Data-Over-Cable Service Interface Specifications
DOCSIS 1.0

Operations Support System Interface Specification
Baseline Privacy Interface MIB

SP-OSSI-BPI-C01-011119

Notice

Document Status Sheet

Document Control Number:	SP-OSSI-BPI-C01-011119			
Document Title:	DOCSIS 1.0 Operations Support System Interface Specification - Baseline Privacy Interface MIB			
Revision History:	I01 – First Release, March 31, 1998 I02 – Second Issued Release, August 29, 2001 C01 – Closed, November 19, 2001			
Date:	November 19, 2001			
Status:	~~Work in Progress~~	~~Draft~~	~~Issued~~	Closed
Distribution Restrictions:	Author Only	~~CL/Member~~	~~CL/ Member/ Vendor~~	Public

Key to Document Status Codes:

Work in Progress	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 Members and vendors. Drafts are susceptible to substantial change during the review process.
Issued	A stable document, which has undergone rigorous member and vendor review and is suitable for product design and development, cross-vendor interoperability, and for certification testing.
Closed	A static document, reviewed, tested, validated, and closed to further engineering change requests to the specification through CableLabs.

DOCSIS 1.0 Specifications
superseded by the ANSI/SCTE 22 suite of standards
see: www/scte.org/standards/

Contents

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 enable prospective vendors of cable modems and other data-over-cable systems to address the operations support 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.

2 BASELINE PRIVACY INTERFACE MANAGEMENT REQUIREMENTS

The Data-Over-Cable Service Baseline Privacy Interface Specification is documented in [DOCSIS1], and is an extension to the Radio Frequency Interface Specification documented in [DOCSIS2]. In addition to the explicit requirements in this specification, the CM and CMTS enabled for Baseline Privacy MUST support all applicable MIB requirements documented in the DOCSIS OSSI Specification [DOCSIS3].

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.

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 BPI MIB Requirement

The BPI MIB includes a set of objects needed to configure, operate, and monitor the baseline privacy interface. The BPI MIB is defined by [RFC-3083].

Due to the editorial error in [RFC-3083], the CMs MUST use the following definition for docsBpiCmAuthState instead of the definition in [RFC-3083].

```
docsBpiCmAuthState OBJECT-TYPE
   SYNTAX INTEGER {
      start(1),
      authWait(2),
      authorized(3),
      reauthWait(4),
      authRejectWait(5)
   }
   MAX-ACCESS     read-only
   STATUS         current
   DESCRIPTION
      "The value of this object is the state of the CM authorization
        FSM. The start date indicates that FSM is in its initial state."
   REFERENCE
      "DOCSIS Baseline Privacy Interface Specification,
        Section 4.1.2.1."
   ::= { docsBpiCmBaseEntry 3 }
```

Appendix I References (Informative)

[DOCSIS1] Data-Over-Cable Service Interface Specifications 1.0, Baseline Privacy Interface Specification, SP-BPI-C01-011119, November 19, 2001.

[DOCSIS2] Data-Over-Cable Service Interface Specifications 1.0, Radio Frequency Interface Specification, SP-RFI-C01-011119, November 19, 2001.

[DOCSIS3] Data-Over-Cable Service Interface Specifications 1.0, Operations Support System Interface Specification, SP-OSSI-C01-011119, November 19, 2001.

[RFC-3083] R. Woundy, "Baseline Privacy Interface Management Information Base for DOCSIS Compliant Cable Modems and Cable Modem Termination Systems", RFC3083, March 2001.

Appendix II Glossary (Informative)

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.

DOCSIS – Data-Over-Cable Service Interface Specification.

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

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.

IETF – See Internet Engineering Task Force.

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

MAC – See Media Access Control (MAC) address and procedure.

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.

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.

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.

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.

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