the Key Request message. The HMAC-Digest's authentication key is derived from the Authorization Key. See clause 10 for details.

7.2.1.5 Key Reply

Code: 8

Attributes:

Table 7-9 – Key Reply attributes

Attribute	Contents
Key-Sequence-Number	Authorization key sequence number
SAID	Security Association ID
TEK-Parameters	"Older" generation of key parameters relevant to SAID
TEK-Parameters	"Newer" generation of key parameters relevant to SAID
HMAC-Digest	Keyed SHA message digest

The TEK-Parameters Attribute is a compound attribute containing all of the keying material corresponding to a particular generation of a SAID's TEK. This would include the TEK, the TEK's remaining key lifetime, its key sequence number, and the CBC initialization vector. The TEK is encrypted. See clause 7.2.2.13 for details.

At all times the CMTS maintains two sets of active generations of keying material per SAID. (A set of keying material includes the TEK and its corresponding CBC initialization vector.) One set corresponds to the "older" generation of keying material, the second set corresponds to the "newer" generation of keying material. The newer generation has a key sequence number one greater than (modulo 16) that of the older generation. Clause 9.1 specifies CMTS requirements for maintaining and using a SAID's two active generations of keying material.

The CMTS distributes to a client CM both generations of active keying material. Thus, the Key Reply message contains two TEK-Parameters Attributes, each containing the keying material for one of the SAIDs two active sets of keying material.

The HMAC-Digest Attribute is a keyed message digest. The HMAC-Digest Attribute MUST be the final Attribute in the Key Reply's Attribute list. The message digest is performed over the BPKM message header (starting with the BPKM Code field) and all of the Key Reply's Attributes, other than the HMAC-Digest, in the order in which they appear within the packet.

Inclusion of the keyed digest allows the receiving client to authenticate the Key Reply message and ensure CM and CMTS have synchronized Authorization Keys. The HMAC-Digest's authentication key is derived from the Authorization Key. See clause 10 for details.

7.2.1.6 Key Reject

Receipt of a Key Reject indicates the receiving client CM is no longer authorized for a particular SAID.

Code: 9

Attributes:

Table 7-10 – Key Reject attributes

Attribute	Contents
Key-Sequence-Number	Authorization key sequence number
SAID	Security Association ID
Error-Code	Error code identifying reason for rejection of Key Request
Display-String (optional)	Display string containing reason for Key Reject
HMAC-Digest	Keyed SHA message digest

The HMAC-Digest Attribute is a keyed message digest. The HMAC-Digest Attribute MUST be the final Attribute in the Key Reject's Attribute list. The message digest is performed over the BPKM message header (starting with the BPKM Code field) and all of the Key Reject's Attributes, other than the HMAC-Digest, in the order in which they appear within the packet.

Inclusion of the keyed digest allows the receiving client to authenticate the Key Reject message and ensure CM and CMTS have synchronized Authorization Keys. The HMAC-Digest's authentication key is derived from the Authorization Key. See clause 10 for details.

7.2.1.7 Authorization Invalid

The CMTS can send an Authorization Invalid message to a client CM as:

- an unsolicited indication; or
- a response to a message received from that CM.

In either case, the Authorization Invalid message instructs the receiving CM to reauthorize with its CMTS.

The CMTS sends an Authorization Invalid in response to a Key Request if:

- 1) the CMTS does not recognize the CM as being authorized (i.e., no valid Authorization Key associated with the requesting cable modem); or
- 2) verification of the Key Request's keyed message digest (in HMAC-Digest Attribute) failed, indicating a loss of Authorization Key synchronization between CM and CMTS.

Code: 10

Attributes:

Table 7-11 – Authorization Invalid attributes

Attribute	Contents
Error-Code	Error code identifying reason for Authorization Invalid
Display-String (optional)	Display String describing failure condition

7.2.1.8 TEK Invalid

The CMTS sends a TEK Invalid message to a client CM if the CMTS determines that the CM encrypted an upstream Packet Data PDU with an invalid TEK; i.e., a SAID's TEK key sequence number, contained within the received packet's Baseline Privacy Extended Header element, is out of the CMTS's range of known, valid sequence numbers for that SAID.

Code: 11

Attributes:

Table 7-12 – TEK Invalid attributes

Attribute	Contents
Key-Sequence-Number	Authorization key sequence number
SAID	Security Association ID
Error-Code	Error code identifying reason for TEK Invalid message
Display-String (optional)	Display string containing vendor-defined information
HMAC-Digest	Keyed SHA message digest

The HMAC-Digest Attribute is a keyed message digest. The HMAC-Digest Attribute MUST be the final Attribute in the TEK Invalid's Attribute list. The message digest is performed over the BPKM message header (starting with the BPKM Code field) and all of the TEK Invalid's Attributes, other than the HMAC-Digest, in the order in which they appear within the packet.

Inclusion of the keyed digest allows the receiving client to authenticate the TEK Invalid message and ensure CM and CMTS have synchronized Authorization Keys. The HMAC-Digest's authentication key is derived from the Authorization Key. See clause 10 for details.

7.2.1.9 Authentication Information (Authent Info)

The Authentication Info message contains a single CA-Certificate Attribute, containing an X.509 CA certificate for the manufacturer of the CM. The CM's X.509 user certificate MUST have been issued by the certification authority identified by the X.509 CA certificate. All X.509 CA certificates MUST be issued by a DOCSIS root certification authority.

Authentication Information messages are strictly informative: while the CM MUST transmit Authent Info messages as indicated by the Authentication state model (clause 7.1.2), the CMTS MAY ignore them.