



INTERNATIONAL TELECOMMUNICATION UNION

# ITU-T

TELECOMMUNICATION  
STANDARDIZATION SECTOR  
OF ITU

## J.222.3

(11/2007)

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

Interactive systems for digital television distribution

---

**Security services for third-generation  
transmission systems for interactive cable  
television services – IP cable modems**

***CAUTION !***

***PREPUBLISHED RECOMMENDATION***

This prepublication is an unedited version of a recently approved Recommendation. It will be replaced by the published version after editing. Therefore, there will be differences between this prepublication and the published version.

Downloaded from https://www.ava.com/

## FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. 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/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.



## ITU-T Recommendation J.222.3 (formerly J.ss)

### Recommendation J.222.3, Security services for third-generation transmission systems for interactive cable television services - IP cable modems

#### Summary

<Mandatory material>

#### Keywords

<Optional>

11/2007

# Contents

|          |                                                                     |           |
|----------|---------------------------------------------------------------------|-----------|
| <b>1</b> | <b>SCOPE.....</b>                                                   | <b>7</b>  |
| <b>2</b> | <b>REFERENCES .....</b>                                             | <b>7</b>  |
| 2.1      | NORMATIVE REFERENCES .....                                          | 7         |
| 2.2      | INFORMATIVE REFERENCES.....                                         | 8         |
| 2.3      | REFERENCE ACQUISITION.....                                          | 9         |
| <b>3</b> | <b>TERMS AND DEFINITIONS.....</b>                                   | <b>9</b>  |
| <b>4</b> | <b>ABBREVIATIONS, ACRONYMS AND CONVENTIONS.....</b>                 | <b>10</b> |
| 4.1      | ABBREVIATIONS AND ACRONYMS .....                                    | 10        |
| 4.2      | CONVENTIONS.....                                                    | 12        |
| <b>5</b> | <b>OVERVIEW .....</b>                                               | <b>12</b> |
| 5.1      | NEW DOCSIS 3.0 SECURITY FEATURES.....                               | 13        |
| 5.2      | TECHNICAL OVERVIEW .....                                            | 14        |
| 5.2.1    | <i>BPI+ Architecture .....</i>                                      | <i>14</i> |
| 5.2.2    | <i>Secure Provisioning.....</i>                                     | <i>16</i> |
| 5.3      | OPERATION .....                                                     | 16        |
| 5.3.1    | <i>Cable Modem Initialization.....</i>                              | <i>16</i> |
| 5.3.2    | <i>Cable Modem Key Update Mechanism .....</i>                       | <i>18</i> |
| 5.3.3    | <i>Cable Modem Secure Software Download.....</i>                    | <i>18</i> |
| <b>6</b> | <b>ENCRYPTED DOCSIS MAC FRAME FORMATS .....</b>                     | <b>18</b> |
| 6.1      | CM REQUIREMENTS .....                                               | 18        |
| 6.2      | CMTS REQUIREMENTS .....                                             | 18        |
| 6.3      | VARIABLE-LENGTH PDU MAC FRAME FORMAT.....                           | 19        |
| 6.3.1    | <i>Piggybacked Bandwidth Requests .....</i>                         | <i>20</i> |
| 6.4      | FRAGMENTATION MAC FRAME FORMAT.....                                 | 22        |
| 6.5      | REGISTRATION REQUEST (REG-REQ-MP) MAC MANAGEMENT MESSAGES .....     | 23        |
| 6.6      | USE OF THE BASELINE PRIVACY EXTENDED HEADER IN THE MAC HEADER ..... | 25        |
| <b>7</b> | <b>BASELINE PRIVACY KEY MANAGEMENT (BPKM) PROTOCOL .....</b>        | <b>26</b> |
| 7.1      | STATE MODELS .....                                                  | 26        |
| 7.1.1    | <i>Introduction .....</i>                                           | <i>26</i> |
| 7.1.2    | <i>Encrypted Multicast.....</i>                                     | <i>29</i> |
| 7.1.3    | <i>Selecting Cryptographic Suites.....</i>                          | <i>31</i> |
| 7.1.4    | <i>Authorization State Machine .....</i>                            | <i>31</i> |
| 7.1.5    | <i>TEK State Machine.....</i>                                       | <i>39</i> |
| 7.2      | KEY MANAGEMENT MESSAGE FORMATS .....                                | 45        |
| 7.2.1    | <i>Packet Formats.....</i>                                          | <i>45</i> |
| 7.2.2    | <i>BPKM Attributes.....</i>                                         | <i>52</i> |
| <b>8</b> | <b>EARLY AUTHENTICATION AND ENCRYPTION (EAE).....</b>               | <b>67</b> |
| 8.1      | INTRODUCTION.....                                                   | 67        |
| 8.2      | EAE SIGNALING.....                                                  | 67        |
| 8.3      | EAE ENCRYPTION .....                                                | 68        |
| 8.4      | EAE ENFORCEMENT.....                                                | 69        |
| 8.4.1    | <i>CMTS and CM behaviors when EAE is Enabled.....</i>               | <i>69</i> |
| 8.4.2    | <i>EAE enforcement determination.....</i>                           | <i>69</i> |
| 8.4.3    | <i>DHCP Relay and EAE Enforcement Verification.....</i>             | <i>70</i> |
| 8.4.4    | <i>CMTS and CM Behavior when EAE is Disabled.....</i>               | <i>70</i> |
| 8.4.5    | <i>EAE Exclusion List .....</i>                                     | <i>70</i> |
| 8.4.6    | <i>Interoperability issues .....</i>                                | <i>70</i> |
| 8.5      | AUTHENTICATION REUSE .....                                          | 71        |

|           |                                                                |           |
|-----------|----------------------------------------------------------------|-----------|
| 8.6       | BPI+ CONTROL BY CONFIGURATION FILE .....                       | 71        |
| 8.6.1     | EAE Enabled.....                                               | 71        |
| 8.6.2     | EAE Disabled .....                                             | 71        |
| <b>9</b>  | <b>SECURE PROVISIONING.....</b>                                | <b>73</b> |
| 9.1       | INTRODUCTION.....                                              | 73        |
| 9.2       | ENCRYPTION OF PROVISIONING MESSAGES.....                       | 73        |
| 9.3       | SECURING DHCP .....                                            | 73        |
| 9.3.1     | Securing DHCP on the Cable Network Link .....                  | 73        |
| 9.3.2     | DHCPv6 .....                                                   | 73        |
| 9.4       | TFTP CONFIGURATION FILE SECURITY .....                         | 73        |
| 9.4.1     | Introduction .....                                             | 73        |
| 9.4.2     | CMTS Security Features for Configuration File Download.....    | 73        |
| 9.5       | SECURING REG-REQ-MP MESSAGES.....                              | 75        |
| 9.6       | SOURCE ADDRESS VERIFICATION.....                               | 75        |
| 9.7       | ADDRESS RESOLUTION SECURITY CONSIDERATIONS .....               | 76        |
| <b>10</b> | <b>USING CRYPTOGRAPHIC KEYS.....</b>                           | <b>78</b> |
| 10.1      | CMTS .....                                                     | 78        |
| 10.2      | CABLE MODEM .....                                              | 80        |
| 10.3      | AUTHENTICATION OF DYNAMIC SERVICE REQUESTS .....               | 81        |
| 10.3.1    | CM .....                                                       | 81        |
| 10.3.2    | CMTS.....                                                      | 81        |
| <b>11</b> | <b>CRYPTOGRAPHIC METHODS .....</b>                             | <b>82</b> |
| 11.1      | PACKET DATA ENCRYPTION.....                                    | 82        |
| 11.2      | ENCRYPTION OF THE TEK .....                                    | 83        |
| 11.3      | HMAC-DIGEST ALGORITHM.....                                     | 83        |
| 11.4      | TEKS, KEKS AND MESSAGE AUTHENTICATION KEYS .....               | 83        |
| 11.5      | PUBLIC-KEY ENCRYPTION OF AUTHORIZATION KEY .....               | 84        |
| 11.6      | DIGITAL SIGNATURES.....                                        | 84        |
| 11.7      | THE MMH-MIC.....                                               | 84        |
| 11.7.1    | The MMH Function .....                                         | 84        |
| 11.7.2    | $MMH[16, \sigma, 4]$ .....                                     | 86        |
| 11.7.3    | Definition of MMH-MAC.....                                     | 87        |
| 11.7.4    | Calculating the MMH-MAC .....                                  | 87        |
| 11.7.5    | MMH Key Derivation for CMTS MIC .....                          | 88        |
| 11.7.6    | Shared Secret Recommendations.....                             | 88        |
| 11.8      | KEY GENERATION FUNCTION .....                                  | 88        |
| <b>12</b> | <b>PHYSICAL PROTECTION OF KEYS IN THE CM.....</b>              | <b>90</b> |
| <b>13</b> | <b>BPI+ X.509 CERTIFICATE PROFILE AND MANAGEMENT .....</b>     | <b>91</b> |
| 13.1      | BPI+ CERTIFICATE MANAGEMENT ARCHITECTURE OVERVIEW .....        | 91        |
| 13.2      | CABLE MODEM CERTIFICATE STORAGE AND MANAGEMENT IN THE CM ..... | 93        |
| 13.3      | CERTIFICATE PROCESSING AND MANAGEMENT IN THE CMTS .....        | 94        |
| 13.3.1    | CMTS Certificate Management Model.....                         | 94        |
| 13.3.2    | Certificate Validation .....                                   | 95        |
| 13.4      | CERTIFICATE REVOCATION .....                                   | 95        |
| 13.4.1    | Certificate Revocation Lists.....                              | 95        |
| 13.4.2    | Online Certificate Status Protocol.....                        | 97        |
| <b>14</b> | <b>SECURE SOFTWARE DOWNLOAD .....</b>                          | <b>98</b> |
| 14.1      | INTRODUCTION.....                                              | 98        |
| 14.2      | OVERVIEW.....                                                  | 98        |
| 14.3      | SOFTWARE CODE UPGRADE REQUIREMENTS.....                        | 100       |
| 14.3.1    | Code File Processing Requirements.....                         | 100       |
| 14.3.2    | Code File Access Controls.....                                 | 101       |
| 14.3.3    | Cable Modem Code Upgrade Initialization .....                  | 102       |

|                    |                                                                                     |            |
|--------------------|-------------------------------------------------------------------------------------|------------|
| 14.3.4             | Code Signing Guidelines .....                                                       | 104        |
| 14.3.5             | Code Verification Requirements .....                                                | 104        |
| 14.3.6             | DOCSIS Interoperability .....                                                       | 105        |
| 14.3.7             | Error Codes .....                                                                   | 105        |
| 14.4               | SECURITY CONSIDERATIONS (INFORMATIVE) .....                                         | 107        |
| <b>ANNEX A</b>     | <b>TFTP CONFIGURATION FILE EXTENSIONS (NORMATIVE) .....</b>                         | <b>108</b> |
| A.1                | ENCODINGS .....                                                                     | 108        |
| A.1.1              | Baseline Privacy Configuration Setting .....                                        | 108        |
| A.2                | PARAMETER GUIDELINES .....                                                          | 110        |
| <b>ANNEX B</b>     | <b>TFTP OPTIONS (NORMATIVE) .....</b>                                               | <b>112</b> |
| <b>ANNEX C</b>     | <b>DOCSIS 1.1/2.0 DYNAMIC SECURITY ASSOCIATIONS (NORMATIVE) .....</b>               | <b>120</b> |
| C.1                | INTRODUCTION .....                                                                  | 120        |
| C.2                | THEORY OF OPERATION .....                                                           | 120        |
| C.3                | SA MAPPING STATE MODEL .....                                                        | 121        |
| C.3.1              | Brief Description of States .....                                                   | 122        |
| C.3.2              | Brief Description of Messages .....                                                 | 123        |
| C.3.3              | Brief Description of Events .....                                                   | 123        |
| C.3.4              | Actions .....                                                                       | 123        |
| <b>APPENDIX I</b>  | <b>EXAMPLE MESSAGES, CERTIFICATES, PDUS AND CODE FILE<br/>(INFORMATIVE) .....</b>   | <b>125</b> |
| I.1                | NOTATION .....                                                                      | 125        |
| I.2                | AUTHENTICATION INFO .....                                                           | 125        |
| I.2.1              | CA Certificate details .....                                                        | 125        |
| I.3                | AUTHORIZATION REQUEST .....                                                         | 127        |
| I.3.1              | CM Certificate details .....                                                        | 128        |
| I.4                | AUTHORIZATION REPLY .....                                                           | 130        |
| I.4.1              | RSA encryption details .....                                                        | 131        |
| I.4.2              | RSA decryption details .....                                                        | 133        |
| I.4.3              | Hashing details .....                                                               | 134        |
| I.5                | KEY REQUEST .....                                                                   | 136        |
| I.5.1              | HMAC digest details .....                                                           | 136        |
| I.6                | KEY REPLY .....                                                                     | 137        |
| I.6.1              | TEK encryption details .....                                                        | 138        |
| I.6.2              | HMAC details .....                                                                  | 139        |
| I.7                | PACKET PDU ENCRYPTION (DES) .....                                                   | 139        |
| I.7.1              | CBC only .....                                                                      | 140        |
| I.7.2              | CBC with residual block processing .....                                            | 141        |
| I.7.3              | Runt frame .....                                                                    | 142        |
| I.7.4              | 40-bit key .....                                                                    | 143        |
| I.8                | ENCRYPTION OF PDU WITH PAYLOAD HEADER SUPPRESSION (DES) .....                       | 145        |
| I.8.1              | Downstream .....                                                                    | 145        |
| I.8.2              | Upstream .....                                                                      | 146        |
| I.9                | FRAGMENTED PACKET ENCRYPTION (DES) .....                                            | 146        |
| I.10               | PACKET PDU ENCRYPTION (AES) .....                                                   | 148        |
| I.10.1             | CBC only .....                                                                      | 148        |
| I.10.2             | CBC with residual block processing .....                                            | 149        |
| I.10.3             | Runt frame .....                                                                    | 151        |
| I.11               | ENCRYPTION OF PDU WITH PAYLOAD HEADER SUPPRESSION (AES) .....                       | 151        |
| I.11.1             | Downstream .....                                                                    | 152        |
| I.11.2             | Upstream .....                                                                      | 152        |
| I.12               | FRAGMENTED PACKET ENCRYPTION (AES) .....                                            | 153        |
| I.13               | SECURE SOFTWARE DOWNLOAD CM CODE FILE .....                                         | 155        |
| <b>APPENDIX II</b> | <b>EXAMPLE OF MULTILINEAR MODULAR HASH (MMH) ALGORITHM<br/>IMPLEMENTATION .....</b> | <b>171</b> |

## APPENDIX III CERTIFICATE AUTHORITY & PROVISIONING GUIDELINES..... 179

|         |                                                                                     |     |
|---------|-------------------------------------------------------------------------------------|-----|
| III.1   | CERTIFICATE FORMAT & EXTENSIONS .....                                               | 179 |
| III.1.1 | <i>tbsCertificate.validity.notBefore and tbsCertificate.validity.notAfter</i> ..... | 179 |
| III.1.2 | <i>tbsCertificate.serialNumber</i> .....                                            | 180 |
| III.1.3 | <i>tbsCertificate.signature and signatureAlgorithm</i> .....                        | 180 |
| III.1.4 | <i>tbsCertificate.issuer and tbsCertificate.subject</i> .....                       | 180 |
| III.1.5 | <i>tbsCertificate.issuerUniqueID and tbsCertificate.subjectUniqueID</i> .....       | 182 |
| III.1.6 | <i>tbsCertificate.extensions</i> .....                                              | 182 |
| III.1.7 | <i>Code Verification Certificate Format</i> .....                                   | 183 |
| III.1.8 | <i>signatureValue</i> .....                                                         | 184 |
| III.2   | CERTIFICATE PROVISIONING .....                                                      | 184 |
| III.2.1 | <i>DOCSIS Root CA</i> .....                                                         | 184 |
| III.2.2 | <i>Digital Certificate Validity Period and Re-issuance</i> .....                    | 184 |
| III.2.3 | <i>CM Code File Signing Policy</i> .....                                            | 185 |
| III.2.4 | <i>CM Code File Format</i> .....                                                    | 186 |

## Figures

|                                                                                           |     |
|-------------------------------------------------------------------------------------------|-----|
| FIGURE 6-1 - FORMAT OF DOCSIS VARIABLE-LENGTH PDU WITH PRIVACY EH ELEMENT .....           | 19  |
| FIGURE 6-2 - FORMAT OF A DOCSIS MAC FRAGMENTATION FRAME WITH AN ENCRYPTED PAYLOAD .....   | 22  |
| FIGURE 6-3 - FORMAT OF A DOCSIS MAC MANAGEMENT MESSAGE FRAME WITH ENCRYPTED PAYLOAD ..... | 24  |
| FIGURE 7-1 - RELATIONSHIP AMONG AUTHORIZATION AND TEK STATE MACHINES .....                | 28  |
| FIGURE 7-2 - AUTHORIZATION STATE MACHINE FLOW DIAGRAM .....                               | 32  |
| FIGURE 7-3 - TEK STATE MACHINE FLOW DIAGRAM .....                                         | 40  |
| FIGURE 8-1 - EAE SIGNALING FLOW CHART FOR CM .....                                        | 68  |
| FIGURE 10-1 - AUTHORIZATION KEY MANAGEMENT IN CMTS AND CM .....                           | 79  |
| FIGURE 10-2 - TEK MANAGEMENT IN CMTS AND CM .....                                         | 80  |
| FIGURE 13-1 - THE CENTRALIZED MODEL OF THE DOCSIS CERTIFICATE MANAGEMENT ARCHITECTURE ..  | 92  |
| FIGURE 13-2 - THE DISTRIBUTED MODEL OF THE DOCSIS CERTIFICATE MANAGEMENT ARCHITECTURE ... | 93  |
| FIGURE 13-3 - CRL FRAMEWORK .....                                                         | 96  |
| FIGURE 13-4 - OCSP FRAMEWORK .....                                                        | 97  |
| FIGURE 14-1 - TYPICAL CODE VALIDATION HIERARCHY .....                                     | 100 |
| FIGURE C-1 - SA MAPPING STATE MACHINE FLOW DIAGRAM .....                                  | 122 |

## Tables

|                                                                                                                     |     |
|---------------------------------------------------------------------------------------------------------------------|-----|
| TABLE 6-1 - SUMMARY OF THE CONTENTS OF BASELINE PRIVACY EXTENDED HEADERS.....                                       | 20  |
| TABLE 6-2 - SUMMARY OF THE CONTENTS OF A DOCSIS FRAGMENTATION MAC FRAME'S BASELINE PRIVACY<br>EXTENDED HEADER ..... | 23  |
| TABLE 6-3 - SUMMARY OF THE CONTENTS OF DOCSIS MAC MANAGEMENT MESSAGE BASELINE PRIVACY EXTENDED<br>HEADERS.....      | 25  |
| TABLE 7-1 - AUTHORIZATION FSM TRANSITION MATRIX .....                                                               | 32  |
| TABLE 7-2 - TEK FSM STATE TRANSITION MATRIX .....                                                                   | 40  |
| TABLE 7-3 - BASELINE PRIVACY KEY MANAGEMENT MAC MESSAGES .....                                                      | 45  |
| TABLE 7-4 - BASELINE PRIVACY KEY MANAGEMENT MESSAGE CODES .....                                                     | 46  |
| TABLE 7-5 - AUTHORIZATION REQUEST ATTRIBUTES .....                                                                  | 48  |
| TABLE 7-6 - AUTHORIZATION REPLY ATTRIBUTES .....                                                                    | 48  |
| TABLE 7-7 - AUTH REJ ATTRIBUTES .....                                                                               | 49  |
| TABLE 7-8 - KEY REQUEST ATTRIBUTES.....                                                                             | 49  |
| TABLE 7-9 - KEY REPLY ATTRIBUTES.....                                                                               | 49  |
| TABLE 7-10 - KEY REJECT ATTRIBUTES.....                                                                             | 50  |
| TABLE 7-11 - AUTHORIZATION INVALID ATTRIBUTES .....                                                                 | 50  |
| TABLE 7-12 - TEK INVALID ATTRIBUTES .....                                                                           | 50  |
| TABLE 7-13 - AUTHENTICATION INFORMATION ATTRIBUTES.....                                                             | 51  |
| TABLE 7-14 - SA MAP REQUEST ATTRIBUTES .....                                                                        | 51  |
| TABLE 7-15 - SA MAP REPLY ATTRIBUTES .....                                                                          | 52  |
| TABLE 7-16 - SA MAP REJECT ATTRIBUTES .....                                                                         | 52  |
| TABLE 7-17 - BPKM ATTRIBUTE TYPES .....                                                                             | 53  |
| TABLE 7-18 - ATTRIBUTE VALUE DATA TYPES.....                                                                        | 54  |
| TABLE 7-19 - TEK-PARAMETERS SUB-ATTRIBUTES.....                                                                     | 58  |
| TABLE 7-20 - ERROR-CODE ATTRIBUTE CODE VALUES.....                                                                  | 59  |
| TABLE 7-21 - SECURITY-CAPABILITIES SUB-ATTRIBUTES .....                                                             | 61  |
| TABLE 7-22 - DATA ENCRYPTION ALGORITHM IDENTIFIERS.....                                                             | 62  |
| TABLE 7-23 - DATA AUTHENTICATION ALGORITHM IDENTIFIERS.....                                                         | 62  |
| TABLE 7-24 - CRYPTOGRAPHIC-SUITE ATTRIBUTE VALUES .....                                                             | 62  |
| TABLE 7-25 - BPI-VERSION ATTRIBUTE VALUES .....                                                                     | 63  |
| TABLE 7-26 - SA-DESCRIPTOR SUB-ATTRIBUTES .....                                                                     | 63  |
| TABLE 7-27 - SA-TYPE ATTRIBUTE VALUES .....                                                                         | 63  |
| TABLE 7-28 - SA-QUERY SUB-ATTRIBUTES .....                                                                          | 64  |
| TABLE 7-29 - SA-QUERY-TYPE ATTRIBUTE VALUES .....                                                                   | 64  |
| TABLE 13-1 - X.509 CRL FIELDS.....                                                                                  | 96  |
| TABLE A-1 - RECOMMENDED OPERATIONAL RANGES FOR BPI CONFIGURATION PARAMETERS .....                                   | 110 |
| TABLE C-1 - DYNAMIC SAID STATE TRANSITION MATRIX.....                                                               | 122 |
| TABLE I-1 - PRIVATE KEY PARAMETERS .....                                                                            | 133 |
| TABLE III-1 - X.509 BASIC CERTIFICATE FIELDS .....                                                                  | 179 |
| TABLE III-2 - DOCSIS X.509 COMPLIANT CODE VERIFICATION CERTIFICATE.....                                             | 183 |
| TABLE III-3 - DOCSIS PKCS#7 SIGNED DATA .....                                                                       | 187 |

# 1 SCOPE

This Recommendation defines the security requirements for the cable modem in the third generation of high-speed data-over-cable systems (DOCSIS3.0).

For an overview of the third generation cable modem Recommendations see ITU-T Recommendation J.222.1.

# 2 REFERENCES

## 2.1 Normative References

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 were valid. All Recommendations and other references are subject to revision; 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.

- [J.125] ITU-T Rec. J.125 Link privacy for cable modem implementations
- [J.222.2] ITU-T Rec. J. 222.2, Media Access Control and Upper Layer Protocols Interface Specification
- [SCTE OSSI 3.0] Proposed Draft SCTE Standard, DOCSIS Operations Support System Interface Specification version 3.0
- [J.122] ITU-T Rec. J.122 Second-generation transmission systems for interactive cable television services - IP cable modems
- [FIPS-46-3] Federal Information Processing Standards Publication (FIPS PUB) 46-3, Data Encryption Standard, October 1999.
- [FIPS-140-2] Federal Information Processing Standards Publication (FIPS PUB) 140-2, Security Requirements for Cryptographic Modules, June 2001.
- [FIPS-180-2] Federal Information Processing Standards Publication (FIPS PUB) 180-2, Secure Hash Standard, February 2003.
- [FIPS-197] Federal Information Processing Standards Publication (FIPS PUB) 197, Advanced Encryption Standard, November, 2001.
- [ISO8859-1] ISO 8859-1, 1998, "8-bit single-byte coded graphic character sets -- Part 1: Latin alphabet No.1".
- [NIST-800-38A] NIST-800-38A, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Morris Dworkin, 2001 Edition.
- [PKCS#7] IETF RFC2315 PKCS #7: Cryptographic Message Syntax Version 1.
- [PKT-SEC] ITU-T Rec. J.170 IPCablecom security specification
- [RFC 826] IETF RFC 826, D.C. Plummer, Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware, Nov-01-1982.
- [RFC 1350] IETF RFC 1350, K. Sollins, The TFTP Protocol, Revision 2, July 1992.

- [RFC 2616] IETF RFC 2616, R. Fielding, et al., Hypertext Transfer Protocol -- HTTP/1.1, June 1999
- [RFC 2104] IETF RFC 2104, "HMAC: Keyed-Hashing for Message Authentication", H. Krawczyk *et al.*, February, 1997.
- [RFC 3376] IETF RFC 3376 B. Cain, *et al.* Internet Group Management Protocol, Version 3, October 2002.
- [RFC 2347] IETF RFC 2347, G. Malkin, A. Harkin; TFTP Option Extension, May 1998
- [RFC 2348] IETF RFC 2348, G. Malkin, A. Harkin; TFTP Blocksize Option, May 1998
- [RFC 2349] IETF RFC 2349, G. Malkin, A. Harkin; TFTP Timeout Interval and Transfer Size Options, May 1998
- [RFC 2461] IETF RFC 2461, T. Narten, E. Nordmark, W. Simpson, Neighbor Discovery for IP Version 6 (IPv6), December 1998.
- [RFC 2560] IETF RFC 2560, M. Myers *et al.*, "X.509 Internet Public Key Infrastructure Certificate Status Protocol – OCSP", June 1999.
- [RFC 3280] IETF RFC 3280, R. Housley, W. Ford, W. Polk, D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", April 2002.
- [RFC 4131] IETF RFC 4131, S. Green *et al.*, "Management Information Base for Data Over Cable Service Interface Specification (DOCSIS) Cable Modems and Cable Modem Termination Systems for Baseline Privacy Plus", September, 2005.
- [RSA3] IETF RFC2437 PKCS #1: RSA Cryptography Specifications Version 2.0 .
- [X.509] ITU-T Recommendation X.509 (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, August 1997.
- [X.690] ITU-T Recommendation X.690 (2002) | ISO/IEC 8825-1:2002, Information Technology - ASN.1 Encoding Rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)

## 2.2 Informative References

This Recommendation uses the following informative references.

- [DOCSIS CMCI] Data-Over-Cable Service Interface Specifications Cable Modem to Customer Premise Equipment Interface Specification SP-CMCI-I10-050408, April 8, 2005, Cable Television Laboratories, Inc.
- [ISO-3166] ISO, 3166-1, "Codes for the representation of names of countries and their subdivisions -- Part 1: Country codes".
- [MMH] S. Halevi and H. Krawczyk, "MMH: Software Message Authentication in Gbit/sec Rates," *Proceedings of the 4<sup>th</sup> Workshop on Fast Software Encryption, (1997) vol. 1267 Springer-Verlag, pp. 172-189.*
- [RFC 1750] IETF RFC 1750, D. Eastlake, et al., "Randomness Recommendations for Security", December 1994.
- [RFC 2202] IETF RFC 2202, P. Cheng, R. Glenn, "Test cases for HMAC-MD5 and HMAC-SHA-1", September 1997.
- [RFC 3550] IETF RFC 3550, H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson, RTP: A Transport Protocol for Real-Time Applications, July 2003.

- [RSA1] IETF RFC 3447 Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1
- [RSA2] RSA Laboratories, "Some Examples of the PKCS Standards," RSA Data Security, Inc., Bedford, MA, November 1, 1993.
- [SCTE 22-2] ANSI/SCTE 22-2, DOCSIS 1.0 Baseline Privacy Interface.
- [SCTE 52] ANSI/SCTE 52 2003, Data Encryption Standard Cipher Block Chaining Pocket Encryption.
- [SET Book 2] SET, Secure Electronic Transaction Specification Book 2: Programmer's Guide, Version 1.0, May 31, 1997.
- [X.680] ITU-T Recommendation X.680, (July, 2002): Abstract Syntax Notation One (ASN.1): Specification of basic notation.

## 2.3 Reference Acquisition

American National Standards Institute, Inc. 1819 L Street, NW, 6th floor Washington, DC 20036 Phone 202-293-8020; Fax 202-293-9287. <http://www.ansi.org>.

Cable Television Laboratories, Inc., 858 Coal Creek Circle, Louisville, CO 80027; Phone 303-661-9100; Fax 303-661-9199. <http://www.cablemodem.com>.

IETF Secretariat, c/o Corporation for National Research Initiatives, 1895 Preston White Drive, Suite 100, Reston, VA 20191-5434 Phone 703-620-8990; Fax 703-620-9071. <http://www.ietf.org>.

ITU Recommendations: Place des Nations, CH-1211, Geneva 20, Switzerland. Phone +41-22-730-51-11; Fax +41-22-733-7256. <http://www.itu.int>.

Public Key Cryptography Standards: RSA Security Inc. 174 Middlesex Turnpike, Bedford, MA 01730. Phone 781-515-5000; Fax 781-515-5010. <http://www.rsasecurity.com/rsalabs/>.

Federal Information Processing Standards: 100 Bureau Drive, Mail Stop 3200, Gaithersburg, MD 20899-3200. Phone 301-975-4054; Fax 301-926-8091. <http://csrc.nist.gov/publications/fips/>.

## 3 TERMS AND DEFINITIONS

This Recommendation uses the following terms:

|                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>DER Encoded</b>                           | Refers to a value which is encoded using the ASN.1 Distinguished Encoding Rules [X.690].                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Downstream</b>                            | Flow of signals from the cable system control center through the distribution network to the customer. For communication purposes, associated with transmission (down) to the end-user.                                                                                                                                                                                                                                                                                                |
| <b>Dynamically-joined Multicast Sessions</b> | Multicast sessions joined after cable modem registration.                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Key transition period</b>                 | The time period in which an Authentication Key that is near its expiration is replaced by a new Authentication Key through a negotiated update process between the CMTS and the CM.                                                                                                                                                                                                                                                                                                    |
| <b>MAC domain</b>                            | A logical link layer network consisting of a common address scheme (such as IEEE 802.3 Ethernet) in which elements may send and receive OSI layer 2 messages between and among one another. MAC domain boundaries may be established through both physical and logical means; separate channels or subchannels utilizing differing frequency and/or encoding methods, or assigning separate bundles/bridge groups or subinterfaces to common frequency-domain channels or subchannels. |

|                                  |                                                                                         |
|----------------------------------|-----------------------------------------------------------------------------------------|
| <b>Static Multicast Sessions</b> | Multicast sessions joined during cable modem registration.                              |
| <b>Upstream</b>                  | The term used to describe traffic and paths that go from the subscriber to the headend. |

## 4 ABBREVIATIONS, ACRONYMS AND CONVENTIONS

### 4.1 Abbreviations and Acronyms

This Recommendation uses the following abbreviations and acronyms:

|                 |                                                       |
|-----------------|-------------------------------------------------------|
| <b>3DES</b>     | Triple encryption with the Data Encryption Standard   |
| <b>AES</b>      | Advanced Encryption Standard                          |
| <b>AK</b>       | Authorization Key                                     |
| <b>ARP</b>      | Address Resolution Protocol                           |
| <b>ASN.1</b>    | Abstract Syntax Notation 1                            |
| <b>BCP</b>      | Best Current Practice                                 |
| <b>BPI+</b>     | Baseline Privacy Interface Plus                       |
| <b>BPKM</b>     | Baseline Privacy Key Management                       |
| <b>CA</b>       | Certificate Authority                                 |
| <b>CBC</b>      | Cipher Block Chaining                                 |
| <b>CFB</b>      | Cipher Feedback                                       |
| <b>CM</b>       | Cable Modem                                           |
| <b>CMCI</b>     | Cable Modem to Customer Premises Equipment Interface  |
| <b>CMTS</b>     | Cable Modem Termination System                        |
| <b>CMTS-NSI</b> | Cable Modem Termination System Network Side Interface |
| <b>CPE</b>      | Consumer Premises Equipment                           |
| <b>CRC</b>      | Cyclic Redundancy Check                               |
| <b>CRL</b>      | Certificate Revocation List                           |
| <b>CRT</b>      | Chinese Remainder Theorem                             |
| <b>CTR</b>      | Counter: the counter mode of a block cipher           |
| <b>CVC</b>      | Code Verification Certificate                         |
| <b>CVS</b>      | Code Verification Signature                           |
| <b>DA</b>       | Destination Address                                   |
| <b>DER</b>      | Distinguished Encoding Rules                          |
| <b>DES</b>      | Data Encryption Standard                              |
| <b>DHCP</b>     | Dynamic Host Configuration Protocol                   |
| <b>DHCPv6</b>   | Version of DHCP for IPv6                              |
| <b>DOCSIS</b>   | Data-Over-Cable Service Interface Specifications      |
| <b>DoS</b>      | Denial of Service                                     |
| <b>DSID</b>     | Downstream Service Identifier                         |
| <b>EAE</b>      | Early Authentication and Encryption                   |
| <b>ECB</b>      | Electronic Code Book                                  |
| <b>EDE</b>      | Encrypt-Decrypt-Encrypt                               |
| <b>EH</b>       | Extended Header                                       |
| <b>EHDR</b>     | Extended MAC Header                                   |

|                      |                                                                |
|----------------------|----------------------------------------------------------------|
| <b>F<sub>n</sub></b> | The nth Fermat number                                          |
| <b>FC</b>            | Frame Control                                                  |
| <b>FCRC</b>          | Fragment Cyclic Redundancy Check                               |
| <b>FIPS</b>          | Federal Information Processing Standard                        |
| <b>FSM</b>           | Finite State Machine                                           |
| <b>HCS</b>           | Header Check Sequence                                          |
| <b>HFC</b>           | Hybrid Fiber/Coax                                              |
| <b>HMAC</b>          | Keyed-Hash Message Authentication Code                         |
| <b>IEEE</b>          | Institute of Electrical and Electronics Engineers              |
| <b>IGMP</b>          | Internet Group Management Protocol                             |
| <b>IP</b>            | Internet Protocol                                              |
| <b>IPR</b>           | Intellectual Property Rights                                   |
| <b>IPv4</b>          | Version 4 of the Internet Protocol                             |
| <b>IPv6</b>          | Version 6 of the Internet Protocol                             |
| <b>ISO</b>           | International Organization for Standards                       |
| <b>IV</b>            | Initialization Vector                                          |
| <b>KEK</b>           | Key Encryption Key                                             |
| <b>LAN</b>           | Local Area Network                                             |
| <b>LSB</b>           | Least Significant Bit                                          |
| <b>MAC</b>           | Media Access Control                                           |
| <b>MDD</b>           | MAC Domain Descriptor                                          |
| <b>MGF</b>           | Mask Generation Function                                       |
| <b>MIB</b>           | Management Information Base                                    |
| <b>MIC</b>           | Message Integrity Check                                        |
| <b>MLD</b>           | Multicast Listener Discovery                                   |
| <b>MMH</b>           | Multilinear Modular Hash                                       |
| <b>MSB</b>           | Most Significant Bit                                           |
| <b>NMS</b>           | Network Management System                                      |
| <b>OCSF</b>          | Online Certificate Status Protocol                             |
| <b>OID</b>           | Object Identifier                                              |
| <b>OSS</b>           | Operations Support System                                      |
| <b>OUI</b>           | Organizationally Unique Identifier                             |
| <b>PDU</b>           | Protocol Data Unit                                             |
| <b>PHS</b>           | Payload Header Suppression                                     |
| <b>PKI</b>           | Public Key Infrastructure                                      |
| <b>QoS</b>           | Quality of Service                                             |
| <b>RF</b>            | Radio Frequency                                                |
| <b>RFC</b>           | Request For Comments                                           |
| <b>RSA</b>           | Rivest, Shamir, Adleman (a public key cryptographic algorithm) |
| <b>RTP</b>           | Real-time Transport Protocol                                   |
| <b>SA</b>            | Security Association                                           |
| <b>SA</b>            | Source Address                                                 |
| <b>SAID</b>          | Security Association Identifier                                |
| <b>SAV</b>           | Source Address Verification                                    |

|              |                                    |
|--------------|------------------------------------|
| <b>SET</b>   | Secure Electronic Transaction      |
| <b>SHA-1</b> | Secure Hash Algorithm 1            |
| <b>SID</b>   | Service Identifier                 |
| <b>SNMP</b>  | Simple Network Management Protocol |
| <b>SSD</b>   | Secure Software Download           |
| <b>TEK</b>   | Traffic Encryption Key             |
| <b>TFTP</b>  | Trivial File Transfer Protocol     |
| <b>TLV</b>   | Type/Length/Value                  |
| <b>ToD</b>   | Time of Day                        |
| <b>UTC</b>   | Coordinated Universal Time         |
| <b>XOR</b>   | Exclusive Or                       |

## 4.2 Conventions

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

|              |                                                                                                                                                                                                                                                                                   |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| "MUST"       | This word means that the item is an absolute requirement of this Recommendation.                                                                                                                                                                                                  |
| "MUST NOT"   | This phrase means that the item is an absolute prohibition of this Recommendation.                                                                                                                                                                                                |
| "SHOULD"     | This word means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood and the case carefully weighed before choosing a different course.                                                             |
| "SHOULD NOT" | This phrase means that there may exist valid reasons in particular circumstances when the listed behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label. |
| "MAY"        | This word or the adjective "OPTIONAL" means that this item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because it enhances the product, for example; another vendor may omit the same item.                      |

This Recommendation defines many features and parameters, and a valid range for each parameter is usually specified. Equipment (CM and CMTS) requirements are always explicitly stated. Equipment must comply with all mandatory (MUST and MUST NOT) requirements to be considered compliant with this Recommendation. Support of non-mandatory features and parameter values is optional.

In this Recommendation the following convention applies any time a bit field is displayed in a figure. The bit field should be interpreted by reading the figure from left to right, then from top to bottom, with the MSB being the first bit so read and the LSB being the last bit so read.

MIB syntax and XML Schema syntax is represented by this code sample font.

**Notices and/or Warnings are identified by this style font and label.**

## 5 OVERVIEW

The intent of this Recommendation is to describe security services for DOCSIS communications. It has two main goals:

1. To provide cable modem (CM) users with data privacy across the cable network;

2. To prevent unauthorized users from gaining access to the network's RF MAC services.

This Recommendation provides operators with tools to secure the provisioning process of Cable Modems (CM) and protect Cable Modem users by encrypting traffic flows between the CM and the Cable Modem Termination System (CMTS).

The protected RF MAC data communications services fall into three categories:

1. Best-effort high-speed IP data services;
2. Data services with guaranteed QoS;
3. IP multicast group services.

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

The system defined by this Recommendation is used to protect packets on the cable network and is based on DOCSIS Baseline Privacy Plus [J.125], which in turn was based on the original DOCSIS Baseline Privacy scheme [SCTE 22-2].

This Recommendation explicitly assumes the following to be true:

- It is acceptable that DOCSIS 3.0 security features are designed to provide a reasonable level of security for a 10 year time frame;
- The operational life of a CM will not exceed 20 years;
- The interface between the CMTS and provisioning servers is secure;
- CM provisioning servers are trusted;
- At the beginning of the provisioning process, the CM is not trusted. The CM increases its level of trust as it successfully completes different provisioning steps. These steps include device authentication, registration request validation, and service authorization. Once the CM successfully completes the provisioning process with DOCSIS 3.0 security features enabled, it is considered trusted enough to provide data services to subscribers;
- Threat to integrity of encrypted data on the cable network link is low;
- To be backward compatible with existing devices, it is acceptable to continue the support of features that are considered to have low level security characteristics. Operators can enable/disable these features as needed.

## 5.1 New DOCSIS 3.0 Security Features

DOCSIS 3.0 introduces a number of features that build on previous versions of DOCSIS. This Recommendation includes the following new features for security:

- 128 bit AES traffic encryption;
- Early CM authentication and traffic encryption (EAE);
- Enhanced secure provisioning features:
  - Source IP address verification (SAV);
  - TFTP proxy and configuration file learning;
  - MMH algorithm for CMTS MIC.
- Certificate Revocation;
- Support for a mechanism to migrate the CVC certificate chain to a new PKI hierarchy for future use in secure software download.

## 5.2 Technical Overview

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

### 5.2.1 BPI+ Architecture

BPI+ 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;
  3. The rules for applying those algorithms to a DOCSIS MAC frame's packet data.
- A key management protocol (Baseline Privacy Key Management, BPKM) to provide secure distribution of keying data from CMTSs to CMs. Through BPKM, the CM and CMTS synchronize keying data; in addition, the CMTS uses the protocol to implement conditional access to network services.

#### 5.2.1.1 Packet Data Encryption

DOCSIS encryption services are defined as a set of extended services within the DOCSIS MAC sublayer. Packet Header information specific to security is placed in a Baseline Privacy Extended Header element within the MAC Extended Header (see [J.222.2]).

DOCSIS encrypts only the MAC Frame's packet data; the header of the DOCSIS MAC Frame is never encrypted. DOCSIS MAC management messages, except REG-REQ-MP messages, are always unencrypted. REG-REQ-MP messages are encrypted when EAE is enabled. Clause 6 specifies the format of DOCSIS MAC Frames carrying encrypted packet data payloads.

#### 5.2.1.2 Key Management Protocol

CMs use the Baseline Privacy Key Management (BPKM) protocol (see Clause 7) to obtain authorization and traffic encryption keying material from the CMTS, and to support periodic reauthorization and key refresh. The BPKM protocol uses digital certificates, a public-key encryption algorithm, and two-key 3DES to secure key exchanges between the CM and the CMTS.

The BPKM 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 that individual CM clients receive only keying material for which they are authorized. The BPKM protocol is transported over DOCSIS MAC management messages.

DOCSIS uses public-key cryptography to establish a shared secret (an Authorization Key) between the CM and its CMTS. The shared secret is then used to derive secondary keys which are in turn used to secure subsequent BPKM exchanges of traffic encryption keys. This two-tiered mechanism for key distribution permits traffic encryption keys to be updated without incurring the overhead of computationally-intensive public-key operations.

A CMTS authenticates a client CM during the initial authorization exchange, which occurs when Early Authentication and Encryption (EAE) is enabled, or when post registration BPI+ is enabled (see Clause 8). Each CM carries a unique digital certificate issued by the CM's manufacturer. The digital certificate contains the CM's public key, along with the CM MAC address, the identity of the manufacturer, and the CM serial number. When requesting an Authorization Key, a CM presents its digital certificate to a CMTS. The CMTS verifies the digital certificate, then uses the CM's public key to encrypt an Authorization Key, which the CMTS sends to the requesting CM.

#### 5.2.1.3 DOCSIS Security Associations

A DOCSIS 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.

There are three types of DOCSIS Security Associations: Primary, Static, and Dynamic. A Primary Security Association is tied to a single CM, and is established when that CM completes authentication. Static Security

Associations can be shared by multiple CMs and are established, based on a CMTS configuration, when a CM completes authentication. Dynamic Security Associations can be shared by multiple CMs and are normally established dynamically, in response to the request of initiation of specific downstream traffic flows.

A Security Association's shared information comprises the cryptographic suite, traffic encryption keys and CBC initialization vectors, and the lifetime of the keying information. Each Security Association is identified with a 14-bit handle, known as a Security Association Identifier (SAID).

Each CM on which security is enabled, establishes a Primary SA with its CMTS. When the CM encrypts upstream traffic, including the REG-REQ-MP MAC management message, it MUST use the CM's Primary SA. The value of the Primary SAID is established during the initial authorization exchange.

Downstream traffic may be encrypted under any of the three types of SAs. A downstream IP multicast data packet, for example, is typically intended for multiple CMs, and hence, is usually encrypted under a Static or Dynamic SA. Downstream unicast traffic directed at CPE devices behind the CM are typically encrypted under the CM's Primary SA.

A CM MUST support:

- A Primary SA;
- A minimum of 15 SAs each of which can be used as either a Dynamic SA or Static SA.

A CMTS MUST support:

- A Primary SA for every CM;
- At least one Dynamic SA (per CMTS).

A CMTS MAY support Static SAs.

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

An SA's keying material (*e.g.*, 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 before the current keying material expires. The BPKM protocol specifies how CM and CMTS maintain key synchronization.

#### **5.2.1.4 QoS SIDs and DOCSIS SAIDs**

The BPI+ Extended Header Element in downstream DOCSIS MAC frames ([J.222.2]) contains the DOCSIS 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. 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. See Clause 6 for details of the MAC frame format.

Because all upstream traffic is encrypted under the CM's Primary SA, upstream DOCSIS MAC frames do not carry a SAID in their extended headers; instead, the Baseline Privacy EH element may contain a valid QoS SID assigned to the CM (see Clause 6.3 for details).

The Baseline Privacy Extended Header element serves multiple purposes in upstream DOCSIS PDU MAC frames. As an alternative to identifying the particular set of keying material used to encrypt a frame's packet data, it provides a mechanism for issuing piggybacked bandwidth requests (see Clause 6.3.1); it can also carry fragmentation control data (see Clause 6.4). These 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 Primary SAID. The SAID can be deduced by the CMTS from the QoS SID and the logical upstream on which the MAC frame was received.

The SAID associated with a Primary, Static or Dynamic SA can be any 14-bit value. A CMTS MUST NOT assign the same SAID to more than one type of SA within a MAC Domain Downstream Service Group (MD-DS-SG). 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 MD-DS-SG. Likewise, if a CMTS has assigned a SAID to a Static or Dynamic SA, that value cannot be used as the Primary SAID for any modem within that MD-DS-SG. Additionally, a CMTS MUST NOT assign the same SAID to more than one non-Primary (Static or Dynamic) SA within a MD-DS-SG.

## 5.2.2 Secure Provisioning

The processes used to provision a CM are: DHCP, ToD, and TFTP at the IP layer; and registration at the MAC layer. Securing these provisioning processes play a critical role in protecting the CMs and the network from attacks, and in preventing service theft. The CMTS can help secure these processes by assuring that traffic is only forwarded to/from CMs & CPEs, with source IP addresses that have been assigned by the operator. The CMTS can also verify that a CM is registering with the correct service parameters by learning CM provisioning information in DHCP and TFTP messaging flows.

Securing the CM software image download process helps assure that the CM is running the correct/authorized version of code. Authenticating the source and verifying the integrity of downloaded code is vital to the overall operation and security of DOCSIS-based networks. When properly triggered, the CM downloads a software image from a TFTP server and validates the new software image's digital signature before installation.

## 5.3 Operation

### 5.3.1 Cable Modem Initialization

The [J.222.2] Recommendation divides CM 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;
- Establish time of day;
- Transfer operational parameters (download configuration file);
- CMTS Registration.

BPI+ security may be established between the CM and the CMTS following CM ranging (Early Authentication and Encryption (EAE)), or following registration. Ordinarily, BPI+ is established using EAE immediately following ranging, and remains in effect at least until the configuration file has been downloaded. Parameters within the configuration file instruct the CM whether to maintain BPI+ security with the CMTS or to operate in an unsecured mode from that point onward. The CM runs with BPI+ security enabled, unless BPI+ is explicitly disabled in the DOCSIS configuration file.

BPI+ security initialization begins with the CM sending the CMTS an Authentication Information message, containing the CM's Manufacturer CA Certificate, and an Authorization Request message. The Authorization Request contains the following information:

- Data identifying the CM (*e.g.*, MAC address and other information unique to the device);
- The CM's RSA public key;

- A digital certificate to bind the CM's identifying data to the CM's public key<sup>1</sup>;
- A list of the cryptographic suites supported by the CM;
- The Initialization SAID (value 0).

If the CMTS successfully authenticates the requesting CM, it responds with an Authorization Reply, containing the Primary SAID for the CM, and an Authorization Key encrypted by the public key of the CM's certificate. The CM decrypts the encrypted Authorization Key using the private key of its certificate. From the Authorization Key, the CM and the 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 Authorization Reply also contains a list of SA descriptors, which identify the Primary and Static SAs that the requesting CM is authorized to access. Each SA descriptor consists of a collection of SA parameters, including the SA's SAID, type and cryptographic suite. The list contains at least one entry: a descriptor describing the CM's primary SA. Additional entries are optional, and describe any Static SAs that the CM is permitted to access.

After successfully completing authentication and authorization with the CMTS, the CM sends key requests to the CMTS, requesting traffic encryption keys for each of the SA descriptors it received in the Authorization Reply. The CM's traffic key requests are authenticated using a keyed hash (the HMAC algorithm [RFC 2104]); the Message Authentication Key is derived from the Authorization Key, obtained during the authorization exchange. The CMTS responds to each key request with a Key Reply message containing Traffic Encryption Keys (TEKs); TEKs are 3DES encrypted, with a Key Encryption Key (KEK), 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.

BPI+ security Initialization ends when the CM has received the Key Reply messages associated with all the SAIDs identified in the Authorization Reply message, except those with cryptographic suites not supported by the CM.

#### **5.3.1.1 Network Admission Control**

Restricting network access to only authorized devices is an important part of maintaining security. One of the methods used to provide this function is CM authentication using [X.509] certificates. Certificates are issued to trusted vendor companies for installation in their CMs. When EAE or post registration BPI+ is enabled, each CM is authenticated by the CMTS, using these certificates before completing the provisioning process. If the CMTS is not able to validate the CM, it does not allow it to access the network.

Forcing all CMs to successfully complete EAE, or post registration BPI+ before allowing them access to the network, can help prevent hackers from using older CMs to bypass authentication. This capability for EAE BPI+ is defined in this Recommendation (see Clause 8), and for post registration BPI+ is defined in the [J.222.2] Recommendation.

#### **5.3.1.2 EAE and Authentication Reuse**

When EAE is enabled, CM authentication normally occurs following ranging completion, followed by key exchanges and encrypted session establishment (see Clause 8). Because of this, the subsequent provisioning messages (DHCP, ToD, and TFTP) are secured between the CM and CMTS. This allows these provisioning applications to reuse the authentication and encryption functions of the CM for secure communication and avoids having to set up a separate secure session for each application, which would result in longer provisioning times and restrict other security features such as configuration file learning (see Clause 9.4.2.4).

#### **5.3.1.3 Configuration Registration Enforcement**

To help prevent theft-of-service attacks caused by alterations to the configuration file, CMTS TFTP proxy requirements are specified herein. These requirements enable the CMTS to hide the true address of the TFTP server from the CM and other devices on the cable network and for them to learn the contents of the configuration file independently of the configuration information that is sent to it by the CM. When this feature is enabled, the CMTS proxies TFTP messages

<sup>1</sup> This means that the public key appears twice in the message, once as a standalone entity and once as part of the certificate.

between the CM and TFTP server. The CM is provisioned with the CMTS IP address instead of the actual address of the configuration file server. This helps hide the TFTP server address from exposure on the cable network where it might be captured and used for a DoS attack.

The CMTS may also learn the contents of the configuration file as it relays DHCP messages and proxies the information between the configuration file server and the CM. With this information the CMTS can verify that the CM is downloading the correct configuration file and that the registration request contains the correct CM configuration settings.

### 5.3.2 Cable Modem Key Update Mechanism

The Traffic Encryption Keys (TEKs) that the CMTS provides to client CMs have limited lifetimes. The CMTS delivers a key's remaining lifetime, along with the key value, in the Key Reply messages that it sends to its client CMs. The CMTS controls which keys are current by flushing expired keys and generating new keys as required. It is the responsibility of individual CMs to ensure that the keys that they are using match those that the CMTS is using. CMs do this by tracking when a particular SAID's key is scheduled to expire and issuing a new Key Request prior to that time.

In addition, CMs are required to periodically reauthorize with the CMTS (see Clause 7.1.4). As for TEKs, an Authorization Key has a finite lifetime that the CMTS provides to the CM along with the key value. It is the responsibility of each CM to reauthorize and obtain a fresh Authorization Key (and an up-to-date list of SA descriptors) before the CM's current Authorization Key expires. This intermediate period just before the expiration of the Authorization Key is called the key transition period.

### 5.3.3 Cable Modem Secure Software Download

To download a CM software image securely, the CM vendor and/or operator will digitally sign the image using the appropriate code verification certificate (CVC) and place the image on a TFTP server. A CM is enabled to download a software image when it receives a valid CVC in its configuration file. Triggering the download of the software image can be done using parameters in the CM configuration file, or SNMP commands.

After a CM downloads a software image, it validates the image by verifying that the included CVC chains to the DOCSIS Root CA, and by checking the image's digital signature. If this validation is successful, it installs the software image for operation.

## 6 ENCRYPTED DOCSIS MAC FRAME FORMATS

### 6.1 CM Requirements

When operating with BPI+ security enabled, the CM MUST encrypt the Protocol Data Unit (PDU) regions of all of the following types of DOCSIS MAC frames transmitted on to the cable network:

- Variable-length PDU MAC Frames;
- Fragmentation MAC Frames;
- Registration Request (REG-REQ-MP) MAC Management Message Frames.

In each of these cases, a Baseline Privacy Extended Header Element in the DOCSIS MAC Header identifies the Security Association and accompanying keying material that is used to encrypt the PDU. The CM MUST NOT encrypt (see Clause 6.5) MAC Management messages, except REG-REQ-MP messages, unless they are part of a fragment.

### 6.2 CMTS Requirements

When communicating with a CM for which DOCSIS security is enabled, the CMTS MUST encrypt the Protocol Data Unit (PDU) regions of variable-length PDU MAC Frames.

A Baseline Privacy Extended Header Element in the DOCSIS MAC Header identifies the Security Association and accompanying keying material that is used to encrypt the PDU. The CMTS MUST NOT encrypt (see Clause 6.5) MAC Management messages.

### 6.3 Variable-Length PDU MAC Frame Format

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

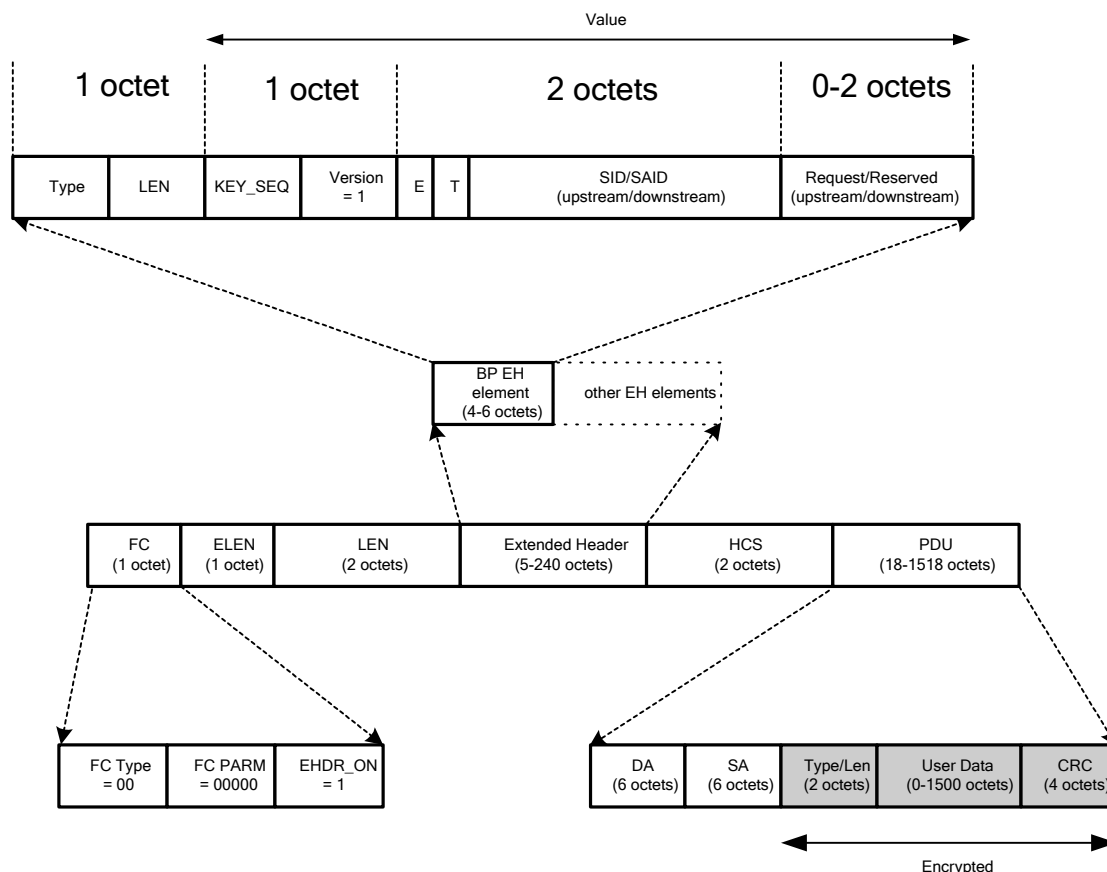


**Figure 6-1 - Format of DOCSIS Variable-length PDU with Privacy EH Element**

{Ed. Note: FC Type needs to be expanded from “00” to “00 or 10”}

The CMTS MUST NOT encrypt the first twelve (12) octets of the PDU, containing the Ethernet/802.3 destination and source addresses (DA/SA). The CM MUST NOT encrypt the first twelve (12) octets of the PDU, containing the Ethernet/802.3 destination and source addresses (DA/SA). The CMTS MUST encrypt the PDU’s Ethernet/802.3 CRC. The CM MUST encrypt the PDU’s Ethernet/802.3 CRC.

The CM MUST include a Baseline Privacy Extended Header in all frames containing encrypted PDUs. The CM MUST make the Baseline Privacy Extended Header element the first Extended Header in an upstream frame. Upstream frames sent by the CM MUST contain the Type value BP\_UP or BP\_UP2 [J.222.2] in the Baseline Privacy EH.

The CMTS MUST include a Baseline Privacy Extended Header in all frames containing encrypted PDUs. The Baseline Privacy Extended Header element MUST be the first Extended Header sent by the CMTS in a downstream frame. Downstream frames sent by the CMTS MUST contain the Type value BP\_DOWN [J.222.2] in the Baseline Privacy EH. The high-order bits of a Baseline Privacy Extended Header Value field contains a key sequence number, KEY\_SEQ. The CMTS manages a key sequence number independently for each SAID and distributes this key sequence number along with the SAID’s keying material to client CMs. For each SAID, the CMTS MUST increment KEY\_SEQ by one each time that it generates new keying material for that SAID. The Baseline Privacy EH element

includes this sequence number, along with the SAID, to identify the keying material that was used to encrypt the frame's PDU.

The four (4) bits following KEY\_SEQ contain a protocol version number. The CMTS MUST set the protocol version number to the value one (1). The CM MUST set the protocol version number to the value one (1).

The next two octets contain two (2) bits of encryption status (ENABLE and TOGGLE) and the fourteen (14)-bit SID/SAID (SID for upstream frames, SAID for downstream frames).

The ENABLE encryption status bit indicates whether encryption is enabled for that PDU. If the PDU is unencrypted, the CMTS MUST set the ENABLE bit to zero (0). If the PDU is unencrypted, the CM MUST set the ENABLE bit to zero (0). If the PDU is encrypted, the CMTS MUST set the ENABLE bit to one (1). If the PDU is encrypted, the CM MUST set the ENABLE bit to one (1).

The CMTS MUST make the TOGGLE bit match the value of the Least Significant Bit (LSB) of KEY\_SEQ. The CM MUST make the TOGGLE bit match the value of the Least Significant Bit (LSB) of KEY\_SEQ.

### 6.3.1 Piggybacked Bandwidth Requests

The DOCSIS MAC protocol [J.222.2] defines a Request EH element that is used to piggyback a bandwidth request on an upstream data transmission. The last octet or last two octets of the upstream Baseline Privacy EH carries an optional piggybacked bandwidth allocation request.

In downstream packets, the last octet is reserved [J.222.2] and the CMTS MUST set its value to zero.

**Table 6–1 - Summary of the contents of Baseline Privacy Extended Headers**

| TYPE                        | LENGTH | VALUE                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| BP_UP<br><br>See [J.222.2]  | 4      | KEY_SEQ (4 bits), Version (4 bits), SID (2 octets), Request [piggyback] (1 octet)<br>[CM → CMTS]<br>KEY_SEQ field (4 bits): Key sequence number<br>Version field (4 bits) is defined as:<br>0x1<br>SID field is defined as:<br>Bit[15]: ENABLE: 1⇒Encryption enabled; 0⇒Encryption Disabled<br>Bit[14]: TOGGLE: 1⇒Odd Key; 0⇒Even Key<br>Bit[13:0]: Service ID.<br>Request field contains the number of mini-slots requested for upstream bandwidth. |
| BP_UP2<br><br>See [J.222.2] | 3      | KEY_SEQ (4 bits), Version (4 bits), SID (2 octets)<br>[CM → CMTS]<br>KEY_SEQ field (4 bits): Key sequence number<br>Version field (4 bits) is defined as:<br>0x1<br>SID field is defined as:<br>Bit[15]: ENABLE: 1⇒Encryption enabled; 0⇒Encryption Disabled<br>Bit[14]: TOGGLE: 1⇒Odd Key; 0⇒Even Key<br>Bit[13:0]: Service ID.                                                                                                                     |

| TYPE                         | LENGTH | VALUE                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| BP_UP2<br><br>See [J.222.2]  | 5      | <p>KEY_SEQ (4 bits), Version (4 bits), SID (2 octets), Request [piggyback] (2 octets)</p> <p>[CM → CMTS]</p> <p>KEY_SEQ field (4 bits): Key sequence number</p> <p>Version field (4 bits) is defined as:</p> <p>0x1</p> <p>SID field is defined as:</p> <p>Bit[15]: ENABLE: 1⇒Encryption enabled; 0⇒Encryption Disabled</p> <p>Bit[14]: TOGGLE: 1⇒Odd Key; 0⇒Even Key</p> <p>Bit[13:0]: Service ID.</p> <p>Request field contains the number of octets requested for upstream bandwidth.</p> |
| BP_DOWN<br><br>See [J.222.2] | 4      | <p>KEY_SEQ (4 bits), Version (4 bits), SID (2 octets), Reserved (1 octet)</p> <p>[CMTS → CM]</p> <p>KEY_SEQ field (4 bits): Key sequence number</p> <p>Version field (4 bits) is defined as:</p> <p>0x1</p> <p>SAID field is defined as:</p> <p>Bit[15]: ENABLE: 1⇒Encryption enabled; 0⇒Encryption Disabled</p> <p>Bit[14]: TOGGLE: 1⇒Odd Key; 0⇒Even Key</p> <p>Bit[13:0]: Security Association ID.</p> <p>Reserved field is set to 0.</p>                                                 |

# 6.4 Fragmentation MAC Frame Format

In order to support fragmentation of upstream DOCSIS MAC frames, the Baseline Privacy EH element may carry both encryption and fragmentation control fields [J.222.2]. When functioning in this role, the upstream Baseline Privacy Extended Header is extended by one octet, the additional octet serving as a fragmentation control field. Figure 6-2 depicts the format of a DOCSIS Fragmentation MAC Frame with an encrypted fragmentation payload.

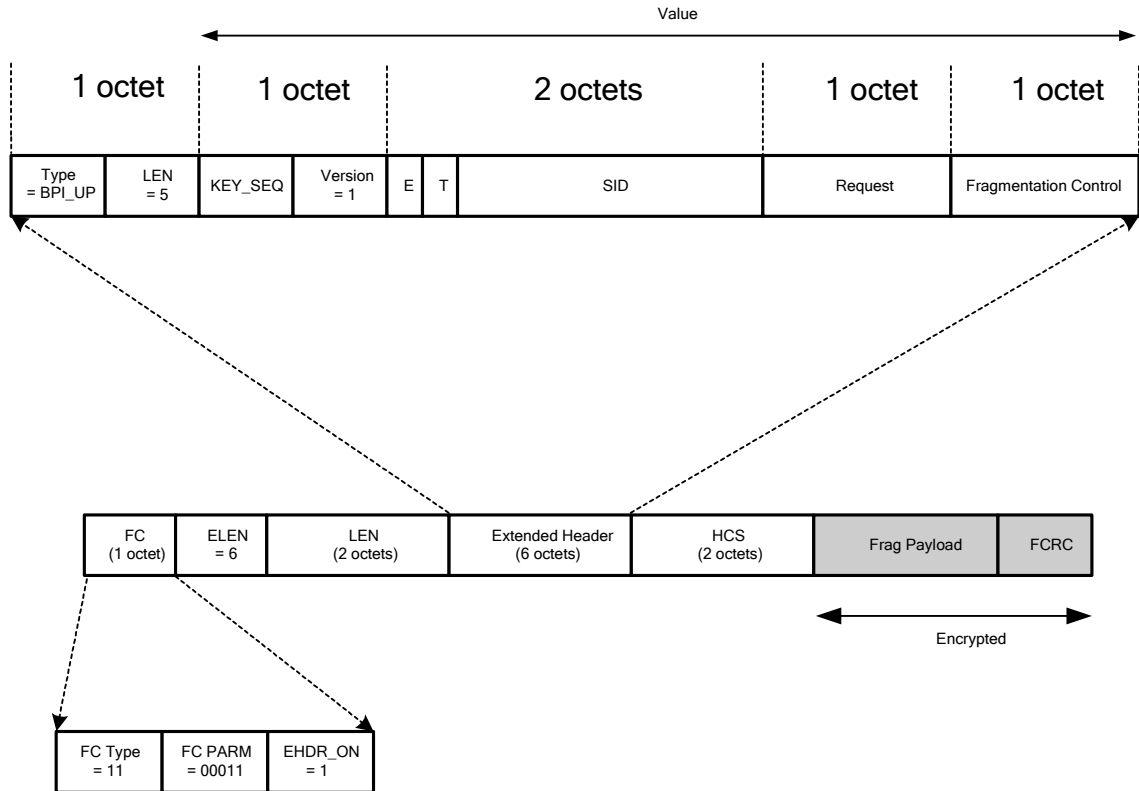


Figure 6-2 - Format of a DOCSIS MAC Fragmentation Frame with an Encrypted Payload

Frames with the fragmentation control (FC) Type, set to 0b11 and FC PARM set to 0b00011, identify a DOCSIS MAC frame as a Fragmentation frame. The Fragmentation MAC header is followed by a Fragment Payload and a Fragment CRC. When encrypting a Fragmentation MAC frame, the CM MUST encrypt the Fragment Payload and the Fragment CRC (FCRC).

The LEN field of the Baseline Privacy EH element in Fragmentation MAC Frames is five (5), rather than four (4), accounting for the additional one (1)-octet fragmentation control field. The definitions and requirements for the KEY\_SEQ field, VERSION field, ENABLE and TOGGLE flags, and SID field are unchanged from those for an upstream PDU MAC Frame.

**Table 6-2 - Summary of the contents of a DOCSIS Fragmentation MAC Frame's Baseline Privacy Extended Header**

| TYPE                       | LEN | VALUE                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------|-----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| BP_UP<br><br>See [J.222.2] | 5   | <p>KEY_SEQ (4 bits), Version (4 bits), SID (2 octets), Request [piggyback] (1 octet), Fragmentation Control (1 octet)</p> <p>[CM → CMTS]</p> <p>KEY_SEQ field (4 bits): Key sequence number</p> <p>Version field (4 bits) is defined as:</p> <p>0x1</p> <p>SID field is defined as:</p> <p>Bit[15]: ENABLE: 1⇒Encryption enabled; 0⇒Encryption Disabled</p> <p>Bit[14]: TOGGLE: 1⇒Odd Key; 0⇒Even Key</p> <p>Bit[13:0]: Service ID.</p> <p>Request field contains the number of mini-slots requested for upstream bandwidth.</p> <p>Fragmentation Control field contains fragmentation-specific control information; see [J.222.2] for details</p> |

The CM determines whether a packet will be fragmented based on its knowledge of the grant size (*i.e.*, the number of mini-slots a CMTS grants to a CM in an Upstream Bandwidth Allocation MAP [J.222.2]). If an encrypted packet is to be fragmented, the CM MUST perform encryption on a fragment-by-fragment basis, not over the PDU as a whole; each fragment will therefore have its own fragmentation header and be encrypted separately.

## 6.5 Registration Request (REG-REQ-MP) MAC Management Messages

When EAE is enabled, the CM MUST encrypt REG-REQ-MP MAC management messages (see Clause 9.5). Figure 6-1 depicts the format of a DOCSIS MAC management message frame with a Privacy Extended Header (EH) Element and encrypted payload.

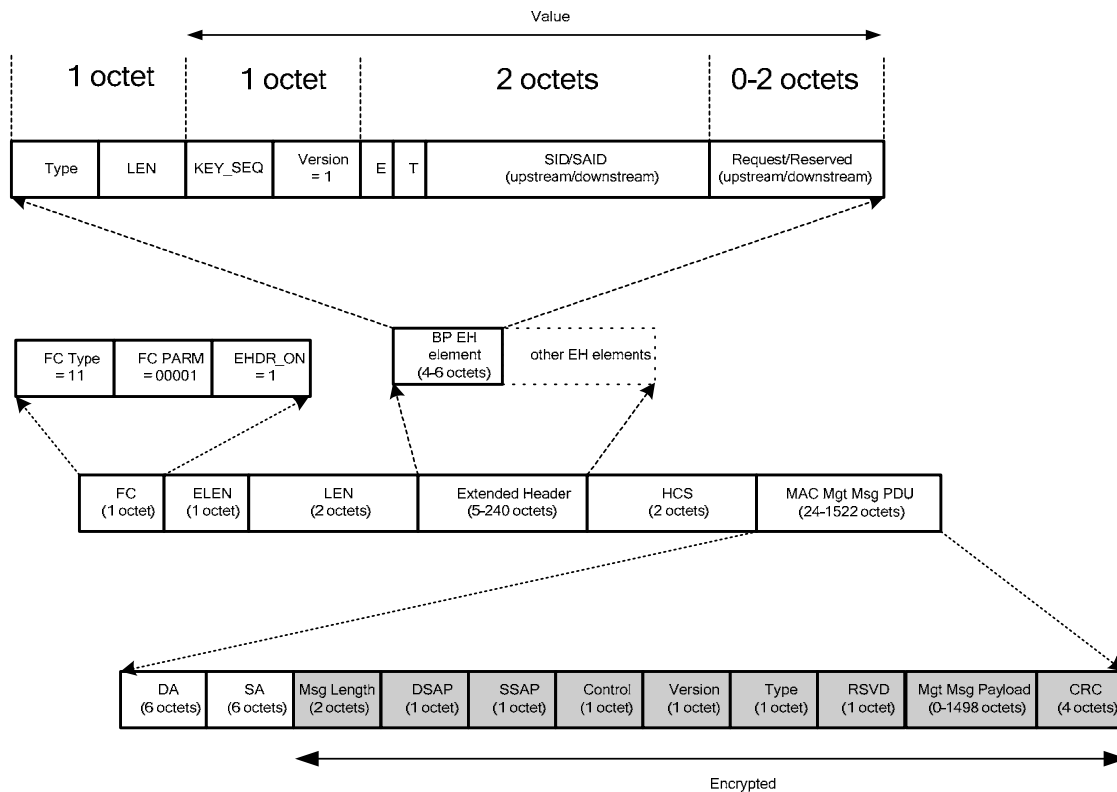


**Figure 6-3 - Format of a DOCSIS MAC Management Message Frame with Encrypted Payload**

The CM MUST encrypt REG-REQ-MP MAC management message frames according to the following rules:

- The first twelve (12) octets of the PDU, containing the Ethernet/802.3 destination and source addresses (DA/SA) MUST not be encrypted;
- The CM MUST encrypt the PDU's Ethernet/802.3 CRC;
- A Baseline Privacy Extended Header MUST be included in the frame;
- The Baseline Privacy Extended Header element MUST be the first Extended Header in the upstream frame;
- The Upstream frames MUST contain the Type value BP\_UP in the Baseline Privacy EH;
- The four (4) bits following KEY\_SEQ contain a protocol version number, which MUST have the value one (1);
- The next two octets contain two (2) bits of encryption status (ENABLE and TOGGLE) and the fourteen (14) bit SID. The ENABLE bit MUST have the value one (1);
- The TOGGLE bit MUST match the value of the Least Significant Bit (LSB) of KEY\_SEQ.

**Table 6-3 - Summary of the contents of DOCSIS MAC Management Message Baseline Privacy Extended Headers**

| TYPE                        | LENGTH | VALUE                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| BP_UP<br><br>See [J.222.2]  | 4      | KEY_SEQ (4 bits), Version (4 bits), SID (2 octets), Request [piggyback] (1 octet)<br>[CM → CMTS]<br>KEY_SEQ field (4 bits): Key sequence number<br>Version field (4 bits) is defined as:<br>0x1<br>SID field is defined as:<br>Bit[15]: ENABLE: 1⇒Encryption enabled; 0⇒Encryption Disabled<br>Bit[14]: TOGGLE: 1⇒Odd Key; 0⇒Even Key<br>Bit[13:0]: Service ID.<br>Request field contains the number of mini-slots requested for upstream bandwidth. |
| BP_UP2<br><br>See [J.222.2] | 3      | KEY_SEQ (4 bits), Version (4 bits), SID (2 octets)<br>[CM → CMTS]<br>KEY_SEQ field (4 bits): Key sequence number<br>Version field (4 bits) is defined as:<br>0x1<br>SID field is defined as:<br>Bit[15]: ENABLE: 1⇒Encryption enabled; 0⇒Encryption Disabled<br>Bit[14]: TOGGLE: 1⇒Odd Key; 0⇒Even Key<br>Bit[13:0]: Service ID.                                                                                                                     |
| BP_UP2<br><br>See [J.222.2] | 5      | KEY_SEQ (4 bits), Version (4 bits), SID (2 octets), Request [piggyback] (2 octets)<br>[CM → CMTS]<br>KEY_SEQ field (4 bits): Key sequence number<br>Version field (4 bits) is defined as:<br>0x1<br>SID field is defined as:<br>Bit[15]: ENABLE: 1⇒Encryption enabled; 0⇒Encryption Disabled<br>Bit[14]: TOGGLE: 1⇒Odd Key; 0⇒Even Key<br>Bit[13:0]: Service ID.<br>Request field contains the number of octets requested for upstream bandwidth.    |

## 6.6 Use of the Baseline Privacy Extended Header in the MAC Header

If encryption is not enabled on a particular downstream traffic flow (*e.g.*, a CM's unicast traffic, or a particular IP multicast group), the CMTS SHOULD NOT place a BP Extended Header element in the frame.

If encryption is not enabled for a CM's unicast traffic, the CM MUST include the Baseline Privacy Extended Header element with the ENABLE bit set to 0 in fragmented upstream frames.

If a CM sends a MAC frame consisting of only a MAC header and, optionally, an EHDR, the CM MUST disable encryption on that frame. If Baseline Privacy EHDR is present on such a frame, the CM MUST set the ENABLE bit to zero (0).

If a CMTS sends a MAC frame consisting of only a MAC header and, optionally, an EHDR, the CMTS MUST disable encryption on that frame. If an Baseline Privacy EHDR is present on such a frame, the CMTS MUST set the ENABLE bit to zero (0).

## 7 BASELINE PRIVACY KEY MANAGEMENT (BPKM) PROTOCOL

### 7.1 State Models

#### 7.1.1 Introduction

The BPKM protocol is controlled by two separate but interdependent state machines: an Authorization state machine and a TEK state machine. This clause describes these two state machines. The state machines are presented here for explanatory purposes only, and are not to be construed as constraining an actual implementation. However, the external behavior of CMTS implementations MUST behave identically to the state machines described in this clause. The external behavior of CM implementations MUST behave identically to the state machines described in this clause.

CM 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 for which the CM is authorized to obtain keying information.

The KEK is a two-key, 3DES encryption key that the CMTS uses to encrypt Traffic Encryption Keys (TEKs) that it sends to the CM. TEKs are used to encrypt and decrypt user data traffic, and REG-REQ-MP MAC management messages. The CM and CMTS use message authentication keys to authenticate, via a keyed message digest, the key requests and responses that they exchange.

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

##### 7.1.1.1 Authorization State Machine Overview

A CM begins the authorization process by sending an Authentication Information message to its CMTS. The Authentication Information message contains the Manufacturer CA or Centralized Mfg CA certificate, issued by the DOCSIS Root CA. The Authentication Information message is usually informative, (*i.e.*, the CMTS may ignore it under some circumstances); however, it does provide a mechanism for a CMTS to learn these CA certificates from its client CMs. See Clause 7.1.4.2.5 for more details.

Immediately after sending the Authentication Information message, the CM sends an Authorization Request message to the CMTS. This is a request for an Authorization Key and for the SAIDs that identify any Static Security Associations in which the CM is authorized to participate. The Authorization Request contains:

- The CM's manufacturer ID and serial number;
- The CM's MAC address;
- The CM's public key;

- A CM Device certificate binding the CM's public key to its other identifying information<sup>2</sup>;
- A description of the cryptographic algorithms supported by the CM. A CM's cryptographic capabilities are 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, supported by the CM;
- The Initialization SAID (see Clause 7.2.1.1). The CM MUST use a value of zero for the Initialization SAID. The CMTS MUST interpret a SAID value of zero as an Initialization SAID.

In response to an Authorization Request message, the CMTS:

- Verifies the CM Device certificate;
- Checks that the CMTS and the CM share at least one cryptographic suite;
- Assigns the CM's Primary SAID.

In addition, the CMTS MUST verify that the MAC-address attribute of the Auth Request, the MAC address in the CM's Device certificate, and the source MAC address of the Auth Request MAC message, all match.

Furthermore, the CMTS SHOULD, by means that are outside the scope of this Recommendation, determine whether the CM is authorized to receive service and, if so, whether it is entitled to access services that are served by any Static SAs.

If these conditions are met, the CMTS MUST:

1. create an Authorization Key for the CM;
2. encrypt the Authorization Key with the CM's public key; and
3. send the encrypted Authorization Key to the CM in an Authorization Reply message.

The Authorization Reply contains:

- An Authorization Key encrypted with the CM's public key;
- A four (4) bit key sequence number;
- A key lifetime;
- The identities (*i.e.*, the SAIDs) and properties of the Primary and zero or more Static Security Associations for which the CM is authorized to obtain keying information.

If the CMTS supports Static SAs, the CMTS MUST include in the Authorization Reply the identities of all Static SAs associated with the CM, in addition to the Primary SA. The CMTS MUST NOT identify any Dynamic SAs (see Clause 7.1.2) in the Authorization Reply. Upon receiving an Authorization Reply, the CM MUST start a separate TEK state machine for each of the SAIDs identified in the Authorization Reply message (see Clause 7.2.1.2). Dynamic SAs are not included in the Authorization Reply and therefore are not shown in Figure 7-1.

<sup>2</sup> This means that the public key appears twice in the message, once as a standalone entity and once as part of the certificate.

### 7.1.1.2 TEK State Machine Overview

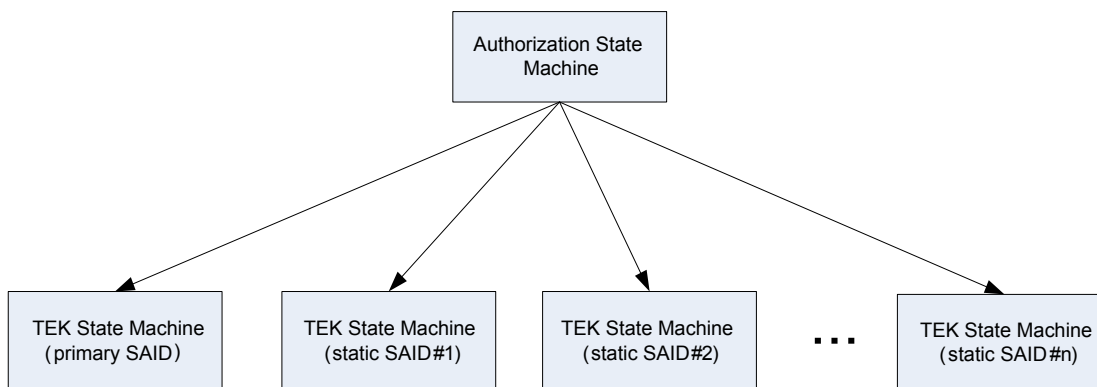


**Figure 7-1 - Relationship Among Authorization and TEK State Machines**

Each TEK state machine is responsible for managing the keying material associated with its respective SAID. TEK state machines send Key Request messages to the CMTS, requesting initial and subsequent keying material for their respective SAIDs. A Key Request contains:

- identifying information unique to the CM, 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 checks the HMAC digest of the Key Request message (see Clause 11 and 12). If the CMTS verifies the HMAC, the CMTS MUST respond with a Key Reply message containing the CMTS's active keying material for the specific SAID. This keying material includes:

- The 3DES-encrypted Traffic Encryption Key (TEK);
- A Cipher Block Chaining (CBC) initialization vector;
- The key sequence number;
- The key's remaining lifetime;
- An HMAC keyed message digest.

The TEK in the Key Reply is 3DES (EDE mode) encrypted, using a two-key, 3DES Key Encryption Key (KEK), derived from the Authorization Key (see Clause 11.2).

At all times, the CMTS maintains two active sets (called “generations”) of keying material for each SAID. A CMTS includes in its Key Replies, both of a SAID's currently-valid generations of keying material.

In addition to the TEK and CBC initialization vector, the Key Reply contains the remaining lifetime of each of the two sets of keying material. The CM uses these remaining lifetimes to estimate when to schedule Key Requests, such that the CM requests and receives new keying material before the CMTS invalidates the keying material currently held by the CM.

The operation of the TEK state machine's Key Request scheduling algorithm, combined with the CMTS's process for updating and using a SAID's keying material, ensures that the CM will be able at all times to exchange encrypted traffic with the CMTS.

Before the current Authorization Key expires, the CM obtains a new Authorization Key, by issuing an Authorization Request to the CMTS. This “reauthorization” is identical to authorization, with the exception that the CM does not send an Authentication Information message. The specification of the authorization state machine defines when Authentication Information messages are sent (see Clause 7.1.4).

To avoid service interruptions during reauthorization, successive generations of the CM’s Authorization Keys have overlapping lifetimes. The CM MUST be able to support at least two simultaneously active Authorization Keys. The CMTS MUST be able to support at least two simultaneously active Authorization Keys for each registered CM. The operation of the Authorization state machine’s Authorization Request scheduling algorithm, combined with the CMTS’s process for updating and using a CM’s Authorization Keys, 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 has a valid Authorization Key; and
- The CMTS continues to provide fresh keying material during TEK re-key cycles.

The parent Authorization state machine stops all its child TEK state machines (see Figure 7-1), when the CM receives 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 authorizations change between successive reauthorizations.

Communication between Authorization and TEK state machines occurs through the passing of events (directly or indirectly) between the two state machines. The Authorization state machine generates events ({Stop}, {Authorized}, {Authorization Pending}, and {Authorization Complete}) that are sent directly to all its child TEK state machines. TEK state machines, however, cannot directly send events to their parent Authorization state machine.

A TEK state machine affects its parent Authorization state machine indirectly through the messaging a CMTS sends in response to a CM’s requests: a CMTS may respond to a TEK machine’s Key Requests with a failure response (*i.e.*, an Authorization Invalid message) that will be handled by the Authorization state machine. In other words, the TEK state machine might transmit a Key Request to the CMTS, which may respond with an Authentication Invalid message. This message is handled not by the TEK state machine responsible for transmitting the Key Request but by its parent Authorization state machine.

### 7.1.2 Encrypted Multicast

The message exchange between the CMTS and the CM for the signaling and initialization of multicast traffic encryption is dependant on the type of multicast session, on the capabilities of the modem and on the multicast forwarding mode selected by the CMTS. The CMTS selects a multicast forwarding mode within the multicast forwarding capabilities reported by the CM.

Multicast sessions can be established dynamically when a Multicast Client sends a join request (IGMP for IPv4 and MLD for IPv6) message. Such multicast sessions are called Dynamically-joined Multicast Sessions. The cable operator can configure the cable modem to join multicast sessions during registration. Such multicast sessions are called Static Multicast Sessions [DOCSIS MULPI].

A CM indicates support for DSID Multicast Forwarding in the Registration Request message with a Multicast DSID Forwarding capability encoding (Annex C.1.3.1.33). A CM that reports in this encoding the value of either 1 (GMAC-Explicit) or 2 (GMAC-Promiscuous) is said to support Multicast DSID forwarding. A CM that omits this encoding or that reports in it a value of 0 (No Support for Multicast DSID Forwarding) is said not to support MDF. The CMTS enables MDF at a CM that supports MDF by setting the MDF capability encoding to the value 1 or 2 in the Registration Response it sends to the modem; such a CM is said to be an MDF enabled CM. The CMTS may disable MDF at a CM that supports MDF by setting the MDF capability encoding to the value 0 in the Registration Response it sends to the modem [DOCSIS MULPI]; such a CM is said to be an MDF disabled CM.

Security Associations are used to support encrypted multicast sessions. SA descriptors containing the SAID, the SA type, and cryptographic suite for encrypted Multicast sessions are included in Auth Reply, REG-RSP(-MP) and DBC-REQ MAC messages and are used by the CM to create or delete the corresponding TEK state machines (see [DOCSIS MULPI]). The CMTS typically communicates in REG-RSP Dynamic SAs associated with static multicast sessions. The CMTS typically communicates in DBC-REQ Dynamic SAs associated with multicast sessions that are explicitly joined

via multicast management protocols such as IGMP/MLD. Note that a REG-RSP may both enable DSID Multicast forwarding and include added Security Associations.

#### **7.1.2.1 Signaling of Dynamic and Static Multicast Session SAs when MDF is Disabled**

If a CM does not support Multicast DSID Forwarding, the CMTS MUST NOT signal Dynamic SAs to the CM in a REG-RSP or DBC-REQ message. For CMs that do not support MDF, the CMTS MUST signal SAs using the DOCSIS 1.1/2.0 Dynamic Security Association mechanism described in Annex C. For backwards compatibility, the CM MUST support Dynamic SA-MAP messaging as described in Annex C.

If the CMTS disables MDF for a CM that supports MDF, the CMTS MUST NOT signal SAs used for encrypted multicast sessions using DBC-REQ or REG-RSP(-MP) to this CM. The CMTS may signal SAs for other purposes to MDF-disabled CMs using DBC-REQ or REG-RSP(-MP). The CM MUST accept SA Descriptor Encodings in REG-RSP (-MP), even if this message disables MDF. If the CMTS disables MDF on a CM that supports MDF, the CMTS MUST signal SAs for encrypting IP multicast traffic to this CM using the DOCSIS 1.1/2.0 Dynamic Security Association mechanism described in Annex C. If the CMTS disables MDF, the CM MUST signal SAs using the DOCSIS 1.1/2.0 Dynamic Security Association mechanism described in Annex C.

A CMTS may communicate static SAs for static multicast session to an MDF-disabled CM in BPI+ Auth Reply messages. The CM accepts static SAs in BPI-Auth Reply messages, even when it operates in MDF disabled mode.

#### **7.1.2.2 Signaling of Dynamic and Static Multicast Session SAs when MDF is Enabled**

When the CMTS enables Multicast DSID Forwarding for a CM in the REG-RSP(-MP) [DOCSIS MULPI], the CM MUST NOT transmit Dynamic SA MAP Requests to the CMTS. The CMTS MUST respond with an SA Map Reject message containing error code 7 if it receives an SA Map Request from an MDF enabled CM.

A CMTS MAY signal in a DBC-REQ the deletion of Dynamic SAs known to the CM. When the MDF enabled CM receives a DBC-REQ that deletes a Dynamic SA, the CM MUST terminate the corresponding TEK state machine prior to sending the DBC-RSP and remove the Dynamic SA's keying material from the CM's key table. This CM MUST discontinue decryption on an SA deleted through a DBC-REQ message. A CM MUST indicate an error response to an attempt to delete an unknown SA.

For encrypting multicast sessions (static or dynamic) forwarded through the MDF-enabled CM, the CMTS MUST use SAs ONLY of type 'Dynamic'. The CMTS MUST NOT signal SAs for multicast sessions in BPI Auth Reply messages to an MDF-enabled CM. The CMTS is allowed to signal SAs in BPI Auth Reply messages for purposes other than multicast encryption to an MDF-enabled CM. The CM accepts static SAs in BPI-Auth Reply messages, even when it operates in MDF enabled mode.

##### **7.1.2.2.1 Requirements Specific to the Signaling of Dynamic SAs for Dynamic Multicast Sessions**

SA descriptors for encrypted multicast sessions joined dynamically are communicated to the MDF enabled CM in a DBC-REQ message. If a dynamic multicast session is encrypted, the CMTS MUST communicate in a DBC-REQ message the session SA Descriptor to an MDF enabled CM. The CMTS MUST set the SA Type in the DBC-REQ message to 'Dynamic' for a dynamic multicast session. A CM for which the CMTS has enabled DSID Multicast Forwarding MUST accept in a DBC-REQ one or more Security Association Encodings that add a new SA of type dynamic.

The CMTS MUST NOT send a Dynamic SA in DBC-REQ messages if BPI+ is disabled for a CM.

When an authorized CM receives a DBC-REQ that contains a Dynamic SA, the CM MUST start a TEK state machine for the Dynamic SA prior to sending a DBC-RSP message. The CMTS MUST NOT send a DBC-REQ with a Dynamic SA to a CM that is not in the "Authorized" State. If an unauthorized CM receives a DBC-REQ message that adds a Dynamic SA, the CM MUST reject the DBC-REQ message. The CMTS is allowed to send a DBC-REQ with an SA that employs a cryptographic suite unsupported by the CM. If an authorized CM receives a DBC-REQ message that adds a Dynamic SA having an unsupported cryptographic suite, the CM MUST reject the DBC-REQ message. If a CM

receives a DBC-REQ message adding a Dynamic SA, in which the TEK state machine for that Dynamic SA is already active, the CM MUST reject the DBC-REQ message.

#### 7.1.2.2.2 Requirements Specific to the Signaling of Dynamic SAs for Static Multicast Sessions

SA descriptors for encrypted multicast sessions joined statically are communicated to the MDF enabled CM in the REG-RSP(-MP) message. If the Static Multicast Session is encrypted, the CMTS MUST communicate in REG-RSP(-MP) the session SA Descriptor to an MDF enabled CM. The CMTS MUST set the SA Type in the REG-RSP(-MP) message to 'Dynamic' for a static multicast session. A CM for which the CMTS has enabled DSID Multicast Forwarding MUST accept in a REG-RSP(-MP) one or more Security Association Encodings that add a new SA of type dynamic.

The CMTS MUST NOT send a Dynamic SA in REG-RSP(-MP) if BPI+ is disabled for a CM.

When an authorized CM receives a REG-RSP(-MP) that adds a Dynamic SA, the CM MUST start a TEK state machine for that Dynamic SA. When an unauthorized CM receives a REG-RSP(-MP) that adds a Dynamic SA, the CM MUST wait until it reaches its Authorized state before starting a TEK state machine for that Dynamic SA. The CMTS is allowed to send a REG-RSP(-MP) with an SA that employs a cryptographic suite unsupported by the CM. If the CM receives a REG-RSP(-MP) message that adds a Dynamic SA having an unsupported cryptographic suite, the CM MUST reject the REG-RSP(-MP) message.

#### 7.1.3 Selecting Cryptographic Suites

As part of their authorization exchange, the CM provides the CMTS with a list of supported cryptographic suites. The CMTS selects from this list a single suite to use with the CM's Primary SA. In the Authorization Reply, the CMTS includes a Primary SA descriptor that identifies the cryptographic suite selected by the CMTS. A CMTS MUST reject the Authorization Request if none of the offered cryptographic suites is permitted by local policy.

The Authorization Reply may contain a list of Static SA descriptors; each Static SA descriptor identifies the cryptographic suite employed by that SA. The selection of a static SA's cryptographic suite is independent of the requesting CM's cryptographic capabilities. A CMTS MAY include in its Authorization Reply Static SA descriptors identifying cryptographic suites unsupported by the CM. The CM MUST NOT start TEK state machines for SAs whose cryptographic suites the CM does not support.

#### 7.1.4 Authorization State Machine

The Authorization Finite State Machine (FSM) contains six states and ten events. The Authorization FSM is presented below as a state flow diagram (Figure 7-2) and as a state transition matrix (Table 7-1).

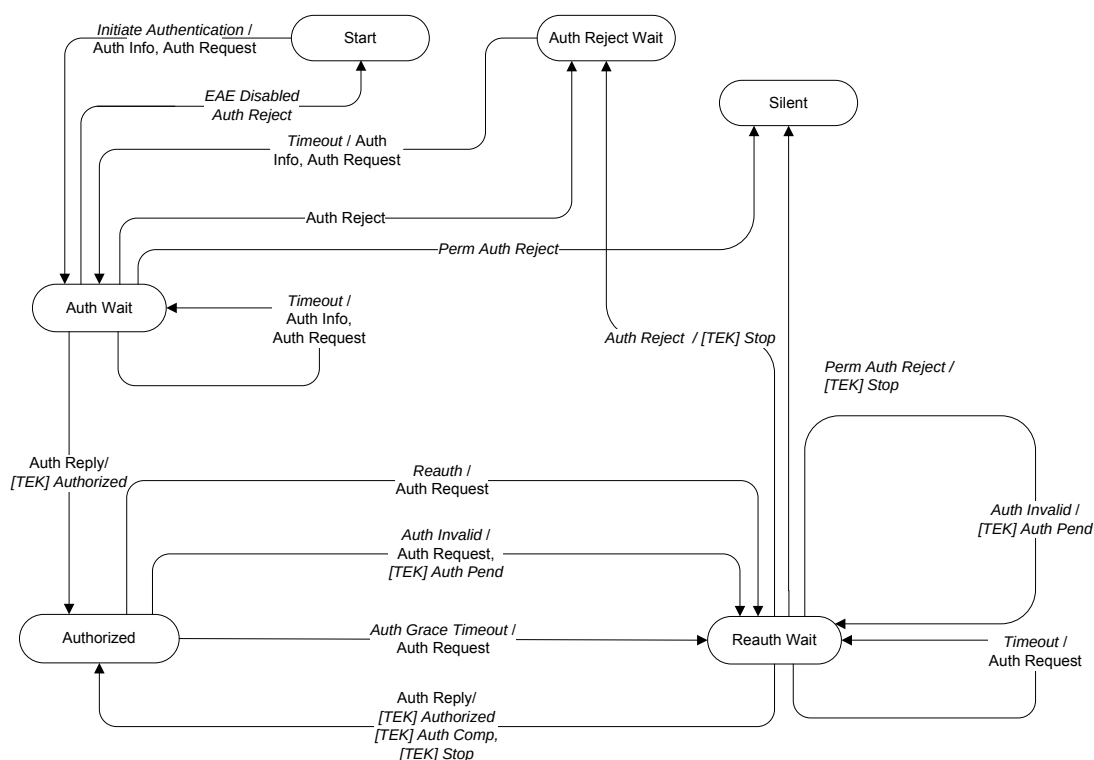


**Figure 7-2 - Authorization State Machine Flow Diagram**

**Table 7-1 - Authorization FSM Transition Matrix**

| State<br>Event or Received<br>Message | [Start]        | [Auth Wait]           | [Authorized]     | [Reauth<br>Wait]      | [Auth<br>Reject<br>Wait] | [Silent] |
|---------------------------------------|----------------|-----------------------|------------------|-----------------------|--------------------------|----------|
| {Initiate Authentication}             | [Auth<br>Wait] |                       |                  |                       |                          |          |
| {Auth Reject}                         |                | [Auth Reject<br>Wait] |                  | [Auth Reject<br>Wait] |                          |          |
| {Perm Auth Reject}                    |                | [Silent]              |                  | [Silent]              |                          |          |
| {EAE Disabled Auth<br>Reject}         |                | [Start]               |                  |                       |                          |          |
| {Auth Reply}                          |                | [Authorized]          |                  | [Authorized]          |                          |          |
| {Timeout}                             |                | [Auth Wait]           |                  | [Reauth<br>Wait]      | [Auth Wait]              |          |
| {Auth Grace Timeout}                  |                |                       | [Reauth<br>Wait] |                       |                          |          |
| {Auth Invalid}                        |                |                       | [Reauth<br>Wait] | [Reauth<br>Wait]      |                          |          |
| {Reauth}                              |                |                       | [Reauth<br>Wait] |                       |                          |          |

The state flow diagram depicts the protocol messages transmitted and internal events generated for each of the machine'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 CM MUST use the text associated with the state transition matrix as the definitive specification of protocol actions associated with each state transition.

The following legend applies to

Figure 7-3:

- States are represented by ovals;
- Events appear in italics;
- Messages appear in normal font;
- State transitions (*i.e.*, the lines between states) are labeled in the manner of “<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 Auth Request message. If there are multiple comma-separated events or messages before the slash “/”, any of them can cause the transition. If there are multiple events or messages listed after the slash, all the identified actions accompany the transition.

The Authorization state transition matrix, presented in Table 7-1, lists the states in the topmost row and the events in the left-most column. Cells within the matrix represent a specific combination of state and event, with the next state (the state to which the machine transitioned) displayed within the cell. For example, one cell represents the receipt of an Authorization Reply message when in the [Auth Wait] state. Within this cell is the name of the next state, [Authorized]. Thus, when a CM’s Authorization state machine is in the [Auth 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 are taken; these are described in Clause 7.1.4.7.

A shaded cell within the state transition matrix (Table 7-1), implies that the specific event should not occur within that state. If the event does occur, the CM MUST NOT transition to another state. For example, if an Authorization Reply message arrives when in the [Authorized] state, that message will not cause any state transition to occur. The CM MAY, in response to such an improper event, log the event’s occurrence, generate an SNMP event, or take some other vendor-defined action.

#### **7.1.4.1 Brief Description of States**

##### **7.1.4.1.1 [Start]**

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

##### **7.1.4.1.2 [Auth Wait]**

The CM has received the {Initiate Authentication} event. In response to receiving the event, the CM has sent both an Authentication Information and an Authorize Request message and is waiting for the reply.

##### **7.1.4.1.3 [Authorized]**

The CM has received an Authorization Reply message that contains a list of valid SAIDs for this CM. The CM has a valid Authorization Key and the list of SAIDs. Transition into this state triggers the creation of one TEK FSM for each of the CM’s privacy-enabled SAIDs.

##### **7.1.4.1.4 [Reauth Wait]**

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

##### **7.1.4.1.5 [Auth Reject Wait]**

The CM received an Authorization Reject message in response to its last Authorization Request. The error code in the Authorization Reject indicated that the error was not permanent or that EAE is not disabled. In response to receiving this reject message, the CM sets a timer and transitioned to the [Auth Reject Wait] state. The CM remains in this state until the timer expires.

#### 7.1.4.1.6 [Silent]

The CM received an Authorization Reject message in response to its last Authorization Request. The Authorization Reject's error code indicated that the error was permanent. This triggers a transition to the [Silent] state.

In the [Silent] state, the CM:

- MUST NOT pass CPE traffic; and
- If the CM has a valid IP address, it MUST respond to SNMP management requests arriving from the cable network.

The CMTS may send unencrypted data traffic to a CM on a SAID for which it has sent an Authorization Reject message, or the CMTS may block such traffic.

#### 7.1.4.2 Brief Description of Messages

The corresponding message formats are specified in Clause 7.2.

##### 7.1.4.2.1 Authorization Request (Auth Request)

Request an Authorization Key and a list of authorized SAIDs. The Authorization Request is sent from the CM to CMTS.

##### 7.1.4.2.2 Authorization Reply (Auth Reply)

Receive an Authorization Key and list containing the primary SAID and static SAIDs. The Authorization Reply is sent from CMTS to CM. The Authorization Key is encrypted with the CM's public key.

##### 7.1.4.2.3 Authorization Reject (Auth Reject)

The attempt to authorize was rejected. The Authorization Reject is sent from the CMTS to CM.

##### 7.1.4.2.4 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 re-authorize with its CMTS.

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

1. There is no valid Authorization Key associated with the CM; or
2. Verification of the Key Request's keyed message digest (in the HMAC-Digest Attribute) failed.

##### 7.1.4.2.5 Authentication Information (Auth Info)

The Authentication Information message contains the Manufacturer CA or Centralized Mfg CA certificate, issued by the DOCSIS Root CA. The Auth Info message is a message sent by the CM to the CMTS. The CMTS MUST first use the out-of-band configuration information to obtain the Manufacturer CA or Centralized Mfg CA certificate (see Clause 13.3.2). If the CMTS does not learn the Manufacturer CA or Centralized Mfg CA certificate from the out-of-band configuration information then the CMTS MUST use the Manufacturer CA or Centralized Mfg CA certificate from the Auth Info message sent by the CM.

### **7.1.4.3 Brief Description of Events**

#### **7.1.4.3.1 Initiate Authentication }**

The CM sends an {Initiate Authentication} event to the Authorization FSM upon completing CMTS registration, or when it completes ranging if EAE is enabled. If the configuration file contains a BPI+ enable setting (see Annex A.1.1) and the CM has not yet enabled BPI+, the {Initiate Authentication} event causes the CM to begin the process of obtaining its Authorization Key and transitions to the [Auth Wait] state.

#### **7.1.4.3.2 {Timeout}**

This event indicates that a retransmission or wait timer timed out. Generally, a request is resent.

#### **7.1.4.3.3 {Auth Grace Timeout}**

This event indicates that the Authorization Grace timer fired. This timer fires a configurable duration (the Authorization Grace Time) before the current authorization expires, signaling the CM to re-authorize before its authorization actually expires. Once the configuration file has been received by the CM, the Authorization Grace Time is obtained from a value in that file; prior to that time, the value of the Authorization Grace Time MUST be the default defined in Annex A.

#### **7.1.4.3.4 {Reauth}**

This event is generated in response to an SNMP SET ([SCTE OSS1 3.0]) that is intended to trigger a reauthorization cycle because the CM's set of authorized static SAIDs may have changed.

#### **7.1.4.3.5 {Auth Invalid}**

This event is generated when there is a failure authenticating a Key Reply, Key Reject or TEK Invalid message, or when the CM receives an Authorization Invalid message. A CMTS responds to a Key Request with an Authorization Invalid message if verification of the request's message authentication code fails. Generation of an {Auth Invalid} event indicates that the CMTS and the CM have lost Authorization Key synchronization.

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

#### **7.1.4.3.6 {Perm Auth Reject}**

This event indicates receipt of an Authorization Reject message containing error code 6. When a CM receives an Authorization Reject containing error code 6, the Authorization State machine moves to the [Silent] state.

#### **7.1.4.3.7 {Auth Reject}**

This event indicates that the CM has received an Authorization Reject in response to an Authorization Request, and that the error code in the Authorization Reject had some value other than 6 or 10. The CM's Authorization state machine will set a wait timer and transition into the [Auth Reject Wait] state. The CM remains in this state until the timer expires, at which time it will re-attempt authorization.

#### **7.1.4.3.8 {EAE Disabled Auth Reject}**

This event indicates that the CM has received an Authorization Reject message containing error code 10 in response to an Authorization Request that was sent to the CMTS as part of EAE. Authorization Reject error code 10 messages are sent to CMs that have been specifically configured in the CMTS to have EAE disabled. When receiving this message the CM's Authorization state machine will transition to the [Start] state.

### **7.1.4.4 Events sent to TEK State Machine**

The following events are sent by the Authorization state machine to a TEK state machine.

#### 7.1.4.4.1 {TEK Stop}

Sent by the Authorization FSM to a TEK FSM that is not in the [Start] state, to terminate the TEK FSM and remove the corresponding SAID's keying material.

#### 7.1.4.4.2 {TEK Authorized}

Sent by the Authorization FSM to a TEK FSM that is in the [Start] state.

#### 7.1.4.4.3 {Auth Pend}

This message is sent by the Authorization FSM to a TEK FSM to place that TEK FSM into a wait state until the Authorization FSM can complete a reauthorization operation.

#### 7.1.4.4.4 {Auth Comp}

Sent by the Authorization FSM to a TEK FSM in the [Op Reauth Wait] or [Rekey Reauth Wait] states, to clear the wait state begun by a {Auth Pend} event.

### 7.1.4.5 Brief Description of Timing Parameters

All configuration parameter values are contained in the configuration file (see Annex A).

#### 7.1.4.5.1 Authorize Wait Timeout (Auth Wait Timeout)

This is the timeout period between sending Authorization Request when in message the [Auth Wait] state.

#### 7.1.4.5.2 Reauthorize Wait Timeout (Reauth Wait Timeout)

This is the timeout period between sending Authorization Request messages when in the [Reauth Wait] state.

#### 7.1.4.5.3 Authorization Grace Time (Auth Grace Timeout)

Amount of time before authorization is scheduled to expire that the CM starts the process of reauthorization.

#### 7.1.4.5.4 Authorize Reject Wait Timeout (Auth Reject Wait Timeout)

Amount of time that a CM's Authorization FSM remains in the [Auth Reject Wait] state before re-attempting authorization.

### 7.1.4.6 Timers

#### 7.1.4.6.1 Authorization Request

Used when awaiting a response to Authorization Requests.

#### 7.1.4.6.2 Authorization Reject

Used after receipt of an Authorization Reject.

#### 7.1.4.6.3 Authorization Grace

Used when determining when to reauthorize.

### 7.1.4.7 Actions

The CM MUST take the following actions in association with state transitions:

[Start] + {Initiate Authentication} → [Auth Wait]:

- send Authentication Information message to CMTS;

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

[Auth Wait] + {Auth Reject} → [Auth Reject Wait]:

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

[Reauth Wait] + {Auth Reject} → [Auth Reject Wait]:

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

[Auth Wait] + {Perm Auth Reject} → [Silent]:

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

[Auth Wait] + {EAE Disabled Auth Reject} → [Start]:

- clear Authorization Request timer.

[Reauth Wait] + {Perm Auth Reject} → [Silent]:

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

[Auth Wait] + {Auth Reply} → [Authorized]:

- clear Authorization Request timer;
- decrypt and record Authorization Key delivered with Authorization Reply;
- start TEK FSMs for all SAIDs listed in Authorization Reply and any pending Dynamic SAIDs received in Registration Response, (provided that 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 fire “Authorization Grace Time” seconds prior to the supplied Authorization Key’s scheduled expiration.

[Reauth Wait] + {Auth Reply} → [Authorized]:

- clear Authorization Request timer;
- decrypt and record Authorization Key delivered with Authorization Reply;
- start TEK FSMs for any newly authorized SAIDs listed in Authorization Reply (provided that the CM supports the cryptographic suite that is associated with the new SAID) and issue TEK FSM {Authorized} events 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 primary or Static SAIDs were not listed in Authorization Reply;
- set the Authorization Grace timer to fire “Authorization Grace Time” seconds prior to the supplied Authorization Key’s scheduled expiration.

[Auth Wait] + {Timeout} → [Auth Wait]:

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

[Reauth Wait] + {Timeout} → [Reauth Wait]:

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

[Auth Reject Wait] + {Timeout} → [Auth Wait]:

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

[Authorized] + {Auth Grace Timeout} → [Reauth Wait]:

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

[Authorized] + {Auth Invalid} → [Reauth Wait]:

- clear Authorization Grace timer;
- send Authorization Request message to CMTS;
- set Authorization Request 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 to which the CMTS responded with an Authorization Invalid message).

[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 to which the CMTS responded with an Authorization Invalid message).

[Authorized] + {Reauth} → [Reauth Wait]:

- Clear Authorization Grace timer;
- Send Authorization Request message to CMTS;
- Set Authorization Request timer to Reauthorize Wait Timeout.

### 7.1.5 TEK State Machine

The TEK state machine contains six states and nine events. The TEK state machine is presented below as both a state flow diagram and a state transition matrix. The CM MUST use the state transition matrix, together with the required actions in Clause 7.1.5.6, as the definitive specification of protocol actions associated with each state transition.

Shaded states in

Figure 7-3 ({Operational}, {Rekey Wait}, and {Rekey Reauthorize Wait}), indicate that the CM holds valid keying material, so encrypted traffic can be passed.

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

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 used. The CM encrypts upstream traffic with the newer of its two TEKs and decrypts downstream traffic with either the older or newer key, depending upon which of the two keys the CMTS used. See Clauses 10.1 and 10.2 for details on CMTS and CM key usage requirements respectively.

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 CM/CMTS clock skew and other system processing and transmission delays, the CM schedules its Key Requests a configurable number of seconds (the TEK Grace Time) before the newer TEK expires.

When it receives a Key Reply, the CM MUST immediately begin to use the TEK Parameters from the TEKs contained in the Key Reply Message.

Figure 7-3 illustrates the CM's scheduling of key refreshes in conjunction with its management of an SA's active TEKs.

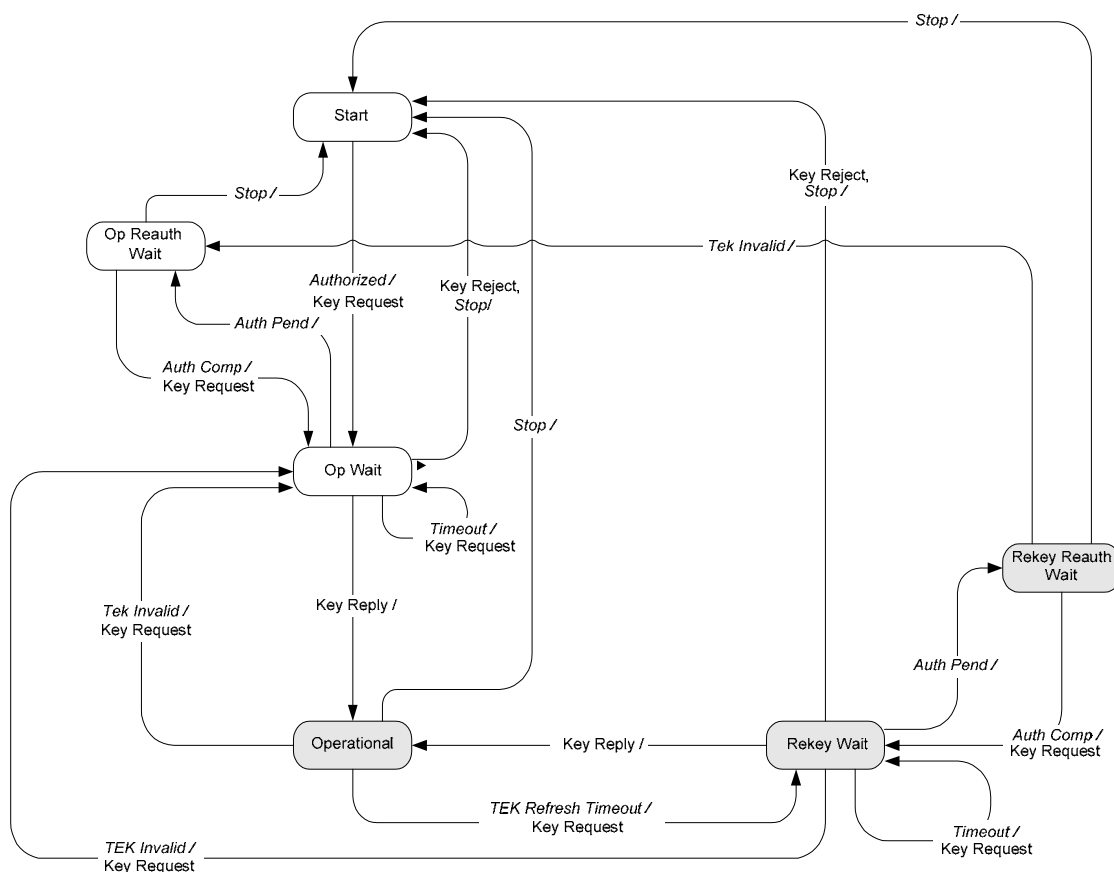


**Figure 7-3 - TEK State Machine Flow Diagram**

**Table 7-2 - TEK FSM State Transition Matrix**

| State<br>Event or<br>Rcyd<br>Message | [Start]   | [Op Wait]           | [Op Reauth<br>Wait] | [Op]            | [Rekey<br>Wait]           | [Rekey<br>Reauth<br>Wait] |
|--------------------------------------|-----------|---------------------|---------------------|-----------------|---------------------------|---------------------------|
| {Stop}                               |           | [Start]             | [Start]             | [Start]         | [Start]                   | [Start]                   |
| {Authorized}                         | [Op Wait] |                     |                     |                 |                           |                           |
| {Auth Pend}                          |           | [Op Reauth<br>Wait] |                     |                 | [Rekey<br>Reauth<br>Wait] |                           |
| {Auth Comp}                          |           |                     | [Op Wait]           |                 |                           | [Rekey<br>Wait]           |
| {TEK<br>Invalid}                     |           |                     |                     | [Op Wait]       | [Op Wait]                 | [Op Reauth<br>Wait]       |
| {Timeout}                            |           | [Op Wait]           |                     |                 | [Rekey<br>Wait]           |                           |
| {TEK<br>Refresh<br>Timeout}          |           |                     |                     | [Rekey<br>Wait] |                           |                           |
| {Key Reply}                          |           | [Op]                |                     |                 | [Op]                      |                           |
| {Key Reject}                         |           | [Start]             |                     |                 | [Start]                   |                           |

### **7.1.5.1 Brief Description of States**

#### **7.1.5.1.1 [Start]**

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

#### **7.1.5.1.2 [Op Wait]**

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

#### **7.1.5.1.3 [Op Reauth Wait]**

The Authorization state machine is in a reauthorization cycle and the CM does not have valid keying material for this SAID.

#### **7.1.5.1.4 [Op]**

The CM has valid keying material for the associated SAID.

#### **7.1.5.1.5 [Rekey Wait]**

The TEK Refresh Timer has expired and the CM has requested a key update for this SAID to replace the older of the two TEKs.

#### **7.1.5.1.6 [Rekey Reauth Wait]**

The CM has valid traffic keying material for this SAID; has an outstanding request for the latest keying material; and the Authorization state machine has initiated a reauthorization cycle.

### **7.1.5.2 Brief Description of Messages**

The message formats are defined in detail in Clause 7.2. All messages contain a keyed message digest for which the key is derived from the Authorization Key (see Clause 11.4).

#### **7.1.5.2.1 Key Request**

Request a TEK for this SAID. The Key Request is sent by the CM to the CMTS.

#### **7.1.5.2.2 Key Reply**

Response from the CMTS carrying the two active sets of traffic keying material for this SAID. It includes the SAID's TEKs, 3DES encrypted with a Key Encryption Key (KEK) derived from the Authorization Key (see Clause 11.4).

#### **7.1.5.2.3 Key Reject**

If the SAID in a Key Request message is invalid, the CMTS MUST respond with a Key Reject message.

#### **7.1.5.2.4 TEK Invalid**

If the TEK used to encrypt an upstream PDU is invalid, the CMTS MUST respond with a TEK Invalid message.

### **7.1.5.3 Brief Description of Events**

#### **7.1.5.3.1 {Stop}**

This event is sent by the Authorization FSM to a TEK FSM not in the [Start] state, to terminate the TEK FSM and remove the corresponding SAID's keying material. See Clause 7.1.4.4.1.

#### 7.1.5.3.2 {Authorized}

This event is sent by the Authorization FSM to a TEK FSM in the [Start] state, to notify the TEK FSM of successful authorization. See Clause 7.1.4.4.2.

#### 7.1.5.3.3 {Auth Pend}

This event is sent by the Authorization FSM to a TEK FSM in order to place the TEK FSM in a wait state while the Authorization FSM completes reauthorization. See Clause 7.1.4.4.3.

#### 7.1.5.3.4 {Auth Comp}

This event is sent by the Authorization FSM to a TEK FSM in the [Op Reauth Wait] or [Rekey Reauth Wait] states, to clear the wait state begun by a prior {Auth Pend} event. See Clause 7.1.4.4.4.

#### 7.1.5.3.5 {TEK Invalid}

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

A CM triggers a {TEK Invalid} event when it recognizes 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 the CM a TEK Invalid message, triggering a {TEK Invalid} event, if the CMTS recognizes a loss of TEK key synchronization between itself and the CM.

#### 7.1.5.3.6 {Timeout}

This specifies the period of the Retry Timer timeout. Generally, the original request is retransmitted.

#### 7.1.5.3.7 {TEK Refresh Timeout}

This is the period defined for the TEK Refresh Timer. This event instructs the TEK state machine to issue a new Key Request in order to refresh its keying material. The refresh timer can be configured for a specific length of time (the TEK Grace Time) before the expiration of the newer TEK currently held by the CM elapses.

### 7.1.5.4 Brief Description of Timing Parameters

All configuration parameter values are contained in the configuration file (see Annex A).

#### 7.1.5.4.1 Operational Wait Timeout

This value specifies the time period between consecutive Key Request messages whenever the state machine is in the [Op Wait] state.

#### 7.1.5.4.2 Rekey Wait Timeout

The timeout period between the sending of Key Request messages when in the [Rekey Wait] state.

#### 7.1.5.4.3 TEK Grace Time

The time interval, in seconds, prior to the expiration of a TEK at which the CM starts re-keying for a new TEK.

### 7.1.5.5 Timers

#### 7.1.5.5.1 Key Request Retry

Used when the response to a Key Request was not received by the CM.

#### 7.1.5.5.2 TEK Refresh

Used when to initiate a request for keys.

#### 7.1.5.6 Actions

The CM MUST take the following actions in association with state transitions:

[Op Wait] + {Stop} → [Start]:

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

[Op Reauth Wait] + {Stop} → [Start]:

- terminate TEK FSM.

[Op] + {Stop} → [Start]:

- clear TEK Refresh timer;
- terminate TEK FSM;
- remove SAID keying material.

[Rekey Wait] + {Stop} → [Start]:

- clear Key Request Retry timer;
- terminate TEK FSM;
- remove SAID keying material.

[Rekey Reauth Wait] + {Stop} → [Start]:

- terminate TEK FSM;
- remove SAID keying material.

[Start] + {Authorized} → [Op Wait]:

- send Key Request Message to CMTS;
- set Key Request Retry timer to the value of Operational Wait Timeout.

[Op Wait] + {Auth Pend} → [Op Reauth Wait]:

- clear Key Request Retry timer.

[Rekey Wait] + {Auth Pend} → [Rekey Reauth Wait]:

- clear Key Request Retry timer.

[Op Reauth Wait] + {Auth Comp} → [Op Wait]:

- send Key Request message to CMTS;
- set Key Request Retry timer to Operational Wait Timeout.

[Rekey Reauth Wait] + {Auth Comp} → [Rekey Wait]:

- send Key Request message to CMTS;
- set Key Request Retry timer to Rekey Wait Timeout.

[Op] + {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.

[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.

[Rekey Reauth Wait] + {TEK Invalid} → [Op Reauth Wait]:

- remove SAID keying material.

[Op Wait] + {Timeout} → [Op Wait]:

- send Key Request message to CMTS;
- set Key Request Retry timer to Operational Wait Timeout.

[Rekey Wait] + {Timeout} → [Rekey Wait]:

- send Key Request message to CMTS;
- set Key Request Retry timer to Rekey Wait Timeout.

[Op] + {TEK Refresh Timeout} → [Rekey Wait]:

- send Key Request message to CMTS;
- set Key Request Retry timer to Rekey Wait Timeout.

[Op Wait] + {Key Reply} → [Op] (Key Reply passed message authentication):

- clear Key Request Retry timer;
- process contents of Key Reply message and incorporate new keying material;
- set the TEK Refresh timer to fire “TEK Grace Time” seconds prior to the key’s scheduled expiration.

[Rekey Wait] + {Key Reply} → [Op] (Key RejectReply passed message authentication):

- clear Key Request Retry timer;
- process contents of Key Reply message and incorporate new keying material;
- set the TEK Refresh timer to fire “TEK Grace Time” seconds prior to the key’s scheduled expiration.

[Op Wait] + {Key Reject} → [Start] (Key RejectReply passed message authentication):

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

[Rekey Wait] + {Key Reject} → [Start]:

- clear Key Request Retry timer;
- terminate TEK FSM;
- remove SAID keying material.

## 7.2 Key Management Message Formats

Baseline Privacy Key Management employs two MAC message types: BPKM-REQ and BPKM-RSP. The CMTS MUST support the BPKM formats as defined in this clause. The CM MUST support the BPKM formats as defined in this clause. [J.222.2] defines the specific type values assigned to these messages (see also Table 7-3).

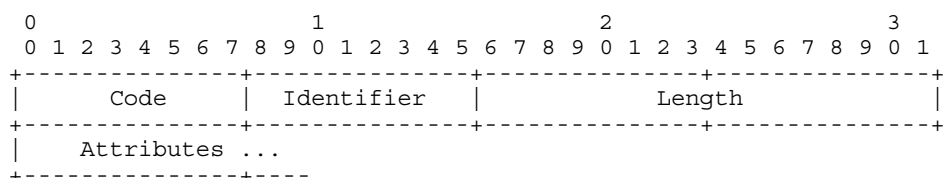
**Table 7-3 - Baseline Privacy Key Management MAC Messages**

| Type Value    | Message Name | Message Description                         |
|---------------|--------------|---------------------------------------------|
| See [J.222.2] | BPKM-REQ     | Privacy Key Management Request [CM → CMTS]  |
| See [J.222.2] | BPKM-RSP     | Privacy Key Management Response [CMTS → CM] |

### 7.2.1 Packet Formats

One BPKM message is encapsulated in the Management Message Payload field of a single MAC management message.

A summary of the BPKM message format follows. The CMTS MUST transmit fields and their respective contents from left to right. The CM MUST transmit fields and their respective contents from left to right.



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     | Auth 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 this field to match a CMTS's responses to the CM's requests.

The CM MUST change the value of 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 CM MUST keep the Identifier field unchanged from the value in the message being retransmitted.

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

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

On receipt of a BPKM response message, the CM MUST associate 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, using the