

Superseded

Data-Over-Cable Service Interface Specifications

Operations Support System Interface Specification Baseline Privacy Interface MIB

SP-OSSI-BPI-I01-980331

**INTERIM
SPECIFICATION**

Notice

This document is a cooperative effort undertaken at the direction of Cable Television Laboratories, Inc. for the benefit of MCNS Holdings, L.P. and the cable industry in general. Neither CableLabs, MCNS Holdings, L.P., nor any other participating entity including Media One (Continental CableVision) and Rogers Cablesystems Limited (collectively, the "Other Participants") is responsible for any liability of any nature whatsoever resulting from or arising out of use or reliance upon this test suite by any party. This document is furnished on an "AS IS" basis and neither CableLabs, MCNS Holdings, L.P., nor the Other Participants provide any representation or warranty, expressed or implied, regarding its accuracy, completeness, or fitness for a particular purpose. Distribution of this document is restricted pursuant to the terms of separate access agreements negotiated with each of the parties to whom this document has been furnished.

© Copyright 1997 and 1998 MCNS Holdings, L.P.

All rights reserved.

Document Status Sheet

Document Control Number: SP-OSSI-BPI-I01-980331

Reference: Operations Support System Interface Specification
Baseline Privacy Interface MIB

Revision History: I01 3/31/98: Released for publication

Date: March 31, 1998

Editor: Richard Woundy, American Internet

Status Code:	Work in process	Draft	Interim	Released
Distribution Restrictions:	CableLab only	CableLabs/MCNS	MCNS/Vendor	Public

Key to Document Status Codes

Work in Process	An incomplete document, designed to guide discussion and generate feedback, that may include several alternative requirements for consideration.
Draft	A document in specification format considered largely complete, but lacking review by MCNS and vendors. Drafts are susceptible to substantial change during the review process.
Interim	A document which has undergone rigorous MCNS and vendor review, suitable for use by vendors to design in conformance with, and suitable for field testing.
Released	A stable document, reviewed, tested and validated, suitable to enable cross-vendor interoperability.

Table of Contents

1	SCOPE	1
1.1	REQUIREMENTS	1
2	BASELINE PRIVACY INTERFACE MANAGEMENT REQUIREMENTS	3
3	MANAGEMENT INFORMATION BASE (MIB)	5
3.1	MIB ORGANIZATION	5
3.2	STRUCTURE OF THE BASELINE PRIVACY INTERFACE MIB	5
	APPENDIX A CONCISE MIB DEFINITION	7
	A.1 – DEFINITION OF MANAGED OBJECTS FOR DATA-OVER-CABLE BASELINE PRIVACY INTERFACES	7
	APPENDIX B REFERENCES	29
	APPENDIX C GLOSSARY	31

This page intentionally left blank.

1 Scope

This document (SP-OSSI-BPI) defines the baseline privacy interface management information base (MIB) for high-speed data-over-cable systems developed by the Data Over Cable Services working group. The MIB is defined as a Simple Network Management Protocol (SNMP) MIB.

This specification is intended to provide a uniform and consistent means for the data over cable systems to address the operational requirements in a uniform and consistent manner.

1.1 Requirements

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

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

This page intentionally left blank.

2 Baseline Privacy Interface Management Requirements

The data-over-cable-system baseline privacy interface specification is documented in [MCNS1], and is an extension to the radio frequency interface specification documented in [MCNS2] and the telephony return interface specification documented in [MCNS4]. In addition to the explicit requirements in this specification, the CM and CMTS enabled for baseline privacy MUST support all applicable MCNS and IETF requirements and MIB objects. These requirements and MIB objects are documented in the MCNS OSSI Specification [MCNS3], the MCNS Telephony Return OSSI Specification [MCNS5], the IETF RF MIB [IPCDN1], and the IETF Cable Device MIB [IPCDN2].

The explicit management requirements of the baseline privacy interface, which motivate the development of the MIB in this document, are detailed below:

- The baseline privacy management interface needs to support dynamic modifications of membership lists for multicast groups. The CMTS MUST support configuring and viewing all multicast group memberships within the MAC domains of the CMTS. The CM and CMTS MUST support viewing relevant RSA public keys, for future subscriber authentication applications.
- The management interface needs to support operator configuration of Finite State Machine (FSM) parameters, for performance tuning and security incident handling. The CMTS MUST support configuring and viewing all FSM parameters, including baseline privacy status (enabled or disabled), key lifetimes, key grace times, and state timeout values. The CM MUST support viewing these parameters where possible.
- The management interface needs to support operator analysis and override of FSM behavior, for fault management, subscriber service de-provisioning, and security incident handling. The CM MUST support viewing the current FSM states. The CM and CMTS MUST support viewing message error codes and message error strings, and counters for invalid KEK and TEK events, for key expirations and renewals, and for duplicate messages. The CM and CMTS MUST support viewing current authorization key sequence numbers and key expiration times.

This page intentionally left blank.

3 Management Information Base (MIB)

This section defines the minimum set of managed objects required to support a data-over-cable baseline privacy interface. Vendors may augment this MIB with objects from other standard or vendor-specific MIBs where appropriate.

3.1 MIB Organization

The MIB includes a set of objects needed to configure, operate, and monitor the baseline privacy interface. The structure of the MIB is outlined in Section 3.2, and is formally defined in Appendix A.

3.2 Structure of the Baseline Privacy Interface MIB

```

docsBpiMIBObjects
  docsBpiCmObjects
    docsBpiCmBaseTable
      docsBpiCmPrivacyEnable
      docsBpiCmPublicKey
      docsBpiCmAuthState
      docsBpiCmAuthKeySequenceNumber
      docsBpiCmAuthExpires
      docsBpiCmAuthReset
      docsBpiCmAuthGraceTime
      docsBpiCmTEKGraceTime
      docsBpiCmAuthWaitTimeout
      docsBpiCmReauthWaitTimeout
      docsBpiCmOpWaitTimeout
      docsBpiCmRekeyWaitTimeout
      docsBpiCmAuthRejectWaitTimeout
      docsBpiCmAuthRequests
      docsBpiCmAuthReplies
      docsBpiCmAuthRejects
      docsBpiCmAuthInvalids
      docsBpiCmAuthRejectErrorCode
      docsBpiCmAuthRejectErrorString
      docsBpiCmAuthInvalidErrorCode
      docsBpiCmAuthInvalidErrorString
    docsBpiCmTEKTable
      docsBpiCmTEKPrivacyEnable
      docsBpiCmTEKState
      docsBpiCmTEKExpiresOld
      docsBpiCmTEKExpiresNew
      docsBpiCmTEKKeyRequests
      docsBpiCmTEKKeyReplies
      docsBpiCmTEKKeyRejects
      docsBpiCmTEKInvalids
      docsBpiCmTEKAuthPends
      docsBpiCmTEKKeyRejectErrorCode
      docsBpiCmTEKKeyRejectErrorString
      docsBpiCmTEKInvalidErrorCode
      docsBpiCmTEKInvalidErrorString

  docsBpiCmtsObjects
    docsBpiCmtsBaseTable
      docsBpiCmtsDefaultAuthLifetime

```

- docsBpiCmtsDefaultTEKLifetime
- docsBpiCmtsDefaultAuthGraceTime
- docsBpiCmtsDefaultTEKGraceTime
- docsBpiCmtsAuthRequests
- docsBpiCmtsAuthReplies
- docsBpiCmtsAuthRejects
- docsBpiCmtsAuthInvalids
- docsBpiCmtsAuthTable
 - docsBpiCmtsAuthCmMacAddress
 - docsBpiCmtsAuthCmPublicKey
 - docsBpiCmtsAuthCmKeySequenceNumber
 - docsBpiCmtsAuthCmExpires
 - docsBpiCmtsAuthCmLifetime
 - docsBpiCmtsAuthCmGraceTime
 - docsBpiCmtsAuthCmReset
 - docsBpiCmtsAuthCmRequests
 - docsBpiCmtsAuthCmReplies
 - docsBpiCmtsAuthCmRejects
 - docsBpiCmtsAuthCmInvalids
 - docsBpiCmtsAuthRejectErrorCode
 - docsBpiCmtsAuthRejectErrorString
 - docsBpiCmtsAuthInvalidErrorCode
 - docsBpiCmtsAuthInvalidErrorString
- docsBpiCmtsTEKTable
 - docsBpiCmtsTEKLifetime
 - docsBpiCmtsTEKGraceTime
 - docsBpiCmtsTEKExpiresOld
 - docsBpiCmtsTEKExpiresNew
 - docsBpiCmtsTEKReset
 - docsBpiCmtsKeyRequests
 - docsBpiCmtsKeyReplies
 - docsBpiCmtsKeyRejects
 - docsBpiCmtsTEKInvalids
 - docsBpiCmtsKeyRejectErrorCode
 - docsBpiCmtsKeyRejectErrorString
 - docsBpiCmtsTEKInvalidErrorCode
 - docsBpiCmtsTEKInvalidErrorString
- docsBpiMulticastControl
 - docsBpiIpMulticastMapTable
 - docsBpiIpMulticastAddress
 - docsBpiIpMulticastPrefixLength
 - docsBpiIpMulticastServiceId
 - docsBpiIpMulticastMapControl
 - docsBpiMulticastAuthTable
 - docsBpiMulticastCmMacAddress
 - docsBpiMulticastServiceId
 - docsBpiMulticastAuthControl

Appendix A Concise MIB Definition

This appendix contains formal definitions of the Data over Cable Baseline Privacy Interface MIB. It is presented in the SNMP Version 2 Concise MIB Definition format.

A.1 – Definition of Managed Objects for Data-over-Cable Baseline Privacy Interfaces

The following groups and sub-groups are provided for management of the Data-over-Cable Baseline Privacy interfaces:

docsBpiCmObjects – DOCS Baseline Privacy Objects for CMs

docsBpiCmBaseTable – DOCS Baseline Privacy CM Base and Authorization Table

docsBpiCmTEKTable – DOCS Baseline Privacy CM Traffic Encryption Key Table

docsBpiCmtsObjects – DOCS Baseline Privacy Objects for CMTSs

docsBpiCmtsBaseTable – DOCS Baseline Privacy CMTS Base Table

docsBpiCmtsAuthTable – DOCS Baseline Privacy CMTS Authorization Table

docsBpiCmtsTEKTable – DOCS Baseline Privacy CMTS Traffic Encryption Key Table

docsBpiMulticastControl – DOCS Baseline Privacy CMTS Multicast Control Group

DOCS-BPI-MIB DEFINITIONS ::= BEGIN

IMPORTS

MODULE-IDENTITY, OBJECT-TYPE,
Integer32, Counter32, IpAddress

FROM SNMPv2-SMI

TEXTUAL-CONVENTION, DisplayString, MacAddress, RowStatus, TruthValue
FROM SNMPv2-TC

OBJECT-GROUP, MODULE-COMPLIANCE
FROM SNMPv2-CONF

ifIndex

FROM RFC1213-MIB

docsIfMib, docsIfCmServiceId, docsIfCmtsServiceId
FROM DOCS-IF-MIB

;

docsBpiMIB MODULE-IDENTITY

LAST-UPDATED "9801311130Z"

ORGANIZATION "MCNS Holdings, L.P."

CONTACT-INFO "Rich Woundy

Postal: American Internet

4 Preston Court

Bedford, MA 01730

Tel: +1 781 276 4509

Fax: +1 781 275 4930

E-mail: rwoundy@american.com"

DESCRIPTION

“This is the MIB Module for the MCNS Baseline Privacy Interface (BPI) at cable modems (CMs) and cable modem termination systems (CMTSs).”

::= { docsIfMib 5 }

docsBpiMIBObjects OBJECT IDENTIFIER ::= { docsBpiMIB 1 }

-- Cable Modem Group

docsBpiCmObjects OBJECT IDENTIFIER ::= { docsBpiMIBObjects 1 }

--

-- The BPI base and authorization table for CMs, indexed by ifIndex

--

docsBpiCmBaseTable OBJECT-TYPE
 SYNTAX SEQUENCE OF DocsBpiCmBaseEntry
 MAX-ACCESS not-accessible
 STATUS current

DESCRIPTION

“Describes the basic and authorization-related Baseline Privacy attributes of each CM MAC interface.”

::= { docsBpiCmObjects 1 }

docsBpiCmBaseEntry OBJECT-TYPE
 SYNTAX DocsBpiCmBaseEntry
 MAX-ACCESS not-accessible
 STATUS current

DESCRIPTION

“An entry containing objects describing attributes of one CM MAC interface. An entry in this table exists for each ifEntry with an ifType of docsCableMaclayer(127).”

INDEX { ifIndex }

::= { docsBpiCmBaseTable 1 }

```
DocsBpiCmBaseEntry ::= SEQUENCE {
    docsBpiCmPrivacyEnable          TruthValue,
    docsBpiCmPublicKey              OCTET STRING,
    docsBpiCmAuthState              INTEGER,
    docsBpiCmAuthKeySequenceNumber INTEGER,
    docsBpiCmAuthExpires            DateAndTime,
    docsBpiCmAuthReset              TruthValue,
    docsBpiCmAuthGraceTime          INTEGER,
    docsBpiCmTEKGraceTime           INTEGER,
    docsBpiCmAuthWaitTimeout        INTEGER,
    docsBpiCmReauthWaitTimeout      INTEGER,
    docsBpiCmOpWaitTimeout          INTEGER,
    docsBpiCmRekeyWaitTimeout       INTEGER,
    docsBpiCmAuthRejectWaitTimeout  INTEGER,
    docsBpiCmAuthRequests           Counter32,
    docsBpiCmAuthReplies            Counter32,
    docsBpiCmAuthRejects            Counter32,
    docsBpiCmAuthInvalids           Counter32,
    docsBpiCmAuthRejectErrorCode    INTEGER,
    docsBpiCmAuthRejectErrorString  DisplayString,
    docsBpiCmAuthInvalidErrorCode   INTEGER,
    docsBpiCmAuthInvalidErrorString DisplayString
}
```

docsBpiCmPrivacyEnable OBJECT-TYPE

SYNTAX TruthValue

MAX-ACCESS read-only

STATUS current

DESCRIPTION

“This identifies whether this CM is provisioned to run Baseline Privacy. This is analogous to the presence (or absence) of the Baseline Privacy Configuration Setting option as described in BPI Appendix A.1.1. The status of each individual SID with respect to Baseline Privacy is captured in the docsBpiCmTEKPrivacyEnable object. Note: this object will be read-write accessible only after the ability to start and stop the authorization state machine is understood.”

::= { docsBpiCmBaseEntry 1 }

docsBpiCmPublicKey OBJECT-TYPE

SYNTAX OCTET STRING

MAX-ACCESS read-only

STATUS current

DESCRIPTION

“Public key of the CM encoded as an ASN.1 SubjectPublicKeyInfo object as defined in the RSA Encryption Standard (PKCS #1) [RSA1].”

::= { docsBpiCmBaseEntry 2 }

docsBpiCmAuthState OBJECT-TYPE

SYNTAX INTEGER {
start(1),
authWait(2),
authorized(3),
reauthWait(4),
authRejectWait(5)
}

MAX-ACCESS read-only

STATUS current

DESCRIPTION

“The state of the CM authorization FSM. The start state indicates that FSM is in its initial state.”

::= { docsBpiCmBaseEntry 3 }

docsBpiCmAuthKeySequenceNumber OBJECT-TYPE

SYNTAX INTEGER (0..15)

MAX-ACCESS read-only

STATUS current

DESCRIPTION

“The authorization key sequence number for this FSM.”

::= { docsBpiCmBaseEntry 4 }

docsBpiCmAuthExpires OBJECT-TYPE

SYNTAX DateAndTime

MAX-ACCESS read-only

STATUS current

DESCRIPTION

“Actual clock time when the current authorization for this FSM expires. If the CM does not have an active authorization, then the value is of the expiration date and time of the last active authorization.”

::= { docsBpiCmBaseEntry 5 }

docsBpiCmAuthReset OBJECT-TYPE

SYNTAX TruthValue

MAX-ACCESS read-write

STATUS current

DESCRIPTION
 “Setting this object to TRUE generates a Reauthorize event in the authorization FSM, as described in section 4.1.2.3.4 of the Baseline Privacy Interface Specification. Reading this object always returns FALSE.”
 ::= { docsBpiCmBaseEntry 6 }

docsBpiCmAuthGraceTime OBJECT-TYPE
 SYNTAX INTEGER (300..1800)
 UNITS “seconds”
 MAX-ACCESS read-only
 STATUS current
 DESCRIPTION
 “Grace time for an authorization key. A CM is expected to start trying to get a new authorization key beginning AuthGraceTime seconds before the authorization key actually expires. The value of this object cannot be changed while the authorization state machine is running. Note: this object will be read-write accessible only after the ability to start and stop the authorization state machine is understood.”
 ::= { docsBpiCmBaseEntry 7 }

docsBpiCmTEKGraceTime OBJECT-TYPE
 SYNTAX INTEGER (300..1800)
 UNITS “seconds”
 MAX-ACCESS read-only
 STATUS current
 DESCRIPTION
 “Grace time for a TEK. A CM is expected to start trying to get a new TEK beginning TEKGraceTime seconds before the TEK actually expires. The value of this object cannot be changed while the authorization state machine is running. Note: this object will be read-write accessible only after the ability to start and stop the authorization state machine is understood.”
 ::= { docsBpiCmBaseEntry 8 }

docsBpiCmAuthWaitTimeout OBJECT-TYPE
 SYNTAX INTEGER (2..30)
 UNITS “seconds”
 MAX-ACCESS read-only
 STATUS current
 DESCRIPTION
 “Authorize Wait Timeout. The value of this object cannot be changed while the authorization state machine is running. Note: this object will be read-write accessible only after the ability to start and stop the authorization state machine is understood.”
 ::= { docsBpiCmBaseEntry 9 }

docsBpiCmReauthWaitTimeout OBJECT-TYPE
 SYNTAX INTEGER (2..30)
 UNITS “seconds”
 MAX-ACCESS read-only
 STATUS current
 DESCRIPTION
 “Reauthorize Wait Timeout in seconds. The value of this object cannot be changed while the authorization state machine is running. Note: this object will be read-write accessible only after the ability to start and stop the authorization state machine is understood.”
 ::= { docsBpiCmBaseEntry 10 }

docsBpiCmOpWaitTimeout OBJECT-TYPE
 SYNTAX INTEGER (1..10)

UNITS "seconds"
 MAX-ACCESS read-only
 STATUS current

DESCRIPTION

"Operational Wait Timeout in seconds. The value of this object cannot be changed while the authorization state machine is running. Note: this object will be read-write accessible only after the ability to start and stop the authorization state machine is understood."

::= { docsBpiCmBaseEntry 11 }

docsBpiCmRekeyWaitTimeout OBJECT-TYPE
 SYNTAX INTEGER (1..10)
 UNITS "seconds"
 MAX-ACCESS read-only
 STATUS current

DESCRIPTION

"Rekey Wait Timeout in seconds. The value of this object cannot be changed while the authorization state machine is running. Note: this object will be read-write accessible only after the ability to start and stop the authorization state machine is understood."

::= { docsBpiCmBaseEntry 12 }

docsBpiCmAuthRejectWaitTimeout OBJECT-TYPE
 SYNTAX INTEGER (60..1800)
 UNITS "seconds"
 MAX-ACCESS read-only
 STATUS current

DESCRIPTION

"Authorization Reject Wait Timeout in seconds. The value of this object cannot be changed while the authorization state machine is running. Note: this object will be read-write accessible only after the ability to start and stop the authorization state machine is understood."

::= { docsBpiCmBaseEntry 13 }

docsBpiCmAuthRequests OBJECT-TYPE
 SYNTAX Counter32
 MAX-ACCESS read-only
 STATUS current

DESCRIPTION

"Count of times the CM has transmitted an Authorization Request message."

::= { docsBpiCmBaseEntry 14 }

docsBpiCmAuthReplies OBJECT-TYPE
 SYNTAX Counter32
 MAX-ACCESS read-only
 STATUS current

DESCRIPTION

"Count of times the CM has received an Authorization Reply message."

::= { docsBpiCmBaseEntry 15 }

docsBpiCmAuthRejects OBJECT-TYPE
 SYNTAX Counter32
 MAX-ACCESS read-only
 STATUS current

DESCRIPTION

"Count of times the CM has received an Authorization Reject message."

::= { docsBpiCmBaseEntry 16 }

docsBpiCmAuthInvalids OBJECT-TYPE

SYNTAX Counter32

MAX-ACCESS read-only

STATUS current

DESCRIPTION

“Count of times the CM has received an Authorization Invalid message.”

::= { docsBpiCmBaseEntry 17 }

docsBpiCmAuthRejectErrorCode OBJECT-TYPE

SYNTAX INTEGER {
 none(1),
 unknown(2),
 unauthorized-cm(3),
 unauthorized-sid(4)
 }

MAX-ACCESS read-only

STATUS current

DESCRIPTION

“Error-Code in most recent Authorization Reject message received by the CM. This has value unknown(2) if the last Error-Code value was 0, and none(1) if no Authorization Reject message has been received since reboot.”

::= { docsBpiCmBaseEntry 18 }

docsBpiCmAuthRejectErrorString OBJECT-TYPE

SYNTAX DisplayString

MAX-ACCESS read-only

STATUS current

DESCRIPTION

“Display-String in most recent Authorization Reject message received by the CM. This is a zero length string if no Authorization Reject message has been received since reboot.”

::= { docsBpiCmBaseEntry 19 }

docsBpiCmAuthInvalidErrorCode OBJECT-TYPE

SYNTAX INTEGER {
 none(1),
 unknown(2),
 unauthorized-cm(3),
 unsolicited(5),
 invalid-key-sequence(6),
 key-request-authentication-failure(7)
 }

MAX-ACCESS read-only

STATUS current

DESCRIPTION

“Error-Code in most recent Authorization Invalid message received by the CM. This has value unknown(2) if the last Error-Code value was 0, and none(1) if no Authorization Invalid message has been received since reboot.”

::= { docsBpiCmBaseEntry 20 }

docsBpiCmAuthInvalidErrorString OBJECT-TYPE

SYNTAX DisplayString

MAX-ACCESS read-only

STATUS current

DESCRIPTION

“Display-String in most recent Authorization Invalid message received by the CM. This is a zero length string if no Authorization Invalid message has been received since reboot.”

::= { docsBpiCmBaseEntry 21 }

--

-- The CM TEK Table, indexed by ifIndex and SID

--

docsBpiCmTEKTable OBJECT-TYPE
 SYNTAX SEQUENCE OF DocsBpiCmTEKEntry
 MAX-ACCESS not-accessible
 STATUS current

DESCRIPTION

“Describes the attributes of each CM Traffic Encryption Key (TEK) association. The CM maintains (no more than) one TEK association per SID per CM MAC interface.”

::= { docsBpiCmObjects 2 }

docsBpiCmTEKEntry OBJECT-TYPE
 SYNTAX DocsBpiCmTEKEntry
 MAX-ACCESS not-accessible
 STATUS current

DESCRIPTION

“An entry containing objects describing the TEK association attributes of one SID. The CM MUST create one entry per unicast or multicast SID, regardless of whether the SID was obtained from a Registration Response message, from an Authorization Reply message, or from any future dynamic SID establishment mechanisms.”

INDEX { ifIndex, docsIfCmServiceId }

::= { docsBpiCmTEKTable 1 }

DocsBpiCmTEKEntry ::= SEQUENCE {
 docsBpiCmTEKPrivacyEnable TruthValue,
 docsBpiCmTEKState INTEGER,
 docsBpiCmTEKExpiresOld DateAndTime,
 docsBpiCmTEKExpiresNew DateAndTime,
 docsBpiCmTEKKeyRequests Counter32,
 docsBpiCmTEKKeyReplies Counter32,
 docsBpiCmTEKKeyRejects Counter32,
 docsBpiCmTEKInvalids Counter32,
 docsBpiCmTEKAuthPends Counter32,
 docsBpiCmTEKKeyRejectErrorCode INTEGER,
 docsBpiCmTEKKeyRejectErrorString DisplayString,
 docsBpiCmTEKInvalidErrorCode INTEGER,
 docsBpiCmTEKInvalidErrorString DisplayString
 }

docsBpiCmTEKPrivacyEnable OBJECT-TYPE
 SYNTAX TruthValue
 MAX-ACCESS read-write
 STATUS current

DESCRIPTION

“This identifies whether this SID is provisioned to run Baseline Privacy. This is analogous to enabling Baseline Privacy on a provisioned SID using the Class-of-Service Privacy Enable option as described in BPI Appendix A.1.2. This object may be set to TRUE or FALSE at any time (causing the CM to send a Reauth event to the authorization machine), regardless of whether Baseline Privacy is enabled for the CM. However, Baseline Privacy is not effectively enabled for any SID unless Baseline Privacy is enabled for the CM, which is managed via the docsBpiCmPrivacyEnable object.”

::= { docsBpiCmTEKEntry 1 }

docsBpiCmTEKState OBJECT-TYPE

SYNTAX INTEGER {
 start (1),
 opWait (2),
 opReauthWait (3),
 operational (4),
 rekeyWait (5),
 rekeyReauthWait (6)
 }
 MAX-ACCESS read-only
 STATUS current
 DESCRIPTION
 “The state of the indicated TEK FSM. The start(1) state indicates that FSM is in its initial state.”
 ::= { docsBpiCmTEKEntry 2 }

docsBpiCmTEKExpiresOld OBJECT-TYPE
 SYNTAX DateAndTime
 MAX-ACCESS read-only
 STATUS current
 DESCRIPTION
 “Actual clock time for expiration of the oldest active key for this FSM. If this FSM has no active keys,
 then the value is of the expiration date and time of the last active key.”
 ::= { docsBpiCmTEKEntry 3 }

docsBpiCmTEKExpiresNew OBJECT-TYPE
 SYNTAX DateAndTime
 MAX-ACCESS read-only
 STATUS current
 DESCRIPTION
 “Actual clock time for expiration of the newest active key for this FSM. If this FSM has no active
 keys, then the value is of the expiration date and time of the last active key.”
 ::= { docsBpiCmTEKEntry 4 }

docsBpiCmTEKKeyRequests OBJECT-TYPE
 SYNTAX Counter32
 MAX-ACCESS read-only
 STATUS current
 DESCRIPTION
 “Count of times the CM has transmitted a Key Request message.”
 ::= { docsBpiCmTEKEntry 5 }

docsBpiCmTEKKeyReplies OBJECT-TYPE
 SYNTAX Counter32
 MAX-ACCESS read-only
 STATUS current
 DESCRIPTION
 “Count of times the CM has received a Key Reply message.”
 ::= { docsBpiCmTEKEntry 6 }

docsBpiCmTEKKeyRejects OBJECT-TYPE
 SYNTAX Counter32
 MAX-ACCESS read-only
 STATUS current
 DESCRIPTION
 “Count of times the CM has received a Key Reject message.”
 ::= { docsBpiCmTEKEntry 7 }

docsBpiCmTEKInvalids OBJECT-TYPE

SYNTAX Counter32

MAX-ACCESS read-only

STATUS current

DESCRIPTION

“Count of times the CM has received a TEK Invalid message.”

::= { docsBpiCmTEKEntry 8 }

docsBpiCmTEKAuthPends OBJECT-TYPE

SYNTAX Counter32

MAX-ACCESS read-only

STATUS current

DESCRIPTION

“Count of times an Authorization Pending (Auth Pend) event occurred in this FSM.”

::= { docsBpiCmTEKEntry 9 }

docsBpiCmTEKKeyRejectErrorCode OBJECT-TYPE

SYNTAX INTEGER {
 none(1),
 unknown(2),
 unauthorized-sid(4)
 }

MAX-ACCESS read-only

STATUS current

DESCRIPTION

“Error-Code in most recent Key Reject message received by the CM. This has value unknown(2) if the last Error-Code value was 0, and none(1) if no Key Reject message has been received since reboot.”

::= { docsBpiCmTEKEntry 10 }

docsBpiCmTEKKeyRejectErrorString OBJECT-TYPE

SYNTAX DisplayString

MAX-ACCESS read-only

STATUS current

DESCRIPTION

“Display-String in most recent Key Reject message received by the CM. This is a zero length string if no Key Reject message has been received since reboot.”

::= { docsBpiCmTEKEntry 11 }

docsBpiCmTEKInvalidErrorCode OBJECT-TYPE

SYNTAX INTEGER {
 none(1),
 unknown(2),
 invalid-key-sequence(6)
 }

MAX-ACCESS read-only

STATUS current

DESCRIPTION

“Error-Code in most recent TEK Invalid message received by the CM. This has value unknown(2) if the last Error-Code value was 0, and none(1) if no TEK Invalid message has been received since reboot.”

::= { docsBpiCmTEKEntry 12 }

docsBpiCmTEKInvalidErrorString OBJECT-TYPE

SYNTAX DisplayString

MAX-ACCESS read-only

```

STATUS                current
DESCRIPTION
    "Display-String in most recent TEK Invalid message received by the CM. This is a zero length string
    if no TEK Invalid message has been received since reboot."
::= { docsBpiCmTEKEntry 13 }

-- Cable Modem Termination System Group

docsBpiCmtsObjects OBJECT IDENTIFIER ::= { docsBpiMIBObjects 2 }

--
-- The BPI base table for CMTSs, indexed by ifIndex
--

docsBpiCmtsBaseTable OBJECT-TYPE
SYNTAX                SEQUENCE OF DocsBpiCmtsBaseEntry
MAX-ACCESS            not-accessible
STATUS                current
DESCRIPTION
    "Describes the basic Baseline Privacy attributes of each CMTS MAC interface."
::= { docsBpiCmtsObjects 1 }

docsBpiCmtsBaseEntry OBJECT-TYPE
SYNTAX                DocsBpiCmtsBaseEntry
MAX-ACCESS            not-accessible
STATUS                current
DESCRIPTION
    "An entry containing objects describing attributes of one CMTS MAC interface. An entry in this table
    exists for each ifEntry with an ifType of docsCableMaclayer(127)."
INDEX                 { ifIndex }
::= { docsBpiCmtsBaseTable 1 }

DocsBpiCmtsBaseEntry ::= SEQUENCE {
    docsBpiCmtsDefaultAuthLifetime    INTEGER,
    docsBpiCmtsDefaultTEKLifetime     INTEGER,
    docsBpiCmtsDefaultAuthGraceTime   INTEGER,
    docsBpiCmtsDefaultTEKGraceTime    INTEGER,
    docsBpiCmtsAuthRequests           Counter32,
    docsBpiCmtsAuthReplies            Counter32,
    docsBpiCmtsAuthRejects            Counter32,
    docsBpiCmtsAuthInvalids           Counter32
}

docsBpiCmtsDefaultAuthLifetime OBJECT-TYPE
SYNTAX                INTEGER (86400..6048000)
UNITS                 "seconds"
MAX-ACCESS            read-write
STATUS                current
DESCRIPTION
    "Default lifetime, in seconds, the CMTS assigns to a new authorization key."
::= { docsBpiCmtsBaseEntry 1 }

docsBpiCmtsDefaultTEKLifetime OBJECT-TYPE
SYNTAX                INTEGER (1800..604800)
UNITS                 "seconds"
MAX-ACCESS            read-write

```

STATUS current

DESCRIPTION

“Default lifetime, in seconds, the CMTS assigns to a new Traffic Encryption Key (TEK).”

::= { docsBpiCmtsBaseEntry 2 }

docsBpiCmtsDefaultAuthGraceTime OBJECT-TYPE
SYNTAX INTEGER (300..1800)
UNITS “seconds”
MAX-ACCESS read-write
STATUS current

DESCRIPTION

“Default grace time, in seconds, the CMTS uses for an authorization key. This controls how far in advance of authorization key expiration that the CMTS is expected to produce the next generation of keying material. This value is expected to agree with the Authorization Grace Time that the provisioning system provides to CMs.”

::= { docsBpiCmtsBaseEntry 3 }

docsBpiCmtsDefaultTEKGraceTime OBJECT-TYPE
SYNTAX INTEGER (300..1800)
UNITS “seconds”
MAX-ACCESS read-write
STATUS current

DESCRIPTION

“Default grace time, in seconds, the CMTS uses for a Traffic Encryption Key (TEK). This controls how far in advance of TEK expiration that the CMTS is expected to produce the next generation of keying material. This value is expected to agree with the TEK Grace Time that the provisioning system provides to CMs. Note that this object is particularly relevant for multicast SIDs, where multiple grace time values cannot be honored.”

::= { docsBpiCmtsBaseEntry 4 }

docsBpiCmtsAuthRequests OBJECT-TYPE
SYNTAX Counter32
MAX-ACCESS read-only
STATUS current

DESCRIPTION

“Count of times the CMTS has received an Authorization Request message from any CM.”

::= { docsBpiCmtsBaseEntry 5 }

docsBpiCmtsAuthReplies OBJECT-TYPE
SYNTAX Counter32
MAX-ACCESS read-only
STATUS current

DESCRIPTION

“Count of times the CMTS has transmitted an Authorization Reply message to any CM.”

::= { docsBpiCmtsBaseEntry 6 }

docsBpiCmtsAuthRejects OBJECT-TYPE
SYNTAX Counter32
MAX-ACCESS read-only
STATUS current

DESCRIPTION

“Count of times the CMTS has transmitted an Authorization Reject message to any CM.”

::= { docsBpiCmtsBaseEntry 7 }

docsBpiCmtsAuthInvalids OBJECT-TYPE
SYNTAX Counter32

```

MAX-ACCESS          read-only
STATUS              current
DESCRIPTION
    "Count of times the CMTS has transmitted an Authorization Invalid message to any CM."
 ::= { docsBpiCmtsBaseEntry 8 }

--
-- The CMTS Authorization Table, indexed by ifIndex and CM MAC address
--

docsBpiCmtsAuthTable OBJECT-TYPE
SYNTAX              SEQUENCE OF DocsBpiCmtsAuthEntry
MAX-ACCESS          not-accessible
STATUS              current
DESCRIPTION
    "Describes the attributes of each CM authorization association. The CMTS maintains one
    authorization association with each Baseline Privacy-enabled CM on each CMTS MAC interface."
 ::= { docsBpiCmtsObjects 2 }

docsBpiCmtsAuthEntry OBJECT-TYPE
SYNTAX              DocsBpiCmtsAuthEntry
MAX-ACCESS          not-accessible
STATUS              current
DESCRIPTION
    "An entry containing objects describing attributes of one authorization association. The CMTS MUST
    create one entry per CM per MAC interface, based on the receipt of an Authorization Request
    message, and MUST not delete the entry before the CM authorization permanently expires."
INDEX               { ifIndex, docsBpiCmtsAuthCmMacAddress }
 ::= { docsBpiCmtsAuthTable 1 }

DocsBpiCmtsAuthEntry ::= SEQUENCE {
    docsBpiCmtsAuthCmMacAddress      MacAddress,
    docsBpiCmtsAuthCmPublicKey      OCTET STRING,
    docsBpiCmtsAuthCmKeySequenceNumber INTEGER,
    docsBpiCmtsAuthCmExpires        DateAndTime,
    docsBpiCmtsAuthCmLifetime       INTEGER,
    docsBpiCmtsAuthCmGraceTime      INTEGER,
    docsBpiCmtsAuthCmReset          INTEGER,
    docsBpiCmtsAuthCmRequests       Counter32,
    docsBpiCmtsAuthCmReplies        Counter32,
    docsBpiCmtsAuthCmRejects        Counter32,
    docsBpiCmtsAuthCmInvalids       Counter32,
    docsBpiCmtsAuthRejectErrorCode  INTEGER,
    docsBpiCmtsAuthRejectErrorString DisplayString,
    docsBpiCmtsAuthInvalidErrorCode INTEGER,
    docsBpiCmtsAuthInvalidErrorString DisplayString
}

docsBpiCmtsAuthCmMacAddress OBJECT-TYPE
SYNTAX              MacAddress
MAX-ACCESS          not-accessible
STATUS              current
DESCRIPTION
    "The physical address of the CM to which the authorization association applies."
 ::= { docsBpiCmtsAuthEntry 1 }

```

docsBpiCmtsAuthCmPublicKey OBJECT-TYPE
 SYNTAX OCTET STRING
 MAX-ACCESS read-only
 STATUS current
 DESCRIPTION
 "Public key of the CM encoded as an ASN.1 SubjectPublicKeyInfo object as defined in the RSA Encryption Standard (PKCS #1) [RSA1]. This is a zero-length string if the CMTS does not retain the public key."
 ::= { docsBpiCmtsAuthEntry 2 }

docsBpiCmtsAuthCmKeySequenceNumber OBJECT-TYPE
 SYNTAX INTEGER (0..15)
 MAX-ACCESS read-only
 STATUS current
 DESCRIPTION
 "The authorization key sequence number for this CM."
 ::= { docsBpiCmtsAuthEntry 3 }

docsBpiCmtsAuthCmExpires OBJECT-TYPE
 SYNTAX DateAndTime
 MAX-ACCESS read-only
 STATUS current
 DESCRIPTION
 "Actual clock time when the current authorization for this CM expires. If this CM does not have an active authorization, then the value is of the expiration date and time of the last active authorization."
 ::= { docsBpiCmtsAuthEntry 4 }

docsBpiCmtsAuthCmLifetime OBJECT-TYPE
 SYNTAX INTEGER (86400..6048000)
 UNITS "seconds"
 MAX-ACCESS read-write
 STATUS current
 DESCRIPTION
 "Lifetime, in seconds, the CMTS assigns to an authorization key for this CM."
 ::= { docsBpiCmtsAuthEntry 5 }

docsBpiCmtsAuthCmGraceTime OBJECT-TYPE
 SYNTAX INTEGER (300..1800)
 UNITS "seconds"
 MAX-ACCESS read-only
 STATUS current
 DESCRIPTION
 "Grace time for the authorization key in seconds. The CM is expected to start trying to get a new authorization key beginning AuthGraceTime seconds before the authorization key actually expires."
 ::= { docsBpiCmtsAuthEntry 6 }

docsBpiCmtsAuthCmReset OBJECT-TYPE
 SYNTAX INTEGER {
 no-reset-requested(1),
 invalidate-auth(2),
 send-auth-invalid(3),
 invalidate-teks(4)
 }
 MAX-ACCESS read-write
 STATUS current
 DESCRIPTION

“Setting this object to invalidate-auth(2) causes the CMTS to invalidate the current CM authorization key, but not to transmit an Authorization Invalid message nor to invalidate unicast TEKS. Setting this object to send-auth-invalid(3) causes the CMTS to invalidate the current CM authorization key, and to transmit an Authorization Invalid message to the CM, but not to invalidate unicast TEKS. Setting this object to invalidate-teks(4) causes the CMTS to invalidate the current CM authorization key, to transmit an Authorization Invalid message to the CM, and to invalidate all unicast TEKS associated with this CM authorization. Reading this object returns the most-recently-set value of this object, or returns no-reset-requested(1) if the object has not been set since the last CMTS reboot.”

::= { docsBpiCmtsAuthEntry 7 }

docsBpiCmtsAuthCmRequests OBJECT-TYPE

SYNTAX Counter32

MAX-ACCESS read-only

STATUS current

DESCRIPTION

“Count of times the CMTS has received an Authorization Request message from this CM.”

::= { docsBpiCmtsAuthEntry 8 }

docsBpiCmtsAuthCmReplies OBJECT-TYPE

SYNTAX Counter32

MAX-ACCESS read-only

STATUS current

DESCRIPTION

“Count of times the CMTS has transmitted an Authorization Reply message to this CM.”

::= { docsBpiCmtsAuthEntry 9 }

docsBpiCmtsAuthCmRejects OBJECT-TYPE

SYNTAX Counter32

MAX-ACCESS read-only

STATUS current

DESCRIPTION

“Count of times the CMTS has transmitted an Authorization Reject message to this CM.”

::= { docsBpiCmtsAuthEntry 10 }

docsBpiCmtsAuthCmInvalids OBJECT-TYPE

SYNTAX Counter32

MAX-ACCESS read-only

STATUS current

DESCRIPTION

“Count of times the CMTS has transmitted an Authorization Invalid message to this CM.”

::= { docsBpiCmtsAuthEntry 11 }

docsBpiCmtsAuthRejectErrorCode OBJECT-TYPE

SYNTAX INTEGER {
 none(1),
 unknown(2),
 unauthorized-cm(3),
 unauthorized-sid(4)
 }

MAX-ACCESS read-only

STATUS current

DESCRIPTION

“Error-Code in most recent Authorization Reject message transmitted to the CM. This has value unknown(2) if the last Error-Code value was 0, and none(1) if no Authorization Reject message has been transmitted to the CM.”

::= { docsBpiCmtsAuthEntry 12 }

```

docsBpiCmtsAuthRejectErrorString    OBJECT-TYPE
SYNTAX                               DisplayString
MAX-ACCESS                           read-only
STATUS                               current
DESCRIPTION
    "Display-String in most recent Authorization Reject message transmitted to the CM. This is a zero
    length string if no Authorization Reject message has been transmitted to the CM."
 ::= { docsBpiCmtsAuthEntry 13 }

docsBpiCmtsAuthInvalidErrorCode      OBJECT-TYPE
SYNTAX                               INTEGER {
                                        none(1),
                                        unknown(2),
                                        unauthorized-cm(3),
                                        unsolicited(5),
                                        invalid-key-sequence(6),
                                        key-request-authentication-failure(7)
                                    }
MAX-ACCESS                           read-only
STATUS                               current
DESCRIPTION
    "Error-Code in most recent Authorization Invalid message transmitted to the CM. This has value
    unknown(2) if the last Error-Code value was 0, and none(1) if no Authorization Invalid message has
    been transmitted to the CM."
 ::= { docsBpiCmtsAuthEntry 14 }

docsBpiCmtsAuthInvalidErrorString    OBJECT-TYPE
SYNTAX                               DisplayString
MAX-ACCESS                           read-only
STATUS                               current
DESCRIPTION
    "Display-String in most recent Authorization Invalid message transmitted to the CM. This is a zero
    length string if no Authorization Invalid message has been transmitted to the CM."
 ::= { docsBpiCmtsAuthEntry 15 }

--
-- The CMTS TEK Table, indexed by ifIndex and SID
--

docsBpiCmtsTEKTable    OBJECT-TYPE
SYNTAX                 SEQUENCE OF DocsBpiCmtsTEKEntry
MAX-ACCESS             not-accessible
STATUS                 current
DESCRIPTION
    "Describes the attributes of each CM Traffic Encryption Key (TEK) association. The CMTS maintains
    one TEK association per SID on each CMTS MAC interface."
 ::= { docsBpiCmtsObjects 3 }

docsBpiCmtsTEKEntry    OBJECT-TYPE
SYNTAX                 DocsBpiCmtsTEKEntry
MAX-ACCESS             not-accessible
STATUS                 current
DESCRIPTION
    "An entry containing objects describing attributes of one TEK association on a particular CMTS MAC
    interface. The CMTS MUST create one entry per SID per MAC interface, based on the receipt of an

```

Key Request message, and MUST not delete the entry before the CM authorization for the SID permanently expires.”

INDEX { ifIndex, docsIfCmtsServiceId }
 ::= { docsBpiCmtsTEKTable 1 }

DocsBpiCmtsTEKEntry ::= SEQUENCE {
 docsBpiCmtsTEKLifetime INTEGER,
 docsBpiCmtsTEKGraceTime INTEGER,
 docsBpiCmtsTEKExpiresOld DateAndTime,
 docsBpiCmtsTEKExpiresNew DateAndTime,
 docsBpiCmtsTEKReset TruthValue,
 docsBpiCmtsKeyRequests Counter32,
 docsBpiCmtsKeyReplies Counter32,
 docsBpiCmtsKeyRejects Counter32,
 docsBpiCmtsTEKInvalids Counter32,
 docsBpiCmtsKeyRejectErrorCode INTEGER,
 docsBpiCmtsKeyRejectErrorString DisplayString,
 docsBpiCmtsTEKInvalidErrorCode INTEGER,
 docsBpiCmtsTEKInvalidErrorString DisplayString
 }

docsBpiCmtsTEKLifetimeOBJECT-TYPE
 SYNTAX INTEGER (1800..604800)
 UNITS “seconds”
 MAX-ACCESS read-write
 STATUS current
 DESCRIPTION
 “Lifetime, in seconds, the CMTS assigns to keys for this TEK association.”
 ::= { docsBpiCmtsTEKEntry 1 }

docsBpiCmtsTEKGraceTime OBJECT-TYPE
 SYNTAX INTEGER (300..1800)
 UNITS “seconds”
 MAX-ACCESS read-only
 STATUS current
 DESCRIPTION
 “Grace time for the TEK in seconds. The CM is expected to start trying to get a new TEK beginning
 TEKGraceTime seconds before the TEK actually expires.”
 ::= { docsBpiCmtsTEKEntry 2 }

docsBpiCmtsTEKExpiresOld OBJECT-TYPE
 SYNTAX DateAndTime
 MAX-ACCESS read-only
 STATUS current
 DESCRIPTION
 “Actual clock time for expiration of the oldest active key for this TEK association. If this TEK
 association has no active keys, then the value is of the expiration date and time of the last active key.”
 ::= { docsBpiCmtsTEKEntry 3 }

docsBpiCmtsTEKExpiresNew OBJECT-TYPE
 SYNTAX DateAndTime
 MAX-ACCESS read-only
 STATUS current
 DESCRIPTION

“Actual clock time for expiration of the newest active key for this TEK association. If this TEK association has no active keys, then the value is of the expiration date and time of the last active key.”
 ::= { docsBpiCmtsTEKEntry 4 }

docsBpiCmtsTEKReset OBJECT-TYPE
 SYNTAX TruthValue
 MAX-ACCESS read-write
 STATUS current
 DESCRIPTION

“Setting this object to TRUE causes the CMTS to invalidate the current active TEK(s) (plural due to key transition periods), and to generate a new TEK for the associated SID. Reading this object always returns FALSE.”

::= { docsBpiCmtsTEKEntry 5 }

docsBpiCmtsKeyRequests OBJECT-TYPE
 SYNTAX Counter32
 MAX-ACCESS read-only
 STATUS current
 DESCRIPTION

“Count of times the CMTS has received a Key Request message.”

::= { docsBpiCmtsTEKEntry 6 }

docsBpiCmtsKeyReplies OBJECT-TYPE
 SYNTAX Counter32
 MAX-ACCESS read-only
 STATUS current
 DESCRIPTION

“Count of times the CMTS has transmitted a Key Reply message.”

::= { docsBpiCmtsTEKEntry 7 }

docsBpiCmtsKeyRejects OBJECT-TYPE
 SYNTAX Counter32
 MAX-ACCESS read-only
 STATUS current
 DESCRIPTION

“Count of times the CMTS has transmitted a Key Reject message.”

::= { docsBpiCmtsTEKEntry 8 }

docsBpiCmtsTEKInvalids OBJECT-TYPE
 SYNTAX Counter32
 MAX-ACCESS read-only
 STATUS current
 DESCRIPTION

“Count of times the CMTS has transmitted a TEK Invalid message.”

::= { docsBpiCmtsTEKEntry 9 }

docsBpiCmtsKeyRejectErrorCode OBJECT-TYPE
 SYNTAX INTEGER {
 none(1),
 unknown(2),
 unauthorized-sid(4)
 }
 MAX-ACCESS read-only
 STATUS current
 DESCRIPTION

“Error-Code in the most recent Key Reject message sent in response to a Key Request for this BPI SID. This has value unknown(2) if the last Error-Code value was 0, and none(1) if no Key Reject message has been received since reboot.”

```
 ::= { docsBpiCmtsTEKEntry 10 }
```

docsBpiCmtsKeyRejectErrorString OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
DESCRIPTION
“Display-String in the most recent Key Reject message sent in response to a Key Request for this BPI SID. This is a zero length string if no Key Reject message has been received since reboot.”

```
 ::= { docsBpiCmtsTEKEntry 11 }
```

docsBpiCmtsTEKInvalidErrorCode OBJECT-TYPE
SYNTAX INTEGER {
none(1),
unknown(2),
invalid-key-sequence(6)
}
MAX-ACCESS read-only
STATUS current
DESCRIPTION
“Error-Code in the most recent TEK Invalid message sent in association with this BPI SID. This has value unknown(2) if the last Error-Code value was 0, and none(1) if no TEK Invalid message has been received since reboot.”

```
 ::= { docsBpiCmtsTEKEntry 12 }
```

docsBpiCmtsTEKInvalidErrorString OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
DESCRIPTION
“Display-String in the most recent TEK Invalid message sent in association with this BPI SID. This is a zero length string if no TEK Invalid message has been received since reboot.”

```
 ::= { docsBpiCmtsTEKEntry 13 }
```

--
-- The CMTS Multicast Control Group
--

docsBpiMulticastControl OBJECT IDENTIFIER ::= { docsBpiCmtsObjects 4 }

--
-- The CMTS IP Multicast Mapping Table, indexed by IP multicast address and prefix, and by ifindex
--

docsBpiIpMulticastMapTable OBJECT-TYPE
SYNTAX SEQUENCE OF DocsBpiIpMulticastMapEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
“Describes the mapping of IP multicast address prefixes to multicast SIDs on each CMTS MAC interface.”

```
 ::= { docsBpiMulticastControl 1 }
```

```

docsBpiIpMulticastMapEntry      OBJECT-TYPE
SYNTAX                          DocsBpiIpMulticastMapEntry
MAX-ACCESS                      not-accessible
STATUS                          current
DESCRIPTION
    "An entry containing objects describing the mapping of one IP multicast address prefix to one
    multicast SID on one CMTS MAC interface. The CMTS uses the mapping when forwarding
    downstream IP multicast traffic."
INDEX                            { ifIndex, docsBpiIpMulticastAddress, docsBpiIpMulticastPrefixLength }
 ::= { docsBpiIpMulticastMapTable 1 }

DocsBpiIpMulticastMapEntry ::= SEQUENCE {
    docsBpiIpMulticastAddress      IpAddress,
    docsBpiIpMulticastPrefixLength INTEGER,
    docsBpiIpMulticastServiceId   INTEGER,
    docsBpiIpMulticastMapControl   RowStatus
}

docsBpiIpMulticastAddress      OBJECT-TYPE
SYNTAX                          IpAddress
MAX-ACCESS                      not-accessible
STATUS                          current
DESCRIPTION
    "The IP multicast address (prefix) to be mapped."
 ::= { docsBpiIpMulticastMapEntry 1 }

docsBpiIpMulticastPrefixLength OBJECT-TYPE
SYNTAX                          INTEGER (0..32)
MAX-ACCESS                      not-accessible
STATUS                          current
DESCRIPTION
    "The IP multicast address prefix length to be mapped."
 ::= { docsBpiIpMulticastMapEntry 2 }

docsBpiIpMulticastServiceId    OBJECT-TYPE
SYNTAX                          INTEGER (8192..16368)
MAX-ACCESS                      read-create
STATUS                          current
DESCRIPTION
    "The multicast SID to be used in this IP multicast address prefix mapping entry."
 -- DEFVAL is unused multicast SID value chosen by CMTS.
 ::= { docsBpiIpMulticastMapEntry 3 }

docsBpiIpMulticastMapControl   OBJECT-TYPE
SYNTAX                          RowStatus
MAX-ACCESS                      read-create
STATUS                          current
DESCRIPTION
    "Controls and reflects the IP multicast address prefix mapping entry."
 ::= { docsBpiIpMulticastMapEntry 4 }

--
-- The CMTS Multicast SID Authorization Table, indexed by ifIndex by multicast SID by CM MAC address
--

docsBpiMulticastAuthTable      OBJECT-TYPE

```

SYNTAX SEQUENCE OF DocsBpiMulticastAuthEntry
 MAX-ACCESS not-accessible
 STATUS current
 DESCRIPTION
 “Describes the multicast SID authorization for each CM on each CMTS MAC interface.”
 ::= { docsBpiMulticastControl 2 }

docsBpiMulticastAuthEntry OBJECT-TYPE
 SYNTAX DocsBpiMulticastAuthEntry
 MAX-ACCESS not-accessible
 STATUS current
 DESCRIPTION
 “An entry containing objects describing the key authorization of one cable modem for one multicast SID for one CMTS MAC interface.”
 INDEX { ifIndex, docsBpiMulticastSID, docsBpiMulticastCmMacAddress }
 ::= { docsBpiMulticastAuthTable 1 }

DocsBpiMulticastAuthEntry ::= SEQUENCE {
 docsBpiMulticastServiceId INTEGER,
 docsBpiMulticastCmMacAddress MacAddress,
 docsBpiMulticastAuthControl RowStatus
 }

docsBpiMulticastServiceId OBJECT-TYPE
 SYNTAX INTEGER (8192..16368)
 MAX-ACCESS not-accessible
 STATUS current
 DESCRIPTION
 “The multicast SID for authorization.”
 ::= { docsBpiMulticastAuthEntry 1 }

docsBpiMulticastCmMacAddress OBJECT-TYPE
 SYNTAX MacAddress
 MAX-ACCESS not-accessible
 STATUS current
 DESCRIPTION
 “The MAC address of the CM to which the multicast SID authorization applies.”
 ::= { docsBpiMulticastAuthEntry 2 }

docsBpiMulticastAuthControl OBJECT-TYPE
 SYNTAX RowStatus
 MAX-ACCESS read-create
 STATUS current
 DESCRIPTION
 “Controls and reflects the CM authorization for each multicast SID.”
 ::= { docsBpiMulticastAuthEntry 3 }

--
 -- The BPI MIB Conformance Statements (with a placeholder for notifications)
 --

docsBpiNotification OBJECT IDENTIFIER ::= { docsBpiMIB 2 }
 docsBpiConformance OBJECT IDENTIFIER ::= { docsBpiMIB 3 }
 docsBpiCompliances OBJECT IDENTIFIER ::= { docsBpiConformance 1 }
 docsBpiGroups OBJECT IDENTIFIER ::= { docsBpiConformance 2 }

```

docsBpiBasicCompliance MODULE-COMPLIANCE
STATUS          current
DESCRIPTION
    "The compliance statement for devices which implement the DOCS Baseline Privacy Interface."

MODULE -- docsBpiMIB

-- conditionally mandatory group
GROUP docsBpiCmGroup
    DESCRIPTION
        "This group is implemented only in CMs, not in CMTSs."

-- conditionally mandatory group
GROUP docsBpiCmtsGroup
    DESCRIPTION
        "This group is implemented only in CMTSs, not in CMs."

 ::= { docsBpiCompliances 1 }

docsBpiCmGroup      OBJECT-GROUP
OBJECTS {
    docsBpiCmPrivacyEnable,
    docsBpiCmPublicKey,
    docsBpiCmAuthState,
    docsBpiCmAuthKeySequenceNumber,
    docsBpiCmAuthExpires,
    docsBpiCmAuthReset,
    docsBpiCmAuthGraceTime,
    docsBpiCmTEKGraceTime,
    docsBpiCmAuthWaitTimeout,
    docsBpiCmReauthWaitTimeout,
    docsBpiCmOpWaitTimeout,
    docsBpiCmRekeyWaitTimeout,
    docsBpiCmAuthRejectWaitTimeout,
    docsBpiCmAuthRequests,
    docsBpiCmAuthReplies,
    docsBpiCmAuthRejects,
    docsBpiCmAuthInvalids,
    docsBpiCmAuthRejectErrorCode,
    docsBpiCmAuthRejectErrorString,
    docsBpiCmAuthInvalidErrorCode,
    docsBpiCmAuthInvalidErrorString,
    docsBpiCmTEKPrivacyEnable,
    docsBpiCmTEKState,
    docsBpiCmTEKExpiresOld,
    docsBpiCmTEKExpiresNew,
    docsBpiCmTEKKeyRequests,
    docsBpiCmTEKKeyReplies,
    docsBpiCmTEKKeyRejects,
    docsBpiCmTEKInvalids,
    docsBpiCmTEKAuthPends,
    docsBpiCmTEKKeyRejectErrorCode,
    docsBpiCmTEKKeyRejectErrorString,
    docsBpiCmTEKInvalidErrorCode,
    docsBpiCmTEKInvalidErrorString
}

```

```

STATUS                current
DESCRIPTION
    "A collection of objects providing CM BPI status and control."
 ::= { docsBpiGroups 1 }

docsBpiCmtsGroup      OBJECT-GROUP
OBJECTS {
    docsBpiCmtsDefaultAuthLifetime,
    docsBpiCmtsDefaultTEKLifetime,
    docsBpiCmtsDefaultAuthGraceTime,
    docsBpiCmtsDefaultTEKGraceTime,
    docsBpiCmtsAuthRequests,
    docsBpiCmtsAuthReplies,
    docsBpiCmtsAuthRejects,
    docsBpiCmtsAuthInvalids,
    docsBpiCmtsAuthCmMacAddress,
    docsBpiCmtsAuthCmPublicKey,
    docsBpiCmtsAuthCmKeySequenceNumber,
    docsBpiCmtsAuthCmExpires,
    docsBpiCmtsAuthCmLifetime,
    docsBpiCmtsAuthCmGraceTime,
    docsBpiCmtsAuthCmReset,
    docsBpiCmtsAuthCmRequests,
    docsBpiCmtsAuthCmReplies,
    docsBpiCmtsAuthCmRejects,
    docsBpiCmtsAuthCmInvalids,
    docsBpiCmtsAuthRejectErrorCode,
    docsBpiCmtsAuthRejectErrorString,
    docsBpiCmtsAuthInvalidErrorCode,
    docsBpiCmtsAuthInvalidErrorString,
    docsBpiCmtsTEKLifetime,
    docsBpiCmtsTEKGraceTime,
    docsBpiCmtsTEKExpiresOld,
    docsBpiCmtsTEKExpiresNew,
    docsBpiCmtsTEKReset,
    docsBpiCmtsKeyRequests,
    docsBpiCmtsKeyReplies,
    docsBpiCmtsKeyRejects,
    docsBpiCmtsTEKInvalids,
    docsBpiCmtsKeyRejectErrorCode,
    docsBpiCmtsKeyRejectErrorString,
    docsBpiCmtsTEKInvalidErrorCode,
    docsBpiCmtsTEKInvalidErrorString,
    docsBpiIpMulticastAddress,
    docsBpiIpMulticastPrefixLength,
    docsBpiIpMulticastServiceId,
    docsBpiIpMulticastMapControl,
    docsBpiMulticastServiceId,
    docsBpiMulticastCmMacAddress,
    docsBpiMulticastAuthControl
}
STATUS                current
DESCRIPTION
    "A collection of objects providing CMTS BPI status and control."
 ::= { docsBpiGroups 2 }
END

```

Appendix B References

- [IPCDN1] G. Roeck, “Cable Device Management Information Base for MCNS compliant Cable Modems and Cable Modem Termination Systems”, draft-ietf-ipcdn-cable-device-mib-03.txt, March 1998.
- [IPCDN2] G. Roeck, “Radio Frequency (RF) Interface Management Information Base for MCNS compliant RF Interfaces”, draft-ietf-ipcdn-rf-interface-mib-03.txt, January 1998.
- [MCNS1] Data-Over-Cable Service Interface Specifications, Baseline Privacy Interface Specification, SP-BPI-I01-970922.
- [MCNS2] Data-Over-Cable Service Interface Specifications, Radio Frequency Interface Specification, SP-RFI-I02-971008.
- [MCNS3] Data-Over-Cable Service Interface Specifications, Operations Support System Interface Specification, SP-OSSI-I01-970403.
- [MCNS4] Data-Over-Cable Service Interface Specifications, Cable Modem Telephony Return Interface Specification, SP-CMTRI-I01-970804.
- [MCNS5] Data-Over-Cable Service Interface Specifications, OSSI Specification Overview – Telephony Return MIB, SP-OSSI-TRD02-970901.
- [RSA1] RSA Laboratories, “The Public-Key Cryptography Standards”, RSA Data Security Inc., Redwood City, CA.

This page intentionally left blank.

Appendix C Glossary

Cable Modem (CM) – A modulator-demodulator at subscriber locations intended for use in conveying data communications on a cable television system.

Cable Modem Termination System (CMTS) – Cable modem termination system, located at the cable television system headend or distribution hub, which provides complementary functionality to the cable modems to enable data connectivity to a wide-area network.

CM – See Cable Modem.

CMTS – See Cable Modem Termination System.

DHCP – See Dynamic Host Configuration Protocol.

Downstream – In cable television, the direction of transmission from the headend to the subscriber.

Dynamic Host Configuration Protocol (DHCP) – An Internet protocol used for assigning network-layer (IP) addresses.

Headend – The central location on the HFC network that is responsible for injecting broadcast video and other signals in the downstream direction. See also Master Headend, Distribution Hub.

HFC – See Hybrid Fiber/Coax (HFC) System.

Hybrid Fiber/Coax (HFC) System – A broadband bidirectional shared-media transmission system using fiber trunks between the headend and the fiber nodes, and coaxial distribution from the fiber nodes to the customer locations.

ICMP – See Internet Control Message Protocol.

IEEE – See Institute of Electrical and Electronic Engineers.

IETF – See Internet Engineering Task Force.

Internet Control Message Protocol (ICMP) – An Internet network-layer protocol.

International Electrotechnical Commission (IEC) – An international standards body.

Institute of Electrical and Electronic Engineers (IEEE) – A voluntary organization which, among other things, sponsors standards committees and is accredited by the American National Standards Institute.

Internet Engineering Task Force (IETF) – A body responsible, among other things, for developing standards used in the Internet.

Internet Protocol (IP) – An Internet network-layer protocol.

International Organization for Standardization (ISO) – An international standards body, commonly known as the International Standards Organization.

IP – See Internet Protocol.

Latency – The time, expressed in quantity of symbols, taken for a signal element to pass through a device.

Layer – A subdivision of the Open System Interconnection (OSI) architecture, constituted by subsystems of the same rank

LLC – See Logical Link Control (LLC) procedure.

Local Area Network (LAN) – A non-public data network in which serial transmission is used for direct data communication among data stations located on the user's premises.

Logical Link Control (LLC) procedure – In a local area network (LAN) or a Metropolitan Area Network (MAN), that part of the protocol that governs the assembling of data link layer frames and their exchange between data stations, independent of how the transmission medium is shared.

MAC – See Media Access Control (MAC) procedure.

MAC Service Access Point (MSAP) – The conceptual binding of a MAC-layer service provider to the protocol entities (i.e., data link layers) above it.

Master Headend – A headend which collects television program material from various sources by satellite, microwave, fiber and other means, and distributes this material to Distribution Hubs in the same metropolitan or regional area.

MCNS – See Multimedia Cable Network System (MCNS) partners.

Mean Time to Repair (MTTR) – In cable television systems, the MTTR is the average elapsed time from the moment a loss of RF channel operation is detected up to the moment the RF channel operation is fully restored.

Media Access Control (MAC) address – The “built-in” hardware address of a device connected to a shared medium.

Media Access Control (MAC) procedure – In a subnetwork, that part of the protocol that governs access to the transmission medium independent of the physical characteristics of the medium, but taking into account the topological aspects of the subnetworks, in order to enable the exchange of data between nodes. MAC procedures include framing, error protection, and acquiring the right to use the underlying transmission medium.

Multimedia Cable Network System (MCNS) partners – A consortium of Comcast Cable Communications, Inc., Cox Communications, Tele-Communications, Inc., and Time Warner Cable, interested in deploying high-speed data communications systems on cable television systems.

Network Layer – Layer 3 in the Open System Interconnection (OSI) architecture; the layer that provides services to establish a path between open systems.

Network Management – The functions related to the management of data link layer and physical layer resources and their stations across the data network supported by the hybrid fiber/coax system.

Open Systems Interconnection (OSI) – A framework of ISO standards for communication between different systems made by different vendors, in which the communications process is organized into seven different categories that are placed in a layered sequence based on their relationship to the user. Each layer uses the layer immediately below it and provides a service to the layer above. Layers 7 through 4 deal with end-to-end communication between the message source and destination, and layers 3 through 1 deal with network functions.

Operations Support System (OSS) – The backoffice software used for configuration, performance, fault, accounting and security management.

Organization Unique Identifier (OUI) – A 3-octet IEEE assigned identifier that OUI can be used to generate Universal LAN MAC addresses and Protocol Identifiers per ANSI/IEEE Std 802 for use in Local and Metropolitan Area Network applications.

OSI – See Open Systems Interconnection.

OSS – See Operations Support System.

OUI – See Organization Unique Identifier.

PDU – See Protocol Data Unit.

PHY – See Physical (PHY) Layer.

Physical (PHY) Layer – Layer 1 in the Open System Interconnection (OSI) architecture; the layer that provides services to transmit bits or groups of bits over a transmission link between open systems and which entails electrical, mechanical and handshaking procedures.

Protocol – A set of rules and formats that determines the communication behavior of layer entities in the performance of the layer functions.

Request For Comments (RFC) – A technical policy document of the IETF; these documents can be accessed on the World Wide Web at <http://ds.internic.net/ds/rfcindex.html>.

RFC – See Request for Comments.

Simple Network Management Protocol (SNMP) – A network management protocol of the IETF.

SNMP – See Simple Network Management Protocol.

Subscriber – See End User.

Systems Management – Functions in the application layer related to the management of various open systems Interconnection (OSI) resources and their status across all layers of the OSI architecture.

Transmission Control Protocol (TCP) – A transport-layer Internet protocol which ensures successful end-to-end delivery of data packets without error.

Trivial File-Transfer Protocol (TFTP) – An Internet protocol for transferring files without the requirement for user names and passwords that is typically used for automatic downloads of data and software.

Upstream – The direction from the subscriber location toward the headend.