UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T J.125

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

(04/2004)

SERIE J: REDES DE CABLE Y TRANSMISIÓN DE PROGRAMAS RADIOFÓNICOS Y TELEVISIVOS, Y DE OTRAS SEÑALES MULTIMEDIOS

Sistemas interactivos para distribución de televisión digital

Privacidad de enlace para la implementación de módems de cable

Recomendación UIT-T J.125

Recomendación UIT-T J.125

Privacidad de enlace para la implementación de módems de cable

Resumen

La presente Recomendación constituía el anexo O al anexo B/J.112. Puesto que también se aplica a los servicios de privacidad de capa MAC para la Rec. UIT-T J.122, se ha transformado en Recomendación (J.125). Esta Recomendación, a la que a menudo se hace referencia como interfaz de privacidad básica plus o BPI+, tiene los dos objetivos siguientes:

- proporcionar a los usuarios de módem de cable privacidad de datos en toda la red de cable, y
- proporcionar a los operadores de cable protección de los servicios, es decir, impedir que usuarios no autorizados accedan a los servicios MAC de RF (radiofrecuencia).

La BPI+ permite un nivel de privacidad de los datos en toda la red por cable de medio compartido igual o mejor que el que proporcionan los servicios de acceso a red por línea especializada (módems analógicos o líneas de abonado digitales).

Orígenes

La Recomendación UIT-T J.125 fue aprobada el 22 de abril de 2004 por la Comisión de Estudio 9 (2001-2004) del UIT-T por el procedimiento de la Recomendación UIT-T A.8.

PREFACIO

La UIT (Unión Internacional de Telecomunicaciones) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones. El UIT-T (Sector de Normalización de las Telecomunicaciones de la UIT) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB.

ÍNDICE

Recomendación UIT-T J.125

Privacidad de enlace para la implementación de módems de cable

1 Alcance

La presente Recomendación contiene los servicios de privacidad de capa MAC (criptación y autenticación) para comunicaciones DOCSIS CMTS-CM. Esta Recomendación, a la que a menudo se hace referencia como interfaz de privacidad de referencia plus o BPI+, tiene los dos objetivos siguientes:

- proporcionar a los usuarios de módem de cable privacidad de datos en toda la red de cable, y
- proporcionar a los operadores de cable protección de los servicios, es decir, impedir que usuarios no autorizados accedan a los servicios MAC de RF (radiofrecuencia).

La BPI+ permite un nivel de privacidad de los datos en toda la red por cable de medio compartido igual o mejor que el que proporcionan los servicios de acceso a red por línea especializada (módems analógicos o líneas de abonado digitales).

2 Referencias

2.1 Normativas

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes. En esta Recomendación, la referencia a un documento, en tanto que autónomo, no le otorga el rango de una Recomendación.

[SCTE22-2] ANSI/SCTE 22-2 2002, *DOCSIS 1.0 Part 2: Baseline Privacy Interface Specification*, www.scte.org.

[SCTE23-3] ANSI/SCTE 23-3 2003, *DOCSIS 1.1 Part 3: Operations Support System Interface*, www.scte.org.

[SCTE79-2] ANSI/SCTE 79-2 2002, *DOCS 2.0 Operations Support System Interface*, www.scte.org.

[J.112-B] Recomendación UIT-T J.112, anexo B (2004), *Especificaciones de interfaces de servicio de datos por cable: Especificación de la interfaz de radiofrecuencia*.

[J.122] Recomendación UIT-T J.122 (2002), *Sistemas de transmisión de segunda generación para servicios interactivos de televisión por cable – Módems de cable para protocolo Internet*.

[FIPS-46-3] Federal Information Processing Standards Publications 46-3, *Data Encryption Standard (DES)*, octubre de 1999.

[FIPS-140-2] Federal Information Processing Standards Publication 140-2, *Security Requirements for Cryptographic Modules*, mayo de 2001.

[FIPS-180-2] Federal Information Processing Standards Publication 180-2, *Secure Hash Standard (SHS)*, agosto de 2002.

[PKCS #7] IETF RFC 2315 (1998), *PKCS #7: Cryptographic Message Syntax Version 1.5*.

[RFC2104] IETF RFC 2104 (1997), *HMAC: Keyed-Hashing for Message Authentication*.

[RFC3083] IETF RFC 3083 (2001), *Baseline Privacy Interface Management Information Base for DOCSIS Compliant Cable Modems and Cable Modem Termination Systems*.

[RFC3280] IETF RFC 3280 (2002), *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.

[RSA3] *PKCS #1: RSA Cryptography Specifications Version 2.0*, octubre de 1998.

[X.509] Recomendación UIT-T X.509 (2000) | ISO/CEI 9594-8:2001, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Marcos para certificados de claves públicas y de atributos*.

2.2 Informativas

[SCTE22-1] ANSI/SCTE 22-1 2002, *DOCSIS 1.0 Part 1: Radio Frequency Interface,* www.scte.org.

[SCTE22-3] ANSI/SCTE 22-3 2002, *DOCSIS 1.1 Part 3: Operations Support System Interface*, www.scte.org.

[DOCSIS4] *Data-Over-Cable Service Interface Specifications, Cable Modem to Customer Premise Equipment Interface Specification*, SP-CMCI-I09-030730.

[DOCSIS8] *Management Information Base for DOCSIS Cable Modems and Cable Modem Termination Systems for Baseline Privacy Plus*, draft-ietf-ipcdn-bpiplus-mib-05.txt, 8 de mayo de 2001.

[FIPS-74] Federal Information Processing Standards Publication 74, *Guidelines for Implementing and Using the NBS Data Encryption Standard*, abril de 1981.

[FIPS-81] Federal Information Processing Standards Publication 81, *DES Modes of Operation*, December 1980 (Includes Change Notice, noviembre de1981).

[FIPS-186-2] Federal Information Processing Standards Publication 186-2, *Digital Signature Standard (DSS)*, enero de 2000.

[RFC2868] IETF RFC 2868 (2000), *RADIUS Attributes for Tunnel Protocol Support*.

[RSA1] RSA Laboratories, *PKCS #1: RSA Encryption Standard, Version 1.5*, RSA Security, Inc., Bedford, MA, noviembre de 1993.

[RSA2] RSA Laboratories, *Some Examples of the PKCS Standards*, RSA Data Security, Inc., Redwood City, CA, noviembre de 1993.

3 Términos y definiciones

En esta Recomendación se definen los términos siguientes.

3.1 DOCSIS: Término para un dispositivo o sistema que cumple alguna de las versiones de las especificaciones de Cable Television Laboratories, Inc. ("CableLabs") ubicadas en: http//www.cablemodem.com/specifications/.

3.2 DOCSIS 1.0: Sistema o dispositivo que cumple las siguientes especificaciones de interfaz del servicio de datos por cable [SCTE22-1], [SCTE22-2], [SCTE22-3], [DOCSIS4].

3.3 DOCSIS 1.1: Sistema o dispositivo que cumple las siguientes especificaciones de interfaz del servicio de datos por cable [J.112-B], [SCT23-3], [DOCSIS4] y esta Recomendación.

3.4 DOCSIS 2.0: Sistema o dispositivo que cumple las siguientes especificaciones de interfaz del servicio de datos por cable [J122], [SCTE79-2], [DOCSIS4] y esta Recomendación.

4 Abreviaturas

En esta Recomendación se utilizan las siguientes siglas.

BPI+ Interfaz de privacidad de referencia plus (*baseline privacy interface plus*)

BPKM Gestión de claves de privacidad de referencia (*baseline privacy key management*)

CBC Concatenación de bloques cifrados (*cipher block chaining*)

CM Módem de cable (*cable modem*)

CMTS Sistema de terminación de módem de cable (*cable modem termination system*)

DES Norma de criptación de datos de los Estados Unidos (*US data encryption standard*)

HMAC Troceo con aplicación de clave para autenticación de mensaje (*keyed-hashing for message authentication*)

QoS Calidad de servicio (*quality of service*)

RSA Laboratorios RSA (*RSA laboratories*)

SA Asociación de seguridad (*security association*)

SAID Identificador de asociación de seguridad (*security association identifier*)

SID Identificador de servicio (*service identifier*)

TEK Clave de criptación de tráfico (*traffic encryption key*)

5 Antecedentes y visión de conjunto de la privacidad básica

A los operadores de cable les interesa instalar sistemas de comunicaciones por paquetes de alta velocidad en los sistemas de televisión por cable que permitan proporcionar una amplia variedad de servicios. Entre los servicios objeto de atención por parte de los operadores de cable figura el acceso a Internet a alta velocidad, el servicio de telefonía por paquetes, el servicio de videoconferencia, el servicio equivalente al de retransmisión de tramas T1, y muchos otros servicios.

El servicio cuya prestación se pretende permitirá la transferencia bidireccional transparente de tráfico de protocolo Internet (IP, *Internet protocol*), entre la cabecera del sistema de cable y las posiciones de los clientes, por una red de televisión por cable totalmente coaxial o híbrida de fibra óptica/cable coaxial (HFC, *hybrid fibre/coax*). Esto es lo que se muestra de forma simplificada en la figura 5-1.

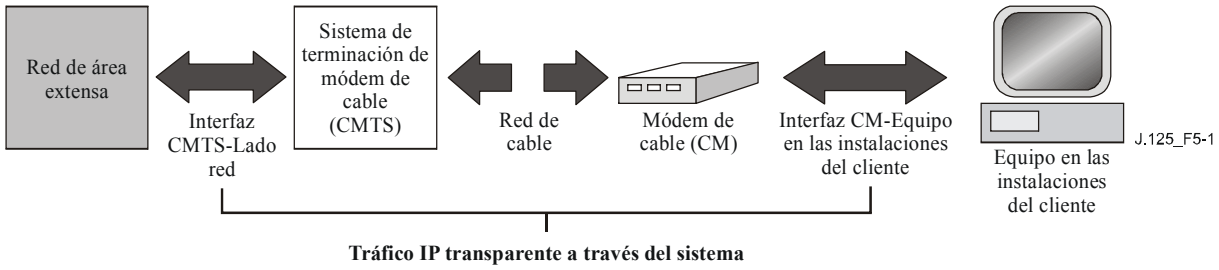


Figura 5-1/J.125 – Tráfico IP transparente a través del sistema de datos por cable

El trayecto de transmisión por el sistema de cable se materializa en un CMTS en la cabecera, y en un CM en la posición de cada cliente. En la cabecera (o centro de distribución), la interfaz con el sistema de datos por cable se denomina interfaz sistema de terminación de módem de cable-lado red (CMTS-NSI, *cable modem termination system – network-side interface*). En las posiciones de los clientes, la interfaz se llama interfaz módem de cable-equipo en las instalaciones del cliente (CMCI, *cable-modem-to-customer-premise-equipment interface*). Lo que se pretende es que los operadores de cable transfieran de manera transparente tráfico IP entre esas interfaces incluyendo, pero sin limitarse a ello, diagramas DHCP, ICPM y direccionamiento de grupo IP (radiodifusión y multidifusión).

La interfaz de privacidad básica (BPI, *baseline privacy*) y la interfaz de privacidad de referencia plus (BPI+, *baseline privacy plus*) proporcionan a los usuarios de módem de cable privacidad de datos en la red de cable. Lo hacen criptando los flujos de tráfico entre CM y CMTS. La privacidad básica es la versión original de esta característica y se explica en la referencia [SCTE22-2]. La privacidad de referencia plus es una versión actualizada de esta característica y constituye el objeto de la presente Recomendación. Véase el anexo C para un análisis más detallado de las diferencias entre las dos versiones.

Además, BPI+ proporciona a los operadores de cable un alto grado de protección frente a quienes piratean el servicio. Los servicios de comunicaciones de datos DOCSIS MAC protegidos se dividen en tres categorías:

- servicios de datos IP del mejor esfuerzo y alta velocidad;
- servicios de datos con QoS (por ejemplo, velocidad binaria constante); y
- servicios de grupo de multidifusión IP.

Con BPI+, el CMTS protege contra los accesos no autorizados a esos servicios de transporte de datos implantando la criptación de los flujos de tráfico asociados a través de la red de cable. BPI+ emplea un protocolo de gestión de clave de cliente/servidor autenticada en el que el CMTS, el servidor, controla la distribución del material de aplicación de claves a los CM clientes.

5.1 Visión general de la arquitectura

La privacidad de referencia plus tiene dos protocolos componentes:

- Un protocolo de encapsulación para la criptación de datos por paquetes a través de la red de cable. Dicho protocolo define:
  1) el formato de trama para el transporte de datos por paquetes criptados dentro de las tramas DOCSIS MAC,
  2) un conjunto de series criptográficas soportadas, es decir, emparejamientos de algoritmos de criptación y autenticación de datos, y
  3) las reglas para la aplicación de esos algoritmos a los datos por paquetes de una trama DOCSIS MAC.
- Un protocolo de gestión de claves (gestión de claves de privacidad básica, o "BPKM") que permite la distribución segura de datos de aplicación de claves del CMTS a los CM. Mediante dicho protocolo de gestión de claves, el CM y el CMTS sincronizan los datos de aplicación de claves; además, el CMTS utiliza el protocolo para forzar el acceso condicional a los servicios de la red.

5.1.1 Criptación de datos por paquetes

Los servicios de criptación de BPI+ se definen como un conjunto de servicios ampliados dentro de la subcapa DOCSIS MAC. La información de encabezamiento de paquete específica de BPI+ se sitúa en el elemento encabezamiento ampliado de privacidad básica dentro del encabezamiento ampliado MAC.

En el momento en que se publica esta Recomendación, BPI+ soporta un solo algoritmo de criptación de datos por paquetes: el modo concatenación de bloques cifrados (CBC, *cipher block chaining*) del algoritmo norma de criptación de datos de Estados Unidos (DES, *US data encryption standard*) [FIPS 46-2] [FIPS 81]. BPI+ no empareja el CBC de DES con ningún algoritmo de autenticación de datos por paquetes. Algoritmos de criptación de datos adicionales pueden ser soportados en perfeccionamientos futuros de la especificación del protocolo BPI+, y esos algoritmos podrán ser emparejados con algoritmos de autenticación de datos.

BPI+ cripta los datos por paquetes de una trama DOCSIS MAC; el encabezamiento de la trama DOCSIS MAC no se cripta. Se DEBEN enviar mensajes de gestión DOCSIS MAC en claro para facilitar el registro, la alineación y el funcionamiento normal de la subcapa MAC[1].

La cláusula 6 especifica el formato de las tramas DOCSIS MAC que llevan cabidas útiles de datos por paquetes criptados.

5.1.2 Protocolo de gestión de claves

Los CM utilizan el protocolo de gestión de claves de privacidad básica para obtener la autorización y el material de aplicación de claves de tráfico del CMTS, y soportar reautorizaciones y renovaciones periódicas de claves. El protocolo de gestión de claves utiliza certificados digitales X.509 [UIT1], un algoritmo de criptación de claves públicas [RSA3] y DES triple de dos claves para que los intercambios de claves entre CM y CMTS se produzcan de manera segura.

El protocolo de gestión de claves de privacidad básica se atiene al modo cliente/servidor, en el que el CM, un "cliente" BPKM, pide material de aplicación de claves, y el CMTS, un "servidor" BPKM, responde a esas peticiones, garantizándose que los CM clientes individuales sólo reciben el material de aplicación de claves para el que están autorizados. El protocolo BPKM sólo utiliza mensajería de gestión DOCSIS MAC.

BPI+ utiliza criptografía de claves públicas para establecer un secreto compartido (es decir, una clave de autorización) entre CM y CMTS. El secreto compartido se emplea a continuación para asegurar los intercambios de claves de criptación de tráfico del protocolo BPKM subsiguientes. Este mecanismo de distribución de claves en dos etapas permite la renovación de claves de criptación de tráfico sin incurrir en laboriosas operaciones de complejo cálculo de claves públicas.

Un CMTS autentica un CM cliente durante el intercambio de autorización inicial. Cada CM lleva un certificado digital X.509 único expedido por el fabricante del CM. El certificado digital contiene la clave pública del CM junto con otra información de identificación, a saber, la dirección MAC del CM, el identificador ID del fabricante y el número de serie. Cuando se solicita una clave de autorización, el CM presenta su certificado digital a un CMTS. El CMTS verifica el certificado digital, y a continuación utiliza la clave pública verificada para criptar una clave de autorización, que envía seguidamente al CM solicitante.

El CMTS asocia la identidad autenticada de un módem de cable a un abonado de pago, y en consecuencia a los servicios de datos a los que el abonado está autorizado a acceder. Así pues, con el intercambio de clave de autorización, el CMTS establece la identidad autenticada de un CM cliente, y los servicios (es decir, las claves de criptación de tráfico específicas) a los que el CM está autorizado a acceder.

Puesto que el CMTS autentica los CM, puede proteger contra cualquier atacante que emplee un módem *clonado* (falsificado), fingiendo ser un módem de abonado legítimo. La utilización de los certificados X.509 impide que los módems clonados pasen credenciales falsas a un CMTS.

---

[1] Los encabezamientos DOCSIS MAC de las PDU de datos por paquetes y los mensajes de gestión DOCSIS MAC ajenos a BPI+ PUEDEN ser criptados cuando formen parte de un paquete concatenado fragmentado según [J.112-B] o [J.122].

Los CM DEBEN tener pares de claves privada/pública RSA instaladas en fábrica o proporcionar un algoritmo interno para generar esos pares de claves de forma dinámica. Si un CM depende de un algoritmo interno para generar su par de claves RSA, DEBE generarlo antes de que se produzca su primera inicialización de privacidad básica, descrita en 5.2.1. Los CM con pares de claves RSA instaladas en fábrica DEBEN tener también certificados X.509 instalados en fábrica. Los módems de cable que dependen de un algoritmo interno para generar un par de claves RSA DEBEN soportar un mecanismo de instalación del certificado X.509 expedido por el fabricante tras la generación de las claves.

En la cláusula 7 se define de forma detallada el protocolo BPKM.

5.1.3 Asociaciones de seguridad de BPI+

Una *asociación de seguridad* (SA, *security association*) de BPI+ es el conjunto de información de seguridad que comparten un CMTS y uno o más de sus CM clientes para hacer posible unas comunicaciones seguras a través de la red de cable. BPI+ define tres tipos de asociaciones de seguridad: *primario, estático* y *dinámico*. Una asociación de seguridad primaria está vinculada únicamente a un solo CM, y se establece cuando el CM completa el registro DOCSIS MAC. Las asociaciones de seguridad estáticas se aprovisionan dentro del CMTS. Las asociaciones de seguridad dinámicas se establecen y eliminan, sobre la marcha, en respuesta a la iniciación y terminación de flujos de tráfico (en sentido descendente) específicos. Tanto las SA estáticas como las dinámicas pueden ser compartidas por múltiples CM.

La información compartida de asociación de seguridad incluye las claves de criptación de tráfico y los vectores de inicialización del CBC. Para soportar, en perfeccionamientos futuros de BPI+, algoritmos alternativos de criptación y datos y autenticación de datos, los parámetros de asociación de seguridad de BPI+ incluyen un identificador de serie criptográfica que indica un emparejamiento particular de algoritmos de criptación de datos por paquetes y autenticación de datos por paquetes empleados por la asociación de seguridad. Al publicarse esta Recomendación, los únicos algoritmos de criptación de datos por paquetes eran DES de 56 bits y DES de 40 bits, y ninguno de ellos está emparejado con un algoritmo de autenticación de datos por paquetes[2].

BPI+ identifica las asociaciones de seguridad con un *identificador de asociación de seguridad (SAID, security association identifier)* de 14 bits.

Cada CM (BPI+ habilitada) establece una asociación de seguridad primaria con su CMTS. Todo el tráfico en sentido ascendente de un CM DEBE ser criptado en el marco de la asociación de seguridad primaria exclusiva del CM. El SAID correspondiente a la SA primaria de un CM DEBE ser igual al identificador de servicio (SID) primario DOCSIS 1.1 o DOCSIS 2.0 [J.112-B] o [J.122] del CM. Por otro lado, aunque normalmente el tráfico de unidifusión en sentido descendente dirigido al o a los dispositivos CPE, que se hallan detrás de un CM, son criptados de acuerdo con la asociación de seguridad primaria exclusiva del CM, flujos de tráfico de unidifusión en sentido descendente seleccionados pueden ser criptados de acuerdo con las SA estáticas o dinámicas. Es decir, tráfico en sentido descendente PUEDE ser criptado de conformidad con cualquiera de los tres tipos de SA. No obstante, un paquete de datos de multidifusión IP en sentido descendente está destinado por lo general a múltiples CM y, por tanto, lo más probable es que se cripte de conformidad con SA estáticas o dinámicas, a las que pueden acceder múltiples CM, al contrario que una SA primaria, que se circunscribe a un único CM.

El CM correcto DEBE soportar una SA primaria, una o más SA dinámicas y una o más SA estáticas. El CMTS correcto DEBE soportar una SA primaria, una o más SA dinámicas y PUEDE

---

[2] BPI+ cripta la CRC Ethernet/802.3 de una PDU paquete. Si bien esto equivale a un cierto grado de autenticación de datos, no representa una autenticación de datos segura desde el punto de vista criptográfico.

soportar una o más SA estáticas. La especificación de BPI+ no indica la cantidad de SA estáticas o dinámicas requeridas por los dispositivos.

Utilizando el protocolo BPKM, un CM pide a su CMTS el material de aplicación de claves de una SA. El CMTS garantiza que cada CM cliente sólo tenga acceso a las asociaciones de seguridad a las que está autorizado a acceder.

El material de aplicación de claves de una SA (por ejemplo, la clave DES y el vector de inicialización del CBC) tiene un tiempo de vida limitado. Cuando el CMTS entrega material de aplicación de claves de SA a un CM, le proporciona también el tiempo de vida restante de ese material. Corresponde al CM pedir material de aplicación de claves nuevo al CMTS antes de que expire en el CMTS el tiempo de vida del material de que dispone a la sazón el CM. El protocolo BKPM especifica cómo mantienen el CM y el CMTS la sincronización de la clave.

5.1.4 Identificadores de servicio (SID) de QoS e identificadores de asociación de seguridad (SAID) de BPI+

El elemento encabezamiento ampliado de BPI+ en tramas DOCSIS MAC en sentido descendente contiene el identificador de la asociación de seguridad (SAID) de BPI+ de acuerdo con el cual se cripta la trama en sentido descendente. Si la trama en sentido descendente es un paquete de unidifusión dirigido a un dispositivo CPE situado detrás de un determinado CM, será criptada normalmente de acuerdo con la SA primaria del CM, siendo entonces el SAID igual al SID primario del CM objetivo. Si la trama en sentido descendente es un paquete de multidifusión que se pretende que reciban múltiples CM, el elemento encabezamiento ampliado contendrá el SAID estático o dinámico del que se ha establecido la correspondencia con ese grupo de multidifusión. El SAID (primario, estático o dinámico), junto con otros campos de datos del elemento encabezamiento ampliado en sentido descendente, identifica a un módem receptor el conjunto particular de material de aplicación de claves que se requiere para descriptar el campo datos por paquetes criptados de la trama DOCSIS MAC.

Puesto que todo el tráfico en sentido ascendente de un CM se cripta de conformidad con su SA primaria exclusiva, las tramas DOCSIS MAC en sentido ascendente, al contrario que las tramas DOCSIS MAC en sentido descendente, no necesitan llevar un SAID de BPI+ en sus encabezamientos ampliados; en cambio, el elemento EH de privacidad básica PUEDE contener cualquier SID de QoS válido asignado al CM.

El elemento encabezamiento ampliado de privacidad básica sirve para múltiples fines en las tramas DOCSIS MAC de una PDU datos por paquetes en sentido ascendente. Además de identificar el material de aplicación de claves que, en concreto, se ha utilizado para criptar los datos por paquetes de una trama, proporciona un mecanismo para la emisión de peticiones de anchura de banda adosadas, y puede llevar datos de control de fragmentación. Estas dos últimas funciones están vinculadas a un SID de QoS particular y, por este motivo, los elementos encabezamiento ampliado de privacidad básica en sentido ascendente contienen un SID de QoS en vez de un SAID primario de BPI+, que se puede deducir del SID de QoS.

5.2 Visión de conjunto operativa

5.2.1 Inicialización de módem de cable

[J.112-B] o [J.122] dividen la inicialización del módem de cable en las fases siguientes:

- exploración del canal en sentido descendente y establecimiento de la sincronización con el CMTS;
- obtención de los parámetros de transmisión;
- realización de la alineación;
- establecimiento de la conectividad IP (DHCP);

- establecimiento de la hora del día;
- transferencia de los parámetros operativos (telecarga de ficheros de parámetros vía TFTP);
- registro en el CMTS.

El establecimiento de la privacidad básica sigue al registro en el CMTS.

Si un CM está en condiciones de aplicar privacidad básica, la fijación de habilitación de privacidad (tipo 29) en los ficheros de configuración de estilo DOCSIS 1.1 ó 2.0 DEBE fijarse explícitamente o implícitamente a habilitado, independientemente de la presencia de las fijaciones de configuración de privacidad básica (tipo 17). En otras palabras, las fijaciones de configuración de privacidad básica no precisan estar presentes en el fichero de configuración para obtener privacidad básica. En el anexo A se definen esas fijaciones de configuración adicionales.

Una vez completado el registro del CM, el CMTS asigna uno o más ID de servicio (SID) estático al CM que se registra en concordancia con el aprovisionamiento de clase de servicio estática del CM. El primer SID estático asignado durante el proceso de registro es el SID primario, y este SID servirá también como SAID primario de BPI+ del CM. Si un CM está configurado de modo que aplique privacidad básica, el registro en el CMTS va seguido inmediatamente por la inicialización de las funciones de seguridad de privacidad básica del CM.

La inicialización de la privacidad básica empieza con el envío por el CM al CMTS de un mensaje de información de autenticación con el certificado CA del fabricante del CM y una petición de autorización con la información siguiente:

- datos que identifiquen el CM (por ejemplo, la dirección MAC);
- la clave pública RSA del CM;
- un certificado X.509 que demuestre la vinculación entre los datos que identifican el CM, y la clave pública del CM;
- una lista de las capacidades de seguridad del CM (es decir, los emparejamientos particulares de algoritmos de criptación y autenticación que soporta el CM); y
- el SAID primario del CM (es decir, el SID primario).

Si el CMTS determina que el CM solicitante está autorizado para el SAID primario de la petición de autorización, contesta con una respuesta de autorización que contiene una clave de autorización, a partir de la cual el CM y el CMTS obtienen las claves necesarias para asegurar las peticiones subsiguientes de un CM de claves de criptación de tráfico y las respuestas del CMTS a esas peticiones. El CMTS cripta la clave de autorización con la clave pública del módem de cable receptor.

La respuesta de autorización contiene también una lista de descriptores de asociación de seguridad, que identifican las SA primaria y estáticas a las que el CM solicitante está autorizado a acceder. Cada descriptor de SA consta de un conjunto de parámetros de SA, incluidos el SAID, el tipo y la serie criptográfica. La lista contiene por lo menos una entrada: un descriptor que describe la asociación de seguridad primaria del CM. Otras entradas son opcionales, y describirían cualesquiera SA estáticas a las que el CM pudiera acceder.

Tras completar de manera satisfactoria la autenticación y obtener la autorización del CMTS, el módem de cable envía peticiones de clave al CMTS, solicitando claves de criptación de tráfico a utilizar con cada uno de sus SAID. Las peticiones de clave de tráfico de un CM se autentican aplicando un troceo con clave (el algoritmo HMAC [RFC 2104]); la clave de autenticación de mensajes se deduce de la clave de autorización obtenida durante el intercambio de autorización previo. El CMTS contesta con respuestas de clave, que contienen las claves de criptación de tráfico (TEK, *traffic encryption keys*); las TEK son DES triples criptadas con una clave de criptación de claves obtenida a partir de la clave de autorización. Al igual que las peticiones de clave, las

respuestas de clave son autenticadas aplicando un troceo con clave, en el que la clave de autenticación de mensajes se deriva de la clave de autorización.

La inicialización de privacidad básica finaliza cuando el CMTS envía o el CM recibe los mensajes de contestación de clave asociados con todos los SAID en el mensaje de contestación de autorización.

5.2.2 Mecanismo de actualización de clave de módem de cable

Las claves de criptación de tráfico que el CMTS proporciona a los CM clientes tienen un tiempo de vida limitado. El CMTS entrega el tiempo de vida restante de la clave, junto con el valor de la clave, en las respuestas de clave que envía a sus CM clientes. El CMTS controla cuáles son las claves vigentes eliminando las claves cuyo tiempo de vida haya expirado y generando nuevas claves. Corresponde a cada uno de los módems de cable asegurarse de que las claves que está utilizando concuerdan con las que utiliza el CMTS. Para ello, rastrean el momento en que está previsto que prescriba la clave de un determinado SAID y emiten una petición de clave nueva, la de la clave más reciente, antes de que se produzca esa prescripción.

Además, es preciso que los módems de cable renueven periódicamente la autorización del CMTS; como ocurre con las claves de criptación de tráfico, una clave de autorización tiene un tiempo de vida finito que el CMTS entrega al CM junto con el valor de la clave. Corresponde a cada módem de cable obtener una nueva autorización y una clave de autorización renovada (así como una lista actualizada de descriptores de SA) antes de que el CMTS haga que prescriba la clave de autorización vigente del CM.

La inicialización de la privacidad básica y la actualización de claves están implementadas dentro del protocolo de gestión de claves de privacidad básica, definido con detalle en la cláusula 7.

6 Formatos de trama DOCSIS MAC

Cuando se funciona con BPI+ habilitada, en cualquier instante después de la terminación de la inicialización de privacidad básica, el CMTS y el CM DEBEN criptar las regiones PDU datos de todas las tramas de los siguientes dos tipos de trama DOCSIS MAC transmitidas en la red de cable y NO DEBEN enviar ninguna por la red de cable sin criptación, a menos que lo permita explícitamente la especificación DOCSIS o que de forma explícita el operador proporcione:

- tramas MAC de PDU datos por paquetes de longitud variable;
- tramas MAC de fragmentación.

En cada uno de los dos casos, un elemento encabezamiento ampliado de privacidad básica del encabezamiento DOCSIS MAC identifica la asociación de seguridad y el material de aplicación de claves acompañante utilizado para criptar la PDU datos.

6.1 Formato de trama MAC de PDU datos por paquetes de longitud variable

La figura 6-1 muestra el formato de una PDU datos por paquetes de longitud variable DOCSIS con un elemento encabezamiento ampliado (EH, *extended header*) de privacidad y cabida útil de PDU paquete criptada.

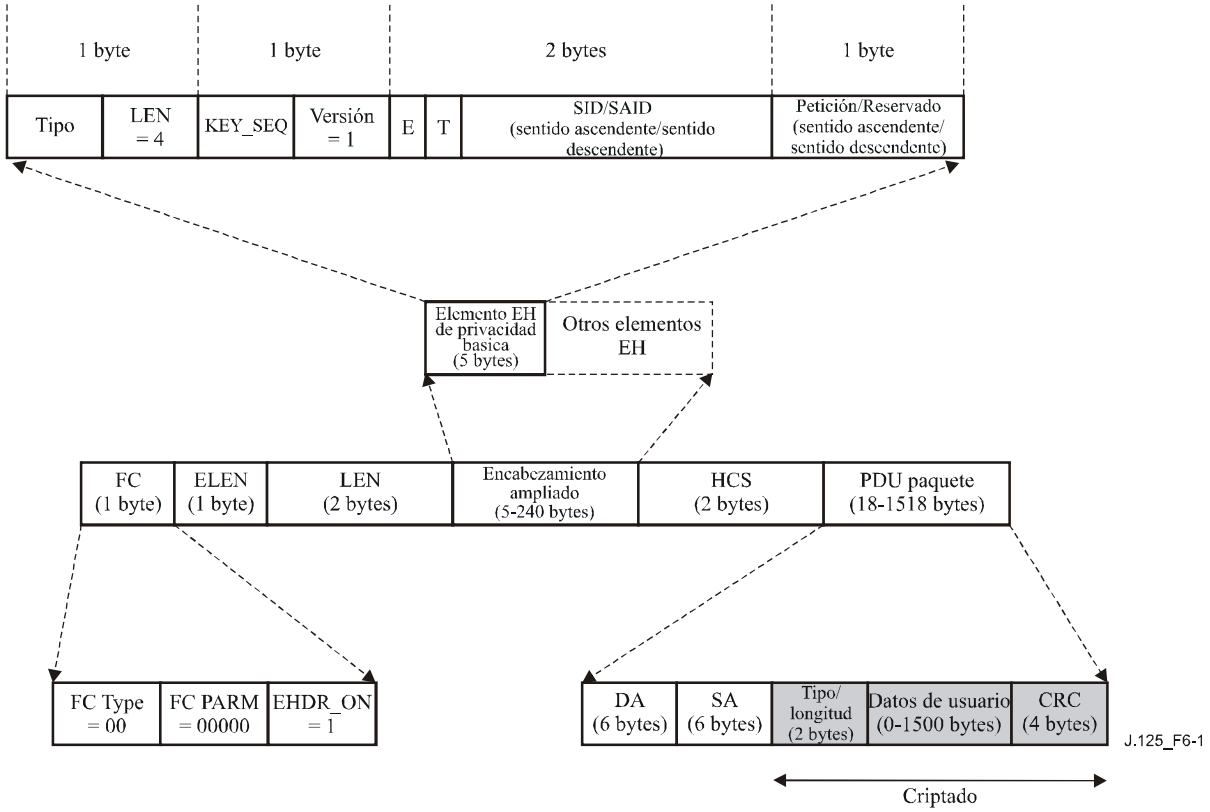


Figura 6-1/J.125 – Formato de PDU datos por paquetes de longitud variable DOCSIS con elemento EH de privacidad

Los 12 primeros octetos de la PDU paquete, que contienen las direcciones de destino y origen (DA/SA, *destination address/source address*) Ethernet/802.3, no son criptados. La transmisión de las direcciones de origen y destino de una trama en claro da a los vendedores un mayor grado de flexibilidad a la hora de integrar la criptación/descriptación con la funcionalidad DOCSIS MAC; por ejemplo, los vendedores pueden optar libremente entre filtrado de DA/SA o de SID primero. La CRC Ethernet/802.3 de la PDU paquete es criptada.

El CMTS incluye el elemento EH de privacidad básica en todas las PDU datos por paquetes en sentido descendente que cripta en el marco de la privacidad de referencia plus. De manera similar, un CM incluye el elemento EH de privacidad básica en todas las PDU datos por paquetes en sentido descendente que cripta en el marco de la privacidad básica plus. Si en el encabezamiento DOCSIS MAC están presentes múltiples elementos encabezamiento ampliado, el elemento encabezamiento ampliado de privacidad básica DEBE ser el primero.

El elemento encabezamiento ampliado de privacidad emplea dos valores de tipo de elemento EH, BPI_UP y BPI_DOWN, a utilizar con las PDU datos por paquetes en sentido ascendente y en sentido descendente, respectivamente. [J.112-B] o [J.122] define los valores de tipos de elemento EH específicos asignados a BPI_UP y BPI_DOWN.

Los 4 bits de orden superior del campo valor de un elemento encabezamiento ampliado de BPI+ contienen un número de secuencia de clave, KEY_SEQ. Se recuerda que el material de aplicación de claves asociado con un SAID de BPI+ tiene un tiempo de vida útil limitado, y que el CMTS renueva periódicamente el material de aplicación de claves de un SAID. El CMTS gestiona un número de secuencia de clave de 4 bits independientemente para de cada SAID y distribuye dicho número de secuencia de clave junto con el material de aplicación de claves del SAID entre los CM clientes. El CMTS incrementa el número de secuencia de clave con cada nueva generación de material de aplicación de claves. El elemento EH de privacidad incluye este número de secuencia,

junto con el SAID, para identificar la generación específica del material de aplicación de claves de ese SAID que está siendo utilizado para criptar la PDU datos por paquetes adjunta. Puesto que se trata de una cantidad expresada con 4 bits, el número de secuencia retorna a 0 cuando llega a 15.

Comparando el número de secuencia de clave de una trama recibida con lo que se piensa que es el número de secuencia de clave "actual", un CM o un CMTS puede reconocer fácilmente una pérdida de sincronización de clave con su elemento par. Un CM DEBE mantener las dos generaciones más recientes de material de aplicación de claves para cada SAID de BPI+. Es preciso tener a mano esas dos generaciones más recientes para que el servicio permanezca ininterrumpido durante la transición de clave de un SAID.

Los 4 bits que siguen a KEY_SEQ contienen un número de versión de protocolo. Dicho número se fija a 1 en los encabezamientos MAC de PDU datos por paquetes de longitud variable DOCSIS.

Los dos bytes siguientes contienen los 2 bits de situación de criptación y el SID/SAID de 14 bits (SID para tramas en sentido ascendente, SAID para tramas en sentido descendente). El bit de situación de criptación HABILITAR indica si la criptación está habilitada o inhabilitada para esa PDU. Si el bit HABILITAR es 0, la PDU datos por paquetes no está criptada y el elemento EH de privacidad básica DEBE ser ignorado (salvo en el caso de la petición de anchura de banda básica porteada opcional, véase más adelante). El bit BASCULAR DEBE concordar con el estado del bit menos significativo (LSB, *least significant bit*) de KEY_SEQ, el número de secuencia de clave.

El protocolo DOCSIS MAC [J.112-B] o [J.122] define un elemento EH de petición para el adosamiento de una petición de anchura de banda en una transmisión de datos. La privacidad básica define un mecanismo adicional para el adosamiento de peticiones de anchura de banda: el último byte del elemento EH en sentido ascendente de privacidad básica (elemento EH tipo BPI_UP) lleva una petición de atribución de anchura de banda adosada opcional. Si hay una petición adosada, el bit representa el número de miniintervalos solicitados. El SID de 14 bits dentro del elemento EH de privacidad básica en sentido ascendente identifica el ID de servicio al que se aplica la petición de anchura de banda. Si no hay petición adosada dentro del elemento EH de privacidad básica, el byte de petición se fija a 0. Una petición adosada dentro del elemento EH de privacidad básica DEBE ser procesada con independencia de la situación del bit HABILITAR.

En los paquetes en sentido descendente (elemento encabezamiento ampliado tipo BPI_DOWN), el cuarto y último byte está reservado y fijado a cero.

Cuadro 6-1/J.125 – Resumen del contenido de los dos elementos EH de privacidad básica

EH_TYPE	EH_LEN	EH_VALUE
BPI_UP Véase [J.112-B] o [J.122]	4	KEY_SEQ (4 bits), Versión (4 bits), SID (2 bytes), Petición [adosado] (1 byte) [CM → CMTS] Campo KEY_SEQ (4 bits): Número de secuencia de clave Campo versión (4 bits) definido como: 0x1 Campo SID definido como: Bit[15]: HABILITAR: 1..Criptación habilitada; 0..Criptación inhabilitada Bit[14]: BASCULAR: 1..Clave impar; 0..Clave par Bit[13:0]: ID de servicio. El campo petición contiene el número de miniintervalos solicitados para anchura de banda en sentido ascendente.
BPI_DOWN Véase [J.112-B] o [J.122]	4	KEY_SEQ (4 bits), Versión (4 bits), SID (2 bytes), Reservado (1 byte) [CMTS → CM] Campo KEY_SEQ (4 bits): Número de secuencia de clave Campo versión (4 bits) definido como: 0x1 Campo SAID definido como: Bit[15]: HABILITAR: 1..Criptación habilitada; 0..Criptación inhabilitada Bit[14]: BASCULAR: 1..Clave impar; 0..Clave par Bit[13:0]: ID de asociación de seguridad. Campo reservado fijado a 0.

En el caso de las PDU datos por paquetes criptadas transmitidas en un intervalo de contienda de datos en sentido ascendente, el SID del elemento EH de privacidad básica DEBE identificar el SID de QoS; NO DEBE fijarse al ID de servicio de multidifusión del intervalo de contienda petición/datos.

6.2 Formato de trama MAC de fragmentación

Para soportar la fragmentación de tramas DOCSIS MAC en sentido ascendente, DOCSIS 1.1 o DOCSIS 2.0 ha reconstruido el elemento EH de privacidad básica de modo que lleve campos control de criptación y control de fragmentación [J.112-B] o [J.122]. Cuando desempeña este doble cometido, el elemento EH de privacidad básica (elemento EH tipo BPI_UP) se amplía en un byte, sirviendo el byte final como campo de control de la fragmentación. La figura 6-2 muestra el formato de una trama DOCSIS MAC de fragmentación con una cabida útil de fragmentación criptada.

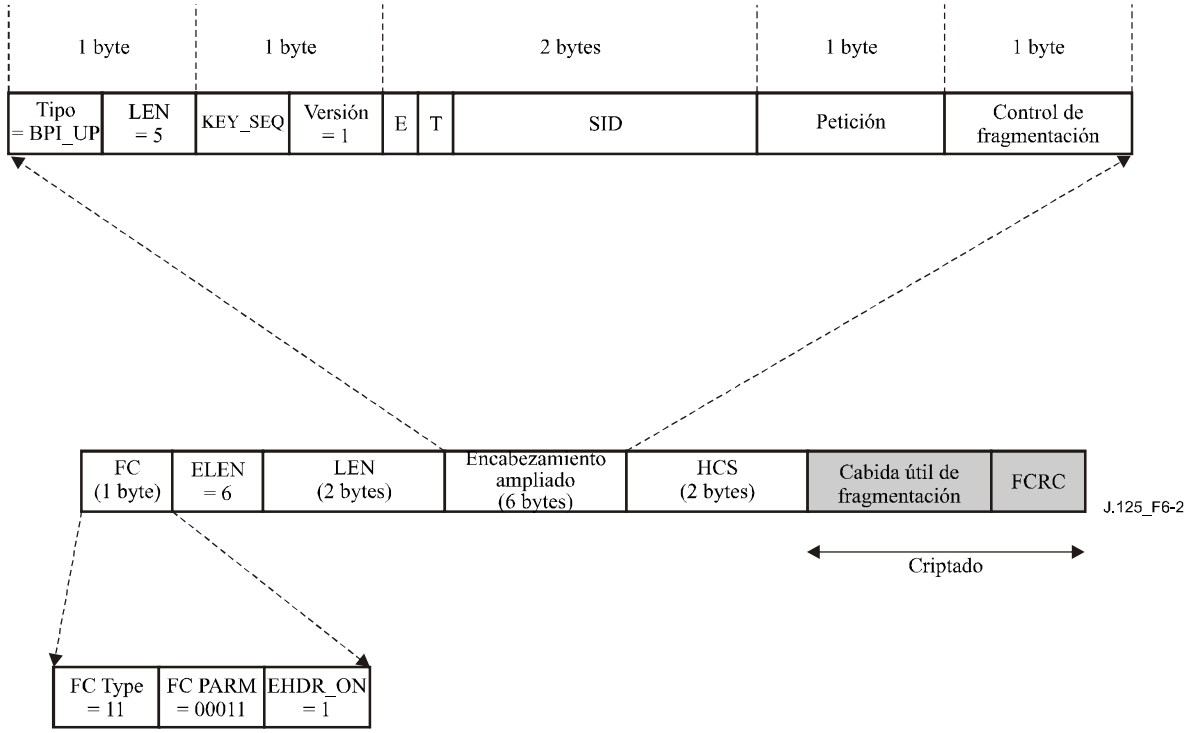


Figura 6-2/J.125 – Formato de una trama DOCSIS MAC de fragmentación con una cabida útil criptada

Un FC_Type = 11 y un FC_PARM = 00011 identifican una trama DOCSIS MAC como trama de fragmentación. A diferencia de las tramas MAC de PDU datos por paquetes, las tramas MAC de fragmentación tienen un encabezamiento ampliado MAC de tamaño fijo (6 bytes) que contiene el elemento EH de privacidad básica "estirado".

El encabezamiento MAC de fragmentación va seguido por una cabida útil de fragmentos y una CRC de fragmentos. Cuando se aplica la criptación de privacidad básica a una trama MAC de fragmentación, se cripta la cabida útil de fragmentos en su *totalidad* junto con la CRC de fragmento. En otras palabras, al contrario que en la criptación de privacidad básica de las PDU datos por paquetes, no hay un desplazamiento de 12 bytes en la cabida útil antes de empezar la criptación[3].

El campo LEN del elemento EH de privacidad básica de las tramas MAC de fragmentación es de 5 bytes en vez de 4, con lo que se tiene en cuenta el campo control de fragmentación adicional de 1 byte. El campo KEY_SEQ, el campo VERSION, las banderas HABILITAR y BASCULAR y el campo SID son tal como serían en una trama MAC de PDU datos por paquetes en sentido ascendente.

[3] En el caso de tramas no fragmentadas, los primeros 12 bytes se dejan en claro para hacer posible un filtrado de DA/SA previo a la descriptación. Si las tramas están fragmentadas, el filtrado de DA/SA no puede tener lugar antes del reensamblado de paquetes; por tanto, no tiene sentido soportar el desplazamiento de la criptación de 12 bytes en tramas DOCSIS MAC de fragmentación.

Cuadro 6-2/J.125 – Contenido del elemento EH de privacidad básica de una trama DOCSIS MAC de fragmentación

EH_TYPE	EH_LEN	EH_VALUE
BPI__UP Véase [J.112-B] o [J.122]	5	KEY_SEQ (4 bits), Versión (4 bits), SID (2 bytes), Petición [adosado] (1 byte), Control de fragmentación (1 byte) [CM → CMTS] Campo KEY_SEQ (4 bits): Número de secuencia de clave Campo versión (4 bits) definido como: 0x1 Campo SID definido como: Bit[15]: HABILITAR: 1..Criptación habilitada; 0..Criptación inhabilitada Bit[14]: BASCULAR: 1..Clave impar; 0..Clave par Bit[13:0]: ID de servicio. El campo petición contiene el número de miniintervalos solicitados para anchura de banda en sentido ascendente. El campo control de fragmentación contiene información de control específica de la fragmentación; véase [J.112-B] o [J.122] para más detalles.

El funcionamiento de la fragmentación invalida la BPI+ en el sentido de que el CM debe determinar primero si un paquete será o no fragmentado en base al tamaño de la concesión (el número de miniintervalo que un CMTS concede a un CM en un MAP de atribución de anchura de banda en sentido ascendente [J.112-B] o [J.122]). Si el paquete ha de ser fragmentado, la criptación de BPI+ DEBE producirse fragmento por fragmento, y no en la PDU como un todo; cada fragmento tendrá su propio encabezamiento de fragmentación y será criptado por separado. Si el paquete no ha de ser fragmentado, DEBE ser criptado como una sola unidad, con un encabezamiento de privacidad único.

6.3 Requisitos para la utilización de un elemento encabezamiento ampliado de privacidad básica en un encabezamiento MAC

Si BPI+ no está habilitada en un determinado flujo de tráfico en sentido descendente (por ejemplo, el tráfico de unidifusión de un CM o un determinado grupo de multidifusión IP), NO DEBERÍA ser utilizado el elemento encabezamiento ampliado de privacidad básica (BP).

Si BPI+ no está habilitada para el tráfico de unidifusión de un CM, las tramas en sentido ascendente fragmentadas DEBEN utilizar aún el elemento encabezamiento ampliado de BP, con el bit HABILITAR criptación desactivado (0). De esta forma, el encabezamiento ampliado de BP todavía puede utilizarse para peticiones de anchura de banda porteadas de conformidad con las reglas de fragmentación descritas en [J.112-B] o [J.122].

En el caso de tramas MAC que constan sólo de un encabezamiento MAC y EHDR opcional, la privacidad básica DEBE estar inhabilitada. Un EHDR de privacidad básica PUEDE estar presente en esas tramas, pero el bit de habilitación DEBE ser desactivado para inhabilitar la privacidad.

7 Protocolo de gestión de claves de privacidad básica (BPKM)

7.1 Modelos de estados

7.1.1 Introducción

El protocolo BPKM se especifica mediante dos modelos de estados separados pero independientes: un modelo de estados de autorización (la máquina de estados autorización) y un modelo de estados

de clave de servicio operativa (la clave de criptación de tráfico, o máquina de estados *TEK*). En esta cláusula se definen ambos modelos de estados. Los modelos de estados sólo tienen una finalidad explicatoria, y no deben interpretarse en el sentido de que imponen una implementación determinada.

La autorización de un módem de cable, controlada por la máquina de estados autorización, es el proceso por el cual:

- El CMTS autentica la identidad de un CM cliente.
- El CMTS proporciona al CM autenticado una clave de autorización, de la que se deriva una clave de criptación de claves (KEK, *key encryption key*) y claves de autenticación de mensajes.
- El CMTS proporciona al CM autenticado las identidades (es decir, los SAID) y las propiedades de asociaciones de seguridad primarias y estáticas respecto a las que el CM está autorizado a obtener información sobre aplicación de claves.

La KEK es una clave de criptación DES triple de dos claves que utiliza el CMTS para criptar las claves de criptación de tráfico (TEK) que envía al módem. Las claves de criptación de tráfico se utilizan para criptar tráfico de datos de usuario. El CM y el CMTS utilizan claves de autenticación de mensajes para autenticar, vía compendio de mensajes con clave, las peticiones de clave y las respuestas que intercambian.

Tras conseguir la autorización inicial, el módem de cable solicita de manera periódica la reautorización, en el CMTS, reautorización gestionada también por la máquina de estados autorización del CM. Un CM DEBE mantener su situación de autorización en el CMTS para poder renovar las claves de criptación de tráfico que vayan prescribiendo. Las máquinas de estados TEK gestionan la renovación de las claves de criptación de tráfico.

Un módem de cable comienza el proceso de autorización enviando un mensaje información de autenticación a su CMTS. El mensaje información de autenticación contiene el certificado X.509 del fabricante del módem de cable. Se trata de un mensaje estrictamente informativo, es decir, el CMTS puede optar por ignorarlo; sin embargo, representa un mecanismo mediante el cual el CMTS se entera de los certificados de fabricante de sus CM clientes.

El módem de cable envía un mensaje petición de autorización a su CMTS inmediatamente después de enviar el mensaje información de autenticación. Es una petición de clave de autorización, así como de los SAID que identifican cualesquiera asociaciones de seguridad estáticas en las que el CM está autorizado a participar. La petición de autorización incluye:

- el ID del fabricante y el número de serie del módem de cable;
- la dirección MAC del módem de cable;
- la clave pública del módem de cable;
- un certificado X.509 expedido por el fabricante que vincula la clave pública del módem de cable al resto de su información identificadora;
- una descripción de los algoritmos criptográficos que soporta el módem de cable solicitante; las capacidades criptográficas de un CM se presentan al CMTS como una lista de identificadores de series criptográficas, cada una de las cuales indica un determinado emparejamiento de los algoritmos de criptación de datos por paquetes y autenticación de datos por paquetes que soporta el CM;
- el SAID primario del módem de cable, *que es igual al SID primario del CM* (el SID primario es el primer SID estático que el CMTS asigna a un CM durante el registro MAC de RF).

En respuesta a un mensaje petición de autorización, si un CMTS valida la entidad del CM solicitante y determina el algoritmo de criptación y el soporte de protocolos que comparte con el

CM, el CMTS DEBE activar una clave de autorización para el CM, la cripta con la clave pública del módem de cable y la devuelve al CM en un mensaje respuesta de autorización. La respuesta de autorización incluye:

- una clave de autorización criptada con la clave pública del CM;
- un número de secuencia de clave de 4 bits, utilizado para distinguir entre generaciones sucesivas de claves de autorización;
- el tiempo de vida de una clave;
- las identidades (es decir, los SAID) y las propiedades de la única asociación de seguridad primaria y las cero o más asociaciones de seguridad estáticas respecto a las que el CM está autorizado a obtener información sobre aplicación de claves.

Si el CMTS soporta SA estáticas, la respuesta de autorización al CM DEBE identificar SA estáticas asociadas con el CM, además de la SA primaria cuyo SAID concuerda con el SID de mejor esfuerzo del CM solicitante. La respuesta de autorización NO DEBE identificar ninguna SA dinámica.

El CMTS determinará, al responder a la petición de autorización de un CM, si el módem de cable solicitante, cuya identidad se puede verificar mediante el certificado digital X.509, está autorizado para servicios de unidifusión básicos, y a qué otros servicios prestados estáticamente (es decir, los SAID estáticos) está abonado el usuario del módem de cable.

NOTA 1 – Los servicios protegidos que un CMTS pone a disposición de un CM cliente pueden depender de las series criptográficas particulares cuyo soporte comparten el CM y el CMTS.

Tras conseguir la autorización, el CM pone en marcha una máquina de estados TEK distinta por cada SAID identificado en el mensaje respuesta de autorización. Cada máquina de estados TEK que funciona dentro del CM es responsable de la gestión del material de aplicación de claves asociado con su correspondiente SAID. Las máquinas de estados TEK envían periódicamente mensajes de petición de clave al CMTS, solicitando la renovación del material de aplicación de claves para sus SAID respectivos. Una petición de clave incluye:

- información de identificación exclusiva del módem de cable, consistente en el ID del fabricante, el número de serie, la dirección MAC y la clave pública RSA;
- el SAID cuyo material de aplicación de claves se está solicitando;
- un compendio de mensajes con clave HMAC, con el que se autentica la petición de clave.

El CMTS DEBE responder a un mensaje de petición de clave con un mensaje respuesta de clave que contiene el material de aplicación de claves activo del CMTS para un SAID específico, si el CMTS valida el compendio HMAC del mensaje de petición de clave, la identidad del CM solicitante y el SAID. Dicho material incluye:

- la clave de criptación de tráfico criptada según DES triple;
- un vector de inicialización del CBC;
- un número de secuencia de clave;
- el tiempo de vida restante de una clave;
- un mensaje con clave HMAC, con el que se autentica la respuesta de clave.

La clave de criptación de tráfico (TEK) de la respuesta de clave se cripta según DES triple (criptación-descriptación-criptación o modo EDE), utilizando una clave de criptación de claves (KEK) de DES triple de dos claves derivada de la clave de autorización.

NOTA 2 – El CMTS mantiene en todo momento dos conjuntos activos de material de aplicación de claves por cada SAID. Los tiempos de vida de las dos generaciones se superponen de tal manera que cada generación pasa a estar activa a mitad de la vida activa de su predecesora y prescribe a mitad de la de su sucesora. Un CMTS incluye en sus respuestas de clave las *dos* generaciones activas de material de aplicación de claves de un SAID.

La respuesta de clave proporciona al solicitante, además de la TEK y el vector de inicialización del CBC, el resto del tiempo de vida de cada uno de los dos conjuntos de material de aplicación de claves. El CM receptor utiliza esos tiempos de vida restantes para estimar cuándo invalidará el CMTS una TEK determinada y, por tanto, para cuándo ha de programar futuras peticiones de clave de tal manera que sus peticiones y recepciones de nuevo material de aplicación de claves se produzcan antes de que el CMTS haga que prescriba el material de ese tipo de claves que a la sazón retiene el CM.

El funcionamiento del algoritmo de programación de peticiones de clave de la máquina de estados TEK, combinado con el procedimiento del CMTS de actualización y utilización del material de aplicación de claves de un SAID (véase la cláusula 9), asegura que el CM podrá intercambiar continuamente tráfico criptado con el CMTS.

Un CM DEBE renovar periódicamente su clave de autorización reenviando una petición de autorización al CMTS. La reautorización es idéntica a la autorización con la salvedad de que el CM no envía mensajes información de autenticación durante los ciclos de reautorización. En la descripción de la máquina de estados autorización (véase 7.1.2) se indica claramente cuándo se envían los mensajes información de autenticación.

Para evitar interrupciones del servicio durante la reautorización, se superponen los tiempos de vida de las generaciones sucesivas de claves de autorización del CM. Tanto el CM como el CMTS DEBEN poder soportar hasta dos claves de autorización activas simultáneamente durante esos periodos de transición. El funcionamiento del algoritmo de programación de peticiones de autorización de la máquina de estados autorización, junto con el procedimiento del CMTS de actualización y utilización de las claves de autorización de un CM cliente (véase la cláusula 9), asegura que los CM podrán renovar la información de aplicación de claves TEK sin interrupción mientras transcurren los periodos de reautorización del CM.

Una máquina de estados TEK permanece activa siempre que:

- el CM esté autorizado para funcionar en el dominio de seguridad del CMTS; es decir, tiene una clave de autorización válida, *y*
- el CM esté autorizado para participar en esa asociación de seguridad particular; es decir, el CMTS continúa proporcionando material de aplicación de claves renovado durante los ciclos de nueva aplicación de clave.

La máquina de estados autorización progenitora detiene *todas* sus máquinas de estados TEK vástagos cuando el CM recibe del CMTS un rechazo de autorización durante un ciclo de reautorización. Se pueden arrancar o detener máquinas de estados TEK específicas durante un ciclo de reautorización si las autorizaciones de SAID estático de un CM cambian durante reautorizaciones sucesivas.

La comunicación entre máquinas de estados autorización y TEK se produce mediante el traspaso de eventos y la mensajería de protocolos. La máquina de estados autorización genera eventos (esto es, los eventos parada, autorizado, autorización pendiente y autorización completa) a los que se dirigen sus máquinas de estados TEK vástagos. Las máquinas de estados TEK no trabajan con eventos de su máquina de estados autorización progenitora. La máquina de estados TEK afecta a la máquina de estados autorización indirectamente por los mensajes que un CMTS envía en respuesta a las peticiones de un módem: un CMTS PUEDE responder a las peticiones de clave de una máquina TEK con una respuesta de fallo (es decir, mensaje de autorización no válida) que será tratada por la máquina de estados autorización.

7.1.1.1 Comentario preliminar sobre las asociaciones de seguridad dinámicas y el establecimiento de la correspondencia de las SA dinámicas

En la cláusula 5 se presentan las SA dinámicas y se menciona la manera según la cual un CMTS puede establecer o eliminar una SA dinámica en respuesta a la iniciación o terminación de flujos de

tráfico en sentido descendente (por ejemplo, el tráfico de un determinado grupo de multidifusión IP). Para que un CM utilice una máquina de estados TEK a fin de obtener el material de aplicación de claves de una asociación de seguridad dinámica, el CM ha de conocer cuál es el valor del SAID correspondiente. El CMTS, sin embargo, no manifiesta a los CM clientes de forma voluntaria la existencia de las SA dinámicas; por el contrario, corresponde a los CM pedir al CMTS las correspondencias entre identificadores de flujo de tráfico (por ejemplo, una dirección de multidifusión IP) y SAID dinámicos.

La BPI+ define el intercambio de mensajes mediante el cual un CM se entera del establecimiento de la correspondencia entre un flujo de tráfico en sentido descendente y una SA dinámica (todo el tráfico en sentido ascendente se cripta de conformidad con la SA primaria del CM). Una máquina de estados establecimiento de correspondencia de SA especifica cómo gestionan los módems de cable la transmisión de esos mensajes de petición de establecimiento de correspondencia. En la actualidad, sólo los servicios de gestión de multidifusión IP de DOCSIS utilizan este mecanismo. En el futuro, nuevos servicios pueden emplear SA dinámicas de BPI+.

La máquina de estados autorización controla el establecimiento y la terminación de las máquinas de estados TEK asociadas con la SA primaria y cualesquiera SA estáticas; no controla, sin embargo, el establecimiento y la terminación de las máquinas de estados TEK asociadas con SA dinámicas. Los CM DEBEN implementar la lógica necesaria para establecer y terminar la máquina de estados TEK de una SA dinámica. De todos modos, la presente especificación de interfaz no especifica cómo deberían gestionar los CM sus máquinas de estados TEK de SA dinámica.

La descripción completa del modelo de estados establecimiento de correspondencia de SA se pospone hasta la cláusula 8.

7.1.1.2 Selección de capacidades de seguridad

Como parte de su intercambio de autorización BPI+, el CM proporciona al CMTS una lista de todas las series criptográficas (emparejamiento de algoritmos de criptación de datos y de autenticación de datos) que soporta el CM. El CMTS selecciona de esa lista una sola serie criptográfica para emplearla con la SA primaria del CM solicitante. La respuesta de autorización que el CMTS devuelve al CM incluye un descriptor de SA primaria que, entre otras cosas, identifica la serie criptográfica que el CMTS seleccionó para utilizarla con la SA primaria del CM. Un CMTS DEBE rechazar la petición de autorización si determina que ninguna de la series criptográficas ofrecidas es satisfactoria.

La respuesta de autorización contiene también una lista facultativa de descriptores de SA estáticas; cada descriptor de SA estática identifica la serie criptográfica empleada dentro de la SA. La selección de la serie criptográfica de una SA estática se lleva a cabo normalmente con independencia de las capacidades criptográficas del CM solicitante. Un CMTS PUEDE incluir en su respuesta de autorización descriptores de SA estáticas que identifiquen series criptográficas que el CM solicitante no soporta. Si tal es el caso, el CM NO DEBE arrancar las máquinas de estados TEK para SA estáticas cuyas series criptográficas no soporta.

El marco de selección anterior se incorporó en BPI+ para soportar perfeccionamientos futuros del soporte físico basado en DOCSIS y del protocolo BPI+. En el momento de publicarse la presente especificación, los únicos algoritmos de criptación de datos por paquetes soportados eran DES de 56 bits y DES de 40 bits, y ninguno de ellos está emparejado con un algoritmo de autenticación de datos por paquetes.

7.1.2 Máquina de estados autorización

La máquina de estados autorización consta de seis estados y ocho eventos distintos (incluida la recepción de mensajes) que pueden provocar transiciones de estados. La máquina de estados finitos (FSM, *finite state machine*) autorización se presenta más adelante con formato gráfico, como un

modelo de flujos de estados (figura 7-1) y con formato tabular, como una matriz de transiciones de estados (cuadro 7-1).

El diagrama de flujos de estados muestra los mensajes de protocolo transmitidos y los eventos internos generados para cada una de las transiciones de estados del modelo; sin embargo, el diagrama no indica acciones internas adicionales, tales como la detención o el arranque de temporizadores, que acompañan a las transiciones de estados específicas. La matriz de transiciones de estados que se adjunta es una descripción detallada de las acciones específicas que se efectúan junto con cada transición de estado; la matriz de transiciones de estados DEBE ser utilizada como la especificación definitiva de las acciones de protocolo asociadas con cada transición de estado.

En el diagrama de flujos de la máquina de estados autorización que se muestra en la figura 7-1 se han aplicado las reglas de representación siguientes:

- Los óvalos representan estados.
- Los eventos están en letra *cursiva*.
- Los mensajes están en letra de tipo normal.
- Las transiciones de estados (es decir, las líneas entre estados) se han etiquetado con <lo que provoca la transición>/<mensajes y eventos provocados por la transición>. Así pues "*temporización*/petición autoriz." significa que el estado ha recibido un evento "temporización" y ha enviado un mensaje petición de autorización ("petición autoriz."). Si hay múltiples eventos o mensajes antes de "/" separados por una coma, *cualquiera* de ellos puede provocar una transición. Si hay múltiples eventos o mensajes tras la barra inclinada, *todas* las acciones especificadas deben acompañar a la transición.

La matriz de transiciones de estados de autorización presentada en el cuadro 7-1 contiene siete máquinas de estados autorización en la fila superior y ocho eventos de máquina de autorización (incluidas las recepciones de mensajes) en la columna situada más a la izquierda. Cualquier casilla de la matriz representa una combinación específica de estado y evento, mostrándose dentro de la casilla el estado siguiente (el estado al que se transita). Por ejemplo, la casilla 4-B representa la recepción de un mensaje respuesta de autorización (respuesta autoriz.) cuando se está en el estado espera de autorización (espera autoriz.). Dentro de la casilla 4-B figura el nombre del estado siguiente, "autorizado". Así pues, cuando la máquina de estados autorización de un CM está en el estado espera de autorización y se recibe el mensaje respuesta de autorización, la máquina de estados autorización pasa al estado autorizado. Junto con esta transición de estado deben llevarse a cabo varias acciones, que se describen en la relación de acciones de protocolo que figura bajo el epígrafe 4-B de 7.1.2.5.

Una célula sombreada en la matriz de transiciones de estados significa que el evento de que se trate no puede o no debe ocurrir dentro de ese estado, y que si el evento se produce, la máquina de estados DEBE ignorarlo. Por ejemplo, si llega un mensaje respuesta de autorización cuando se está en el estado autorizado, dicho mensaje debería ser ignorado (casilla 4-C). El CM PUEDE, no obstante, en respuesta a un evento inapropiado, registrar cronológicamente su ocurrencia, generar un evento SNMP o efectuar cualquier otra acción definida por el vendedor. Ahora bien, esas acciones no se especifican dentro del contexto de la máquina de estados autorización, que simplemente ignora los eventos improcedentes.

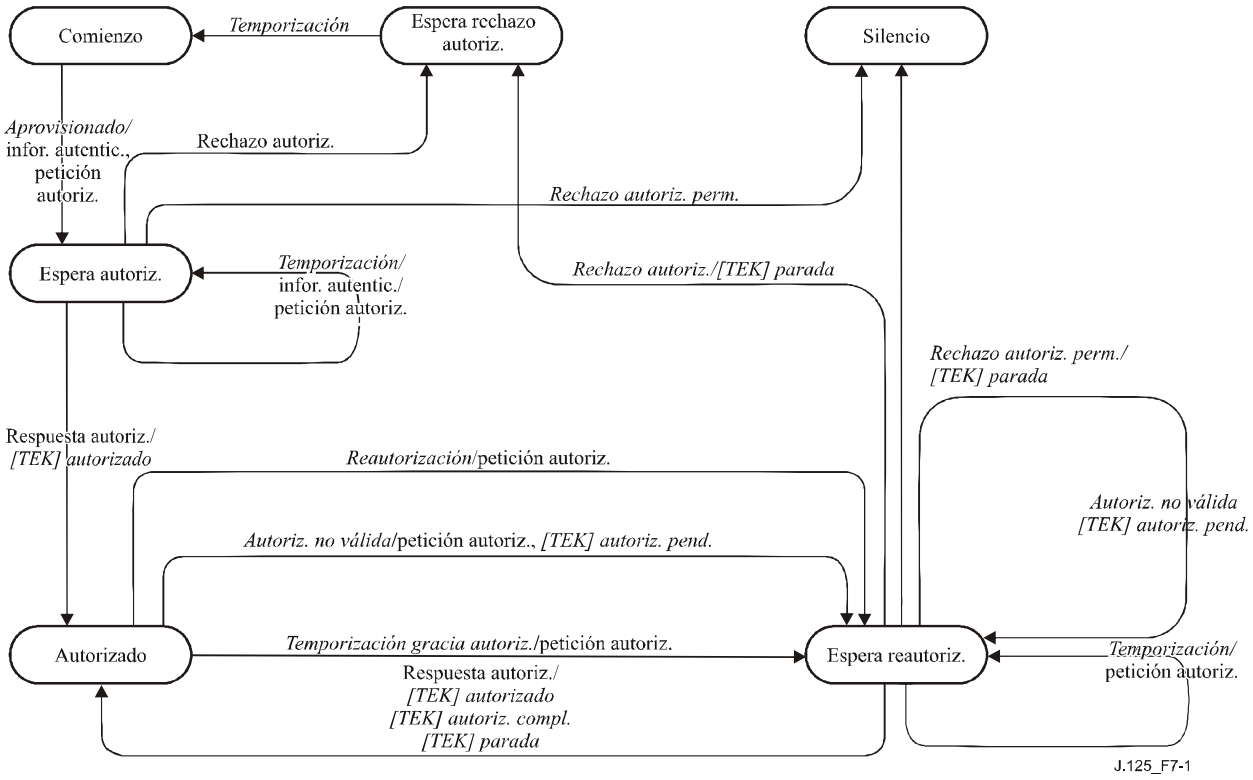


Figura 7-1/J.125 – Diagrama de flujos de la máquina de estados autorización

Cuadro 7-1/J.125 – Matriz de transición de estados de FSM autorización

Estado / ***Evento o mensaje recibido***	**(A) Comienzo**	**(B) Espera autoriz.**	**(C) Autorizado**	**(D) Espera reautoriz.**	**(E) Espera rechazo autoriz.**	**(F) Silencio**
(1) Aprovisionado	Espera autoriz.					
(2) Rechazo autoriz.		Espera rechazo autoriz.		Espera rechazo autoriz.		
(3) Rechazo autoriz.		Silencio		Silencio		
(4) Respuesta autoriz.		Autorizado		Autorizado		
(5) Temporización		Espera autoriz.		Espera reautoriz.	Comienzo	
(6) Temporización gracia autoriz.			Espera reautoriz.			
(7) Autoriz. no válida			Espera reautoriz.	Espera reautoriz.		
(8) Reautoriz.			Espera reautoriz.			

7.1.2.1 Estados

7.1.2.1.1 Comienzo

Éste es el estado inicial de la máquina de estados finitos (FSM). No hay ningún recurso asignado a la FSM, ni utilizado por la misma, en este estado; por ejemplo, todos los temporizadores están desactivados, y no está programado ningún procesamiento.

7.1.2.1.2 Espera de autorización (espera autoriz.)

El CM ha recibido el evento "aprovisionado" que indica que ha completado el registro MAC de RF en el CMTS. En respuesta a la recepción del evento, el CM ha enviado un mensaje información de autenticación y un mensaje petición de autorización al CMTS y está esperando la respuesta.

7.1.2.1.3 Autorizado

El CM ha recibido un mensaje respuesta de autorización que contiene una lista de SAID válidos para ese CM. En este momento, el módem tiene una clave de autorización y una lista de SAID válidos. La transición a este estado provoca la creación de una FSM TEK para cada uno de los SAID de privacidad habilitada del CM.

7.1.2.1.4 Espera de reautorización (espera reautoriz.)

El CM tiene una petición de reautorización pendiente. El CM estaba a punto de agotar el tiempo de su autorización actual o había recibido una indicación (un mensaje autorización no válida del CMTS) de que su autorización ya no era válida. El CM envió un mensaje petición de autorización al CMTS y está esperando la respuesta.

7.1.2.1.5 Espera de rechazo de autorización (espera rechazo autoriz.)

El CM recibió un mensaje rechazo de autorización en respuesta a su última petición de autorización. El código de error del rechazo de autorización indicaba que el error no era de carácter permanente. En respuesta a la recepción de este mensaje de rechazo, el CM fijó un temporizador y transitó al estado espera de rechazo de autorización. El CM permanece en este estado hasta que expira el temporizador.

7.1.2.1.6 Silencio

El CM recibió un mensaje rechazo de autorización en respuesta a su última petición de autorización. El código de error del rechazo de autorización indicaba que el error era de carácter permanente. Esto provocó la transición al estado silencio. En el estado de silencio el CM NO DEBE transferir tráfico CPE, pero DEBE ser capaz de responder a peticiones de gestión SNMP que lleguen procedentes de toda la red de cable. El CMTS PUEDE decidir el envío de tráfico de datos a un CM que se encuentre en el estado de silencio sin cifrar, o el CMTS PUEDE bloquear ese tráfico.

7.1.2.2 Mensajes

Los formatos de los mensajes se definen con detalle en la cláusula 7.2.

7.1.2.2.1 Petición de autorización (petición autoriz.)

Petición de una clave de autorización y de una lista de SAID autorizados. Enviado del CM al CMTS.

7.1.2.2.2 Respuesta de autorización (respuesta autoriz.)

Recepción de una clave de autorización y de una lista SAID autorizados y estáticos. Enviado del CMTS al CM. La clave de autorización es criptada con la clave pública del CM.

7.1.2.2.3 Rechazo de autorización (rechazo autoriz.)

La tentativa de autorización es rechazada. Enviado del CMTS al CM.

7.1.2.2.4 Autorización no válida (autoriz. no válida)

El CMTS puede enviar un mensaje autorización no válida a un CM cliente como:

- una indicación no solicitada, o
- una respuesta a un mensaje recibido de ese CM.

En cualquier caso, el mensaje autorización no válida ordena al CM receptor que obtenga una nueva autorización de su CMTS.

El CMTS DEBE responder a una petición de clave con un mensaje autorización no válida, si:

1) no reconoce que el CM está siendo autorizado (es decir, no hay ninguna clave de autorización válida asociada con el módem de cable); o
2) falla la verificación del compendio de mensajes con clave de la petición de clave (en el atributo compendio de HMAC).

NOTA – El evento autorización no válida, al que se hace referencia en el diagrama de flujos de estados y en la matriz de transiciones de estados, significa la recepción de un mensaje autorización no válida o un evento generado internamente.

7.1.2.2.5 Información de autenticación (infor. autentic.)

El mensaje información de autenticación contiene el certificado X.509 del fabricante del módem expedido por DOCSIS. Es un mensaje estrictamente informativo que el CM envía al CMTS; con él, un CMTS PUEDE enterarse dinámicamente del certificado del fabricante de los CM clientes. De manera alternativa, el CMTS PUEDE requerir una configuración fuera de banda de su lista de certificados de fabricante.

7.1.2.3 Eventos

7.1.2.3.1 Aprovisionado

La máquina de estados autorización genera este evento tras pasar al estado comienzo si el MAC de RF ha completado la inicialización, es decir, el registro en el CMTS. Si la inicialización del MAC de RF no se ha completado, el CM envía un evento aprovisionado a la FSM autorización tras completar el registro en el CMTS. El evento aprovisionado hace que el CM inicie el proceso de obtención de su clave de autorización y sus TEK.

7.1.2.3.2 Temporización

Ha concluido la temporización de un temporizador de retransmisión o espera. Por lo general se reenvía una petición.

7.1.2.3.3 Temporización de gracia de autorización (temporización gracia autoriz.)

Ha concluido la temporización del temporizador de periodo de gracia de autorización. Este temporizador fija una duración de tiempo configurable (el tiempo de gracia de autorización) antes de que la autorización en curso prescriba según lo previsto, indicando al CM que obtenga una nueva autorización antes de que su autorización prescriba efectivamente. El tiempo de gracia de autorización se especifica en una fijación de configuración dentro del fichero de parámetros telecargado vía TFTP.

7.1.2.3.4 Reautorización (reautoriz.)

El conjunto de SAID estáticos autorizados del CM puede haber cambiado. Este evento se genera en respuesta a un conjunto del SNMP, [DOCSIS8], que tiene por objeto activar un ciclo de reautorización.

7.1.2.3.5 Autorización no válida (autoriz. no válida)

Este evento puede ser generado internamente por el CM cuando se produce el fallo de autenticación de un mensaje respuesta de clave, rechazo de clave o TEK no válida, o generado externamente por la recepción de un mensaje autorización no válida, enviado del CMTS al CM. Un CMTS responde a una petición de clave con un mensaje autorización no válida si falla la verificación del código de autenticación de mensajes de la petición. Ambos casos indican que el CMTS y el CM han perdido la sincronización de la clave de autorización.

Un CMTS PUEDE enviar también a un CM un mensaje autorización no válida no solicitado, forzando un evento autorización no válida.

7.1.2.3.6 Rechazo de autorización permanente (rechazo autoriz. perm.)

El CMTS DEBE enviar un mensaje de rechazo de autorización con el código de error 6 (rechazo de autorización permanente) en respuesta a un mensaje de petición de autorización en cualesquiera de los casos siguientes:

- Fracaso en la validación del certificado de CM según 12.4.2 (es decir, el certificado de CM está marcado como no válido).
- Capacidades de seguridad incompatibles.

El documento OSS asociado con BPI+ [DOCSIS8] proporciona una descripción de los objetos MIB de CMTS que controlan las decisiones que adopta el CMTS en el caso en que se produzca cualquier condición de error descrita anteriormente.

Cuando un CM recibe un rechazo de autorización que indique una condición de fallo permanente, la máquina de estados de autorización pasa al estado de silencio. Los CM DEBEN emitir un evento DOCSIS al entrar en el estado de silencio.

7.1.2.3.7 Rechazo de autorización (rechazo autoriz.)

El CM recibe un mensaje rechazo de autorización en respuesta a un mensaje petición de autorización. El código de error del rechazo de autorización no indica que el fallo se deba a una condición de error permanente. Como resultado de ello, la máquina de estados de autorización del CM fija un temporizador de espera y transita al estado espera de rechazo de autorización. El CM permanece en este estado hasta que expire el temporizador, en cuyo momento volverá a intentar la autorización.

NOTA – Los eventos que siguen son enviados por la máquina de estados autorización a la máquina de estados TEK.

7.1.2.3.8 [TEK] Parada

Enviado por la FSM autorización a una FSM TEK activa (no estado COMIENZO) para terminar la FSM TEK y retirar el material de aplicación de claves del SAID correspondiente del cuadro de claves del CM.

7.1.2.3.9 [TEK] Autorizado

Enviado por la FSM autorización a una FSM TEK no activa (estado COMIENZO), pero válida.

7.1.2.3.10 [TEK] Autorización pendiente (autoriz. pend.)

Enviado por la FSM autorización a una FSM TEK específica para poner la FSM TEK en un estado de espera hasta que la FSM autorización pueda completar su operación de reautorización.

7.1.2.3.11 [TEK] Autorización completa (autoriz. compl.)

Enviado por la FSM autorización a una FSM TEK en los estados espera de reautorización operativa (espera reautoriz. oper.) o espera de reautorización de nueva aplicación de la clave (espera

reautoriz. nueva aplic. clave) para eliminar el estado de espera iniciado por un evento autorización pendiente de la FSM TEK.

7.1.2.4 Parámetros

Todos los valores de los parámetros de la configuración se especifican en el fichero de parámetros telecargado vía TFTP (véase el anexo A: Extensiones de fichero de configuración TFTP).

7.1.2.4.1 Temporización de espera de autorización (temporización espera autoriz.)

Periodo de temporización entre envíos de mensajes petición autorización desde el estado espera de autorización. Véase A.1.1.1.1.

7.1.2.4.2 Temporización de espera de reautorización (temporización espera reautoriz.)

Periodo de temporización entre envíos de mensajes petición de autorización desde el estado espera de reautorización. Véase A.1.1.1.2.

7.1.2.4.3 Tiempo de gracia de autorización (temporización gracia autoriz.)

Periodo de tiempo en que el CM se adelanta a la prescripción prevista de la autorización, comenzando la reautorización. Véase A.1.1.1.3.

7.1.2.4.4 Temporización de espera de rechazo de autorización (temporización espera rechazo autoriz.)

Periodo de tiempo que la FSM autorización de un CM permanece en el estado espera de rechazo de autorización antes de transitar al estado comienzo. Véase A.1.1.1.7.

7.1.2.5 Acciones

Las acciones efectuadas en asociación con transiciones de estados se indican mediante <evento/mensaje recibido> → <estado> en lo que sigue:

1-A Comienzo (*Aprovisionado*) → Espera autoriz.

- enviar mensaje información de autenticación a CMTS;
- enviar mensaje petición de autorización a CMTS;
- fijar temporizador de reintento de petición de autorización a temporización de espera de autorización.

2-B Espera autoriz. (*Rechazo autoriz.*) → Espera rechazo autoriz.

- detener temporizador de reintento de petición de autorización;
- fijar un temporizador de espera a temporización de espera de rechazo de autorización.

2-D Espera reautoriz. (*Rechazo autoriz.*) → Espera rechazo autoriz.

- detener temporizador de reintento de petición de autorización;
- generar eventos parada de FSM TEK para todas las máquinas de estados TEK activas;
- fijar un temporizador de espera a temporización de espera de rechazo de autorización.

3-B Espera autoriz. (*Rechazo autoriz. perm.*) → Silencio

- detener temporizador de reintento de petición de autorización;
- inhabilitar todo reenvío de tráfico CPE.

3-D Espera reautoriz. (*Rechazo autoriz. perm.*) → Silencio

- detener temporizador de reintento de petición de autorización;
- generar eventos parada de FSM TEK para todas las máquinas de estados TEK activas;
- inhabilitar todo reenvío de tráfico CPE.

4-B Espera autoriz. (*Respuesta autoriz.*) → Autorizado

- detener temporizador de reintento de petición de autorización;
- descriptar y registrar la clave de autorización entregada con el mensaje respuesta de autorización;
- arrancar las FSM TEK de todos los SAID indicados en la respuesta de autorización (siempre que el CM soporte la serie criptográfica asociada con cada SAID) y emitir un evento autorizado de FSM TEK por cada una de las FSM TEK nuevas;
- fijar el temporizador de tiempo de gracia de autorización para que arranque "tiempo de gracia de autorización" segundos antes de que se produzca la prescripción prevista de la clave de autorización suministrada.

4-D Espera reautoriz. (*Respuesta autoriz.*) → Autorizado

- detener temporizador de reintento de petición de autorización;
- descriptar y registrar la clave de autorización entregada con el mensaje respuesta de autorización;
- arrancar las FSM TEK correspondientes a cualesquiera SAID recién autorizados indicados en la respuesta de autorización (siempre que el CM soporte la serie criptográfica asociada con cada SAID nuevo) y emitir un evento autorizado de FSM TEK por cada una de las FSM TEK nuevas;
- generar eventos autorización completa de FSM TEK para cualesquiera FSM TEK activas cuyos SAID correspondientes estén indicados en la respuesta de autorización;
- generar eventos parada de FSM TEK para cualesquiera FSM TEK activas a la sazón cuyos SAID correspondientes no estén indicados en la respuesta de autorización;
- fijar el temporizador de tiempo de gracia de autorización para que arranque "tiempo de gracia de autorización" segundos antes de que se produzca la prescripción programada de la clave de autorización suministrada.

5-B Espera autoriz. (*Temporización*) → Espera autoriz.

- enviar mensaje información de autenticación a CMTS;
- enviar mensaje petición de autorización a CMTS;
- fijar temporizador de reintento de petición de autorización a temporización de espera de autorización.

5-D Espera reautoriz. (*Temporización*) → Espera reautoriz.

- enviar mensaje petición de autorización a CMTS;
- fijar temporizador de reintento de petición de autorización a temporización de espera de reautorización.

5-E Espera rechazo autoriz. (*Temporización*) → Comienzo

- ninguna acción de protocolo asociada con la transición de estado.

6-C Autorizado (*Temporización de tiempo de gracia de autoriz.*) → Espera reautoriz.

- enviar mensaje petición de autorización a CMTS;
- fijar temporizador de reintento de petición de autorización a temporización de espera de reautorización.

7-C Autorizado (*Autoriz. no válida*) → Espera reautoriz.

- detener temporizador de tiempo de gracia de autorización;
- enviar mensaje petición de autorización a CMTS;

- fijar temporizador de reintento de petición de autorización a temporización de espera de reautorización;
- si el evento autorización no válida está asociado con una determinada FSM TEK, generar un evento autorización pendiente de FSM TEK para la máquina de estados TEK responsable del evento autorización no válida (es decir, la FSM TEK que generó el evento, o envió el mensaje petición de clave al que el CMTS respondió con un mensaje autorización no válida).

7-D Espera reautoriz. (*Autoriz. no válida*) → Espera reautoriz.

- si el evento autorización no válida está asociado con una determinada FSM TEK, generar un evento autorización pendiente de FSM TEK para la máquina de estados TEK responsable del evento autorización no válida (es decir, la FSM TEK que generó el evento, o envió el mensaje petición de clave al que el CMTS respondió con un mensaje autorización no válida).

8-C Autorizado (*Reautoriz.*) → Espera reautoriz.

- detener temporizador de tiempo de gracia de autorización;
- enviar mensaje de petición de autorización a CMTS;
- fijar temporizador de reintento de petición de autorización a temporización de espera de reautorización.

7.1.3 Máquinas de estados TEK

La máquina de estados TEK consta de seis estados y nueve eventos (incluida la recepción de mensajes) que pueden provocar transiciones de estados. Al igual que la máquina de estados autorización, la máquina de estados TEK se presenta en un diagrama de flujos de estados y una matriz de transiciones de estados y como ocurrió con la máquina de estados autorización, la matriz de transiciones de estados DEBE ser utilizada como especificación definitiva de las acciones de protocolo asociadas con cada transición de estado.

Los estados sombreados de la figura 7-2 (operativo, espera de nueva aplicación de clave y espera de reautorización de nueva aplicación de clave) tienen material de aplicación de claves válido y se puede pasar tráfico criptado.

La máquina de estados autorización arranca una máquina de estados TEK independiente por cada uno de sus SAID autorizados.

Como se mencionó en 7.1.1, el CMTS mantiene dos TEK activas por cada SAID. El CMTS incluye en sus respuestas de clave esas TEK junto con el tiempo de vida restante de las mismas. El CMTS cripta tráfico en sentido descendente con la más antigua de las dos TEK y descripta tráfico en sentido ascendente con la TEK más antigua o más reciente, dependiendo de cuál de las dos claves está utilizando el CM en ese momento. El CM cripta tráfico en sentido ascendente con la más reciente de sus dos TEK y descripta tráfico en sentido descendente con la TEK más antigua o más reciente, dependiendo de cuál de las dos claves está utilizando el CMTS en ese momento. Véase en la cláusula 9 los detalles de los requisitos de utilización de claves por parte del CM y el CMTS.

Mediante el funcionamiento de una máquina de estados TEK, el CM intenta guardar sus copias de las TEK de un SAID sincronizadas con las de su CMTS. Una máquina de estados TEK emite peticiones de clave para renovar copias del material de aplicación de claves de su SAID después del momento de prescripción prevista de la más antigua de sus dos TEK y antes de que prescriba su TEK más reciente. Para acomodar la oblicuidad de reloj del CM/CMTS y otros retardos de procesamiento de sistemas y transmisiones, el CM programa sus peticiones de clave con un número configurable de segundos (es decir, el "tiempo de gracia TEK") antes de que se produzca la prescripción estimada de la TEK más reciente en el CMTS. Al recibir la respuesta de clave, el CM DEBE actualizar siempre sus registros con los parámetros de TEK de ambas TEK contenidos en el

mensaje respuesta de clave. La figura 9-2 ilustra la programación por parte del CM de sus renovaciones de clave junto con su gestión de las TEK activas de una SA de BPI+.

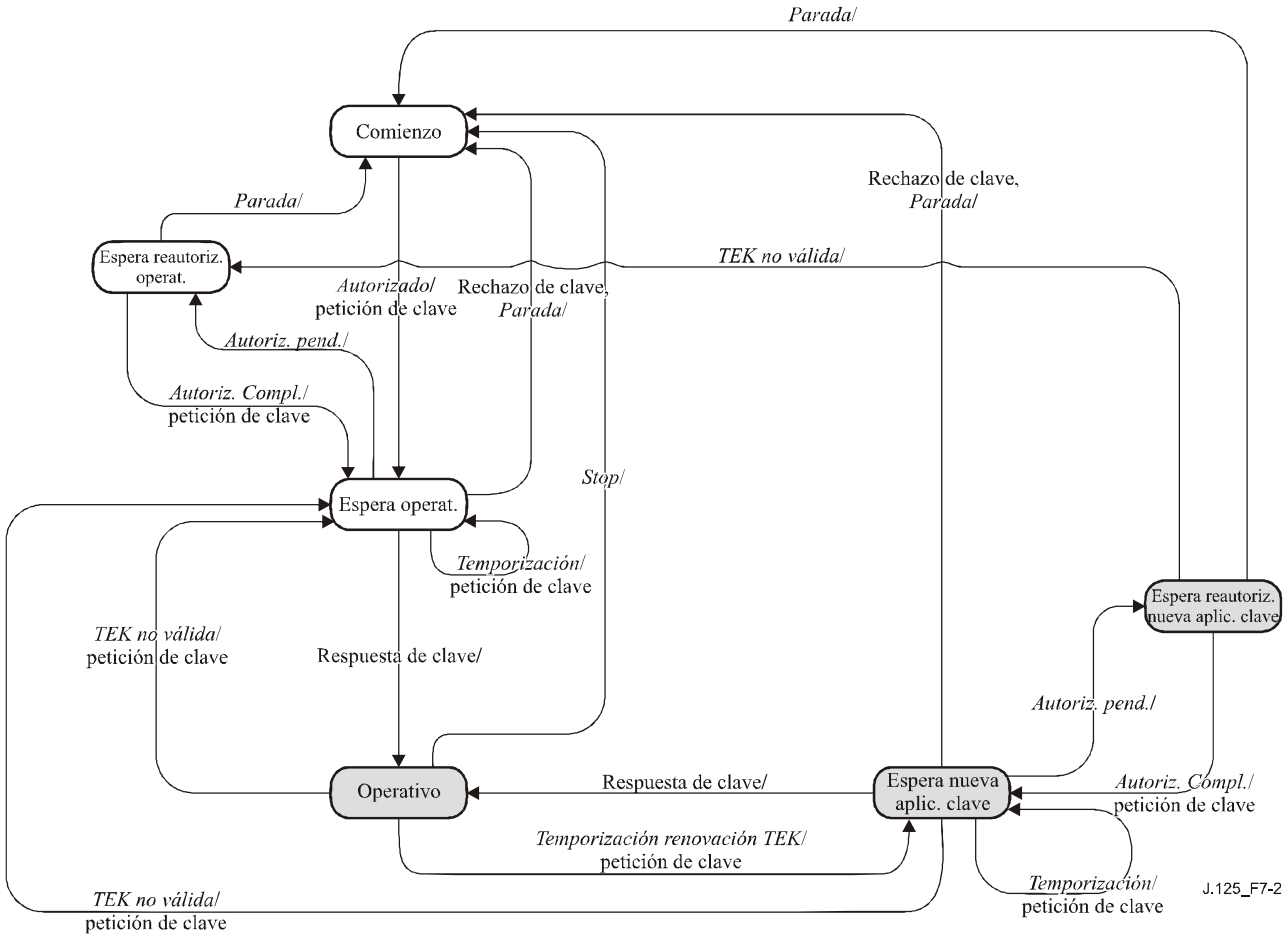


Figura 7-2/J.125 – Diagrama de flujos de máquina de estados TEK

Cuadro 7-2/J.125 – Matriz de transiciones de estados de FSM TEK

Estado / *Evento o mensaje recibido*	**(A) Comienzo**	**(B) Espera operat.**	**(C) Espera reautoriz. operat.**	**(D) Operat.**	**(E) Espera nueva aplic. clave**	**(F) Espera reautoriz. nueva aplic. clave**
(1) Parada		Comienzo	Comienzo	Comienzo	Comienzo	Comienzo
(2) Autorizado	Espera operat.					
(3) Autoriz. pend.		Espera reautoriz. operat.			Espera reautoriz. nueva aplic. clave	
(4) Autoriz. compl.			Espera operat.			Espera nueva aplic. clave
(5) TEK no válida				Espera operat.	Espera operat.	Espera reautoriz. operat.
(6) Temporización		Espera operat.			Espera nueva aplic. clave	
(7) Temporización renovación TEK				Espera nueva aplic. clave		
(8) Respuesta clave		Operativo			Operativo	
(9) Rechazo clave		Comienzo			Comienzo	

7.1.3.1 Estados

7.1.3.1.1 Comienzo

Éste es el estado inicial de la FSM. No hay ningún recurso asignado a la FSM, ni inutilizado por la misma, en este estado; por ejemplo, todos los temporizadores están desactivados y no está programado ningún procesamiento.

7.1.3.1.2 Espera operativa (espera operat.)

La máquina de estados TEK ha enviado su petición inicial (petición de clave) de material de aplicación de claves para su SAID (clave de criptación de tráfico y vector de inicialización del CBC), y está esperando la respuesta del CMTS.

7.1.3.1.3 Espera de reautorización operativa (espera reautoriz. operat.)

Es el estado de espera en que se coloca la máquina de estados TEK si no tiene material de aplicación de claves válido mientras que la máquina de estados autorización está en medio de un ciclo de reautorización.

7.1.3.1.4 Operativo

El CM tiene material de aplicación de claves válido para el SAID.

7.1.3.1.5 Espera de nueva aplicación de clave

La temporización del temporizador de renovación de TEK ha expirado y el CM ha pedido una actualización de clave para este SAID.

NOTA – La más reciente de sus dos TEK no ha prescrito y puede ser utilizada todavía para criptación y descriptación de tráfico de datos.

7.1.3.1.6 Espera de reautorización de nueva aplicación de clave (espera autoriz. nueva aplic. clave)

Es el estado de espera en que se coloca la máquina de estados TEK si tiene material de aplicación de claves de tráfico válido, tiene pendiente una petición de material de aplicación de claves más reciente y la máquina de estados autorización inicia un ciclo de reautorización.

7.1.3.2 Mensajes

Los formatos de los mensajes se definen en detalle en 7.2.

7.1.3.2.1 Petición de clave

Petición de una TEK para este SAID. Enviado por el CM al CMTS y autenticado con un compendio de mensajes con clave. La clave de autenticación de mensajes se obtiene a partir de la clave de autorización.

7.1.3.2.2 Respuesta de clave

Respuesta del CMTS que lleva los dos conjuntos activos de material de aplicación de claves de tráfico para este SAID. Enviado por el CMTS al CM, incluye las claves de criptación de tráfico del SAID, DES triple criptada con una clave de criptación de claves obtenida a partir de la clave de autorización. El mensaje respuesta de clave es autenticado con un compendio de mensajes con clave; la clave de autenticación se obtiene a partir de la clave de autorización.

7.1.3.2.3 Rechazo de clave

El CMTS DEBE enviar un mensaje de rechazo de clave al CM en respuesta al mensaje de petición de clave para indicar que no se va a enviar ninguna clave si el SAID en el mensaje de petición de clave ha dejado de ser válido. El mensaje rechazo de clave es autenticado con un compendio de mensajes con clave; la clave de autenticación se obtiene a partir de la clave de autorización.

7.1.3.2.4 TEK no válida

El CMTS DEBE enviar a un CM el mensaje TEK no válida, si determina que el CM ha criptado una PDU datos por paquetes en sentido ascendente con una TEK no válida; es decir, el número de secuencia de clave TEK de un SAID, contenido dentro del elemento encabezamiento ampliado de privacidad básica del paquete recibido, está fuera de la gama conocida de números de secuencia válidos del CMTS para ese SAID.

7.1.3.3 Eventos

7.1.3.3.1 Parada

Enviado por la FSM autorización a una FSM TEK activa (no estado comienzo) para terminar la FSM TEK y retirar el material de aplicación de claves del SAID correspondiente del cuadro de claves del CM. Véase 7.1.2.3.8.

7.1.3.3.2 Autorizado

Enviado por la FSM autorización a una FSM TEK no activa (estado comienzo) para notificar a la FSM TEK la autorización exitosa. Véase 7.1.2.3.9.

7.1.3.3.3 Autorización pendiente (autoriz. pend.)

Enviado por la FSM autorización a una FSM TEK para poner la FSM TEK en un estado de espera mientras que la FSM autorización completa la reautorización. Véase 7.1.2.3.10.

7.1.3.3.4 Autorización completa (autoriz. compl.)

Enviado por la FSM autorización a una FSM TEK en los estados espera de reautorización operativa o espera de reautorización de nueva aplicación de clave para eliminar el estado de espera iniciado por un evento autorización pendiente previo. Véase 7.1.2.3.11.

7.1.3.3.5 TEK no válida

Este evento puede ser provocado por la lógica de descriptación de paquetes de datos de un CM, o por la recepción de un mensaje TEK no válida procedente del CMTS.

La lógica de descriptación de paquetes de datos de un CM provoca un evento TEK no válida si reconoce pérdida de sincronización de clave TEK entre él mismo y el CMTS criptador; es decir, el número de secuencia de clave TEK de un SAID, contenido dentro del elemento encabezamiento ampliado de privacidad básica del paquete en sentido descendente recibido, está fuera de la gama de números de secuencia conocidos del CM para ese SAID.

Un CMTS envía a un CM un mensaje TEK no válida, provocando un evento TEK no válida dentro del CM, si la lógica de descriptación del CMTS reconoce pérdida de sincronización de clave TEK entre él mismo y el CM.

7.1.3.3.6 Temporización

Temporización de un temporizador de reintentos. Por lo general, se retransmite la petición particular.

7.1.3.3.7 Temporización de renovación de TEK

Ha concluido la temporización del temporizador de renovación TEK. Este evento de temporizador ordena a la máquina de estados TEK que emita una nueva petición de clave para renovar su material de aplicación de claves. El temporizador de la renovación se fija de manera que haga posible una duración de tiempo configurable (*tiempo de gracia de TEK*) antes de que prescriba la TEK más reciente que retiene a la sazón el CM. Esto se configura mediante el CMTS para que ocurra tras la prescripción programada de la más antigua de las dos TEK.

7.1.3.4 Parámetros

Todos los valores de parámetros de la configuración se especifican en el fichero de parámetros telecargado vía TFTP (véase el anexo A).

7.1.3.4.1 Temporización de espera operativa

Periodo de temporización entre envíos de mensajes petición de clave desde el estado espera operativa. Véase A.1.1.1.4.

7.1.3.4.2 Temporización de espera de nueva aplicación de clave

Periodo de temporización entre envíos de mensajes petición de clave desde el estado espera de nueva aplicación de clave. Véase A.1.1.1.5.

7.1.3.4.3 Tiempo de gracia de TEK

Periodo de tiempo, en segundos, en que el CM se adelanta a la prescripción estimada de una TEK, comenzando una nueva aplicación de clave para una nueva TEK.

El tiempo de gracia de TEK se especifica en una fijación de configuración dentro del fichero de parámetros telecargado vía TFTP, y es el mismo en todos los SAID. Véase A.1.1.1.6.

7.1.3.5 Acciones

1-B Espera operat. (*Parada*) → Comienzo

- detener temporizador de reintento de petición de clave;
- terminar FSM TEK.

1-C Espera reautoriz. operat. (*Parada*) → Comienzo

- terminar FSM TEK.

1-D Operativo (*Parada*) → Comienzo

- detener temporizador de renovación de TEK, que es el temporizador fijado para que arranque "*tiempo de gracia de TEK*" segundos antes de que se produzca la prescripción prevista de la TEK;
- terminar FSM TEK;
- retirar el material de aplicación de claves del SAID del cuadro de claves.

1-E Espera de nueva aplicación de clave (*Parada*) → Comienzo

- detener temporizador de reintento de petición de clave;
- terminar FSM TEK;
- retirar el material de aplicación de claves del SAID del cuadro de claves.

1-F Espera reautoriz. nueva aplic. clave (*Parada*) → Comienzo

- terminar FSM TEK;
- retirar el material de aplicación de claves del SAID del cuadro de claves.

2-A Comienzo (*Autorizado*) → Espera operat.

- enviar mensaje petición de clave a CMTS;
- fijar temporizador de reintento de petición de clave a temporización de espera operativa.

3-B Espera operat. (*Autoriz. pend.*) → Espera reautoriz. operat.

- detener temporizador de reintento de petición de clave.

3-E Espera nueva aplic. clave (*Autoriz. pend.*) → Espera reautoriz. nueva aplic. clave

- detener temporizador de reintento de petición de clave.

4-C Espera reautoriz. operat. (*Autoriz. compl.*) → Espera operat.

- enviar mensaje petición de clave a CMTS;
- fijar temporizador de reintento de petición de clave a temporización de espera operativa.

4-F Espera reautoriz. nueva aplic. clave (*Autoriz. compl.*) → Espera nueva aplic. clave

- enviar mensaje petición de clave a CMTS;
- fijar temporizador de reintento de petición de clave a temporización de espera de nueva aplicación de clave.

5-D Operativo (*TEK no válida*) → Espera operat.

- detener temporizador de renovación de TEK;
- enviar mensaje petición de clave a CMTS;
- fijar temporizador de reintento de petición de clave a temporización de espera operativa;
- retirar material de aplicación de claves de SAID de cuadro de claves.

5-E Espera de nueva aplic. clave (*TEK no válida*) → Espera operat.

- detener temporizador de reintento de petición de clave;
- enviar mensaje de petición de clave a CMTS;

- fijar temporizador de reintento de petición de clave a temporización de espera operativa;
- retirar material de aplicación de claves de SAID de cuadro de claves.

5-F Espera reautoriz. nueva aplic. clave (*TEK no válida*) → Espera reautoriz. operat.

- retirar material de aplicación de claves de SAID de cuadro de claves.

6-B Espera operat. (*Temporización*) → Espera operat.

- enviar mensaje petición de clave a CMTS;
- fijar temporizador de reintento de petición de clave a temporización de espera operativa.

6-E Espera nueva aplic. clave (*Temporización*) → Espera nueva aplic. clave

- enviar mensaje petición de clave a CMTS;
- fijar temporizador de reintento de petición de clave a temporización de espera de nueva aplicación de clave.

7-D Operativo (*Temporización de tiempo de gracia de TEK*) → Espera nueva aplic. clave

- enviar mensaje petición de clave a CMTS;
- fijar temporizador de reintento de petición de clave a temporización de espera de nueva aplicación de clave.

8-B Espera operat. (*Respuesta de clave*) → Operativo

NOTA 1 – La respuesta de clave pasó la autenticación del mensaje.

- detener temporizador de reintento de petición de clave;
- procesar contenido de mensaje respuesta de clave e incorporar nuevo material de aplicación de claves en base de datos de claves;
- fijar temporizador de renovación de TEK para que arranque "tiempo de gracia de TEK" segundos antes de la prescripción prevista de la clave.

8-E Espera nueva aplic. clave (*Respuesta de clave*) → Operativo

NOTA 2 – La respuesta de clave pasó la autenticación del mensaje.

- detener temporizador de reintento de petición de clave;
- procesar contenido de mensaje respuesta de clave e incorporar nuevo material de aplicación de claves en base de datos de claves;
- fijar temporizador de renovación de TEK para que se arranque "tiempo de gracia de TEK" segundos antes de la prescripción prevista de la clave.

9-B Espera operat. (*Rechazo de clave*) → Comienzo

NOTA 3 – El rechazo de clave pasó la autenticación del mensaje.

- detener temporizador de reintento de petición de clave;
- terminar FSM TEK.

9-E Espera nueva aplic. clave (*Rechazo de clave*) → Comienzo

- detener temporizador de reintento de petición de clave;
- terminar FSM TEK;
- retirar material de aplicación de claves de SAID de cuadro de claves.

7.2 Formatos de mensajes de gestión de claves[4]

La gestión de claves de privacidad básica emplea dos tipos de mensajes MAC: BPKM-REQ y BPKM-RSP. [J.112-B] y [J.122] definen los valores de tipo específico asignados a los mismos.

Cuadro 7-3/J.125 – Mensajes MAC de gestión de claves de privacidad básica

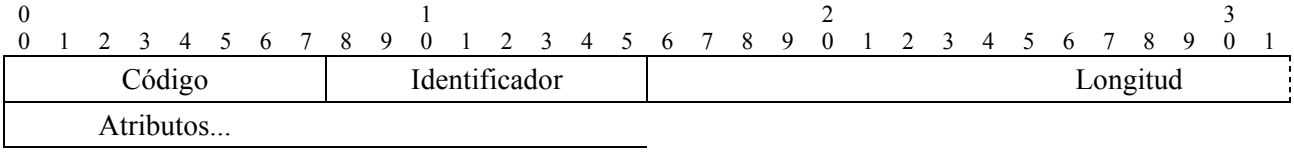
Valor de tipo	Nombre del mensaje	Descripción del mensaje
Véase [J.112-B] o [J.122]	BPKM-REQ	Petición de gestión de clave de privacidad [CM → CMTS]
Véase [J.112-B] o [J.122]	BPKM-RSP	Respuesta de gestión de clave de privacidad [CMTS → CM]

Si bien estos dos tipos de mensaje de gestión MAC distinguen entre peticiones (CM a CMTS) y respuestas (CMTS a CM) de BPKM, en los propios mensajes BPKM se codifica información más detallada a propósito del contenido de los mismos. Así se mantiene una separación clara entre funciones de gestión de privacidad y atribución de anchura de banda en sentido ascendente MAC de RF, temporización y sincronización (principales responsabilidades de la gestión MAC de RF).

7.2.1 Formatos de paquetes

En el campo cabida útil de mensaje de gestión de un mensaje de gestión MAC se encapsula exactamente un mensaje BPKM.

A continuación se muestra de forma resumida el formato de un mensaje BPKM. Los campos se transmiten de izquierda a derecha.



Código

El campo código es de un octeto, e identifica el tipo de paquete BPKM. Si se recibiera un paquete con un campo código no válido, DEBERÍA ser descartado en silencio.

[4] Los formatos de los mensajes del protocolo de gestión de claves de privacidad básica se modelan de acuerdo con los del protocolo servicio de usuario de marcación directa de extensiones para autenticación a distancia (RADIUS, *remote authentication dial in user service*), definido en [RFC 2868], y un protocolo de seguimiento de las normas Internet. BPKM, al igual que RADIUS, se atiene a un modelo cliente/servidor. A diferencia de RADIUS, BPKM no se aplicará a UDP/IP. Los mensajes BPKM se encapsulan dentro de los mensajes de gestión MAC de RF.

Los códigos BPKM (decimales) se asignan como sigue.

Cuadro 7-4/J.125 – Códigos de mensajes de gestión de claves de privacidad básica

Código	Tipo de mensaje BPKM	Nombre de mensaje de gestión MAC
0-3	Reservado	–
4	Petición de autorización	BPKM-REQ
5	Respuesta de autorización	BPKM-RSP
6	Rechazo de autorización	BPKM-RSP
7	Petición de clave	BPKM-REQ
8	Respuesta de clave	BPKM-RSP
9	Rechazo de clave	BPKM-RSP
10	Autorización no válida	BPKM-RSP
11	TEK no válida	BPKM-RSP
12	Información de autenticación	BPKM-REQ
13	Petición de relación de correspondencia	BPKM-REQ
14	Respuesta de relación de correspondencia	BPKM-RSP
15	Rechazo de relación de correspondencia	BPKM-RSP
16-255	Reservado	–

Identificador

El campo identificador es de un octeto. Un CM utiliza el identificador para que concuerden las respuestas de un CMTS con las peticiones del CM.

El CM DEBE cambiar (por ejemplo, incrementar, volviendo a 0 tras llegar a 255) el campo identificador cuando emita un mensaje BPKM nuevo. Un mensaje "nuevo" es una petición de autorización, petición de clave, o petición de relación de correspondencia de SA que no sea una retransmisión enviada en respuesta a un evento temporización. Para las retransmisiones, el campo identificador DEBE permanecer inalterado.

El campo identificador de los mensajes información de autenticación, que son informativos y no efectúan ninguna mensajería de respuesta, PUEDE fijarse a cero.

El campo identificador del mensaje de respuesta BPKM de un CMTS DEBE concordar con el campo identificador del mensaje de petición BPKM al que responde el CMTS. El campo identificador de mensajes TEK no válida, no enviados en respuesta a peticiones BPKM, DEBE fijarse a cero. El campo identificador de mensajes autorización no válida no solicitados DEBE fijarse a cero.

Al recibir un mensaje de respuesta BPKM, el CM asocia el mensaje con una máquina de estados determinada (la máquina de estados autorización en el caso de respuestas de autorización, rechazos de autorización y autorizaciones no válidas; una máquina de estados TEK particular en el caso de respuestas de clave, rechazos de clave y TEK no válidas; una máquina de estados establecimiento de correspondencia de SA particular en el caso de respuestas de relación de correspondencia de SA y rechazos de relación de correspondencia de SA).

Un CM PUEDE efectuar el seguimiento del identificador de su petición de autorización más reciente y pendiente. El CM PUEDE descartar en silencio las respuestas de autorización y los rechazos de autorización cuyos campos identificador no concuerden con los de las peticiones pendientes.

Un CM PUEDE efectuar el seguimiento del identificador de su petición de clave más reciente y pendiente. El CM PUEDE descartar en silencio las peticiones de clave y los rechazos de clave cuyos campos identificador no concuerden con los de las peticiones pendientes.

Un CM PUEDE efectuar el seguimiento del identificador de su petición de relación de correspondencia de SA más reciente y pendiente. El CM PUEDE descartar en silencio las respuestas de relación de correspondencia de SA y los rechazos de relación de correspondencia de SA cuyos campos identificador no concuerden con los de las peticiones pendientes.

Longitud

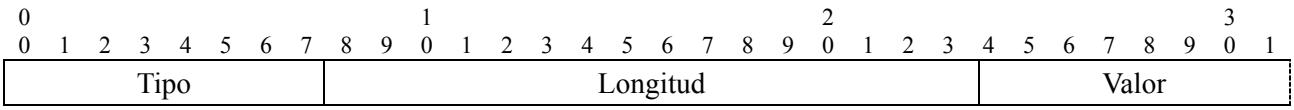
El campo longitud es de dos octetos. Indica la longitud de los campos atributo en octetos. El campo longitud no incluye los campos código, identificador y longitud. Los octetos fuera de la gama del campo longitud DEBEN ser tratados como relleno e ignorados en recepción. Si el paquete fuese más corto que lo que indica el campo longitud, DEBERÍA ser descartado en silencio. La longitud mínima es 0 y la máxima es 1490.

Atributos

Los atributos BPKM llevan los datos específicos de autenticación, autorización y gestión de las claves intercambiadas entre el cliente y el servidor. Cada tipo de paquete BPKM tiene su propio conjunto de atributos requeridos y opcionales. A menos que se indique de manera explícita, no hay ningún requisito respecto al orden de los atributos dentro de un mensaje BPKM.

El final de la lista de atributos viene indicada por la longitud del paquete BPKM.

Los atributos se codifican en forma tipo/longitud/valor (TLV, *type/length/value*), como se muestra seguidamente. Los campos se transmiten de izquierda a derecha.



A continuación se describen los formatos de los paquetes de cada mensaje BPKM. Las descripciones dan la relación de atributos BPKM contenidos dentro de cada tipo de mensaje BPKM. Los propios atributos se describen en 7.2.2. Los atributos desconocidos DEBEN ser ignorados en recepción, y se pasarán por alto cuando se explore buscando atributos reconocidos.

El CMTS DEBE descartar en silencio todas las peticiones que no contengan TODOS los atributos requeridos. El CM DEBE descartar en silencio todas las respuestas que no contengan TODOS los atributos requeridos.

7.2.1.1 Petición de autorización (petición autoriz.)

Código: 4

Atributos:

Cuadro 7-5/J.125 – Atributos de petición de autorización

Atributo	Contenido
CM-Identification	Contiene información utilizada para identificar el módem de cable al CMTS
CM-Certificate	Contiene el certificado de usuario X.509 del CM
Security-Capabilities	Describe la petición de capacidades de seguridad del CM solicitante
SAID	SAID primario del CM igual al SID primario

El atributo CM-Identification (identificación de CM) contiene un conjunto de datos que identifican el módem de cable solicitante al CMTS.

NOTA – El CMTS utiliza, con toda probabilidad, un solo elemento del atributo CM-Identification (por ejemplo, la dirección MAC de CM) como un asa del CM. Aunque podría seleccionarse un elemento específico para incorporarlo en el mensaje petición de autorización, la inclusión del atributo CM-Identification a efectos de identificación del cliente proporciona a los vendedores un mayor grado de flexibilidad a la hora de diseñar el sistema de cabecera.

El atributo CM-Certificate (certificado de CM) contiene un certificado X.509 de CM expedido por el fabricante del CM. El certificado X.509 del CM es un certificado de clave pública que vincula la información de identificación del CM a su clave pública RSA de manera verificable. El certificado X.509 va firmado digitalmente por el fabricante del CM, y esa firma (signatura) puede ser verificada por un CMTS que conozca la clave pública del fabricante. La clave pública del fabricante se pone en un certificado expedido por la autoridad de certificación (CA, *certification authority*), conforme a X.509, que a su vez va firmado por una autoridad de certificación de nivel superior.

El atributo Security-Capabilities (capacidades de seguridad) es un atributo compuesto que describe las capacidades de seguridad del módem de cable solicitante. Se incluyen aquí el algoritmo o los algoritmos de criptación de datos por paquetes que soporta un CM y el algoritmo o los algoritmos de autenticación de datos por paquetes soportados (de los que actualmente no hay ninguno) y la versión del protocolo de privacidad básica soportado (de las que actualmente hay una: la versión 1 para BPI+).

Un atributo SAID contiene el identificador de asociación de seguridad de privacidad básica, o SAID. En este caso, el SAID proporcionado es el SAID primario de BPI+ del CM, que es igual al SID primario asignado al módem de cable durante el registro MAC de RF.

7.2.1.2 Respuesta de autorización (respuesta autoriz.)

Enviado por el CMTS al CM cliente en respuesta a una petición de autorización, el mensaje respuesta de autorización contiene una clave de autorización, el tiempo de vida de la misma, su número de secuencia y una lista de descriptores de SA que identifican las asociaciones de seguridad primaria y estáticas a las que el módem de cable solicitante está autorizado a acceder y sus propiedades particulares (por ejemplo, tipo, serie criptográfica, etc.). La clave de autorización DEBE ser criptada con la clave pública del CM. La lista de descriptores de SA DEBE incluir un descriptor para el SAID de BPI+ primario notificado al CMTS en la petición de autorización correspondiente. La lista de descriptores de SA PUEDE incluir descriptores de SAID estáticos a los que el CM está autorizado a acceder.

Campo de código: 5

Atributos:

Cuadro 7-6/J.125 – Atributos de respuesta de autorización

Atributo	Contenido
AUTH-Key	Clave de autorización (AUTH), criptada con la clave pública del CM cliente objetivo
Key-Lifetime	Tiempo de vida de la clave de autorización
Key-Sequence-Number	Número de secuencia de clave de autorización
SA-Descriptor (uno o más)	Cada atributo compuesto descriptor de SA especifica un SAID y propiedades adicionales de la SA

7.2.1.3 Rechazo de autorización (rechazo autoriz.)

El CMTS responde a la petición de autorización de un CM con un mensaje rechazo de autorización si el CMTS rechaza la petición de autorización del CM.

Campo de código: 6

Atributos:

Cuadro 7-7/J.125 – Atributos de rechazo de autorización

Atributo	Contenido
Error-Code	Código de error que identifica el motivo del rechazo de la petición de autorización
Display-String (opcional)	Cadena de presentación que da el motivo del rechazo de la petición de autorización

Los atributos Error-Code (código de error) y Display-String (cadena de presentación) describen al CM solicitante el motivo del fallo de la autorización.

7.2.1.4 Petición de clave

Código: 7

Atributos:

Cuadro 7-8/J.125 – Atributos de petición de clave

Atributo	Contenido
CM-Identification	Contiene información utilizada para identificar el módem de cable al CMTS
Key-Sequence-Number	Número de secuencia de clave de autorización
SAID	ID de asociación de seguridad
HMAC-Digest	Compendio de mensajes SHA con clave

El atributo HMAC-Digest (compendio de HMAC) es un compendio de mensajes con clave. Este atributo DEBE ser el atributo final de la lista de atributos de la petición de clave. El compendio de mensajes se efectúa con el encabezamiento del paquete y todos los atributos de la petición de clave, distintos del HMAC-Digest, en el orden en que aparecen dentro del paquete.

La inclusión del compendio con clave permite al CMTS autenticar el mensaje petición de clave. La clave de autenticación del HMAC-Digest se obtiene a partir de la clave de autorización. Para los detalles, véase la cláusula 10.

7.2.1.5 Respuesta de clave

Código: 8

Atributos:

Cuadro 7-9/J.125 – Atributos de respuesta de clave

Atributo	Contenido
Key-Sequence-Number	Número de secuencia de clave de autorización
SAID	ID de asociación de seguridad
TEK-Parameters	Generación "más antigua" de parámetros de clave pertinentes para el SAID
TEK-Parameters	Generación "más reciente" de parámetros de clave pertinentes para el SAID
HMAC-Digest	Compendio de mensajes SHA con clave

El atributo TEK-Parameters (parámetros de TEK) es un atributo compuesto que contiene todo el material de aplicación de claves correspondiente a una generación particular de la TEK de un SAID. Se incluyen aquí la TEK, el tiempo de vida restante de la TEK, su número de secuencia de clave y el vector de inicialización del CBC. La TEK es criptada. Véanse los detalles en 7.2.2.13.

El CMTS mantiene en todo momento dos conjuntos de generaciones activas de material de aplicación de claves por cada SAID. (Un conjunto de material de aplicación de claves incluye una TEK y su vector de inicialización del CBC correspondiente.) Un conjunto corresponde a la generación "más antigua" de material de aplicación de claves y el otro a la generación "más reciente" de dicho material. La generación más reciente tiene un número de secuencia de clave superior en una unidad (módulo 16) al de la generación más antigua. La cláusula 9.1 especifica los requisitos del CMTS a efectos de mantenimiento y utilización de las dos generaciones activas de material de aplicación de claves de un SAID.

El CMTS entrega a un CM cliente ambas generaciones de material de aplicación de claves activo. Por ello, el mensaje respuesta de clave contiene dos atributos TEK-Parameters, cada uno de los cuales contiene el material de aplicación de claves de uno de los dos conjuntos activos de material de aplicación de claves del SAID.

El atributo HMAC-Digest (compendio de HMAC) es un compendio de mensajes con clave. Este atributo DEBE ser el atributo final de la lista de atributos de la respuesta de clave. El compendio de mensajes se efectúa con el encabezamiento del mensaje BPKM (empezando con el campo código de BPKM) y todos los atributos de la respuesta de clave, distintos del HMAC-Digest, en el orden en que aparecen dentro del paquete.

La inclusión del compendio con clave permite al cliente receptor autenticar el mensaje respuesta de clave y asegurarse de que el CM y el CMTS tienen claves de autorización sincronizadas. La clave de autenticación del HMAC-Digest se obtiene a partir de la clave de autorización. Para los detalles, véase la cláusula 10.

7.2.1.6 Rechazo de clave

La recepción de un rechazo de clave indica que el CM cliente receptor ya no está autorizado para un SAID particular.

Código: 9

Atributos:

Cuadro 7-10/J.125 – Atributos de rechazo de clave

Atributo	Contenido
Key-Sequence-Number	Número de secuencia de clave de autorización
SAID	ID de asociación de seguridad
Error-Code	Código de error que identifica el motivo del rechazo de la petición de clave
Display-String (opcional)	Cadena de presentación que da el motivo del rechazo de la clave
HMAC-Digest	Compendio de mensajes SHA con clave

El atributo HMAC-Digest (compendio de HMAC) es un compendio de mensajes con clave. Este atributo DEBE ser el atributo final de la lista de atributos del rechazo de clave. El compendio de mensajes se efectúa con el encabezamiento del mensaje BPKM (empezando con el campo código de BPKM) y todos los atributos del rechazo de clave, distintos del HMAC-Digest, en el orden en que aparecen dentro del paquete.

La inclusión del compendio con clave permite al cliente receptor autenticar el mensaje rechazo de clave y asegurarse de que el CM y el CMTS tienen claves de autorización sincronizadas. La clave de autenticación del HMAC-Digest se obtiene a partir de la clave de autorización. Para los detalles, véase la cláusula 10.

7.2.1.7 Autorización no válida

El CMTS puede enviar un mensaje autorización no válida a un CM cliente, como:

- una indicación no solicitada, o
- una respuesta a un mensaje recibido de ese CM.

En cualquiera de ambos casos, el mensaje autorización no válida ordena al CM receptor que se ponga en contacto con su CMTS para obtener una nueva autorización.

El CMTS envía un mensaje autorización no válida en respuesta a una petición de clave si:

1) el CMTS no reconoce que el CM está autorizado (es decir, no hay ninguna clave de autorización válida asociada con el módem de cable solicitante); o
2) falla la verificación del compendio de mensajes con clave de la petición de clave (en el atributo HMAC-Digest), lo que indica una pérdida de sincronización de claves de autorización entre el CM y el CMTS.

Código: 10

Atributos:

Cuadro 7-11/J.125 – Atributos de autorización no válida

Atributo	Contenido
Error-Code	Código de error que identifica el motivo de la autorización no válida
Display-String (opcional)	Cadena de presentación que describe la condición de fallo

7.2.1.8 TEK no válida

El CMTS envía un mensaje TEK no válida a un CM cliente si el CMTS determina que el CM ha criptado una PDU datos por paquetes en sentido ascendente con una TEK no válida; es decir, el número de secuencia de clave TEK de un SAID, contenido dentro del elemento encabezamiento ampliado de privacidad básica del paquete recibido, está fuera de la gama de números de secuencia válidos y conocidos del CMTS para ese SAID.

Código: 11

Atributos:

Cuadro 7-12/J.125 – Atributos de TEK no válida

Atributo	Contenidos
Key-Sequence-Number	Número de secuencia de clave de autorización
SAID	ID de asociación de seguridad
Error-Code	Código de error que identifica el motivo del mensaje TEK no válida
Display-String (opcional)	Cadena de presentación que contiene información definida por el vendedor
HMAC-Digest	Compendio de mensajes SHA con clave

El atributo HMAC-Digest (compendio de HMAC) es un compendio de mensajes con clave. Este atributo DEBE ser el atributo final de la lista de atributos de TEK no válida. El compendio de mensajes se efectúa con el encabezamiento del mensaje BPKM (empezando con el campo código BPKM) y todos los atributos de TEK no válida, distintos del HMAC-Digest, en el orden en que aparecen dentro del paquete.

La inclusión del compendio con clave permite al cliente receptor autenticar el mensaje TEK no válida y asegurarse de que el CM y el CMTS tienen claves de autorización sincronizadas. La clave de autorización del HMAC-Digest se obtiene a partir de la clave de autorización. Para los detalles, véase cláusula 10.

7.2.1.9 Información de autenticación (infor. autentic.)

El mensaje información de autenticación contiene un solo atributo CA-Certificate (certificado de CA), con un certificado de CA X.509 para el fabricante del CM. El certificado de usuario X.509 del CM DEBE haber sido expedido por la autoridad de certificación (CA) identificada por el certificado de CA X.509. Todos los certificados de CA X.509 DEBEN ser expedidos por una autoridad de certificación raíz DOCSIS.

Los mensajes información de autenticación son de carácter estrictamente informativo: mientras que el CM DEBE transmitir mensajes información de autenticación según lo indicado por el modelo estados de autenticación (véase 7.1.2), el CMTS PUEDE ignorarlos.

Código: 12

Atributos:

Cuadro 7-13/J.125 – Atributos de información de autenticación

Atributo	Contenido
CA-Certificate	Certificado de fabricante de la CA que expide el certificado de CM

El atributo CA-Certificate (certificado de CA) contiene un certificado de CA X.509 de la CA que expidió el certificado de usuario X.509 del CM. La autoridad de certificación DOCSIS expide estos certificados de CA a fabricantes de CM certificados.

7.2.1.10 Petición de relación de correspondencia de SA (petición Map)

Un CM envía peticiones de relación de correspondencia de SA a su CMTS solicitando que se establezca la correspondencia entre un determinado flujo de tráfico en sentido descendente y una SA de BPI+. En la cláusula 8 se describe el modelo de estados de establecimiento de correspondencia de SA que utiliza el mensaje.

Código: 13

Atributos:

Cuadro 7-14/J.125 – Atributos de petición de relación de correspondencia de SA

Atributo	Contenido
CM-Identification	Contiene información utilizada para identificar el módem de cable al CMTS
SA-Query	Contiene información de direccionamiento que identifica el flujo de tráfico en sentido descendente para el que el CM pide el establecimiento de correspondencia de una SA

7.2.1.11 Respuesta de relación de correspondencia de SA (respuesta Map)

Un CMTS envía una respuesta de relación de correspondencia de SA como respuesta positiva a la petición de relación de correspondencia de SA de un CM cliente. El mensaje respuesta de relación de correspondencia de SA informa al CM del establecimiento de la correspondencia entre una dirección indagada y una SA de BPI+. En la cláusula 8 se describe el modelo de estados de establecimiento de correspondencia de SA que utiliza el mensaje.

Código: 14

Atributos:

Cuadro 7-15/J.125 – Atributos de respuesta de relación de correspondencia de SA

Atributo	Contenido
SA-Query	Contiene información de direccionamiento que identifica el flujo de tráfico en sentido descendente para el que el CM pide el establecimiento de correspondencia de una SA
SA-Descriptor	Atributo compuesto descriptor de SA que especifica el SAID de la SA cuya correspondencia se ha establecido y otras propiedades

7.2.1.12 Rechazo de relación de correspondencia de SAID (rechazo Map)

Un CMTS envía un rechazo de relación de correspondencia de SA como respuesta negativa a la petición de relación de correspondencia de SA de un CM cliente. El mensaje rechazo de relación de correspondencia de SA informa al CM de que:

1) el flujo de tráfico en sentido descendente identificado en el atributo SA-Query (indagación de SA) no está siendo criptado; o
2) el CM solicitante no está autorizado para recibir ese tráfico.

El contenido de un atributo de código de error distingue entre los dos casos. En la cláusula 8 se describe el modelo de estados de establecimiento de correspondencia de SA que utiliza el mensaje.

Código: 15

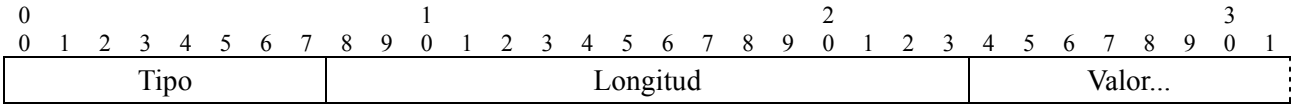
Atributos:

Cuadro 7-16/J.125 – Atributos de rechazo de relación de correspondencia de SA

Atributo	Contenido
SA-Query	Contiene información de direccionamiento que identifica el flujo de tráfico en sentido descendente para el que CM pide el establecimiento de correspondencia de una SA
Error-Code	Código de error que identifica el motivo del rechazo de la petición de relación de correspondencia de SA
Display-String (opcional)	Cadena de presentación que da el motivo del rechazo de relación de correspondencia

7.2.2 Atributos de BPKM

A continuación se muestra de forma resumida el formato de los atributos. Los campos se transmiten de la izquierda a derecha.



Tipo

El campo tipo es de 1 octeto. Los valores del campo tipo de BPKM se especifican más adelante.

NOTA 1 – La especificación de la privacidad básica se definen valores de tipo entre 0 y 127; los valores entre 128 y 255 corresponden a tipos de atributo asignados por el vendedor.

Un servidor BPKM DEBE ignorar aquellos atributos cuyo tipo sea desconocido.

Un cliente BPKM DEBE ignorar aquellos atributos cuyo tipo sea desconocido.

El cliente y el servidor BPKM (es decir, CM y CMTS) PUEDEN registrar cronológicamente la recepción de tipos de atributo desconocidos.

Cuadro 7-17/J.125 – Tipos de atributo de BPKM

Tipo	Atributo de BPKM
0	Reservado
1	Serial-Number (número de serie)
2	Manufacturer-ID (ID de fabricante)
3	MAC-Address (dirección MAC)
4	RSA-Public-Key (clave pública RSA)
5	CM-Identification (identificación de CM)
6	Display-String (cadena de presentación)
7	AUTH-KEY (clave de autorización)
8	TEK
9	Key-Lifetime (tiempo de vida de la clave)
10	Key-Sequence-Number (número de secuencia de clave)

Cuadro 7-17/J.125 – Tipos de atributo de BPKM

Tipo	Atributo de BPKM
11	HMAC-Digest (compendio de HMAC)
12	SAID
13	TEK-Parameters (parámetros de TEK)
14	OBSOLETED, atributo OBSOLETO
15	CBC-IV (vector de inicialización de CBC)
16	Error-Code (código de error)
17	CA-Certificate (certificado de CA)
18	CM-Certificate (certificado de CM)
19	Security-Capabilities (capacidades de seguridad)
20	Cryptographic-Suite (serie criptográfica)
21	Cryptographic-Suite-List (lista de series criptográficas)
22	BPI-Version (versión de BPI)
23	SA-Descriptor (descriptor de SA)
24	SA-Type (tipo de SA)
25	SA-Query (indagación de SA)
26	SA-Query-Type (tipo de indagación de SA)
27	IP-Address (dirección IP)
28	Dowload-Parameters (parámetros de descarga)
29-126	Reservado
127	Vendor-Defined (definido por el vendedor)
128-255	Vendor-assigned attribute types (tipos de atributo asignados por el vendedor)

Longitud

El campo longitud es de 2 octetos e indica la longitud del campo valor de este atributo, en octetos. El campo longitud *no incluye* los campos tipo y longitud[5]. La longitud mínima del atributo es 0, la longitud máxima es 1487.

Los paquetes que contengan atributos con longitudes no válidas DEBERÍAN ser descartados en silencio.

Valor

El campo valor es de 0 o más octetos y contiene información específica del atributo. El formato y la longitud del campo valor vienen determinados por los campos tipo y longitud. Todas las cantidades enteras de multioctetos están en el orden de bytes de la red, es decir, el octeto que contiene los bits más significativos es el primero que se transmite por el cable.

---

[5] Esto es coherente con la codificación de la codificación TLV empleada en los elementos encabezamiento ampliado de MAC de RF, y con la codificación TLV empleada para fijaciones de configuración del fichero de configuraciones del CM [J.112-B] o [J.122]. La codificación de TLV de BPKM difiere de la utilizada por el protocolo RADIUS, en el que se basa la estructura de mensaje básica de BPKM: el campo longitud de los atributos RADIUS incluye los campos tipo y longitud, así como el campo valor de un atributo.

NOTA 2 – No es preciso terminar una "cadena" con un NULO de ASCII porque el atributo ya tiene un campo longitud.

El formato del campo valor corresponde a uno de los cinco tipos de datos que se indican a continuación.

Cuadro 7-18/J.125 – Tipos de datos de valor de atributo

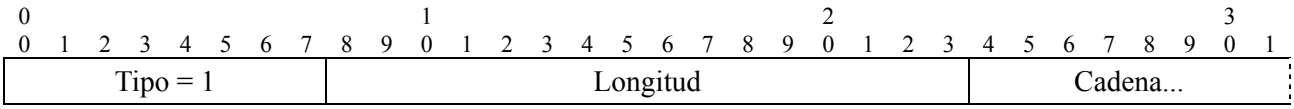
string	0-1487 octetos
uint8	entero sin signo de 8 bits
uint16	entero sin signo de 16 bits
uint32	entero sin signo de 32 bits
compound	conjunto de atributos

7.2.2.1 Número de serie

Descripción

Este atributo indica el número de serie asignado por el fabricante a un dispositivo módem de cable.

A continuación se muestra de forma resumida el formato del atributo Serial-Number (número de serie). Los campos se transmiten de izquierda a derecha.



Tipo

1 para Serial-Number

Longitud

≥0 y ≤255

Cadena

El campo cadena es de 0 o más octetos y contiene un número de serie asignado por el fabricante.

El número de serie asignado por el fabricante DEBE ser codificado de acuerdo con la codificación de caracteres de ISO/CEI 8859-1. Los caracteres empleados DEBEN limitarse a los siguientes:

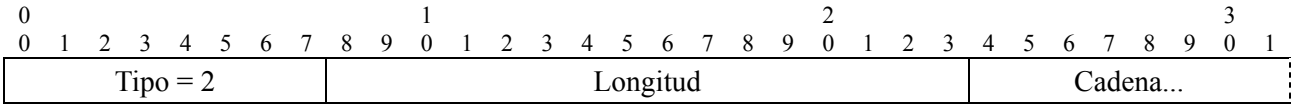
- A-Z (0x41-0x5A)
- a-z (0x61-0x7A)
- 0-9 (0x30-0x39)
- "-" (0xD2)

7.2.2.2 ID de fabricante

Descripción

Este atributo identifica al fabricante. El identificador tiene una longitud de 3 octetos y contiene el identificador único de organización (OUI, *organizationally unique identifier*) de 3 octetos asignado a las organizaciones solicitantes por el IEEE [IEEE1]. Los dos primeros bits de la cadena de 3 octetos se fijan a cero.

A continuación se muestra de forma resumida el formato del atributo Manufacturer-ID (ID de fabricante). Los campos se transmiten de izquierda a derecha.



Tipo

2 para Manufacturer-ID

Longitud

3

Cadena

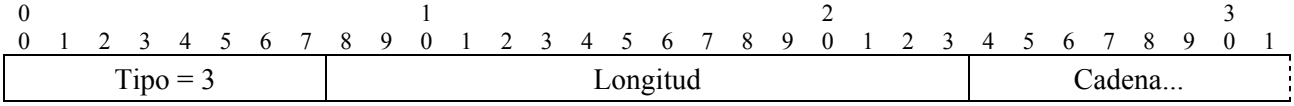
El campo cadena es de 3 octetos y contiene un OUI del IEEE.

7.2.2.3 Dirección MAC

Descripción

Este atributo identifica la dirección MAC del IEEE asignada al CM. Garantizada su unicidad, lo probable es que se utilice como asa/índice de módem de cable en el CMTS.

A continuación se muestra de forma resumida el formato del atributo MAC-Address (dirección MAC). Los campos se transmiten de izquierda a derecha.



Tipo

3 para MAC-Address

Longitud

6

Cadena

El campo cadena contiene una dirección MAC de 6 octetos.

7.2.2.4 Clave pública RSA

Descripción

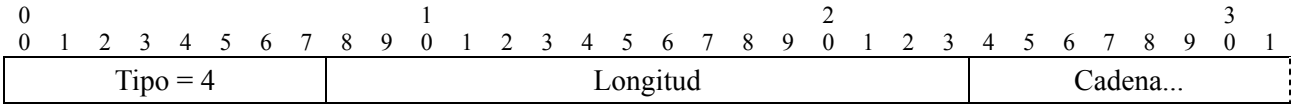
Este atributo es un atributo cadena que contiene un tipo ASN.1 de clave pública RSA codificada según las reglas de codificación distinguida (DER, *distinguished encoding rules*), de acuerdo con lo definido en la norma de criptación de los laboratorios RSA PKCS#1 v2.0 [RSA3].

Según especifica la norma PKCS #1 v2.0, una clave pública RSA está formada por un módulo público RSA y un exponente público RSA; el tipo de clave pública RSA incluye ambas cosas como tipos ENTEROS codificados según DER.

La norma PKCS #1 v2.0 establece que el exponente público RSA puede ser normalizado en aplicaciones específicas, y sugiere valores de 3 ó 65537 (F4). La privacidad de referencia plus normaliza en F4 para un exponente público y emplea un módulo de 1024 bits (la privacidad básica empleaba un módulo de 768 bits). Para poder adaptar a BPI+ el soporte

lógico de equipos DOCSIS 1.0, las implementaciones BPI+ DEBEN soportar un módulo de 768 bits.

A continuación se muestra de forma resumida el formato del atributo Public-Key (clave pública). Los campos se transmiten de izquierda a derecha.



Tipo

4 para RSA-Public-Key

Longitud

106, 140 ó 270 (longitud de codificación DER, utilizando F4 como exponente público y un módulo de 768 bits, 1024 bits o 2048 bits, respectivamente).

Cadena

Clave pública RSA codificada según DER tipo ASN.1.

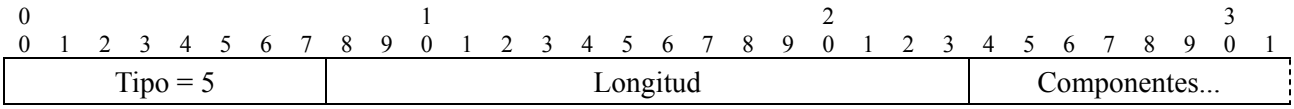
7.2.2.5 Identificación de CM

Descripción

Este atributo es un atributo compuesto, formado por un conjunto de subatributos. Los subatributos contienen información que se puede utilizar para identificar de manera exclusiva un módem de cable. Entre los subatributos DEBEN figurar los siguientes:

- Serial-Number (número de serie).
- Manufacturer-ID (ID de fabricante).
- MAC-Address (dirección MAC).
- RSA-Public-Key (clave pública RSA).

El atributo CM-Identification (identificación de CM) PUEDE contener también atributos facultativos definidos por el vendedor.



Tipo

5

Longitud

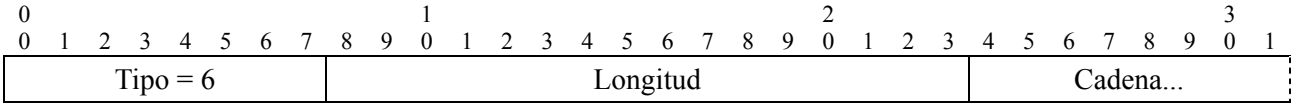
≥126

7.2.2.6 Cadena de presentación

Descripción

Este atributo contiene un mensaje textual. Su utilización típica consiste en explicar una respuesta de fallo, y podría ser registrado cronológicamente por el receptor para su recuperación posterior por un gestor SNMP. Las cadenas de presentación NO DEBEN tener una longitud superior a 128 bytes.

A continuación se muestra de forma resumida el formato del atributo Display-String (cadena de presentación). Los campos se transmiten de izquierda a derecha.



Tipo

6 para Display String

Longitud

≥0 y ≤128

Cadena

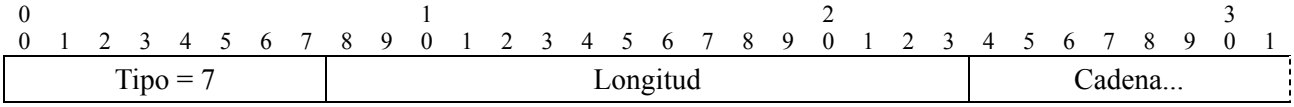
Una cadena de caracteres. No se requiere que la cadena de caracteres termine con NULO; el campo longitud identifica siempre el final de la cadena.

7.2.2.7 Clave de autorización

Descripción

El atributo Authorization Key (clave de autorización) es una cantidad de 20 bytes, de la que se obtienen una clave de criptación de claves y dos claves de autenticación de mensajes (una para peticiones en sentido ascendente y otra para respuestas en sentido descendente).

Este atributo contiene una cantidad de 96 ó 128 octetos que a su vez contienen la clave de autorización criptada según RSA con la clave pública RSA de 768 bits o 1024 bits del CM. En 10.5 se indican detalles del procedimiento de criptación de RSA. El texto cifrado producido por el algoritmo RSA tendrá la longitud del módulo RSA, es decir, 96 ó 128 octetos.



Tipo

7 para AUTH-Key

Longitud

96 ó 128

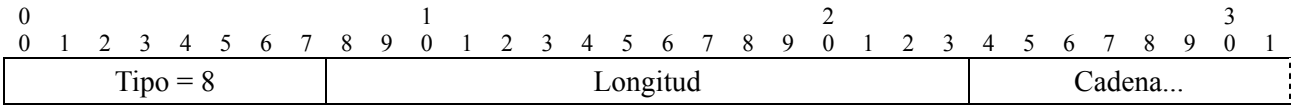
Cadena

Cantidad de 96 ó 128 octetos que representa una clave de autorización criptada según RSA.

7.2.2.8 TEK

Descripción

Este atributo contiene una cantidad de 8 octetos que es una clave DES TEK, criptada con una clave de criptación de claves obtenida a partir de la clave de autorización. Las claves TEK se encriptan utilizando el modo criptación-descriptación-criptación (EDE, *encrypt-decrypt-encrypt*) de DES triple de dos claves. Para los detalles, véase la cláusula 10.



Tipo

8 para TEK

Longitud

8

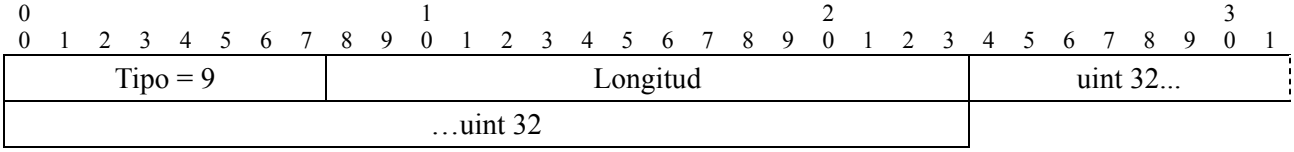
Cadena

Cantidad de 64 bits que representa una clave de criptación de tráfico criptada (modo EDE de DES triple de dos claves).

7.2.2.9 Vida útil de clave

Descripción

El atributo Key-Lifetime (tiempo de vida de clave) contiene el tiempo de vida, en segundos, de una clave de autorización o TEK. Es una cantidad sin signo de 32 bits que representa el número de segundos restantes durante los cuales la clave asociada será válida.



Tipo

9 para Key-Lifetime

Longitud

4

uint32

Cantidad de 32 bits que representa el tiempo de vida de la clave

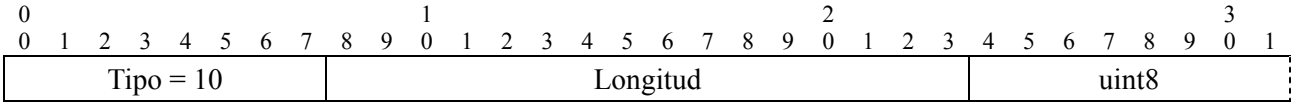
Un tiempo de vida de clave de cero indica que no es válida la clave de autorización o la clave de encriptación de tráfico correspondiente.

7.2.2.10 Número de secuencia de clave

Descripción

Este atributo contiene un número de secuencia de 4 bits para una TEK o una clave de autorización. La cantidad de 4 bits, no obstante, se almacena en un único octeto, con los 4 bits de orden superior fijados a 0.

A continuación se muestra de forma resumida el formato del atributo Key-Sequence-Number (número de secuencia de clave). Los campos se transmiten de izquierda a derecha.



Tipo

10 para Key-Sequence-Number

Longitud

1

uint8

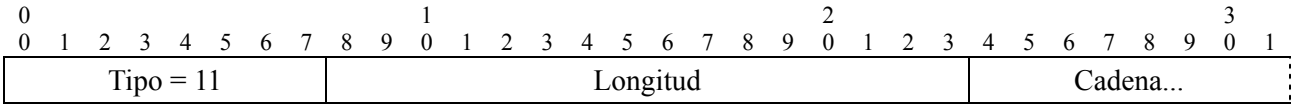
Número de secuencia de 4 bits

7.2.2.11 Compendio de HMAC

Descripción

Este atributo contiene un troceo con clave utilizado para la autenticación de mensajes. El algoritmo HMAC se define en [RFC 2104] y se especifica utilizando un algoritmo de troceo criptográfico genérico. La privacidad básica utiliza una versión particular de HMAC que emplea el algoritmo de troceo seguro (SHA-1, *secure hash algorithm*-1), definido en [FIPS 180-2].

A continuación se muestra de forma resumida el formato del atributo HMAC-Digest (compendio de HMAC). Los campos se transmiten de izquierda a derecha.



Tipo

11 para HMAC-Digest

Longitud

20 octetos

Cadena

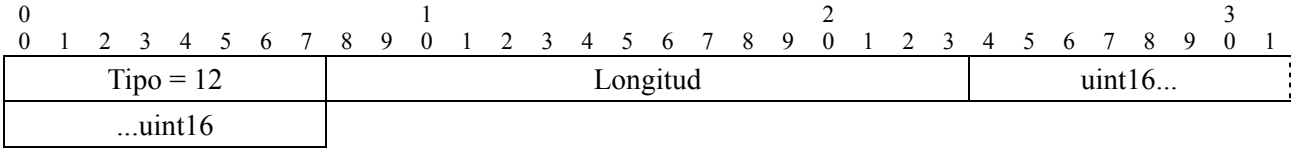
Un troceo SHA con clave de 160 bits (20 octetos).

7.2.2.12 SAID

Descripción

Este atributo contiene un identificador (ID) de asociación de seguridad (SAID) de 14 bits utilizado por privacidad básica plus como identificador de la asociación de seguridad. Los dos bits de orden superior se fijan a cero.

NOTA – El SAID primario de BPI+ de un CM es igual al SID primario de ese CM.



Tipo

12 para SAID

Longitud

2

uint16

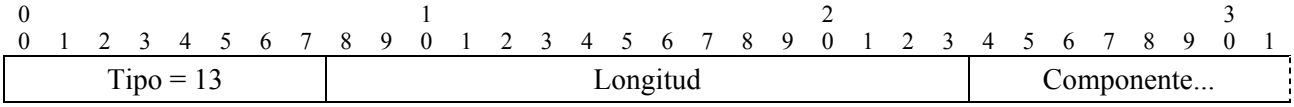
Cantidad de 16 bits que representa un SAID

7.2.2.13 Parámetros de TEK

Descripción

Este atributo es un atributo compuesto, formado por un conjunto de subatributos. Los subatributos representan todos los parámetros de seguridad pertinentes para la generación particular de la TEK de un SAID.

A continuación se muestra de forma resumida el formato del atributo TEK-Parameters (parámetros de TEK). Los campos se transmiten de izquierda a derecha.



Tipo

13 para TEK-Parameters

Longitud

33

Componentes

El campo componentes contiene los subatributos que se indican a continuación:

Cuadro 7-19/J.125 – Subatributos de parámetros de TEK

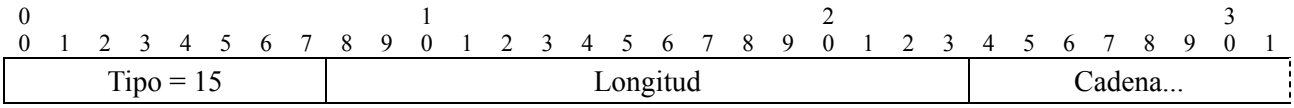
Atributo	Contenido
TEK	TEK, criptada con la KEK (modo EDE de DES triple de dos claves)
Key-Lifetime	Tiempo de vida restante de la TEK
Key-Sequence-Number	Número de secuencia de TEK
CBC-IV	Vector de inicialización de encadenamiento de bloques cifrados (CBC)

7.2.2.14 Vector de inicialización de CBC

Descripción

Este atributo contiene un valor de 64 bits (8 octetos) que especifica un vector de inicialización de encadenamiento de bloques cifrados (CBC).

A continuación se muestra de forma resumida el formato del atributo CBC-IV. Los campos se transmiten de izquierda a derecha.



Tipo

15 para CBC-IV

Longitud

8 octetos

Cadena

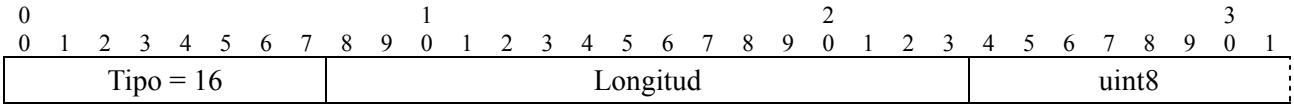
Una cantidad de 64 bits que representa un vector de inicialización de CBC de DES.

7.2.2.15 Código de error

Descripción

Este atributo contiene un código de error de un octeto que proporciona más información sobre un rechazo de autorización, un rechazo de clave, una autorización no válida o una TEK no válida.

A continuación se muestra de forma resumida el formato del atributo Error-Code (código de error). Los campos se transmiten de izquierda a derecha.



Tipo

16 para Error-Code

Longitud

1

uint8

código de error de 1 octeto

Un CMTS DEBE incluir el atributo Error-Code en todos los mensajes rechazo de autorización, autorización no válida, rechazo de clave, TEK no válida y rechazo SA-MAP. El cuadro 7-20 da la relación de valores de código a utilizar con este atributo. El CMTS DEBE emplear los códigos de error distintos de cero que se indican más abajo para mensajes de rechazo de SA-MAP. El CMTS PUEDE emplear los códigos de error cero que se indican más abajo para los restantes tipos de mensajes BPI+; PUEDE, no obstante, devolver un valor de código de cero (0). Los valores de código de error distintos de los definidos en el cuadro 7-20 DEBEN ser ignorados. Si se devuelve un valor de código de cero, no se envía información de fallo adicional al CM; por motivos de seguridad, puede que esto sea lo conveniente.

Cuadro 7-20/J.125 – Valores de código del atributo código de error

Código de error	Mensajes	Descripción
0	Todos	Sin información
1	Rechazo de autorización, autorización no válida	CM no autorizado
2	Rechazo de autorización, rechazo de clave	SAID no autorizado
3	Autorización no válida	No solicitado
4	Autorización no válida, TEK no válida	Número de secuencia de clave no válida
5	Autorización no válida	Fallo de autenticación de mensaje (petición de clave)
6	Rechazo de autorización	Fallo de autorización permanente
7	Rechazo de relación de correspondencia	No autorizado para el flujo de tráfico en sentido descendente solicitado
8	Rechazo de relación de correspondencia	Correspondencia entre flujo de tráfico en sentido descendente y SAID de BPI+ no establecida
9	Rechazo de autorización	Hora del día no adquirida

El código de error 6, fallo de autorización permanente, se utiliza para indicar un cierto número de condiciones de error diferentes que afectan al intercambio de autorización BPKM. Entre ellas figuran las siguientes:

- Fabricante desconocido; es decir, el CMTS no tiene el certificado de CA perteneciente al expedidor de un certificado de CM.
- El certificado de CM tiene una signatura o firma no válida.
- Fallo del análisis sintáctico de la ASN.1 durante la verificación de un certificado de CM.

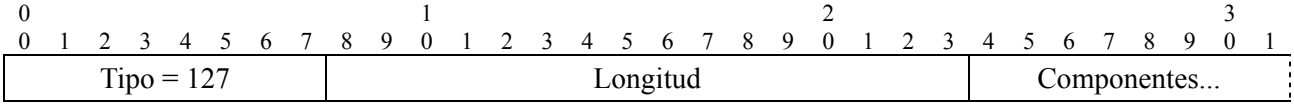
- El certificado de CM está en la lista actualizada permanentemente ("lista caliente").
- Incoherencias entre los datos de un certificado y los datos de los atributos BPKM acompañantes.
- El CM y el CMTS tienen capacidades de seguridad incompatibles.

Su propiedad común consiste en que la condición de fallo se considera permanente: cualquier nueva tentativa de autorización seguiría dando como resultado rechazos de autorización. Los detalles sobre el motivo de un fallo de autorización permanente PUEDEN ser notificados al CM en un atributo cadena de presentación opcional que puede acompañar al atributo código de error en los mensajes rechazo de autorización. El CMTS DEBERÍA proporcionar la capacidad de decidir administrativamente si se envían o no detalles adicionales al CM. El CMTS PUEDE registrar cronológicamente estos fallos de autorización, o incluso atraparlos a continuación para un gestor SNMP.

7.2.2.16 Definido por el vendedor

Descripción

El atributo Vendor-Defined (definido por el vendedor) es un atributo compuesto cuyo primer subatributo DEBE ser el atributo ID de fabricante. El o los atributos subsiguientes son definidos por el usuario, con valores de tipo asignados por el vendedor identificado por el atributo ID de fabricante previo.



Tipo

127 para Vendor-Defined

Longitud

≥6

Componentes

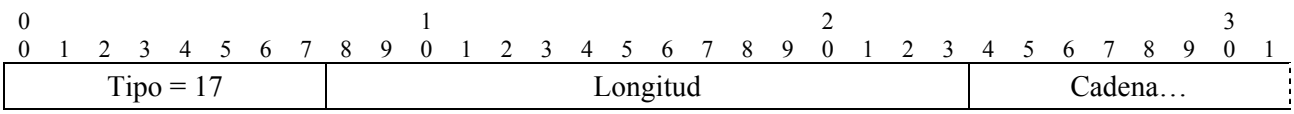
El primer subatributo DEBE ser el ID de fabricante. Los atributos subsiguientes pueden incluir tipos universales (es decir, definidos dentro de la presente Recomendación), y tipos definidos por el vendedor, específicos del vendedor identificado en el subatributo ID de fabricante precedente.

7.2.2.17 Certificado de CA

Descripción

Este atributo es un atributo cadena que contiene un certificado de CA X.509, definido en [X.509].

A continuación se muestra de forma resumida el formato del atributo CA-Certificate (certificado de CA). Los campos se transmiten de izquierda a derecha.



Tipo

17 para CA-Certificate

Longitud

Variable. La longitud NO DEBE hacer que el mensaje de gestión MAC resultante exceda del tamaño máximo permitido.

Cadena

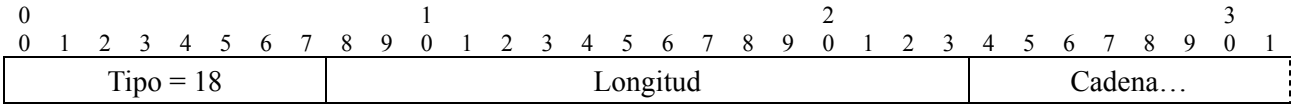
Certificado de CA X.509 (ASN.1 con codificación según DER).

7.2.2.18 Certificado de CM

Descripción

Este atributo es un atributo cadena que contiene el certificado de usuario X.509 de un módem de cable, definido en [X.509].

A continuación se muestra de forma resumida el formato del atributo CM-Certificate (certificado de CM). Los campos se transmiten de izquierda a derecha.



Tipo

18 para CM-Certificate

Longitud

Variable. La longitud NO DEBE hacer que el mensaje de gestión MAC resultante exceda del tamaño máximo permitido.

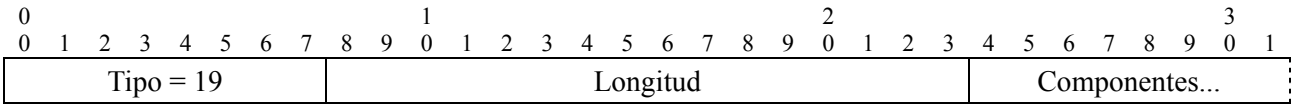
Cadena

Certificado de usuario X.509 (ASN.1 con codificación según DER).

7.2.2.19 Capacidades de seguridad

Descripción

El atributo Security-Capabilities (capacidades de seguridad) es un atributo compuesto cuyos subatributos identifican la versión de BPI+ que soporta un CM y la serie o series criptográficas que soporta.



Tipo

19 para Security-Capabilities

Longitud

≥9

Componentes

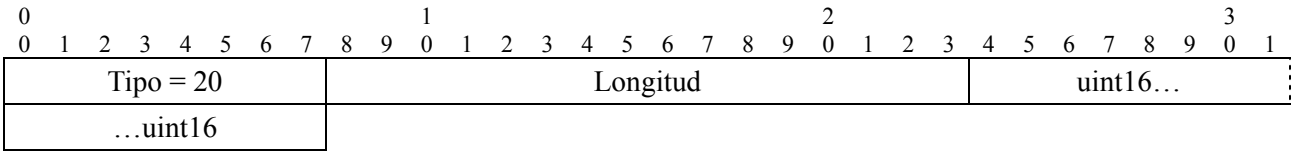
El campo componentes contiene los subatributos que se indican a continuación:

Cuadro 7-21/J.125 – Subatributos de capacidades de seguridad

Atributo	Contenido
Cryptographic-Suite-List	Lista de series criptográficas soportadas
BPI-Version	Versión de BPI+ soportada

7.2.2.20 Serie criptográfica

Descripción



Tipo

20 para Criptographic-Suite

Longitud

2

uint16

Un entero de 16 bits que identifica el emparejamiento de un algoritmo de criptación de datos (codificado en el byte situado más a la izquierda y más significativo) con un algoritmo de autenticación de datos (codificado en el byte situado más a la derecha y menos significativo). En la actualidad, DES de 56 bits y DES de 40 bits son los únicos algoritmos especificados para utilizar dentro de la seguridad DOCSIS, y ninguno de ellos está emparejado con un algoritmo de autenticación de datos.

Cuadro 7-22/J.125 – Identificadores de algoritmo de criptación de datos

Valor	Descripción
0	Reservado
1	Modo CBC, DES de 56 bits
2	Modo CBC, DES de 40 bits
3-255	Reservado

Cuadro 7-23/J.125 – Identificadores de algoritmo de autenticación de datos

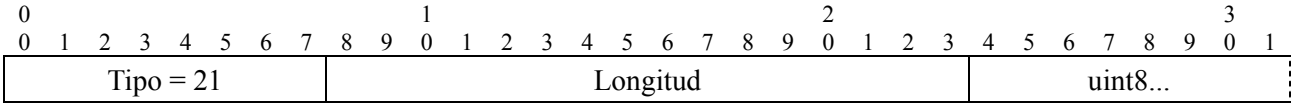
Valor	Descripción
0	Sin autenticación de datos
1-255	Reservado

Cuadro 7-24/J.125 – Valores del atributo serie criptográfica

Valor	Descripción
256 (0x0100 hex)	Modo CBC, DES de 56 bits y sin autenticación de datos
512 (0x0200 hex)	Modo CBC, DES de 40 bits y sin autenticación de datos
Todos los demás valores	Reservado

7.2.2.21 Lista de series criptográficas

Descripción



Tipo

21 para Cryptographic-Suite-List

Longitud

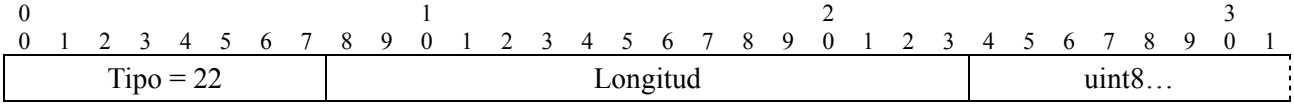
2 × n, siendo n el número de series criptográficas indicadas

uint8

Una lista de pares de bytes que identifica un conjunto de series criptográficas. Cada par de bytes representa una serie criptográfica soportada, con una codificación idéntica a la del campo valor del atributo serie criptográfica (7.2.2.20). El CMTS NO DEBE interpretar el orden relativo de los pares de bytes de la lista como preferencias del CM entre las series criptográficas que soporta.

7.2.2.22 Versión de BPI

Descripción



Tipo

22 para BPI-Version

Longitud

1

uint8

Un código de 1 octeto que identifica una versión de la seguridad de privacidad básica.

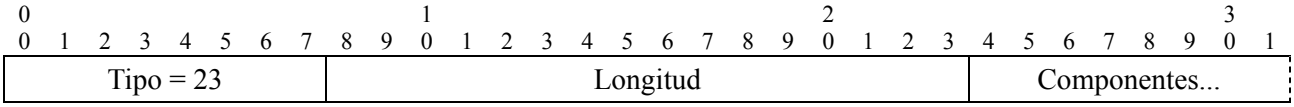
Cuadro 7-25/J.125 – Valores del atributo versión de BPI

Valor	Descripción
0	Reservado
1	BPI+
2-255	Reservado

7.2.2.23 Descriptor de SA

Descripción

El atributo SA-Descriptor (descriptor de SA) es un atributo compuesto cuyos subatributos describen las propiedades de una asociación de seguridad de BPI+. Esas propiedades incluyen el SAID, el tipo de SA y la serie criptográfica empleada dentro de la SA.



Tipo

23 para SA-Descriptor

Longitud

14

Componentes

El campo componentes contiene los subatributos que se indican a continuación:

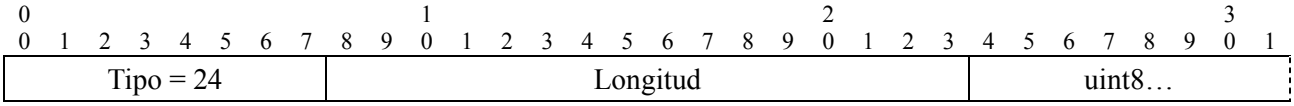
Cuadro 7-26/J.125 – Subatributos de descriptor de SA

Atributo	Contenido
SAID	ID de asociación de seguridad
SA-Type	Tipo de SA
Cryptographic-Suite	Emparejamiento de algoritmos de criptación de datos y autenticación de datos empleados dentro de la SA

7.2.2.24 Tipo de SA

Descripción

Identifica el tipo de SA. La BPI+ define tres tipos de SA: primario, estático y dinámico.



Tipo

24 para SA-Type

Longitud

1

uint8

Un código de 1 octeto que identifica el valor del atributo SA-Type (tipo de SA) definido en el cuadro 7-27.

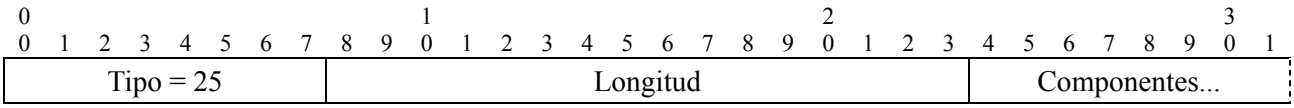
Cuadro 7-27/J.125 – Valores del atributo tipo de SA

Valor	Descripción
0	Primario
1	Estático
2	Dinámico
3-127	Reservado
128-255	Específico del vendedor

7.2.2.25 Indagación de SA

Descripción

Se trata de un atributo compuesto utilizado en la petición de relación de correspondencia de SA para especificar los argumentos de indagación del establecimiento de la correspondencia. Los argumentos de la indagación incluyen el tipo de indagación y cualesquiera atributos de direccionamiento propios de ese tipo de indagación: los atributos de direccionamiento que identifican un determinado flujo de tráfico en sentido descendente para el que se pide el establecimiento de la correspondencia de una SA. En la actualidad, el único tipo de indagación especificado es multidifusión IP, y el argumento de direccionamiento asociado con ese tipo es una dirección de grupo IP.



Tipo

25 para SA-Query

Longitud

11

Componentes

El campo componentes contiene los subatributos que se indican a continuación:

Cuadro 7-28/J.125 – Subatributos de indagación de SA

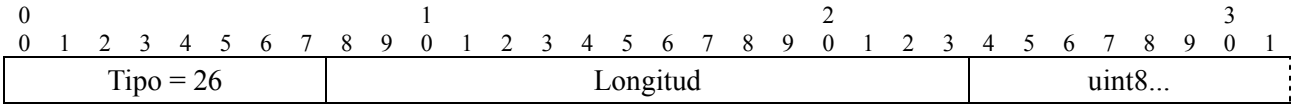
Atributo	Contenido
SA-Query-Type	Tipo de indagación
IP-Address	Se requiere si tipo de indagación de SA = multidifusión IP; contiene una dirección de grupo IP de la que se pide el establecimiento de la correspondencia de SA

7.2.2.26 Tipo de indagación de SA

Descripción

Este atributo identifica una dirección IP utilizada para identificar un flujo de tráfico IP criptado. Se emplea, por ejemplo, para especificar una dirección de grupo de multidifusión IP.

A continuación se muestra de forma resumida el formato del atributo SA-Query-Type (tipo de indagación de SA). Los campos se transmiten de izquierda a derecha.



Tipo

26 para SA-Query-Type

Longitud

1

uint8

Un código de 1 octeto que identifica el valor del atributo tipo de indagación de SA definido en el cuadro 7-29.

Cuadro 7-29/J.125 – Valores del atributo tipo de indagación de SA

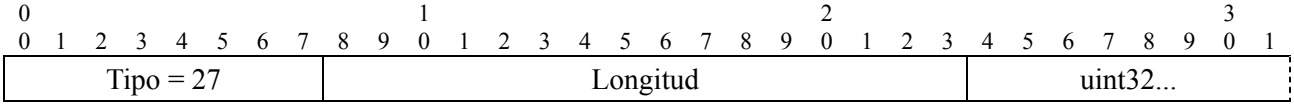
Valor	Descripción
0	Reservado
1	Multidifusión IP
2-127	Reservado
128-255	Específico del vendedor

7.2.2.27 Dirección IP

Descripción

Este atributo identifica la dirección IP utilizada para identificar un flujo de tráfico IP criptado. Se emplea, por ejemplo, para especificar una dirección de grupo de multidifusión IP.

A continuación se muestra de forma resumida el formato del atributo IP-Address (dirección IP). Los campos se transmiten de izquierda a derecha.



Tipo

27 para IP-Address

Longitud

4

uint32

Contiene el entero sin signo de 32 bits (en el orden de los bytes de la red) que representa una dirección IP.

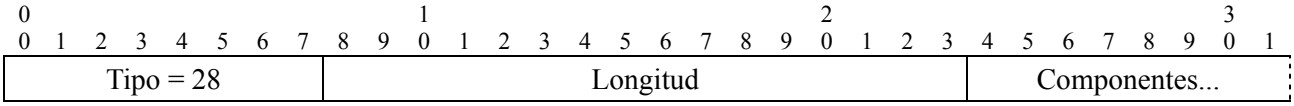
7.2.2.28 Parámetros de descarga

Descripción

Este atributo se utiliza en el fichero de código CM definido en B.3.1. Este atributo es un atributo compuesto, constituido por una colección de atributos.

Los subatributos PUEDEN incluir uno o los dos atributos siguientes en este orden:

- Clave pública RSA (cero o uno).
- Certificado CA (cero, uno o más).



Tipo

28

Longitud

≥0

8 Establecimiento de correspondencia de SA dinámica

8.1 Introducción

Las asociaciones de seguridad dinámicas (SA dinámicas) de BPI+, presentadas en 5.1.3, son las SA que un CMTS establece y elimina, dinámicamente, en respuesta a su habilitación e inhabilitación de flujos específicos de tráfico en sentido descendente. Dichos flujos de tráfico pueden ser iniciados por las acciones de:

- un dispositivo CPE (equipo en las instalaciones del cliente) conectado a uno de los CM clientes del CMTS;
- un servidor de aplicación ubicado en la cabecera;
- un sistema OSS;
- otros mecanismos no especificados.

Con independencia de lo que provoque el establecimiento de una SA dinámica dentro del CMTS, los CM clientes necesitan un mecanismo de aprendizaje del establecimiento de la correspondencia entre un determinado flujo de tráfico en sentido descendente protegido por BPI+ y la asociación de seguridad de BPI+ asignada dinámicamente de ese flujo (y el correspondiente SAID de esa SA).

La máquina de estados establecimiento de correspondencia de SA, definida en esta cláusula, especifica la manera según la cual los módems de cable indagan un CMTS para el establecimiento de la correspondencia entre flujos de tráfico en sentido descendente y SA dinámicas. La máquina de estados controla la transmisión de los mensajes petición de relación de correspondencia de SA a un CMTS.

DOCSIS 1.1 o DOCSIS 2.0 especifica actualmente SA dinámicas para un solo tipo de servicio: el de criptación del tráfico de multidifusión IP en sentido descendente, restringiendo de este modo el acceso a dicho tráfico. Un CMTS puede establecer o eliminar SA dinámicas en respuesta a los cambios que se produzcan en cuanto a la pertenencia o no al grupo IP de dispositivos CPE en sentido descendente. Los mecanismos de gestión IGMP de DOCSIS 1.1 o DOCSIS 2.0 ([J.112-B], cláusula 5.3.1 o [J.122], cláusula 5.3.1 pueden provocar el establecimiento de SA dinámicas en el CMTS. Esos mismos mecanismos DEBEN activar en el CM mensajes petición de relación de correspondencia BPI+ que indaguen el CMTS para el establecimiento de la correspondencia entre una dirección de grupo de multidifusión IP y una SA.

El mecanismo de establecimiento de la correspondencia de una SA de BPI+ PUEDE hacer corresponder un grupo de multidifusión IP con una SA estática, o incluso con una SA primaria de un determinado CM; la respuesta de un CMTS a una petición de establecimiento de correspondencia puede contener cualquiera de los tres tipos de SA. El mecanismo de

establecimiento de correspondencia de SA, no obstante, es el único mecanismo mediante el cual un CM puede enterarse de la identidad de las SA dinámicas.

En la cláusula 8.4 se examina con más detalle el uso particular del mecanismo de establecimiento de la correspondencia de una SA como soporte de dicho establecimiento entre tráfico de multidifusión IP y SA dinámicas. En las dos cláusulas que siguen, sin embargo, la atención se centra en el mecanismo más general de establecimiento de correspondencia de SA.

NOTA – En futuros perfeccionamientos de las especificaciones del servicio DOCSIS se pueden definir aplicaciones adicionales de las SA dinámicas.

8.2 Teoría de funcionamiento

La BPI+ define tres mensajes BPKM nuevos para soportar la indagación por los CM de los establecimientos de correspondencia de SA, a saber, el mensaje de petición de relación de correspondencia de SA, el de respuesta de relación de correspondencia de SA y el de rechazo de relación de correspondencia de SA. Un CM envía una petición de relación de correspondencia a su CMTS solicitando el establecimiento de la correspondencia entre un flujo en sentido descendente conocido y una SA. La petición de relación de correspondencia lleva atributos de datos BPI+ que identifican el CM solicitante y el flujo de tráfico en sentido descendente del que se pide el establecimiento de la correspondencia con la SA.

El CMTS DEBE responder a una petición de relación de correspondencia *sea con*:

- una respuesta de relación de correspondencia, que proporciona al CM el establecimiento de correspondencia de SA solicitado, *o*
- un rechazo de relación de correspondencia, que señala al CM que:
  1) no está autorizado a recibir el flujo de tráfico identificado en la petición de relación de correspondencia; o
  2) no se ha establecido la correspondencia entre el flujo de tráfico solicitado y una SA de BPI+.

Si el CM no recibe ninguna de las respuestas anteriores dentro de un periodo de tiempo de reintento configurable, envía de nuevo la petición de relación de correspondencia. Si no se recibe ninguna respuesta después de un número máximo configurable de reintentos, el CM deja de intentarlo.

Si el CM recibe un rechazo de relación de correspondencia, cesa toda tentativa ulterior de obtener el establecimiento de la correspondencia. En caso de que exista correspondencia entre el acceso al flujo de tráfico en sentido descendente y una SA de BPI+, y el CM solicitante no esté autorizado a acceder a esa SA, se denegará el acceso al CM y a su dispositivo CPE conectado, porque el CM no puede obtener el material de aplicación de claves necesario para descriptar los flujos de tráfico en sentido descendente criptados de conformidad con esa SA. Por ejemplo, el usuario puede estar solicitando un servicio adicional al que no este suscrito. Si el flujo de tráfico solicitado no está criptado (es decir, no existe correspondencia entre dicho flujo y una SA), el tráfico no criptado será simplemente reenviado al dispositivo CPE conectado. Por ejemplo, el CM realiza una petición SA-MAP para la dirección de multidifusión de todos los abonados. Puesto que son necesarios todos los paquetes direccionados a la dirección difundida a todos los usuarios para un funcionamiento correcto del IGPM, no es preciso encriptar esos paquetes.

Si el CM recibe una respuesta de relación de correspondencia que identifica la SA de BPI+ asociada con el flujo de tráfico en sentido descendente solicitado, activa una máquina de estados TEK para la SA, siempre que:

1) el CM no esté utilizando ya una máquina de estados TEK para esa SA; y
2) el CM soporte la serie criptográfica identificada en la respuesta de relación de correspondencia junto con el valor del ID de asociación de seguridad (SAID).

El CM puede estar utilizando ya una máquina de estados TEK si la SA, cuya correspondencia se ha establecido, es:

- una SA dinámica de la que se ha establecido la correspondencia con otro flujo de tráfico protegido y a la que el CM ya tiene acceso;
- la SA primaria del CM solicitante; o
- una SA estática de la que el CM ha tenido conocimiento en una respuesta de autorización recibida previamente.

Un CMTS PUEDE asignar múltiples flujos de tráfico (es decir, direcciones de multidifusión IP) a la misma SA. Si se está criptando más de un flujo de tráfico descendente de conformidad con la misma SA dinámica, puede ocurrir que un CM esté ya utilizando una máquina de estados TEK para la SA identificada en la respuesta de relación de correspondencia. La correspondencia de la SA devuelta en la respuesta de relación de correspondencia no necesariamente ha de ser una SA dinámica: se puede hacer corresponder el flujo de tráfico solicitado con la SA primaria o una SA estática del CM.

La respuesta de relación de correspondencia incluye un atributo descriptor de SA que identifica tanto un SAID como la serie criptográfica empleada dentro de la SA. Como ocurre con las SA estáticas, la selección de una serie criptográfica de una SA dinámica se hace normalmente con independencia de las capacidades criptográficas del CM solicitante. Así pues, un CMTS PUEDE responder a una petición de relación de correspondencia con una SA (estática o dinámica) que emplea una serie criptográfica que el CM no soporta. El CM NO DEBE arrancar máquinas de estado TEK para SA estáticas o dinámicas cuyas series criptográficas no soporta. (No obstante, una SA primaria debe emplear una serie criptográfica soportada por el CM al que pertenece la SA.)

La máquina de estados TEK controla la recuperación del material de aplicación de claves de la SA cuya correspondencia se ha establecido. El CM enviará peticiones de clave para la SA; el CMTS DEBE responder a esas peticiones de clave con uno de los mensajes siguientes:

- un mensaje respuesta de clave, proporcionando al CM el material de aplicación de claves solicitado,
- un mensaje rechazo de clave, señalando al CM que no tiene autorización para el SAID solicitado y cuya correspondencia se ha establecido,
- un mensaje autorización no válida, señalando al CM que ha fallado la autenticación del mensaje petición de clave.

La recepción de un mensaje rechazo de clave fuerza la terminación de la máquina de estados TEK.

Existen dos mecanismos para que el CMTS comunique a un CM cliente que no está autorizado a acceder a un determinado flujo de tráfico: respondiendo a una petición de relación de correspondencia con un rechazo de correspondencia, o respondiendo a una petición de clave con un rechazo de clave. Depende de la implementación el que un CMTS compruebe o no la situación de autorización de un CM antes de responder a una petición de relación de correspondencia. Si la comprobación se efectúa durante el intercambio para el establecimiento de la correspondencia, se evitará que el CM ponga en marcha innecesariamente una máquina de estados TEK y envíe un mensaje petición de clave correspondiente a un SAID para el que no está autorizado.

8.3 Modelo de estados de establecimiento de correspondencia de SA

El modelo de estados de establecimiento de correspondencia de SA especifica el mecanismo por el cual un CM se entera del establecimiento de la correspondencia entre un flujo de tráfico y una SA dinámica.

Se arranca una máquina de estados cuando, dentro del CM, un evento externo al modelo de estados de establecimiento de correspondencia de SA, hace necesario el establecimiento de la correspondencia entre un flujo de tráfico y una SA (por ejemplo, cuando un CM instala los filtros de

permiso para un grupo de multidifusión IP como resultado de los mecanismos de gestión IGMP del CM). El evento externo genera un evento "Map" (relación de correspondencia) interno en la máquina de estados establecimiento de correspondencia de SA.

La máquina de estados termina si el CM no recibe una respuesta después de efectuar el número máximo de reintentos, o cuando el CM determina que ya no necesita el material de aplicación de claves de la SA cuya correspondencia se ha establecido. En este último caso, un evento externo genera un evento "Unmap" (terminación de relación de correspondencia) interno en la máquina de estados establecimiento de correspondencia de SA, forzando su terminación. Así pues, la máquina de estados puede ser utilizada no sólo para obtener la información requerida de establecimiento de correspondencia, sino también para efectuar el seguimiento del periodo de tiempo durante el cual una aplicación externa que utiliza el mecanismo de establecimiento de correspondencia de la SA (por ejemplo, la gestión IGMP) requiere ese establecimiento de correspondencia. La vinculación de un evento "Unmap" a un evento externo, y por tanto la implementación del evento Unmap es OPCIONAL.

Al igual que con las máquinas de estados TEK y autorización BPI+, la máquina de estados establecimiento de correspondencia de SA se presenta en formato gráfico, como un modelo de flujos de estados (figura 8-1), y en formato tabular, como una matriz de transiciones de estados (cuadro 8-1). Y al igual que las máquinas de estados definidas previamente, la matriz de transiciones de estados DEBE ser utilizada como la especificación definitiva de las acciones de protocolo asociadas con cada transición de estado.

Si, mediante el mecanismo de establecimiento de correspondencia de SA, un CM se entera de que necesita acceso al material de aplicación de claves de una SA dinámica, debe establecer una máquina de estados TEK para esa SA dinámica. Mientras que la máquina de estados autorización controla el establecimiento y la terminación de las máquinas de estados TEK asociadas con el SAID primario y cualesquiera SAID estáticos, no controla en cambio el establecimiento y la terminación de máquinas de estados TEK asociadas con SA dinámicas. Los CM DEBEN implementar la lógica necesaria para establecer y terminar máquinas de estados TEK para las SA dinámicas de las que se ha tenido conocimiento a través del mecanismo de establecimiento de correspondencia de SA. La especificación BPI+, no obstante, no define cómo deberían gestionar los CM las máquinas de estados TEK de sus SA dinámicas.

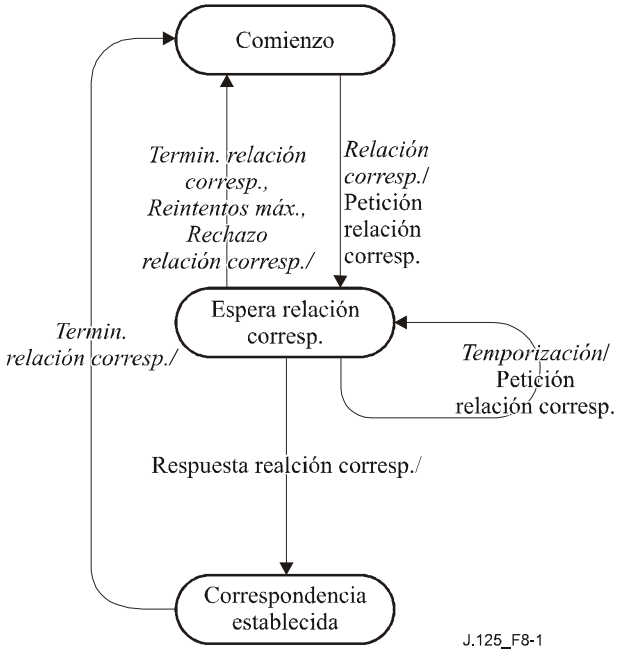


Figura 8-1/J.125 – Diagrama de flujos de máquina de estados establecimiento de correspondencia de SA

Cuadro 8-1/J.125 – Matriz de transición de estado de SAID dinámico

Estado / ***Evento o mensaje recibido***	**(A) Comienzo**	**(B) Espera relación corresp.**	**(C) Correspondencia establecida**
(1) *Relación corresp.*	Espera relación corresp.		
(2) *Termin. relación corresp.*		Comienzo	Comienzo
(3) *Respuesta relación corresp*.		Correspondencia establecida	
(4) *Rechazo relación corresp.*		Comienzo	
(5) *Temporización*		Espera relación corresp.	
(6) *Reintentos máx*.		Comienzo	

8.3.1 Estados

8.3.1.1 Comienzo

Es el estado inicial de la máquina de estados finitos.

8.3.1.2 Espera relación corresp.

El CM ha enviado al CMTS una petición de relación de correspondencia y está esperando la respuesta.

8.3.1.3 Correspondencia establecida

El CM ha recibido una respuesta de relación de correspondencia y se ha enterado de la petición de establecimiento de correspondencia de SA solicitada.

8.3.2 Mensajes

8.3.2.1 Petición de relación de correspondencia de SA (petición relación corresp.)

Enviado por el CM al CMTS para pedir el establecimiento de la correspondencia de una SA.

8.3.2.2 Respuesta de relación de correspondencia de SA (respuesta relación corresp.)

Respuesta positiva del CMTS a la petición de relación de correspondencia que contiene el establecimiento de correspondencia de SA solicitado.

8.3.2.3 Rechazo de relación de correspondencia de SA (rechazo relación corresp.)

Respuesta negativa del CMTS a la petición de relación de correspondencia del CM; señala al CM que:

1) no está autorizado a acceder al flujo de tráfico identificado en la petición de relación de correspondencia; o
2) no se ha establecido la correspondencia entre el flujo de tráfico solicitado y una SA de BPI+.

8.3.3 Eventos

8.3.3.1 Relación de correspondencia

Este evento provoca el arranque de la máquina de estados establecimiento de correspondencia de SA. El evento relación de correspondencia está vinculado a un evento de CM ajeno al protocolo BPI+.

8.3.3.2 Terminación de relación de correspondencia

Este evento provoca la terminación de la máquina de estados establecimiento de correspondencia de SA. El evento terminación de relación de correspondencia está vinculado a un evento de CM ajeno al protocolo BPI+. La implementación del evento Unmap es OPCIONAL.

8.3.3.3 Respuesta de relación de correspondencia

El módem de cable recibe un mensaje respuesta de relación de correspondencia de SA.

8.3.3.4 Rechazo de relación de correspondencia

El módem de cable recibe un mensaje rechazo de relación de correspondencia de SA.

8.3.3.5 Temporización

El módem de cable ha agotado su temporización esperando la respuesta a un mensaje petición de relación de correspondencia de SA pendiente.

8.3.3.6 Reintentos máximos

El módem de cable ha efectuado el número máximo de reintentos y no ha recibido ninguna respuesta.

8.3.4 Parámetros

Todos los valores de parámetros de la configuración se especifican en el fichero de parámetros telecargado vía TFTP (véase el anexo A).

8.3.4.1 Temporización de espera de relación de correspondencia de SA

Es el periodo de temporización entre envíos de mensajes petición de relación de correspondencia de SA desde el estado espera de SA. Véase A.1.1.1.8.

8.3.4.2 Reintentos máximos de relación de correspondencia de SA

Número máximo de veces que el CM intenta la petición de relación de correspondencia de SA antes de dejar de intentarlo.

8.3.5 Acciones

Las acciones efectuadas en asociación con transiciones de estados se indican mediante <evento/mensaje recibido> → <estado> en lo que sigue:

1-A Comienzo (*Relación corresp.*) → Espera de relación de correspondencia

- enviar petición de relación de correspondencia de SA;
- fijar temporizador de reintentos de petición de relación de correspondencia a temporización de espera de relación de correspondencia de SA;
- fijar contador de reintentos de relación de correspondencia a 0.

2-B Espera de relación de correspondencia (*Termin. establ. corresp.*) → Comienzo

- detener temporizador de reintentos de petición de relación de correspondencia;
- terminar máquina de estados establecimiento de correspondencia de SA.

2-C Correspondencia establecida (*Termin. relación corresp.*) → Comienzo

- terminar máquina de estados establecimiento de correspondencia de SA.

3-B Espera de relación de correspondencia (*Respuesta relación corresp.*) → Correspondencia establecida

- detener temporizador de reintentos de petición de relación de correspondencia (Map).

4-B Espera de relación de correspondencia (*Rechazo relación corresp.*) → Comienzo

- detener temporizador de reintentos de petición de relación de correspondencia (Map);
- terminar máquina de estados establecimiento de correspondencia de SA.

5-B Espera de relación de correspondencia (*Temporización*) → Espera de relación de correspondencia

- enviar petición de relación de correspondencia;
- fijar temporizador de reintentos de petición de relación de correspondencia a temporización de espera de relación de correspondencia de SA;
- incrementar contador de reintentos de relación de correspondencia;
- si contador de reintentos de relación de correspondencia > reintentos máximos de relación de correspondencia de SA, generar evento reintentos máximos.

6-B Espera de relación de correspondencia (*Reintentos máx.*) → Comienzo

- terminar máquina de estados establecimiento de correspondencia de SA.

8.4 Tráfico de multidifusión IP y SA dinámicas

DOCSIS 1.1 [J.112-B] o DOCSIS 2.0 [J.122] especifica las reglas para la gestión del tráfico IGMP en el CM y el CMTS. Dichas reglas se han concebido con miras a controlar el flujo de tráfico de multidifusión IP a través de la red de cable y a través de la interfaz CM/CPE de tal manera que:

- un CMTS sólo reenvíe tráfico en sentido descendente asociado con un grupo de multidifusión IP si un dispositivo CPE, conectado a uno de los CM clientes del CMTS, es miembro de ese grupo, y

- un CM sólo reenvíe, a través de su interfaz CPE, tráfico en sentido descendente asociado con un grupo de multidifusión IP si un dispositivo CPE conectado es miembro de ese grupo.

BPI+, funcionando en combinación con la interfaz RFI de DOCSIS 1.1 o DOCSIS 2.0, controla el acceso a los flujos de tráfico de multidifusión IP criptándolos y controlando la distribución del material de aplicación de claves de multidifusión requerido para descriptar los flujos.

Un CMTS puede establecer la correspondencia entre flujos de multidifusión en sentido ascendente y cualquiera de las tres clases de asociaciones de seguridad de BIP+: primaria, estática o dinámica. Si se establece la correspondencia entre el tráfico de un grupo de multidifusión IP y una SA primaria, sólo el único CM perteneciente a esa SA puede acceder a ese grupo. Si se establece la correspondencia con una SA estática o dinámica, múltiples CM pueden acceder a ese grupo, si bien un CMTS puede limitar una SA estática o dinámica a un solo CM.

Cuando un CM de DOCSIS 1.1 o DOCSIS 2.0 habilita el reenvío en sentido descendente de un grupo de multidifusión IP (en respuesta a la recepción de un informe de pertenencia como miembro en su interfaz CPE), el CM DEBE determinar si el tráfico en sentido ascendente del grupo de multidifusión IP está criptado y el SAID de BPI+ está asociado con el flujo de multidifusión criptado en sentido descendente. Una vez que el CM tiene el SAID asociado, puede activar el funcionamiento de una máquina de estados TEK para recuperar el material de aplicación de claves de la SA.

El CM utiliza el mecanismo de establecimiento de correspondencia de SA de BPI+ para pedir a su CMTS el establecimiento de la correspondencia de la SA para un grupo de multidifusión IP al que acaba de unirse. El evento relación de correspondencia de la máquina de estados establecimiento de correspondencia de SA se activa por la habilitación del reenvío de RF a CPE del grupo de multidifusión IP en el CM (véanse B.5.3.1.2 y el anexo L de [J.112-B] o 5.3.1.2 y apéndice V de [J.122]). Una respuesta de relación de correspondencia de SA informa al CM de que se ha establecido la correspondencia entre el grupo al que se ha unido y una SA de BPI+. Si se establece la correspondencia entre el grupo y la SA primaria del CM, el CM ya tiene el material de aplicación de claves requerido. Si se establece la correspondencia entre el grupo y una SA estática o dinámica, el CM determina si ya está utilizando una máquina de estados TEK para esa SA; en caso negativo, arranca una.

La máquina de estados establecimiento de correspondencia de SA define un evento terminación de relación de correspondencia OPCIONAL que termina la máquina de estados establecimiento de correspondencia de SA y PUEDE ser utilizado para indicar al CM que ya no necesita el material de aplicación de claves de la SA cuya correspondencia se ha establecido. En caso de establecimiento de correspondencia entre tráfico de multidifusión IP y una SA, el evento terminación de relación de correspondencia podría indicar que el CM ha eliminado todos los filtros de permiso de multidifusión IP asociados con grupos de multidifusión IP cuya correspondencia con la SA en cuestión se ha establecido. Así pues, la máquina de estados establecimiento de correspondencia SA PUEDE ser utilizada para rastrear la necesidad de un CM de mantener material de aplicación de claves para una SA dinámica a la que se ha hecho corresponder con uno o más grupos de multidifusión IP.

Las máquinas de estados TEK correspondientes a SAID primarios y estáticos se paran de acuerdo con las condiciones de terminación definidas en las máquinas de estados autorización y TEK.

9 Utilización de claves

9.1 CMTS

Tras completar el registro DOCSIS MAC, el CM inicia un intercambio de autorización con su CMTS. La primera recepción por el CMTS de un mensaje petición de autorización procedente del

CM no autorizado inicia la activación de una nueva clave de autorización (AK, *authorization key*), que el CMTS envía al CM solicitante en un mensaje respuesta de autorización. Esta AK permanecerá activa hasta que prescriba de acuerdo con su tiempo de vida predefinido, el *tiempo de vida de clave de autorización*, que es un parámetro de la configuración del sistema CMTS (véase A.2).

El CMTS DEBE utilizar material de aplicación de claves obtenido a partir de la clave de autorización del CM para:

- verificar el compendio de HMAC en peticiones de clave recibidas de ese CM,
- criptar (DES triple de dos claves modo EDE) la TEK en las respuestas de clave que envíe al CM (TEK es un subatributo del atributo parámetros de TEK de una respuesta de clave),
- calcular el compendio de HMAC que escribe en los mensajes respuesta de clave, rechazo de clave y TEK no válida que envía al CM.

El CMTS debe estar siempre preparado para enviar una AK a un CM cuando se le pida. El CMTS DEBE poder soportar hasta dos AK activas simultáneamente para cada CM cliente. El CMTS tiene dos AK activas durante el periodo de transición de clave de autorización; las dos claves activas tienen unos tiempos de vida que se superponen.

El periodo de transición de una clave de autorización empieza cuando el CMTS recibe una petición de autorización procedente de un CM y sólo tiene una AK activa para ese CM. En respuesta a la petición de autorización, el CMTS activa una segunda AK, que envía al CM solicitante en una respuesta de autorización. El CMTS DEBE fijar el tiempo de vida activa de esta segunda AK de modo que sea el tiempo de vida activa restante de la primera AK, más el *tiempo de vida de clave de autorización* predefinida; de este modo, la segunda clave, la "más reciente", permanecerá activa durante un periodo de *tiempo de vida activa de clave de autorización*, tras la prescripción de la primera, la clave "más antigua". El periodo de transición de clave finalizará al prescribir la clave más antigua. Esto es lo que se describe en la mitad superior de la figura 9-1.

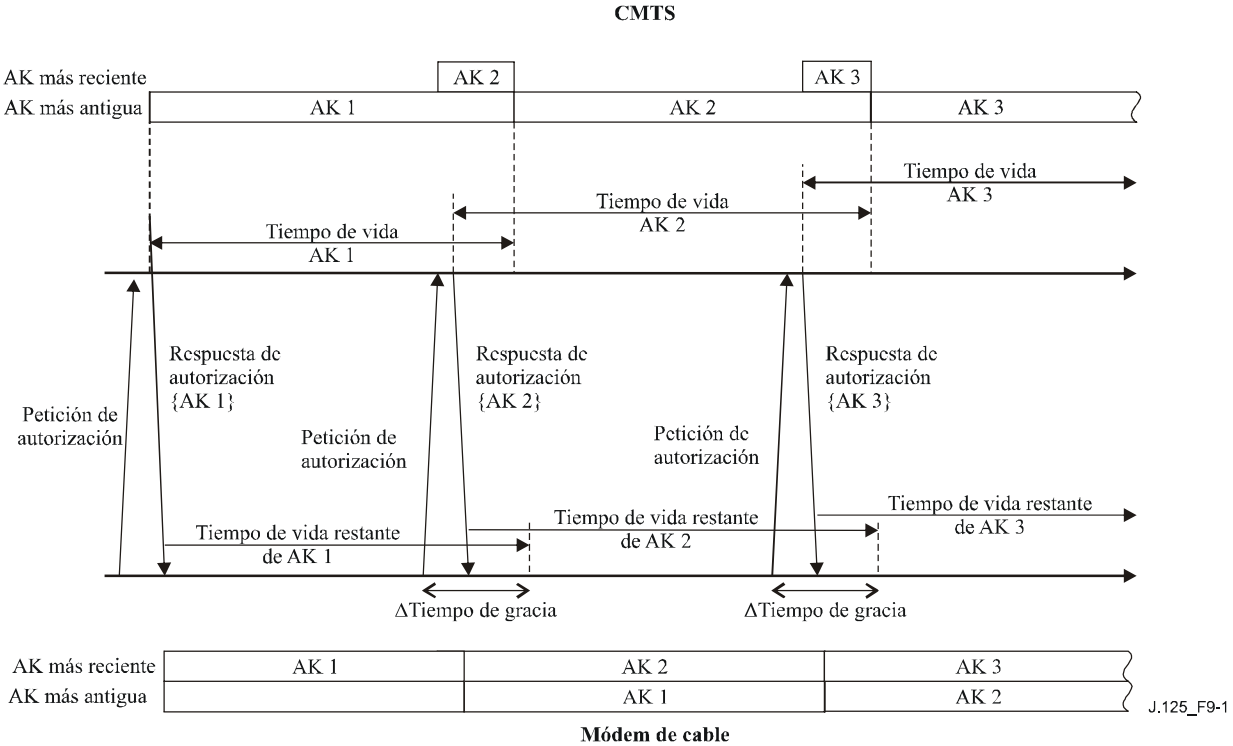


Figura 9-1/J.125 – Gestión de clave de autorización en CMTS y CM

El tiempo de vida de la clave de autorización que un CMTS notifica en una respuesta de autorización DEBE reflejar, de manera tan precisa como permita la implementación, los tiempos de vida restantes de las AK en el momento en que se envía el mensaje de respuesta.

Mientras el CMTS esté en medio del periodo de transición de clave de autorización de un CM, y esté reteniendo por tanto dos claves de autorización activas para ese CM, responderá a las peticiones de autorización con la más reciente de las dos claves activas. Una vez que prescriba la clave más antigua, una petición de autorización provocará la activación de una AK nueva, y el comienzo de un nuevo periodo de transición de clave.

Si la reautorización de un CM no se produce antes de que prescriba su AK más reciente, el CMTS retendrá claves de autorización no activas para ese CM y considerará al CM *no autorizado*. Un CMTS DEBE retirar de sus cuadros de claves todas las TEK asociadas con la SA primaria de un CM no autorizado.

Un CMTS DEBE utilizar la clave o las claves de autorización activas de un CM para verificar el compendio de HMAC en las peticiones de clave recibidas del CM. Si un CMTS recibe una petición de clave durante un periodo de transición de AK, y el número de secuencia de clave de la AK acompañante indica que la petición fue autenticada con la más reciente de las dos AK, el CMTS identifica esto como un *reconocimiento implícito* de que el CM ha obtenido la más reciente de las dos AK activas.

Un CMTS DEBE utilizar una AK activa cuando calcule compendios de HMAC en mensajes respuesta de clave, rechazo de clave y TEK no válida, y cuando cripte la TEK en mensajes respuesta de clave. Cuando envíe mensajes respuesta de clave, rechazo de clave o TEK no válida dentro de un periodo de transición de clave (es decir, cuando estén disponibles dos AK activas), si se ha acusado recibo implícitamente de la clave más reciente, el CMTS DEBE utilizar la más reciente de las dos AK activas; si no se ha acusado recibo de la clave más reciente, el CMTS DEBE utilizar la más antigua de las dos AK activas.

La mitad superior de la figura 9-1 ilustra la estrategia del CMTS a propósito de su utilización de claves de autorización.

El CMTS DEBE mantener dos conjuntos de claves de criptación de tráfico activas (y sus vectores de inicialización de CBC asociados) por cada SAID. Corresponden a dos generaciones sucesivas de material de aplicación de claves, y sus tiempos de vida se superponen. La TEK más reciente DEBE tener un número de secuencia de clave superior en una unidad (módulo 16) al de la TEK más antigua. Cada TEK pasa a estar activa a mitad del tiempo de vida de su predecesora, y prescribe a mitad del tiempo de vida útil de su sucesora. Una vez concluido el tiempo de vida de una TEK, la TEK pasa a estar inactiva y NO DEBE ser ya utilizada.

El CMTS transita entre las dos TEK activas de manera diferente, dependiendo de si la TEK se utiliza para tráfico en sentido descendente o ascendente. Para cada uno de sus SAID, el CMTS DEBE transitar entre TEK activas de acuerdo con las reglas siguientes:

- El CMTS DEBE utilizar la más antigua de las dos TEK activas para criptar tráfico en sentido descendente. Al prescribir la TEK más antigua, el CMTS DEBE pasar a utilizar inmediatamente la TEK más reciente a efectos de criptación.
- Para descriptar tráfico en sentido ascendente, se define un periodo de transición que empieza una vez que el CMTS ha enviado la TEK más reciente a un CM dentro de un mensaje respuesta de clave. El periodo de transición en sentido ascendente empieza a partir del momento en que el CMTS envía la TEK más reciente en un mensaje respuesta de clave y concluye una vez que prescribe la TEK más antigua. Durante el periodo de transición, el CMTS DEBE ser capaz de descriptar tramas en sentido ascendente utilizando cualquiera de las TEK, la más antigua o la más reciente.

El CMTS cripta con una TEK determinada sólo durante la segunda mitad del tiempo de vida total de esa TEK. El CMTS puede, no obstante, descriptar con una TEK durante todo el tiempo de vida de la misma.

El campo KEY_SEQ del elemento EH de privacidad básica identifica con cuál de las dos TEK se criptan los datos por paquetes de la trama en sentido ascendente. El bit BASCULAR del elemento EH de privacidad, que es igual al bit menos significativo del campo KEY_SEQ, puede ser utilizado por el CMTS para identificar la TEK con la que se ha criptado.

La mitad superior de la figura 9-2 ilustra la gestión que este CMTS lleva a cabo de las TEK de una asociación de seguridad de BPI+.

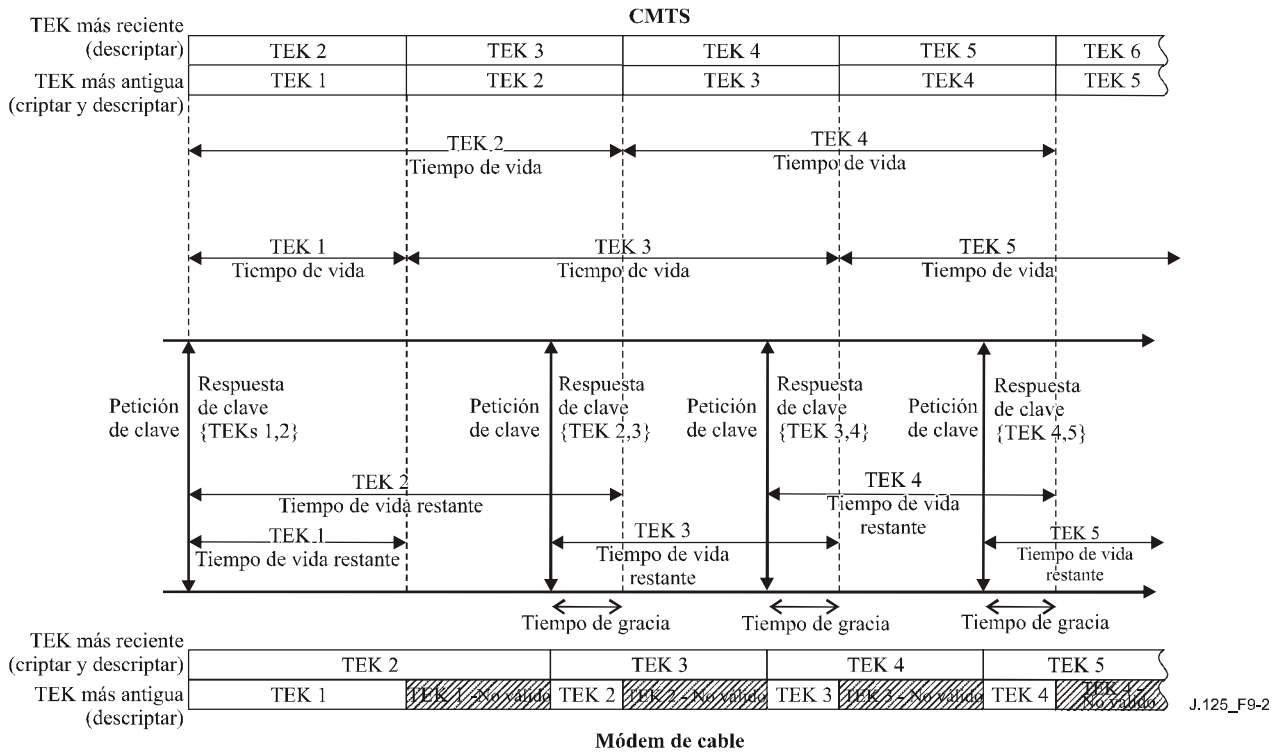


Figura 9-2/J.125 – Gestión de TEK en CMTS y CM

El CMTS se encarga del mantenimiento de la información de aplicación de claves tanto para los SAID primarios como para los SAID de multidifusión de la forma antes indicada. El protocolo de gestión de claves de privacidad básica definido en esta especificación describe un mecanismo para sincronización de esa información de aplicación de claves entre un CMTS y sus CM clientes. Corresponde al CM actualizar sus claves de manera puntual; el CMTS transitará a una nueva clave de encriptación en sentido descendente con independencia de si un CM cliente ha recuperado una copia de esa TEK.

Las respuestas de clave enviadas por un CMTS contienen parámetros de TEK (la propia TEK, un tiempo de vida de clave, un número de secuencia de clave y un vector de inicialización de CBC-IV) para las dos TEK activas. Los tiempos de vida de clave de los que informa el CMTS en un mensaje respuesta de clave DEBEN reflejar, de la manera más precisa que permita la implementación, los tiempos de vida restantes de esas TEK y el momento en que se envía el mensaje respuesta de clave.

9.2 Módem de cable

El CM se encarga de mantener la autorización recibida de su CMTS y de mantener una clave de autorización activa. Un CM DEBE estar preparado para utilizar sus dos AK obtenidas más recientemente.

Las claves de autorización (AK) tienen un tiempo de vida limitado y han de ser renovadas periódicamente. Un CM renueva su clave de autorización reenviando una petición de autorización dirigida al CMTS. La máquina de estados autorización (véase 7.1.2) gestiona la programación de las peticiones de autorización para renovar las AK.

La máquina de estados autorización de un CM programa el comienzo de una reautorización con un plazo de tiempo configurable (el *tiempo de gracia de autorización*) antes de que prescriba según lo previsto la AK más reciente del CM. El tiempo de gracia de autorización se configura de forma que el CM disponga de un periodo de reintentos de autorización suficientemente largo, en previsión de los posibles retardos del sistema, y que disponga asimismo de un plazo de tiempo adecuado para completar de manera satisfactoria el intercambio de autorización antes de que prescriba su AK más reciente.

NOTA – El CMTS no precisa conocer el tiempo de gracia de autorización. El CMTS, no obstante, sigue atentamente el tiempo de vida de las claves de autorización y DEBE desactivarlas una vez que hayan prescrito.

Un módem de cable DEBE utilizar la más nueva de sus dos claves de autorización más recientes cuando calcule los compendios de HMAC que adjunta a las peticiones de clave. DEBE poder utilizar cualquiera de las dos AK más recientes para autenticar mensajes respuesta de clave, rechazo de clave o TEK no válida, y descriptar la TEK criptada de un mensaje respuesta de clave. El CM utiliza el número de secuencia de clave de AK acompañante para determinar cuál de las dos AK utiliza.

La mitad inferior de la figura 9-1 ilustra el mantenimiento y la utilización por parte de un CM de sus claves de autorización.

Un CM DEBE poder mantener dos conjuntos sucesivos de material de aplicación de claves de tráfico por cada SAID autorizado. Con el funcionamiento de sus máquinas de estados TEK, el CM trata de mantener siempre los dos conjuntos más recientes de material de aplicación de claves de tráfico de un SAID.

Para cada uno de sus SAID autorizados, el módem de cable:

- DEBE utilizar la más reciente de sus TEK para criptar tráfico en sentido ascendente recién recibido. El tráfico ya puesto en cola de espera PUEDE utilizar cualquiera de las TEK (sin orden específico) durante un breve periodo de tiempo que abarque la transición de la clave antigua a la clave nueva.
- DEBE poder descriptar tráfico en sentido descendente criptado con cualquiera de las TEK.

El campo KEY_SEQ del elemento EH de privacidad básica identifica el número de secuencia de clave de la TEK utilizada para criptar los datos por paquetes de una PDU. El bit BASCULAR del elemento EH de privacidad, que es igual al bit menos significativo del campo KEY_SEQ, sirve para distinguir entre dos generaciones de claves sucesivas.

9.3 Autenticación de peticiones de servicio dinámico de DOCSIS V1.1/2.0

Si un CM DOCSIS 1.1 o DOCSIS 2.0 se configura para utilizar BPI+, la especificación RFI de DOCSIS 1.1 en [J.112-B] o DOCSIS 2.0 en [J.122] requiere que el CM y el CMTS incluyan compendios de HMAC en todas las peticiones de adición de servicio dinámico (DSA-REQ, *dynamic service addition requests*), peticiones de cambio de servicio dinámico (DSC-REQ, *dynamic service change requests*) y peticiones de supresión de servicio dinámico (DSD-REQ, *dynamic service deletion requests*) que se envíen el uno al otro.

Esos compendios de HMAC de servicio dinámico se manipulan con claves de autenticación de mensajes de BPI+, es decir, las claves de autenticación de mensajes obtenidas a partir de la clave de autorización de BPI+. Los CM y los CMTS DEBEN utilizar las claves de autenticación de mensajes vigentes cuando generen y validen los compendios de HMAC contenidos en peticiones de servicio dinámico.

10 Métodos criptográficos

Esta cláusula especifica los algoritmos criptográficos y los tamaños de clave que utiliza BPI+.

10.1 Criptación de datos por paquetes

La privacidad básica plus DEBE utilizar el modo encadenamiento de bloques cifrados (CBC) [FIPS-81] del algoritmo norma de criptación de datos (DES) de Estados Unidos [FIPS-46-3] para criptar las tramas PDU datos por paquetes de MAC de RF del campo datos por paquetes y los campos cabida útil de fragmentación y CRC de fragmentación de las tramas de fragmentación MAC.

Las implementaciones BPI+ que utilizan soporte físico de DOCSIS 1.1 ó 2.0 (la configuración soporte físico/soporte lógico predominante) DEBEN soportar la clave DES de 56 bits y PUEDE soportar la clave DES de 40 bits.

BPI+ soporta la clave DES de 40 bits sobre todo para hacer posible la interoperabilidad con un soporte físico de DOCSIS 1.0, a 40 bits, perfeccionado para utilizar BPI+. La clave DES de 40 bits es idéntica a la de 56 bits, con la salvedad de que 16 bits de la clave DES de 56 bits se fijan a valores fijos y conocidos. Si un CM o CMTS utiliza DES de 40 bits opcional, DEBE enmascarar (a cero) los 16 bits situados más a la izquierda de cualquier clave DES de 56 bits antes de ejecutar las operaciones de criptación/descriptación.

NOTA – Los bits enmascarados son los 16 bits situados más a la izquierda que estarían presentes DESPUÉS de eliminar todos los bits octavos de la TEK de 64 bits (es decir, los llamados bits de paridad). Los soportes físicos de DOCSIS 1.1 ó 2.0 y de DOCSIS 1.0 a 56 bits que utilicen BPI+ PUEDEN implementar el enmascaramiento de la clave DES de 40 bits en el soporte lógico.

El CBC DEBE ser inicializado con un vector de inicialización proporcionado, junto con otro material de aplicación de cables de SAID, en la respuesta de clave de un CMTS. El encadenamiento se lleva a cabo de bloque a bloque dentro de una trama y se reinicializa trama por trama para que el sistema sea más robusto frente a posibles pérdidas de tramas.

Se DEBE utilizar el procesamiento de bloques de terminación residuales para criptar el bloque final del texto en claro cuando tenga menos de 64 bits. Dado un bloque final con n bits, siendo n inferior a 64, el penúltimo bloque de texto cifrado se cripta de acuerdo con DES una segunda vez, utilizando el modo ECB, y a los n bits menos significativos del resultado se les aplica un operador lógico OR exclusivo con los n bits finales de la cabida útil para generar el bloque de texto cifrado final corto. Para que el receptor descripte este último bloque, la clave DES del receptor cripta el penúltimo bloque de texto cifrado, utilizando el modo ECB, y se aplican operadores lógicos OR exclusivos a los n bits situados más a la izquierda con el bloque de texto cifrado final corto para recuperar el bloque de texto en claro final corto. El procedimiento de criptación se describe en la figura 9-4 (pág. 195) de [SCHNEIER].

En el caso especial de que el texto en claro de la trama que ha de ser criptado sea inferior a 64 bits, el vector de inicialización DEBE ser criptado de acuerdo con DES, y a los n bits situados más a la izquierda del texto cifrado resultante, correspondientes al número de bits de la cabida útil, se les

DEBE aplicar el operador lógico OR exclusivo con los n bits de la cabida útil para generar el bloque de texto cifrado corto[6].

10.2 Criptación de TEK

El CMTS cripta el campo valor de TEK de los mensajes respuesta de clave que envía a los CM clientes. Este campo se cripta utilizando DES triple de dos claves en el modo criptación-descriptación-criptación (EDE) [SCHNEIER]:

criptación: $C = E_{k1}[Dk_2[E_{k1}[P]]]$

descriptación: $P = Dk_1[Ek_2[D_{k1}[C]]]$

P = TEK de 64 bits de texto en claro

C = TEK de 64 bits de texto cifrado

k1 = los 64 bits situados más a la izquierda de la KEK de 128 bits

k2 = los 64 bits situados más a la derecha de la KEK de 128 bits

E[ ] = criptación según el modo ECB (libro de códigos electrónicos) de DES de 56 bits

D[ ] = descriptación ECB de DES de 56 bits

En la cláusula 10.4 se describe la manera de obtener la KEK a partir de la clave de autorización.

10.3 Algoritmo compendio de HMAC

El troceo con clave empleado por el atributo compendio de HMAC DEBE utilizar el método de autenticación de mensajes HMAC [RFC 2104] con el algoritmo de troceo SHA-1 [FIPS 180-2].

Las claves de autenticación de mensajes en sentido ascendente y en sentido descendente se obtienen a partir de la clave de autorización (para los detalles, véase la cláusula 10.4).

10.4 Obtención de las TEK, las KEK y las claves de autenticación de mensajes

El CMTS genera claves de autenticación, TEK (claves de criptación de tráfico) e IV (vectores de inicialización). Se DEBE utilizar un generador de números aleatorios o seudoaleatorios para generar claves de autorización y TEK. También se PUEDE utilizar un generador aleatorio o seudoaleatorio para generar vectores de inicialización; con independencia de cómo se generan, los IV DEBEN ser impredecibles. [RFC 1750] contiene prácticas recomendadas para la generación de números aleatorios a utilizar en los sistemas criptográficos.

[FIPS-81] define claves DES como cantidades de 8 octetos (64 bits) en las que los siete bits más significativos (es decir, los siete bits situados más a la izquierda) de cada octeto son los bits independientes de una clave DES, y el bit menos significativo (es decir, el bit situado más a la derecha) de cada octeto es un bit de paridad que se calcula teniendo en cuenta los siete bits independientes precedentes y se ajusta de manera que el octeto tenga paridad impar.

---

[6] Este método de criptación de cabidas útiles cortas es susceptible de sufrir agresiones: la aplicación del operador lógico OR exclusivo a dos conjuntos de texto cifrado criptado de la manera anterior con el mismo conjunto de material de aplicación de claves dará como resultado el OR exclusivo de los conjuntos correspondientes de texto en claro. En el caso de tramas PDU datos por paquetes, sin embargo, esta cuestión no se plantea porque todas las tramas que lleven datos de usuario protegidos contendrán por lo menos 20 bytes de encabezamiento IP. En el caso de tramas de fragmentación, es posible una trama corta que lleve menos de 8 bytes (64 bits) de texto cifrado; no obstante, los cuatro bytes finales serían la CRC de fragmentación criptada, y los tres o menos bytes antes de la CRC de fragmentación criptada serían la CRC de datos por paquetes criptada.

El material de aplicación de claves para DES triple de dos claves consta de dos claves DES diferentes (únicas).

BPKM no requiere paridad impar. El protocolo BPKM genera y distribuye claves DES de 8 octetos de paridad arbitraria, y precisa que las implementaciones ignoren el valor del bit menos significativo de cada octeto.

De una clave de autorización común se obtienen una clave de criptación de claves (KEK) y dos claves de autenticación de mensajes. A continuación se expone la manera de obtener estas claves:

KEK es la clave de criptación de claves utilizada para criptar claves de criptación de tráfico.

HMAC_KEY_U es la clave de autenticación de mensajes utilizada en mensajes, petición de clave en sentido ascendente.

HMAC_KEY_D es la clave de autenticación de mensajes utilizada en mensajes respuesta de clave, rechazo de clave y TEK no válida.

SHA(x|y) denota el resultado de aplicar la función SHA a las cadenas de bits concatenados x e y.

Truncate(x,n) denota el resultado de truncar x a sus n bits situados más a la izquierda.

```
KEK = Truncate(SHA( K_PAD | AUTH_KEY ), 128)
HMAC_KEY_U = SHA( H_PAD_U | AUTH_KEY )
HMAC_KEY_D = SHA( H_PAD_D | AUTH_KEY )
```

Cada_PAD_ es una cadena de 512 bits:

K_PAD = 0x53 repetido 64 veces.

H_PAD_U = 0x5C repetido 64 veces.

H_PAD_D = 0x3A repetido 64 veces.

10.5 Criptación de clave de autorización con clave pública

Las claves de autorización de los mensajes respuesta de autorización DEBEN ser criptadas con una clave pública RSA, utilizando la clave pública del módem de cable. Las claves RSA de los CM DEBEN utilizar F4 (65537 decimal, o de manera equivalente, 010001 hexadecimal) como su exponente público. BPI+ emplea una longitud de módulo de 768 bits (96 octetos) y de 1024 bits (128 octetos). BPI+ emplea el esquema de criptación RSAES-OAEP especificado en la versión 2.0 de la norma PKCS #1 [RSA3]. El esquema RSAES-OAEP requiere la selección de una función de troceo, de una función de generación de máscaras y una cadena de parámetros de codificación. Cuando se cripta la clave de autorización se DEBEN utilizar las selecciones por defecto especificadas en [RSA3]. Dichas selecciones por defecto son: SHA-1 para la función de troceo, MGF1 con SHA-1 para la función de generación de máscaras y cadena vacía para la cadena de parámetros de codificación.

Cabe destacar que la privacidad básica [SCTE22-2] empleaba el esquema de criptación descrito en la versión 1.5 de la norma PKCS #1 [RSA1]. Se trata del mismo esquema que RSAES-PKCS1-v1_5 de [RSA3]. Para mantener la compatibilidad hacia atrás, los CM y los CMTS DEBEN referirse a RSAES-PKCS1-v1_5 de [RSA3] para criptar la clave de autorización cuando vuelva a BPI.

El protocolo de privacidad básica [SCTE22-2], requerido en los CM DOCSIS 1.0, especifica una longitud de módulo de 768 bits para sus claves RSA. Para permitir la mejora a BPI+ del soporte lógico de los dispositivos CM DOCSIS 1.0, el protocolo BPI+ DEBE soportar longitudes de módulo de 768 y de 1024 bits. Los CM desarrollados originalmente con DOCSIS 1.1 ó 2.0 DEBEN emplear claves RSA con longitudes de módulo de 1024 bits. No obstante, los CM con actualizaciones de DOCSIS 1.0 a DOCSIS 1.1 ó 2.0 PUEDEN emplear claves con una longitud de módulo de 768 bits. Para soportar el interfuncionamiento con los CM v1.0 mejorados, una

implementación BPI+ de CMTS DOCSIS 1.1 ó 2.0 DEBE soportar longitudes de módulo tanto de 768 bits como de 1024 bits.

10.6 Signaturas digitales

BPI+ emplea el algoritmo signatura RSA [RSA3] con SHA-1 [FIPS-186-2] para sus tres tipos de certificado.

Al igual que con sus claves de criptación RSA, BPI+ utiliza F4 (65537 decimal, 010001 hexadecimal) como exponente público para su operación de firma. La CA raíz DOCSIS empleará una longitud de módulo de 2048 bits (256 octetos) para firmar los certificados de CA de fabricante que expide. Las CA de fabricante DEBEN emplear longitudes de módulo de clave de signatura de al menos 1024 bits, y no superiores a 2048 bits. Hay que destacar que la CA raíz DOCSIS se debe considerar como una CA de fabricante para módems de cable conformes a J.122.

10.7 Soporte de algoritmos alternativos

La especificación actual relativa a BPI+ requiere la utilización de DES de 56 bits para criptar datos por paquetes, DES triple de dos claves para criptar claves de criptación de tráfico, RSA de 1024 bits para criptar claves de autorización y RSA de 1024 a 2048 bits para firmar certificados X.509 de BPI+. Las longitudes de clave y los algoritmos elegidos, si bien parecen apropiados para los tipos de amenazas y las capacidades de los soportes lógicos que se consideran actualmente, pueden ser inadecuados en el futuro.

Existe, por ejemplo, un consenso general en el sentido de que DES se está acercando al final de su utilidad práctica en tanto que norma industrial para la criptación simétrica. NIST contempla actualmente el desarrollo y la adopción de un nuevo algoritmo de criptación normalizado, al que se hace referencia habitualmente como norma de criptación avanzada, o AES (*advanced encryption standard*). Dada la naturaleza de los servicios de seguridad cuyo soporte se demanda a BPI+ (privacidad básica a un nivel superior o igual al posible con conductores especializados, y acceso condicional a los servicios de transporte de datos RF) así como la política de gestión de claves de manera flexible del protocolo (es decir, fijación del tiempo de vida de las claves), los proveedores de servicios basados en DOCSIS tendrán motivos para seguir confiando en DES durante, por lo menos, los cinco próximos años. No obstante, en algún momento futuro, los módems de cable de DOCSIS habrán de adoptar un algoritmo de encriptación de tráfico más potente, posiblemente el AES.

La adopción de un algoritmo nuevo para la criptación de datos por paquetes no exigirá el rediseño de BPI+. La utilización coherente del protocolo de codificación de tipo/longitud/valor de los atributos BPKM, los elementos encabezamiento ampliado de encabezamiento MAC y la selección de capacidades de seguridad en el intercambio de autorización garantiza la posibilidad de ampliar el protocolo BPI+. De hecho, los cambios que se introduzcan en cualquier algoritmo criptográfico de BPI+, o las longitudes de claves asociadas, no repercutirán en forma alguna en la estructura general ni en el funcionamiento del protocolo.

11 Protección física de claves en el CM y el CMTS

BPI+ requiere que los CM y los CMTS mantengan las claves de criptación de tráfico y las claves de autorización de CM en su memoria. Un CM DEBE mantener también en memoria permanente, no borrable, un par de claves RSA. Tanto los CM como los CMTS DEBEN impedir el acceso físico no autorizado a este material de aplicación de claves.

El nivel de protección física del material de aplicación de claves que BPI+ exige de los CM y los CMTS se especifica en términos de los niveles de seguridad definidos en [FIPS-140-2]. En particular, los CM y los CMTS DEBEN satisfacer los requisitos del nivel 1 de seguridad de FIPS PUBS 140-2.

El nivel de seguridad 1 de [FIPS-140-2] exige una protección física mínima mediante la utilización de recintos con calidad de producción. Para los requisitos formales, el lector deberá acudir al documento FIPS PUBS; no obstante, a continuación se da un resumen de esos requisitos.

De acuerdo con la clasificación [FIPS-140-2] de las "materializaciones físicas" de los módulos criptográficos, los CMTS y los CM externos son *módulos criptográficos autónomos de múltiples microplaquetas*. [FIPS-140-2] especifica los requisitos siguientes del nivel 1 de seguridad para módulos autónomos de múltiples microplaquetas:

- Las microplaquetas deberán tener calidad de producción, lo que incluye técnicas de pasivación estándar (es decir, aplicación de una pintura sellante sobre la circuitería de las microplaquetas para protegerla contra el deterioro debido al medio ambiente y daños físicos de otro tipo).
- La circuitería deberá implementarse dentro del módulo como una agrupación de múltiples microplaquetas de calidad de producción (es decir, una placa de circuitos impresos integrados, un sustrato cerámico, etc.).
- El módulo deberá estar contenido por completo dentro de un recinto de calidad de producción, metálico o de plástico duro, que puede tener puertas o tapas desmontables.

Un CM interno se clasificaría como un [FIPS-140-2] *módulo criptográfico insertado en múltiples microplaquetas*; los requisitos de seguridad de nivel 1 para estos dispositivos son los que figuran en los dos primeros puntos enumerados anteriormente.

12 Perfil y gestión de certificados X.509 de BPI+

BPI+ de DOCSIS deberá emplear certificados digitales de la versión 3 de [X.509] para autenticar intercambios de clave entre CM y CMTS. [X.509] es una norma de uso general; el perfil del certificado de BPI+, que aquí se describe, especifica además el contenido de los campos definidos del certificado. El perfil del certificado define también la jerarquía de confianza establecida para la gestión y validación de certificados de BPI+ DOCSIS.

Salvo que se indique otra cosa en las cláusulas que siguen, los certificados de BPI+ DOCSIS DEBEN estar en conformidad con las normas PKIX del IETF [RFC 3280]. La utilización de certificados X.509 de DOCSIS está, no obstante, mucho más circunscrita que la de PKIX. El perfil del certificado X.509 de la norma PKIX del IETF está orientado al soporte de un mecanismo de distribución de claves, independiente de la aplicación y basado en el certificado, a través de la Internet pública. El perfil del certificado X.509 de la norma PKIX debe admitir una amplia gama de entornos de comunicación, aplicaciones y relaciones de confianza.

Por el contrario, la utilización por parte de BPI+ de certificados digitales se limita a la salvaguarda de los operadores de cable contra la piratería de los servicios de comunicaciones de datos DOCSIS imponiendo un acceso condicional a las claves de criptación de tráfico. Los servicios de comunicaciones protegidos se dividen en tres categorías:

- servicios de datos IP a alta velocidad y del mejor esfuerzo
- servicios de datos a velocidad primaria constante con recargo
- acceso a grupos de multidifusión IP con recargo.

Así pues, si bien el protocolo BPI+ se apoya de manera notable en trabajos realizados respecto al perfil del certificado X.509 de la norma PKIX del IETF, el perfil X.509 de BPI+ se utiliza mucho más.

El perfil del certificado X.509 de BPI+ procede además, en buena medida, de la norma transacción electrónica segura (SET, *secure electronic transaction*) [SET Book 2]. Tanto la organización global de la presente cláusula como parte de su contenido reflejan esa norma.

12.1 Visión general de la arquitectura de gestión de certificados BPI+

La arquitectura de gestión de certificados BPI+ DOCSIS, mostrada en la figura 12-1, consta de una jerarquía de confianza de tres niveles que soporta tres tipos de certificados de la versión 3 de la X.509.

- un certificado único, auto-firmado, de la autoridad de certificación (CA) DOCSIS raíz;
- certificados de CA de fabricante;
- certificados de CM.

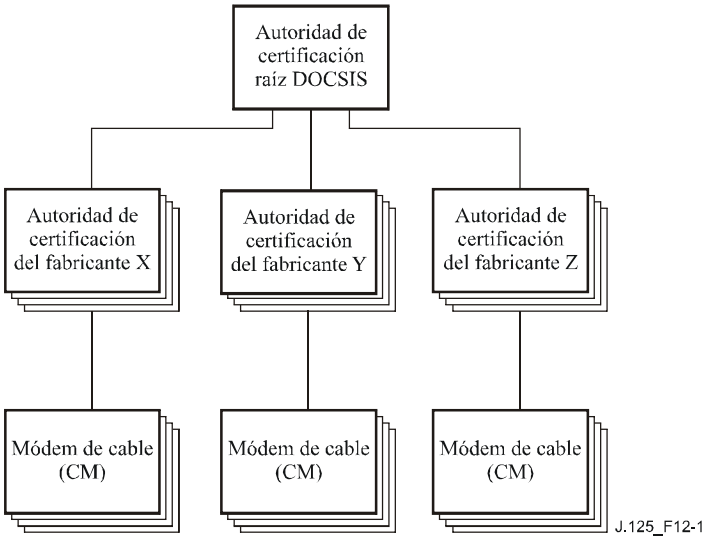


Figura 12-1/J.125 – Arquitectura de gestión de certificados DOCSIS

La autoridad de certificación raíz actúa como la CA raíz que expide certificados a las CA subordinadas mantenidas por los fabricantes. Las CA de los fabricantes expiden certificados a las entidades finales de módem de cable.

NOTA – Un solo fabricante puede mantener múltiples CA (por ejemplo, una CA diferente por cada planta de fabricación).

Actualmente, la autoridad de certificación raíz también es la CA raíz para expedir certificados de verificación de códigos (CVC, *code verification certificate*) para la descarga segura de soporte lógico especificada en el anexo B. No obstante, ninguna razón de seguridad requiere que la misma CA raíz expida el certificado CA de fabricante y el CVC. Por lo tanto el CVC puede ser emitido en el futuro por una autoridad de certificación diferente.

La CA raíz deberá mantenerse bajo estrictos controles físicos. Sólo se accederá a ella de vez en cuando para expedir nuevos certificados de CA de fabricante. La organización responsable de la certificación se encargará del mantenimiento de la CA raíz. La CA raíz generará y distribuirá entre los operadores de cable una lista de revocación de certificados (CRL, *certificate revocation list*) en la que se identifiquen los certificados de fabricante revocados. La manera de distribuir los CRL entre los operadores de cable queda fuera del alcance de la especificación BPI+.

La organización que mantenga la CA raíz deberá definir un protocolo de certificados generados por fabricantes para la CA de fabricante solicitante. La especificación de este protocolo, sin embargo, queda fuera del alcance de la especificación BPI+.

Los fabricantes serán responsables del mantenimiento de su propia CA, desde la que expedirán certificados de CM. Un solo fabricante puede mantener múltiples CA de fabricante. El protocolo para solicitar certificados de una CA de fabricante y distribuir los certificados resultantes entre los módems de cable receptores será un procedimiento interno del fabricante, y queda por tanto fuera

del alcance de la especificación de BPI+. Una CA de fabricante PUEDE generar y distribuir listas de revocación de certificados (CRL) entre los operadores de cable; la manera en que se lleva a cabo esa distribución queda fuera del alcance de la especificación de BPI+.

12.2 Formato de certificado

En esta cláusula se describe el formato del certificado de la versión 3 de la Recomendación X.509 y las extensiones de certificados que se utilizan en BPI+. El cuadro 12-1 siguiente presenta de forma resumida los campos básicos de un certificado versión 3 de X.509.

Cuadro 12-1/J.125 – Campos básicos de un certificado X.509

Campo de versión 3 de X.509	Descripción
tbsCertificate.version	Indica la versión del certificado X.509. Se fija siempre a v3 (valor de 2).
tbsCertificate.serialNumber	Entero único que la CA expedidora asigna al certificado.
tbsCertificate.signature	OID y parámetros opcionales que definen el algoritmo utilizado para firmar el certificado. Este campo DEBE contener el mismo identificador de algoritmo que el campo signatureAlgorithm que figura más adelante.
tbsCertificate.issuer	Nombre distinguido de la CA que expidió el certificado.
tbsCertificate.validity	Especifica cuándo pasa a estar activo el certificado y cuándo prescribe.
tbsCertificate.subject	Nombre distinguido que identifica la entidad cuya clave pública se certifica en el campo información de clave pública del asunto.
tbsCertificate .subjectPublicKeyInfo	Campo que contiene el material de la clave pública (clave pública y parámetros) y el identificador del algoritmo con el que se utiliza la clave.
tbsCertificate .issuerUniqueID	Campo opcional que permite reutilizar nombres de expedidores a lo largo del tiempo.
tbsCertificate .subjectUnique ID	Campo opcional que permite reutilizar nombres de asuntos a lo largo del tiempo.
tbsCertificate.extensions	Datos de la extensión.
signatureAlgorithm	OID y parámetros opcionales que definen el algoritmo utilizado para firmar el certificado. Este campo DEBE contener el mismo identificador de algoritmo que el campo signatura de tbsCertificate.
signatureValue	Signatura digital calculada con el tbsCertificate codificado según las DER de la ASN.1.

Todos los certificados y los CRL que se describen en esta Recomendación DEBEN estar firmados con el algoritmo de signatura (firma) RSA utilizando SHA-1 como función de troceo unidireccional. El algoritmo de signatura RSA se describe en PKCS #1 RSA1; SHA-1 se describe en [FIPS 180-2]. Se trata sólo de un ejemplo de cómo BPI+ restringe los valores de los campos básicos del certificado X.509. A continuación se describen todas estas restricciones.

12.2.1 tbsCertificate.validity.notBefore y tbsCertificate.validity.notAfter

Los certificados de módem de cable no serán renovables, y, deben tener por tanto, un periodo de validez superior al tiempo de vida operativa del módem de cable. Un certificado de CA de fabricante DEBE ser válido durante un periodo de tiempo definido por [SCTE23-3] o [SCTE79-2] y se renovará por un periodo definido por [SCTE23-3] o [SCTE79-2]. El certificado de CA DOCSIS raíz debe ser válido a partir de la fecha en que la CA raíz empieza a actuar, durante un periodo de

tiempo definido por [SCTE23-3] o [SCTE79-2] y se renovará por un periodo definido por [SCTE23-3] o [SCTE79-2].

En la presente Recomendación se supone que el tiempo de vida operativa de un módem de cable no superará los 20 años. El periodo de validez de un certificado de módem de cable DEBE empezar con los datos de fabricación del equipo; el periodo de validez DEBERÍA extenderse durante al menos 20 años a partir de la fecha de fabricación.

Los periodos de validez DEBEN ser codificados como tiempo UTCT (UTCTime). Los valores de tiempo UTCT DEBEN expresarse como tiempo medio de Greenwich (Zulu) y DEBEN incluir los segundos (es decir, los tiempos son YYMMDDHHMMSSZ), incluso cuando el número de segundos sea cero. El campo año (YY) DEBE interpretarse como sigue:

- cuando YY sea superior o igual a 50, el año se interpretará como 19YY;
- cuando YY sea inferior a 50, el año se interpretará como 20YY.

12.2.2 tbsCertificate.serialNumber

Los números de serie de certificados DEBEN ser números enteros positivos asignados por la CA para cada certificado. DEBEN ser únicos para cada certificado expedido por una determinada CA (es decir, el nombre del expedidor y el número de serie identifican a un único certificado). Las CA DEBEN obligar a que el número de serie sea un número entero no negativo. El fabricante NO DEBERÍA imponer o asumir una relación entre el número de serie del certificado y el número de serie del módem para el que se expide el certificado.

Dados los requisitos particulares anteriores, se puede esperar que los números de serie estén constituidos por números enteros grandes. Los usuarios de certificados DEBEN de ser capaces de manejar valores de números de serie de hasta 20 octetos. Las CA expedidoras NO DEBEN utilizar valores superiores a 20 octetos.

NOTA – Los usuarios de certificados de sistemas DOCSIS 1.1 ó 2.0 DEBEN estar preparados para manejar certificados que puedan tener números de serie negativos o cero, para asegurar la compatibilidad hacia atrás.

12.2.3 tbsCertificate.signature y signatureAlgorithm

Todos los certificados y las CRL que se describen en esta Recomendación DEBEN ser firmados con el algoritmo de signatura RSA, utilizando SHA-1 como función de troceo unidireccional. El algoritmo de signatura RSA se describe en PKCS #1 [RSA1]; SHA-1 se describe en [FIPS 180-2].

El ID de objeto (OID, *object ID*) de la ASN.1 utilizado para identificar el algoritmo de signatura "SHA-1 con RSA" es:

```
sha-1WithRSAEncryption OBJECT IDENTIFIER ::= {
     iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)
     pkcs-1(1) 5}
```

Cuando el OID sha-1WithRSAEncryption aparece dentro del AlgorithmIdentifier (identificador de algoritmo) tipo ASN.1, como es el caso tanto en tbsCertificate.signature como en signatureAlgorithm, el componente parámetros de ese tipo es el tipo NULO de ASN.1.

12.2.4 tbsCertificate.issuer y tbsCertificate.subject

Los nombres X.509 son SECUENCIAS de RelativeDistinguishedNames (nombres distinguidos relativos), que a su vez son CONJUNTOS de AttributeTypeAndValue (tipo y valor de atributo). AttributeTypeAndValue es una SECUENCIA de un AttributeType (tipo de atributo) (un IDENTIFICADOR DE OBJETO) y un AttributeValue (valor de atributo). El valor del atributo countryName (nombre de país) DEBE ser una PrintableString (cadena imprimible) de 2 caracteres, tomada de la norma ISO 3166; todos los demás AttributeValues (valores de atributo) DEBEN ser codificados como T.61/TeletexString (cadena de teletexto) o como cadenas de

caracteres PrintableString. Se DEBE utilizar la codificación PrintableString si la cadena de caracteres sólo contiene caracteres del conjunto PrintableString. De manera específica:

abcdefghijklmnopqrstuvwxyz
ABCDEFGHIJKLMNOPQRSTUVWXYZ
0123456789
'()+,-./:=? y espacio.

Se DEBE utilizar la T.61/TeletexString si la cadena de caracteres contiene otros caracteres.

Los OID que se indican a continuación se necesitan para definir nombres de expedidor y asunto en certificados BPI+:

```
id-at OBJECT IDENTIFIER ::= {joint-iso-ccitt(2) ds(5) 4}
id-at-commonName        OBJECT IDENTIFIER ::= {id-at 3}
id-at-countryName       OBJECT IDENTIFIER ::= {id-at 6}
id-at-localityName              OBJECT IDENTIFIER ::= {id-at 7}
id-at-stateOrProvinceName       OBJECT IDENTIFIER ::= {id-at 8}
id-at-organizationName          OBJECT IDENTIFIER ::= {id-at 10}
id-at-organizationalUnitName    OBJECT IDENTIFIER ::= {id-at 11}
```

En las cláusulas que siguen se describe el formato del campo nombre del asunto de cada tipo de certificado de BPI+. El campo nombre del expedidor de un certificado concuerda con el campo nombre del asunto del certificado que se expide. Cualquier certificado transmitido por un CM en un mensaje información de autorización o petición de autorización DEBE tener campos de nombre que se atengan al formato indicado. Un CMTS PUEDE decidir aceptar certificados que tienen campos de nombre no conformes con el formato indicado.

Por lo general, los certificados X.509 soportan un conjunto no estricto de reglas para determinar si el nombre del expedidor de un certificado concuerda con el nombre del asunto de otro. Las reglas permiten incluso que dos campos de nombre se puedan declarar concordantes incluso si de una comparación binaria de ambos campos no se deduce esa concordancia. [RFC 3280] recomienda que las autoridades certificadoras limiten la codificación de campos de nombre para que una implementación pueda declarar concordancia o discrepancia utilizando una comparación binaria simple, y BPI+ sigue esa recomendación. En consecuencia, el campo tbsCertificate.issuer codificado según las DER de un certificado BPI+ DEBE concordar exactamente con el campo tbsCertificate.subject codificado según las DER del certificado de su expedidor. Una implementación PUEDE comparar un nombre de expedidor con un nombre de asunto efectuando una comparación binaria de los campos tbsCertificate.issuer y tbsCertificate.subject codificadas según las DER.

12.2.4.1 Certificado DOCSIS raíz

countryName=EE.UU.

organizationName=Especificaciones de la interfaz del servicio de datos por cable

organizationalUnitName=Módems de cable

commonName=Autoridad de certificación raíz del módem de cable DOCSIS.

Los atributos countryName (nombre de país), organizationName (nombre de organización), organizationalUnitName (nombre de unidad organizacional) y commonName (nombre común) DEBEN ser incluidos y DEBEN tener los valores mostrados. Otros valores no están permitidos y NO DEBEN ser incluidos.

12.2.4.2 Certificado DOCSIS de fabricante

countryName=<país del fabricante>

[stateOrProvinceName=< estado/provincia>]

[localityName=<ciudad>]

organizationName=<nombre de la empresa>

organizationalUnitName= DOCSIS

[organizationalUnitName=<ubicación de la fábrica>]

commonName=<nombre de la empresa> [<identificación de serie>]autoridad de certificación raíz del módem de cable [<identificación de serie>]

Los atributos countryName, organizationName y commonName DEBEN ser incluidos y DEBEN tener los valores mostrados.

commonName PUEDE contener un identificador de serie (por ejemplo, 1, 2, UNO, DOS, A; B; I; II, etc.) para identificar diferentes CA de fabricante emitidos por los mismos fabricantes con el mismo nombre de empresa.

El atributo organizationalUnitName que tiene el valor "DOCSIS" DEBE ser incluido.

El atributo organizationalUnitName que representa la ubicación de la fábrica DEBERÍA ser incluido. Si se incluye, DEBE estar precedido por el atributo organizationalUnitName con el valor "DOCSIS".

Los atributos stateOrProvinceName (nombre del estado o la provincia) y localityName (nombre de la localidad) PUEDEN ser incluidos.

Otros atributos no están permitidos y NO DEBEN ser incluidos.

12.2.4.3 Certificado de módem de cable

countryName=<país del fabricante>

organizationName=<nombre de la empresa>

organizationalUnitName=<ubicación de la fábrica>

commonName=<número de serie>

commonName=<dirección MAC>

Para distinguir entre dos commonNames (nombres comunes), el commonName que representa el "número de serie" DEBE preceder al commonName que representa la "dirección MAC". La utilización del campo número de serie está en desuso. Si se utiliza, el número de serie DEBE ser un identificador de módem de cable único, pero PUEDE ser diferente del número de serie codificado en los atributos BPKM. La dirección MAC del certificado de CM DEBE ser la misma que la dirección MAC de los atributos BPKM.

Los caracteres empleados en la representación PrintableString (cadena imprimible) de los números de serie de CM DEBEN estar limitados al subconjunto de caracteres siguiente:

- A-Z (0x41-0x5A)
- a-z (0x61-0x7A)
- 0-9 (0x30-0x39)
- "–" (0x2D)

La dirección MAC se expresa mediante seis pares de dígitos hexadecimales separados por el signo dos puntos (:), por ejemplo, "00:60:21:A5:0A:23". Los caracteres hexadecimales alfanuméricos (A-F) DEBEN representarse mediante letras mayúsculas.

El organizationalUnitName (nombre de la unidad organizacional) de un certificado de módem de cable, que describe la ubicación del fabricante del módem, DEBERÍA ser el mismo que el organizationalUnitName del nombre del expedidor que describe la ubicación de una fábrica.

Los atributos countryName, organizationName, organizationalUnitName y commonName (dirección MAC) DEBEN ser incluidos. El atributo commonName (número de serie) PUEDE ser incluido. Otros atributos no están permitidos y NO DEBEN ser incluidos.

12.2.5 tbsCertificate.subjectPublicKeyInfo

El campo tbsCertificate.subjectPublicKeyInfo contiene la clave pública y el identificador del algoritmo de la clave pública. La clave pública RSA del certificado de CM DEBE ser la misma que la clave pública RSA de los atributos BPKM.

El campo tbsCertificate.subjectPublicKeyInfo.algorithm es una estructura AlgorithmIdentifier (identificador de algoritmo). El algoritmo del AlgorithemIdentifier DEBE ser una criptación RSA, identificada por el siguiente OID:

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

rsaEncryption OBJECT IDENTIFIER ::= { pkcs-1 1}
```

El campo de parámetros del AlgorithmIdentifier DEBE tener NULO tipo ASN.1.

La clave pública RSA deberá codificarse utilizando la RSAPublicKey tipo ASN.1:

```
RSAPublicKey ::= SEQUENCE {
     modulus            INTEGER, -- n
     publicExponent     INTEGER, -- e -- }
```

donde modulus es el módulo n, y publicExponent es el exponente público e. La RSAPublicKey (clave pública RSA) codificada según las DER es el valor de la CADENA DE BITS tbsCertificate.subjectPublicKeyInfo.subjectPublicKey.

12.2.6 tbsCertificate.issuerUniqueID y tbsCertificate.subjectUniqueID

Los campos issuerUniqueID (ID único de expedidor) y subjectUniqueID (ID único de asunto) DEBEN ser omitidos para los tres tipos de certificado BIP+.

12.2.7 tbsCertificate.extensions

No se exige que los certificados de módem de cable ni los de CA de fabricante DOCSIS incluyan extensión alguna; esto es así incluso si las extensiones son obligatorias según [RFC3280]. Los certificados de módem de cable y los certificados de CA de fabricante DOCSIS pueden incluir las extensiones que se describen en 12.2.7.1 y 12.2.7.2, respectivamente. La subcláusula 12.2.7.3 especifica los requisitos de las extensiones al certificado CA raíz. Las extensiones incluidas en certificados BPI+ DEBEN ser conformes a [RFC 3280].

12.2.7.1 Certificados de módem de cable

Los certificados de módem de cable PUEDEN contener extensiones no críticas; NO DEBEN contener extensiones críticas. Si está presente la extensión KeyUsage (utilización de clave), los bits digitalSignature (firma digital) y keyEncipherment (cifrado de clave) DEBEN ser activados, los bits keyCertSign (signo de certificado de clave) y cRLSign (signo de CRL) DEBEN ser desactivados, y todos los demás bits DEBERÍAN ser desactivados. Las extensiones limitaciones básicas PUEDEN aparecer como extensiones no críticas en los certificados de módem de cable.

12.2.7.2 Certificados de CA de fabricante DOCSIS

Los certificados de CA de fabricante DOCSIS PUEDEN contener la extensión limitaciones básicas y/o la extensión utilización de clave. Si se incluyen, estas extensiones PUEDEN aparecer como extensiones críticas o no críticas.

Los certificados de CA de fabricante DOCSIS PUEDEN contener extensiones no críticas; NO DEBEN contener extensiones críticas distintas de, quizás, la extensión de limitaciones básicas y la de utilización de claves.

Si la extensión KeyUsage está presente en un certificado de CA de fabricante DOCSIS, se DEBE activar el bit keyCertSign, se PUEDE activar el bit cRLSign y se DEBERÍAN desactivar todos los demás bits.

Si la extensión limitaciones básicas está presente, se DEBE fijar cA a VERDADERO y se DEBE fijar a cero pathLenConstraint.

12.2.7.3 Certificados de CA raíz DOCSIS

Los certificados de CA raíz DOCSIS DEBEN contener la extensión limitaciones básicas y/o la extensión utilización de clave como extensiones críticas.

Los certificados de CA raíz DOCSIS PUEDEN contener extensiones no críticas; NO DEBEN contener extensiones críticas distintas de, quizás, la extensión limitaciones básicas y la extensión utilización de claves.

Para la extensión utilización de claves, se DEBE activar el bit keyCertSign, se PUEDE activar el bit cRLSign y se DEBERÍAN desactivar todos los demás bits.

Para la extensión limitaciones básicas, se DEBE fijar CA a VERDADERO y se DEBE fijar a uno pathLenConstraint.

12.2.8 signatureValue

En los tres tipos de certificado de BPI+, el signatureValue (valor de signatura), contiene la signatura RSA (con SHA-1) calculada en el certificado tbsCertificate codificado según las DER de la ASN.1. Este último certificado se utiliza como entrada en la función signatura RSA. El valor de signatura resultante se codifica de acuerdo con la ASN.1 como una CADENA DE BITS y se incluye en el campo signatureValue del certificado.

12.3 Almacenamiento y gestión de certificados de módem de cable en el CM

Los certificados de CM expedidos por los fabricantes DEBEN almacenarse en memoria permanente y no borrable de los CM. Los CM que tienen pares de claves privada/pública RSA instaladas en fábrica DEBEN tener también certificados de CM instalados en fábrica. Los CM que dependen de algoritmos internos para generar un par de claves RSA DEBEN disponer de un mecanismo que permita instalar el certificado de CM expedido por el fabricante tras la generación de las claves.

La clave pública de la autoridad de certificación (CA) raíz para la verificación de CVC, que utiliza el CM para verificar el certificado de verificación de código para la descarga segura de soporte lógico definida en el anexo B, se DEBE situar en la memoria no volátil del CM. Aunque la CA raíz DOCSIS para la cadena de certificados de módem de cable expide el CVC, una CA raíz diferente podrá expedir el CVC en el futuro. Por lo tanto, el CM NO DEBE utilizar la clave pública de CA para la verificación de CVC incluida en la memoria no volátil para comprobar la cadena de certificados de módem de cable.

El certificado de CA de la CA del fabricante que firmó el certificado del CM, DEBE ser almacenado en la memoria no volátil del módem de cable. El módem de cable DEBE ser capaz de actualizar o sustituir el certificado de CA del fabricante vía fichero de telecarga de código DOCSIS (véase el anexo B). El certificado de CA del fabricante PUEDE ser incorporado en el soporte lógico del CM.

Si el certificado de CA del fabricante se incorpora en el soporte lógico del CM, cuando un fabricante expida certificados de CM con múltiples certificados de CA, la memoria del CM deberá incluir TODOS esos certificados de CA de fabricante. El certificado de CA del fabricante específico

instalado por el CM (es decir, anunciado en los mensajes información de autenticación y devuelto por el objeto base de información de gestión (MIB), será el que identifique al expedidor del certificado de CM de ese módem.

12.4 Procesamiento y gestión de certificados en el CMTS

BPKM emplea certificados digitales para permitir a los CMTS verificar la vinculación entre la identidad de un CM (codificado en los nombres del asunto de un certificado digital X.509) y su clave pública. El CMTS hace esto validando el trayecto o la cadena de certificación del certificado del CM. Dicho trayecto constará normalmente de tres certificados encadenados: empezando con el certificado del CM, el trayecto lleva al certificado de la CA del fabricante que expidió el certificado del CM y termina en el certificado auto-firmado de la CA raíz DOCSIS (figura 12-2). Validación de la cadena significa que se verifica la signatura o firma del certificado de la CA del fabricante con la clave pública de la CA raíz DOCSIS y que se verifica a continuación la signatura del certificado del CM con la clave pública de la CA del fabricante.

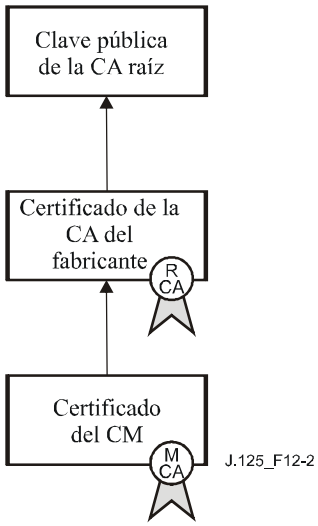


Figura 12-2/J.126 – Cadena de certificación de CM

BPI+ requiere que los CMTS soporten controles administrativos que permitan al operador anular una validación de cadena de certificación especificando si una CA de fabricante o un certificado de CM puede ser o no fiduciado. Se ha de dar una descripción detallada de esos controles administrativos sobre la gestión de certificados del CMTS en un documento OSS asociado de BPI+ [DOCSIS8]. La presente cláusula especifica el modelo de gestión para el ejercicio de esos controles, así como el proceso que lleva a cabo un CMTS para evaluar la validez de un certificado de CM, y verificar así la vinculación entre la identidad del CM y su clave pública.

12.4.1 Modelo de gestión de certificados del CMTS

El CMTS mantiene copias de certificados de CA raíz, CA de fabricante y de módem de cable, que obtiene mediante aprovisionamiento o mensajería BPKM. Se DEBE marcar el estado en que se halla cada uno de los certificados de los que el CMTS tiene conocimiento, y que puede ser uno de los cuatro siguientes: no fiduciado, fiduciado, encadenado o raíz. Sólo el certificado de la CA raíz DOCSIS (un certificado auto-firmado que contiene la clave pública fiduciada de la CA raíz DOCSIS) DEBE ser marcado como raíz. Sin embargo, un CMTS PUEDE soportar múltiples certificados de CA raíz. Los certificados raíz DEBEN ser aprovisionados dentro de un CMTS y el CMTS DEBE soportar la función para mostrar el o los certificados raíz completos y/o su huella dactilar de forma que el operador pueda verificar dichos certificados.

Un CMTS tiene conocimiento de los certificados de CA de fabricante a través de la interfaz de aprovisionamiento del CMTS o por la recepción y procesamiento de mensajes información de autenticación de los CM clientes. Con independencia de cómo obtiene un CMTS su certificado de CA de fabricante, el CMTS DEBE marcarlos como no fiduciados, fiduciados o encadenados. Si un certificado de CA de fabricante *no está* auto-firmado, el CMTS la marca como encadenado. El CMTS, no obstante, DEBE soportar controles administrativos que permitan a un operador anular la marcación de encadenado y especificar que un determinado certificado de CA de fabricante es fiduciado o no fiduciado.

Si un certificado de CA de fabricante *está* auto-firmado, el CMTS lo marca como fiduciado o no fiduciado, de acuerdo con la política del CMTS controlada administrativamente. Un certificado de CA de fabricante auto-firmado cuya signatura (firma) no pueda ser verificada DEBE ser marcado como no fiduciado. La fiduciación por parte de los CMTS de certificados de CA de fabricante auto-firmados DEBE ser configurable. La fiduciación por defecto de certificados de CA de fabricante auto-firmados NO SE RECOMIENDA en sistemas operativos comerciales; la fiduciación por defecto debería utilizarse como soporte de la certificación y de otros modos de prueba. El CMTS DEBE marcar el certificado de CM como encadenado a menos que lo invalide el control administrativo del CMTS.

Un CMTS obtiene copias de certificados de módem de cable en las peticiones de autorización que recibe de los CM clientes. Los certificados de módem de cable DEBEN ser expedidos por una autoridad de certificación (CA) de fabricante; así pues, a no ser que los invalide el control administrativo del CMTS, los certificados de CM serán marcados por el CMTS como encadenados. Un operador puede, como parte del proceso de aprovisionamiento del módem, especificar que el certificado de un CM determinado se marque como no fiduciado o fiduciado.

12.4.2 Validación de certificados

El CMTS valida los trayectos de certificación de CA de fabricante y los certificados de CM aplicando los criterios que se indican a continuación.

NOTA – Los criterios son iterativos y un CMTS DEBE validar el trayecto de certificación de un certificado de CA de fabricante encadenado antes de que pueda validar el trayecto de certificación de un certificado de CM expedido por esa CA de fabricante.

El CMTS DEBE marcar los certificados de CA de fabricante y de módem de cable como válidos o no válidos si sus trayectos de certificación son válidos o no válidos, respectivamente. Los certificados fiduciados son válidos, incluso si el momento en que se examinan no está dentro de su periodo de validez. Los certificados no fiduciados NO DEBEN ser válidos.

Un certificado encadenado es válido si:

1) el certificado se encadena con un certificado raíz, fiduciado o válido;
2) la signatura o firma del certificado puede ser verificada con la clave pública del expedidor;
3) el momento en que se analiza queda dentro del periodo de validez de cada certificado encadenado o raíz dentro de la cadena de certificación (BPI+ no requiere la superposición de los periodos de validez, es decir, no hace falta que todo el periodo de validez de un certificado quede dentro del periodo de validez de su certificado de emisión);
4) el certificado no está en una lista actualizada permanentemente (hot lis) de certificados de CM y CA de fabricante (véase 12.4.4);
5) en el caso de un certificado de CM, la dirección MAC del CM codificada en su campo tbsCertificate.subject y la clave pública RSA codificada en su campo tbsCertificate.subjectPublicKeyInfo concuerdan con la dirección MAC del CM y la clave pública RSA codificada en los atributos BPKM de la petición de autorización;
6) en el caso de un certificado de CM, si la extensión KeyUsage está presente se activan los bits digitalSignature y/o keyAgreement, se activa el bit keyEncipherment y se desactivan

los bits keyCertSign y cRLSign; en el caso de un certificado de CA de fabricante, si está presente la extensión KeyUsage, se activa el bit keyCertSign.

El criterio 3 anterior se tiene en cuenta o se ignora según decida el control administrativo.

Si se HABILITA la comprobación del periodo de validez y el CMTS no ha adquirido la hora del día, se DEBE devolver un mensaje de rechazo de autorización (no permanente) en respuesta a una petición de autorización de estilo BPI+.

Si un certificado encadenado no cumple ninguno de los criterios de validez anteriores, el CMTS DEBE identificarlo como no válido.

12.4.3 Huellas dactilares de un certificado

Las huellas dactilares son funciones de troceo unidireccional resistente a la colisión (por ejemplo SHA-1) de certificados. Representan una manera consistente de identificación de los certificados. Un CMTS PUEDE guardar huellas dactilares de los certificados de CM y CA de fabricante que retiene o que ha validado. Utilizando las huellas dactilares, un CMTS puede guardar en memoria (caché) los resultados de una operación de validación anterior: contrastando la huella dactilar de un certificado recién ofrecido con una huella dactilar guardada en memoria, puede determinar rápidamente la validez del certificado de que se trate.

12.4.4 Listas de certificados de CA de fabricante y de CM actualizadas permanentemente

Cuando el CMTS encadena certificados de validación, no es preciso que compruebe la situación de revocación o no de un certificado (es decir, la presencia o no del certificado en una CRL actualizada). El CMTS, no obstante, DEBE ser capaz de mantener *listas actualizadas permanentemente* de certificados de CA de fabricante y de CM conocidos, no fiduciados. Los certificados de esas listas calientes pueden incluir certificados revocados por sus expedidores; sin embargo, también pueden incluir certificados válidos que el operador de cable que explota el CMTS decide marcar como "no fiduciados".

La definición de los procedimientos y protocolos para el mantenimiento de listas calientes de certificados de CA de fabricante y certificados de CM de un CMTS queda fuera del alcance de la Recomendación BPI+.

Anexo A

Extensiones de fichero de configuración TFTP

Todos los valores de parámetros de configuración de privacidad básica de un CM se especifican en el fichero de configuración telecargado vía TFTP por el CM durante la inicialización MAC de RF. Los campos de fijación de la configuración de privacidad básica se incluyen tanto en los cálculos de MIC del CM como de MIC del CMTS, y en las peticiones de registro de un CM. Para el orden en que se incluyen los campos de fijación de configuración de privacidad básica en el compendio MD5 de MIC del CMTS, véase [J.112-B].

A.1 Codificaciones

Las codificaciones de tipo/longitud/valor que siguen DEBEN ser utilizadas para cualesquiera fijaciones de configuración privacidad básica incluidas en el fichero de la configuración. Las fijaciones de configuración de privacidad básica en las peticiones de registro de CM MAC de RF DEBEN ser las mismas que las incluidas en el fichero de la configuración. Todas las cantidades multioctectos están en el orden de bytes de la red, es decir, el octeto que contiene los bits más significativo es el primero que se transmite por el cable.

A.1.1 Fijación de configuración privacidad básica

La combinación de la fijación de configuración habilitación de privacidad de la RFI 1.1 ó 2.0 ([J.112-B] cláusula B.C.1.1.16) ó [J.122] y de la fijación de capacidad de módem para el soporte de privacidad ([J.112-B] cláusula B.C.1.3.1.6) o [J.122] controla si la privacidad de referencia plus está habilitada o deshabilitada en un CM. Si el operador pretende proveer a un CM para que funcione en el modo BPI+ utilizando los parámetros de configuración BPI por defecto especificados en el cuadro A.1, se PUEDEN omitir las fijaciones de configuración de privacidad básica en el fichero de la configuración. Si el fichero de la configuración no tiene todos los parámetros BPI+ necesarios, el CM DEBE utilizar el valor o valores por defecto especificados en el cuadro A.1 para los restantes parámetros. Por otra parte, si el operador pretende proveer a un CM para que funcione en el modo BPI+ utilizando parámetros de configuración BPI distintos de los valores por defecto del cuadro A.1, DEBEN estar presentes las fijaciones de configuración de privacidad básica. Si la privacidad básica plus no está habilitada, PUEDE estar presente la fijación configuración de privacidad básica. El parámetro diferenciado habilitación de privacidad permite a un operador deshabilitar o volver a habilitar la privacidad básica fijando un único parámetro de configuración, por lo que no se requiere la supresión o reinserción de un conjunto mayor de parámetros de configuración de privacidad básica.

Este campo define los parámetros asociados con el funcionamiento de la privacidad básica. Se compone de un cierto número de campos tipo/longitud/valor encapsulados. Los campos tipos definidos sólo son válidos dentro de la cadena de fijaciones de la configuración privacidad básica encapsuladas.

Tipo	Longitud	Valor
BP_CFG	n	

[J.112-B] o [J.122] define el valor específico de BP_CFG.

A.1.1.1 Codificaciones de privacidad básica internas

A.1.1.1.1 Temporización de espera de autorización

El valor de este campo especifica el intervalo de retransmisión, en segundos, de mensajes petición de autorización desde el estado espera de autorización.

Subtipo	Longitud	Valor
1	4	

Gama válida: 1-30

A.1.1.1.2 Temporización de espera de reautorización

El valor de este campo especifica el intervalo de retransmisión, en segundos, de mensajes petición de autorización desde el estado espera de autorización.

Subtipo	Longitud	Valor
2	4	

Gama válida: 1-30

A.1.1.1.3 Tiempo de gracia de autorización

El valor de este campo especifica el periodo de gracia para la reautorización, en segundos.

Subtipo	Longitud	Valor
3	4	

Gama válida: 1-6 047 999

A.1.1.1.4 Temporización de espera operativa

El valor de este campo especifica el intervalo de retransmisión, en segundos, de peticiones de clave desde el estado espera operativa.

Subtipo	Longitud	Valor
4	4	

Gama válida: 1-10

A.1.1.1.5 Temporización de espera de nueva aplicación de clave

El valor de este campo especifica el intervalo de retransmisión, en segundos, de peticiones de clave desde el estado espera de nueva aplicación de clave.

Subtipo	Longitud	Valor
5	4	

Gama válida: 1-10

A.1.1.1.6 Tiempo de gracia de TEK

El valor de este campo especifica el periodo de gracia, en segundos, de nueva aplicación de la TEK.

Subtipo	Longitud	Valor
6	4	

Gama válida: 1-302399

A.1.1.1.7 Temporización de espera de rechazo de autorización

El valor de este campo especifica la duración de la espera, en segundos, de un CM en el estado espera de rechazo de autorización después de recibir un rechazo de autorización.

Subtipo	Longitud	Valor
7	4	

Gama válida: 1-600

A.1.1.1.8 Temporización de espera de relación de correspondencia de SA

El valor de este campo especifica el intervalo de retransmisión, en segundos, de peticiones de relación de correspondencia de SA desde el estado espera de establecimiento de correspondencia.

Subtipo	Longitud	Valor
8	4	

Gama válida: 1-10

A.1.1.1.9 Reintentos máximos de relación de correspondencia de SA

El valor de este campo especifica el número máximo de reintentos de petición de relación de correspondencia (Map) permitido.

Subtipo	Longitud	Valor
9	4	

Gama válida: 0-10

A.2 Directrices sobre parámetros

A continuación se dan gamas y valores recomendados para los diversos parámetros de configuración y parámetros operativos de la privacidad básica. Esas gamas y esos valores por

defecto pueden cambiar a medida que los proveedores de servicios adquieran experiencia en la aplicación de la privacidad básica.

Cuadro A.1/J.125 – Gamas operativas recomendadas para parámetros de configuración de BPI

Sistema	Nombre	Descripción	Valor mínimo	Valor por defecto	Valor máximo
CMTS	Tiempo de vida de autorización	Tiempo de vida, en segundos, que el CMTS asigna a una clave de autorización nueva	1 día (86 400 s)	7 días (604 800 s)	70 días (6 048 000 s)
CMTS	Tiempo de vida de TEK	Tiempo de vida, en segundos, que el CMTS asigna a una TEK nueva	30 min (1800 s)	12 horas (43 200 s)	7 días (604 800 s)
CM	Temporización de espera de autorización	Intervalo de retransmisión de petición de autorización desde el estado espera de autorización	2 s	10 s	30 s
CM	Temporización de espera de reautorización	Intervalo de retransmisión de petición de autorización desde el estado espera de reautorización	2 s	10 s	30 s
CM	Tiempo de gracia de autorización	Tiempo de adelanto del comienzo de la reautorización por el CM respecto a la autorización	5 min (300 s)	10 min (600 s)	35 días (3 024 000 s)
CM	Temporización de espera operativa	Intervalo de retransmisión de petición de clave desde el estado espera operativa	1 s	10 s	10 s
CM	Temporización de espera de nueva aplicación de clave	Intervalo de retransmisión de petición de clave desde el estado espera de nueva aplicación de clave	1 s	10 s	10 s
CM	Tiempo de gracia de TEK	Tiempo de adelanto del comienzo de la nueva aplicación de clave por el CM respecto a la prescripción de la TEK	5 min (300 s)	1 hora (3600 s)	3,5 días (302 399 s)
CM	Espera de rechazo de autorización	Plazo de tiempo antes de reenviar una petición de autorización tras recibir un rechazo de autorización	10 s	60 s	10 min (600 s)
CM	Temporización de espera de relación de correspondencia de SA	Intervalo de retransmisión de petición de relación de correspondencia desde el estado espera de establecimiento de correspondencia	1 s	1 s	10 s

Cuadro A.1/J.125 – Gamas operativas recomendadas para parámetros de configuración de BPI

Sistema	Nombre	Descripción	Valor mínimo	Valor por defecto	Valor máximo
CM	Reintentos máximos de relación de correspondencia de SA	Número máximo de veces que el CM intenta la petición de relación de correspondencia de SA antes de abandonar	0	4	10

La gama válida (frente a la gama operativa recomendada) de tiempos de vida de autorización y TEK es como sigue:

- Gama válida de tiempo de vida de autorización: 1 a 6 048 000 segundos.
- Gama válida de tiempo de vida de TEK: 1 a 604 800 segundos.

Las gamas válidas definidas para cada uno de los parámetros de la configuración de BPI se extienden por debajo de las gamas operativas recomendadas. A efectos de prueba de protocolos, resulta útil aplicar el protocolo BPI con valores de temporizador muy por debajo del extremo inferior de las gamas operativas recomendadas. Los valores de temporizador más reducidos "aceleran" el reloj de la BPI, provocando la ocurrencia de eventos de máquina de estados de protocolo BPI mucho más rápidamente de lo que sería el caso con una configuración "operativa". Si bien no es preciso diseñar las implementaciones BPI para que funcionen eficazmente a ese ritmo acelerado de BPI, la implementación del protocolo DEBERÍA funcionar de manera correcta con esas temporizaciones más breves. El cuadro A.2 contiene una lista de valores de parámetros reducidos que probablemente se empleen en pruebas de conformidad de protocolos y certificación.

Cuadro A.2/J.125 – Valores de parámetros de BPI reducidos para pruebas de protocolos

Tiempo de vida de autorización	5 min (300 s)
Tiempo de vida de TEK	3 min (180 s)
Tiempo de gracia de autorización	1 min (60 s)
Tiempo de gracia de TEK	1 min (60 s)

El tiempo de gracia de TEK DEBE ser inferior a la mitad del tiempo de vida de la TEK.

Anexo B

Verificación de soporte lógico operativo telecargado

B.1 Introducción

El sistema DOCSIS soporta la telecarga a distancia de un código en los módems de cable de red. El origen y la integridad del código telecargado son importantes a efectos del funcionamiento y la seguridad globales del sistema DOCSIS.

El módulo de telecarga de soporte lógico constituye un objetivo atractivo para cualquier atacante. Si un atacante fuese capaz de organizar un ataque escalable contra el módulo de telecarga de soporte lógico, podría incluso instalar un código que inhabilitara todos los CM dentro de un dominio, o

provocar una perturbación del servicio de gran magnitud. Para impedir esos ataques, habrá que interponer diversas barreras de seguridad entre el atacante y su objetivo.

B.2 Visión de conjunto

Los requisitos definidos en esta cláusula se refieren a los objetivos de seguridad primaria del proceso de telecarga de códigos:

- El CM deberá tener alguna manera de autenticar que el originador de cualquier código telecargado es una fuente conocida y fiduciada.
- El CM deberá disponer de alguna manera de verificar que el código telecargado no ha sido alterado desde la forma original en la que lo proporcionó la fuente fiduciada.
- El proceso deberá tratar de simplificar los requisitos de manejo de ficheros de código de operador de cable y proporcionar los mecanismos que permitan al operador de cable mejorar o rebajar la categoría de la versión del código de los módems de cable de su red.
- El proceso debe permitir además que un operador de cable tenga la posibilidad de establecer y controlar sus propias políticas de primera mano, con respecto a:
  a) los ficheros de código que serán aceptados por los módems de cable dentro de su dominio de red, y
  b) los controles de seguridad que definen la seguridad del proceso en su red.
- Los módems de cable han de poder desplazarse libremente entre sistemas controlados por diferentes organizaciones de operador de cable.
- Clave pública de CA raíz (opcional): Clave pública de CA raíz actualizada que sustituye a la clave pública de CA raíz almacenada en el CM.
- Certificado(s) de fabricante (opcional): Uno o más certificados de fabricante que cumplen la Recomendación X.509 y que sustituyen a los certificados de fabricante almacenados en el CM.

La presente Recomendación se circunscribe a esos requisitos de seguridad primaria de los sistemas, pero tiene en cuenta que en algunos casos quizás sea conveniente una mayor seguridad. Los recelos de algunos operadores de cable o fabricantes de módems de cable pueden tener como resultado un cierto grado de seguridad adicional en relación con la distribución e instalación de códigos en un módem de cable o en otro elemento de red DOCSIS. La presente Recomendación no restringe la utilización de otras formas de protección, en tanto no contravengan los objetivos y las directrices que en ella se exponen.

Para proteger y verificar de manera satisfactoria la telecarga de códigos se requieren múltiples niveles de protección.

- El fabricante del código del CM aplica siempre una signatura o firma digital al fichero de código; signatura que es verificada con una cadena de certificación que llega hasta la raíz DOCSIS. La signatura del fabricante autentica la fuente y la integridad del fichero de códigos al CM. En dicho fichero se incluyen parámetros de control adicionales para controlar el acceso al CM.
- Si bien el fabricante debe firmar siempre sus ficheros de código, un operador de cable puede aplicar posteriormente su signatura o firma de código, además de la del fabricante. El CM debe verificar ambas signaturas con una cadena de certificados que llegue hasta la raíz DOCSIS antes de aceptar un fichero de código.
- Los mecanismos OSS de aprovisionamiento y control del CM son de gran importancia para que la ejecución del proceso se lleve a cabo de manera adecuada. La capacidad de mejorar la categoría del código de un CM se habilita durante el proceso de aprovisionamiento y registro. Las telecargas de códigos se inician durante el proceso de aprovisionamiento y registro; o pueden ser iniciadas en funcionamiento normal mediante una instrucción SNMP.

El fichero de código se construye utilizando una estructura conforme a la norma PKCS #7 que haya sido definida en un formato específico para utilizarla con módems de cable DOCSIS. En la estructura PKCS #7 de DOCSIS debe estar incluido lo siguiente:

- La configuración de código: la configuración del código de mejora.
- La signatura de verificación de código (CVS, *code verification signature*): la signatura digital en la configuración del código y cualesquiera otros atributos autenticados definidos en la estructura PKCS #7 de DOCSIS.
- El certificado de verificación de código (CVC, *code verification certificate*): una estructura de certificado conforme a X.509 que se utiliza para entregar y validar la clave pública de verificación de código que verificará la signatura en la configuración del código. La autoridad de certificación de DOCSIS, una parte fiduciada cuya clave pública ya está almacenada en el módem de cable, firma el certificado. El certificado X.509 se define con un formato específico para utilizarlo con módems de cable DOCSIS.

La figura B.1 muestra los pasos básicos requeridos para la firma de una configuración de código cuando el fichero de código lo firma sólo el fabricante del CM, y cuando el fichero de códigos es firmado por el fabricante del CM y, también, por un operador de cable.

En el sistema DOCSIS, cada módem de cable recibirá una clave pública fiduciada de la autoridad de certificación raíz DOCSIS. El fabricante del código elaborará el fichero de código firmando la configuración de código mediante una estructura de signatura digital de la norma PKCS #7 de DOCSIS con un certificado X.509 de DOCSIS. El fichero de código se envía a continuación al operador de cable. El operador de cable, que posee una clave pública raíz DOCSIS, DEBERÍA verificar que el fichero de código procede de un fabricante DOCSIS fiduciado y no ha sido modificado. En este punto, el operador de cable tiene la opción de cargar el fichero de código en el servidor TFTP tal como está, o de añadir su firma y el CVC del operador de cable al fichero de código. Durante el proceso de mejora del código, el CM accederá al fichero de código desde el servidor TFTP y verificará la configuración del código antes de instalarlo.

Aunque la CA raíz DOCSIS para la cadena de certificados de módem de cable sirve actualmente como CA raíz para la descarga segura de soporte lógico, en el futuro se podrán utilizar diferentes CA raíz. Por lo tanto, el CM NO DEBE suponer que el CVC de fabricante ni el CVC cofirmado son emitidos por la CA raíz DOCSIS para la cadena de certificados de módem de cable.

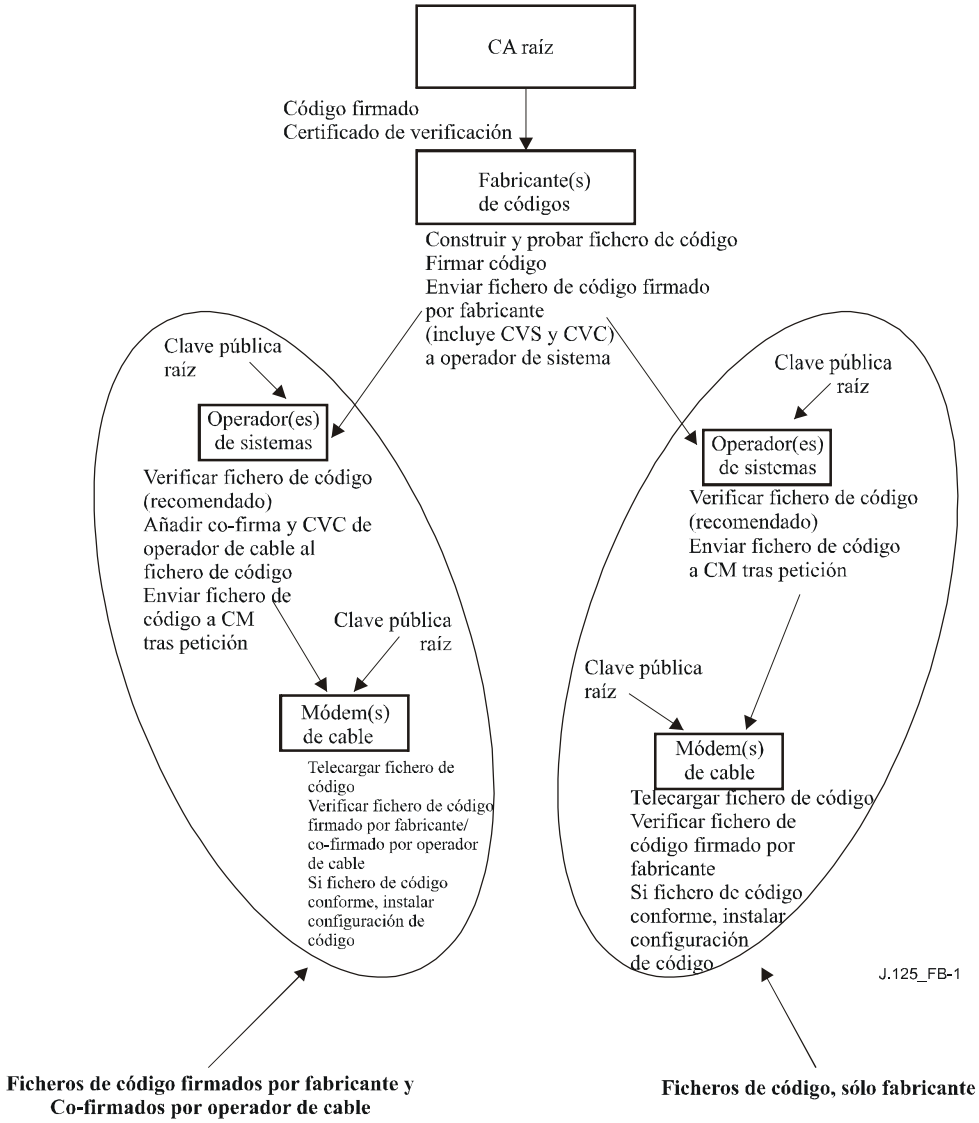


Figura B.1/J.125 – Jerarquía de validación de código típica

B.3 Requisitos de mejora de código

En las subcláusulas que siguen se definen los requisitos para el soporte del proceso de verificación de mejora de códigos. Todas las mejoras de código DOCSIS 1.1 ó 2.0 DEBEN ser preparadas y verificadas como se define en la presente especificación. Todos los módem de cable certificados DOCSIS 1.1 ó 2.0 DEBEN verificar las mejoras de código de acuerdo con esta Recomendación, con independencia de si funcionan o no según un modo conforme a DOCSIS 2.0, DOCSIS 1.1 o DOCSIS 1.0. Todos los módem de cable certificados DOCSIS 1.1 y DOCSIS 2.0 DEBEN verificar las mejoras de código de acuerdo con la presente Recomendación con independencia de si la privacidad básica está habilitada o inhabilitada.

B.3.1 Requisitos de fichero de código

Se utiliza un solo fichero para encapsular el código del módem de cable. El fichero de código es un mensaje datos firmado de la norma PKCS #7 de DOCSIS que incluye:

1) la signatura de verificación de código (CVS) del fabricante;

2) el certificado de verificación de código (CVC) del fabricante firmado por la autoridad de certificación (CA) DOCSIS raíz;

3) la configuración del código (compatible con el módem de cable de destino) a modo de contenido firmado;

4) facultativamente, cuando el operador de cable firma también el fichero del código:
   a) la CVS del operador del cable;
   b) el CVC del operador del cable firmado por la CA DOCSIS raíz.

5) clave pública de CA raíz opcional para la verificación de CVC.

6) certificados de fabricante opcionales.

El fichero de código DEBE cumplir la especificación [PKCS#7] y DEBE ser codificado de acuerdo con las reglas de codificación distinguida (DER). El fichero de código DEBE concordar con la estructura que se muestra en el cuadro B.1. En el apéndice I se presenta un ejemplo.

Cuadro B.1/J.125 – Estructura de fichero de código

Fichero de código	Descripción
PKCS #7 Digital Signature{	
ContentInfo	
contentType	SignedData
SignedData()	Valor de contenido de datos EXPLICITO, incluye CVS y CVC X.509
}	
SignedContent{	
DownloadParameters {	Formato TLV (tipo 28) obligatorio definido en 7.2.2.28 (La longitud es cero si no hay subTLV)
RootCAPublicKey()	TLV opcional para la clave pública de CA raíz para la verificación de CVC, formateado según el formato de TLV de clave pública de RSA (tipo 4) definido en 7.2.2.4.
MfgCerts()	TLV opcional para uno o más certificados de fabricante codificados DER, cada uno de ellos formateado según el formato TLV de certificado de CA (tipo 17) definido en 7.2.2.17.
}	
CodeImage()	Configuración de código mejorada
}	

Si al telecargar la clave pública de CA raíz y/o el certificado de un fabricante como parte del fichero de código CM, la clave pública de CA raíz y/o los certificados de CA de fabricante PUEDEN estar incluidos en el campo RootCAPublicKey y/o MfgCerts, según se especifica en el cuadro B.1, y PUEDEN estar separados de la configuración del código de módem de cable real incluido en el campo CodeImage.

Así es posible distinguir claramente la configuración de código de los otros parámetros del fichero de telecarga del código. También es posible, de esta manera, cambiar la clave pública de CA raíz, los certificados de CA de fabricante o parámetros de SignedData del fichero de telecarga de código sin perturbar o modificar la configuración de código que recibirá el módem de cable. Con ello se puede verificar que la configuración de código no ha cambiado debido a un cambio en la clave pública de CA raíz, los certificados de CA de fabricante o los parámetros de SignedData.

B.3.1.1 Datos firmados de la norma PKCS #7 DOCSIS

La información contenida en el fichero de mejora de soporte lógico será del tipo datos firmados de PKCS #7, como se muestra más adelante. Aun manteniendo la conformidad con [PKCS#7], se ha restringido el formato de la estructura utilizada por DOCSIS para facilitar el procesamiento que lleva a cabo un CM a fin de validar la signatura. Los datos firmados de la norma PKCS #7 DEBEN estar codificados de acuerdo con las DER y concordar exactamente con la estructura mostrada en el cuadro B.2, salvo cualquier cambio en el orden requerido para la codificación según DER (por ejemplo, la ordenación de los atributos SET OF). El CM DEBERÍA rechazar la signatura PKCS #7, si los datos firmados PKCS #7 no concuerdan con la estructura codificada con las DER representada en el cuadro B.2.

Cuadro B.2/J.125 – Datos firmados de la norma PKCS #7 DOCSIS

Campo de PKCS #7	Descripción
Signed Data {	
version	Versión = 1
digestAlgorithmIdentifiers	SHA-1
contentInfo	
contentType	Datos (SignedContent está concatenado al final de la estructura de [PKCS #7])
certificates {	Certificado de verificación de código (CVC) DOCSIS
mfgCVC	REQUERIDO para todos los ficheros de código
msoCVC	OPCIONAL; requerido para co-firmas de operadores de cable
} *end certificates*	
SignerInfo{	
MfgSignerInfo {	REQUERIDO para todos los ficheros de código
version	Versión = 1
issuerAndSerialNumber	Del certificado del firmante
issuerName	Nombre distinguido del expedidor del certificado
CountryName	Estados Unidos
organizationName	Especificaciones de interfaz del servicio de datos por cable
organizationalUnitName	Módems de cable
commonName	Autoridad de certificación raíz DOCSIS de módem de cable
certificateSerialNumber	De CVC; entero, tamaño (1...20) octetos
digestAlgorithm	SHA-1
authenticatedAttributes	
contentType	Datos; tipo del contenido de la configuración del código
signingTime	UTCTime (GMT), YYMMDDhhmmssZ
messageDigest	Compendio del contenido definido en [PKCS #7]
digestEncryptionAlgorithm	rsaEncryption
encryptedDigest	
} *end mfg signer info*	

Cuadro B.2/J.125 – Datos firmados de la norma PKCS #7 DOCSIS

Campo de PKCS #7	Descripción
MsoSignerInfo {	OPCIONAL; requerido para co-firmas de operadores de cable
version	Versión = 1
issuerAndSerialNumber	Del certificado del firmante
issuerName	Nombre distinguido del expedidor del certificado
CountryName	Estados Unidos
organizationName	Especificaciones de interfaz del servicio de datos por cable
organizationalUnitName	Módems de cable
commonName	Autoridad de certificación raíz DOCSIS de módem de cable
certificateSerialNumber	De CVC; entero, tamaño (1...20) octetos
digestAlgorithm	SHA-1
authenticatedAttributes	
contentType	Datos; tipo del contenido de la configuración del código
signingTime	UTCTime (GMT), YYMMDDhhmmssZ
messageDigest	Compendio del contenido definido en [PKCS #7]
digestEncryptionAlgorithm	rsaEncryption
encryptedDigest	
} *end mso signer info*	
} *end signer info*	
} *end signed data*	

B.3.1.1.1 Claves de firma de código

La signatura o firma digital de la norma PKCS #7 utiliza el algoritmo de encriptación RSA [RSA3] con SHA-1 [FIPS-186-2]. El módulo de la clave RSA para la firma del código tiene una longitud de 1024 bits, 1536 bits o 2048 bits. El CM DEBE ser capaz de verificar las signaturas de fichero de código firmadas utilizando cualquiera de esos tamaños de módulo. El exponente público es F4 (65537 decimal).

B.3.1.1.2 Formato de certificado de verificación de código

El formato utilizado para el CVC es conforme a X.509. Sin embargo, en este caso, se ha restringido el formato de la estructura X.509 para facilitar el procesamiento que lleva a cabo un CM a fin de validar el certificado y extraer la clave pública utilizada para verificar la CVS. El CVC DEBE ser codificado de acuerdo con las DER y concordar exactamente con la estructura mostrada en el cuadro B.3, salvo cualquier cambio en el orden requerido para la codificación de acuerdo con las DER (por ejemplo, la ordenación de los atributos SET OF). El CM DEBERÍA rechazar el CVC, si los datos no concuerdan con la estructura codificada con las DER representada en el cuadro B-3.

El CVC requiere también que se añada el ID de finalidad de la clave para la "firma del código" dentro del campo utilización de clave ampliada.

```
-- extended key usage extension OID and syntax
id-ce-exKeyUsage OBJECT IDENTIFIER ::= {id-ce 37}
ExtKeyUsageSyntax ::= SEQUENCE SIZE (1..MAX) OF KeyPurposeId
KeyPuposeID ::= OBJECT IDENTIFIER
```

El CVC DOCSIS DEBE contener un campo extensión, y solamente uno, a saber, el campo extensión de utilización de clave ampliada. La extensión de utilización de clave ampliada DEBE ser marcada como crítica. La extensión de utilización de clave DEBE contener el OID finalidad del código para la firma del código. Si la extensión de utilización de clave ampliada no está presente, o no está marcada como crítica, o incluye cualquier OID de finalidad de clave añadido o diferente del ID finalidad de la firma del código, el CM DEBE detener el proceso de validación y descartar el CVC.

```
-- extended key purpose OIDs
id-kp-codeSigning OBJECT IDENTIFIER ::= { id-kp 3 }
```

Cuadro B.3/J.125 – Certificado de verificación de código DOCSIS X.509

Campo del certificado X.509	Descripción
Certificate {	
tbsCertificate	
version	v3(2)
serialNumber	Entero, tamaño (1...20) octetos
signature	SHA-1 con RSA, parámetros nulos
issuer	
countryName	Estados Unidos
organizationName	Especificaciones de interfaz del servicio de datos por cable
organizationalUnitName	Módems de cable
commonName	Autoridad de certificación raíz DOCSIS de módem de cable
validity	
notBefore	utcTime (GMT), YYMMDDhhmmssZ
notAfter	utcTime (GMT), YYMMDDhhmmssZ
subject	
countryName	<país de la empresa del asunto>
organizationName	<agente co-firmante del código del asunto>
organizationalUnitName	DOCSIS
commonName	Certificado de verificación de código
subjectPublicKeyInfo	
algorithm	Criptación RSA, parámetros nulos
subjectPublicKey	Módulo de 1024 bits, 1536 bits, o 2048 bits
extensions	
extKeyUsage	
critical	Verdad
keypurposeId	ID de finalidad de la clave para la firma del código
signatureAlgorithm	SHA-1 con RSA, parámetros nulos
signature Value	
} *end certificate*	

B.3.1.1.3 Revocación de certificado

Esta Recomendación no requiere o define la utilización de listas de revocación de certificados (CRL, *certificate revocation list*). No se exige al módem de cable que soporte las CRL. Quizá los operadores de cable deseen definir y utilizar las CRL fuera de la red HFC DOCSIS para ayudar en la gestión de los ficheros de código que les proporcionan los fabricantes.

Sin embargo, hay un método de revocación de certificados basado en la fecha de comienzo de la validez de los mismos (que se describe en B.3.3.2.2). Dicho método requiere que se entregue al módem de cable un CVC puesto al día con una fecha de comienzo de validez actualizada. Una vez que el CVC ha sido validado satisfactoriamente, el tiempo de comienzo de validez X.509 actualizará el valor que a la sazón tiene cvcAccessStart (comienzo de acceso a CVC) del CM.

Para acelerar la entrega de un CVC actualizado sin necesidad de que el módem de cable procese una mejora de código, el CVC PUEDE ser entregado en el fichero de configuración del CM o en una base de información de gestión (MIB) del SNMP. El formato de un CVC DOCSIS es el mismo tanto si está en un fichero de código como en un fichero de configuración o en una MIB de SNMP.

B.3.1.2 Contenido firmado

El campo contenido firmado del fichero de código incluye la configuración de código y el campo de parámetros descargados, que probablemente contiene dos elementos facultativos adicionales – una clave pública de CA raíz DOCSIS y un certificado de fabricante.

La configuración de código final está en un formato compatible con el módem de cable de destino. De conformidad con los requisitos de la signatura o firma de la norma [PKCS #7], el contenido del código se escribe como si fueran datos, es decir, una cadena de octetos simple. El formato de la configuración de código final no se especifica aquí y será definido por cada fabricante de acuerdo con sus requisitos.

Cada fabricante DEBERÍA elaborar su código con mecanismos adicionales que permitan verificar si una configuración de código actualizada es compatible con el módem de cable de destino. El CM NO DEBERÍA instalar la configuración de código mejorada a menos que se haya verificado la compatibilidad de la configuración de código con el CM.

Si está incluida en el campo de contenido firmado, la clave pública de CA DOCSIS se emplea para sustituir a la clave pública de CA raíz DOCSIS almacenada en ese instante en el CM. Si la descarga e instalación de código especificadas en B.3.5.1 se realizan con éxito, el CM DEBE sustituir su clave pública de CA raíz DOCSIS almacenada por la clave pública de CA raíz DOCSIS recibida en el campo de contenido firmado. Esta nueva clave pública se utilizará entonces para la subsiguiente verificación de CVC.

Si está incluida en el campo de contenido firmado, el o los certificados de fabricante se emplean para sustituir a los certificados de fabricante almacenados en ese instante en el CM. Si la descarga e instalación de código especificadas en B.3.5.1 se realizan con éxito, el CM DEBE sustituir sus certificados de fabricante almacenados por los certificados de fabricante recibidos en el campo de contenido firmado. Los nuevos certificados de fabricante se enviarán entonces al CMTS durante la inicialización BPI+ subsiguiente.

B.3.2 Controles de acceso a fichero de código

Además de los controles criptográficos proporcionados por la signatura digital y el certificado X.509, en el fichero de código se incluyen valores de control especiales para que el módem de cable efectúe una comprobación antes de validar una configuración de código. Las condiciones impuestas a los valores de esos parámetros de control DEBEN ser satisfechas antes de que el CM valide el CVC o la CVS y acepte la configuración de código.

B.3.2.1 Nombres de organización de asunto

El módem de cable reconocerá, en cualquier momento, hasta dos nombres que considere un agente firmante de código fiduciado en el campo asunto del CVC de un fichero de código. Se incluyen aquí:

- El fabricante del módem de cable: el nombre de fabricante del campo asunto del CVC del fabricante DEBE concordar exactamente con el nombre de fabricante almacenado por el fabricante en la memoria no volátil del CM. El CVC de un fabricante se DEBE incluir siempre en el fichero de código.
- Un agente co-firmante: el fabricante y DOCSIS permiten que otra organización fiducida co-firme ficheros de códigos destinados a sus módems de cable. En la mayoría de los casos, se trata del operador de cable que controla en esos momentos el dominio de explotación del módem de cable. El nombre de la organización del agente co-firmante se comunica al módem de cable vía un CVC del co-firmante en el fichero de configuración cuando se inicializa el proceso de verificación de código del módem de cable. El nombre de organización del co-firmante que figura en el campo asunto del CVC del co-firmante DEBE coincidir exactamente con el nombre de organización del co-firmante recibido previamente en el CVC de inicialización del co-firmante y almacenado por el CM.

El CM PUEDE comparar nombres de organización utilizando una comparación binaria.

B.3.2.2 Controles variables con el tiempo

Para ayudar en el proceso de mejora de código, el CM DEBE mantener dos conjuntos de valores de tiempo UTC asociados con cada agente firmante de código. Un conjunto de valores DEBE estar siempre almacenado y mantenido para el fabricante del módem de cable. Mientras el módem de cable tiene asignado un agente co-firmante del código, DEBE almacenar y mantener también un conjunto aparte de valores de tiempo para el agente co-firmante.

Estos valores se utilizan para controlar el acceso del fichero de código al módem de cable, controlando individualmente la validez de la CVS y el CVC. Los valores son:

codeAccessStart: un valor de tiempo UTC de 12 bytes referencia al tiempo medio de Greenwich (GMT, *Greenwich mean time*).

cvcAccessStart: un valor de tiempo UTC de 12 bytes con referencia al GMT.

Los valores de UTCTime (tiempo UTC) en el CVC DEBEN expresarse como tiempo medio de Greenwich (GMT) y DEBEN incluir segundos. Es decir, DEBEN expresarse en la forma siguiente: YYMMDDhhmmssZ. El campo año (YY) DEBE interpretarse como sigue:

- Cuando YY sea superior o igual a 50, el año se interpretará como 19YY.
- Cuando YY sea inferior a 50, el año se interpretará como 20YY.

Estos valores estarán siempre referidos al tiempo medio de Greenwich (GMT), por lo que el carácter final de ASCII (Z) se puede eliminar cuando sean almacenados por el CM como codeAccessStart y cvcAccessStart. El CM DEBE mantener cada uno de estos valores de tiempo en un formato que contenga información de tiempo y exactitud equivalentes al formato UTV de 12 caracteres (es decir, YYMMDDhhmmss). El CM DEBE comparar con precisión esos valores almacenados con los valores de tiempo UTC que le hayan sido entregados en un CVC. Estos requisitos se analizan más adelante en la presente Recomendación.

Los valores de codeAccessStart y cvcaccessStart correspondientes al fabricante del módem de cable NO DEBEN disminuir. Los valores de codeAccessStart y cvcaccessStart correspondientes al agente co-firmante NO DEBEN cambia mientras el agente co-firmante no cambie y el CM mantenga los valores de control variables con el tiempo del agente co-firmante.

B.3.3 Inicialización de mejora de código de módem de cable

Para que el módem de cable pueda mejorar un código, deberá ser inicializado convenientemente. Su fabricante es quien lo inicializa por primera vez. Cada vez que un módem de cable se registre en una red DOCSIS, DEBE comprobar su estado de inicialización en ese momento con respecto a las necesidades operativas de la red de que se trate. Quizá sea necesario que el módem de cable se reinicialice al registrarse; sobre todo si se traslada de una red a otra.

B.3.3.1 Inicialización de fabricante

Corresponde al fabricante instalar correctamente la versión de código inicial en el CM.

Para ayudar a la verificación de la mejora del código, se DEBEN cargar valores de los parámetros que se indican a continuación en la memoria no volátil del CM:

1) nombre de organización del fabricante del CM;
2) valores de control variables con el tiempo del fabricante:
    a) valor de inicialización del codeAccessStart (comienzo de acceso a código);
    b) valor de inicialización de cvcAccessStart (comienzo de acceso a CVC).

El nombre de organización del fabricante del módem DEBE estar siempre presente en el módem de cable. El organizationName (nombre de organización) del fabricante del módem de cable PUEDE ser almacenado en la configuración de código de los módems de cable. En condiciones normales, el organizationName del fabricante NO DEBERÍA cambiar, pero la presente especificación no impide que un fabricante cambie la forma de almacenar en el CM su organizationName. El nombre del fabricante utilizado para mejorar el código no necesariamente es el mismo nombre que se utiliza en el certificado DOCSIS del fabricante.

Los valores de control variables con el tiempo, codeAccessStart y cvcAccessStart, DEBEN ser inicializados en un tiempo UTC compatible con el tiempo de comienzo de validez del CVC más reciente del fabricante. Estos valores variables con el tiempo serán actualizados periódicamente en funcionamiento normal vía los CVC de fabricante recibidos y verificados por el módem de cable.

Al principio, el módem de cable no reconocerá a un agente co-firmante.

B.3.3.2 Inicialización de red

El método de inicialización y obtención de ficheros de telecarga de código de CM se define en [J.112-B] o [J.122]. Para ayudar a la verificación del código, se utiliza el fichero de configuración como medio autenticado en el que inicializar el proceso de verificación del código. En el fichero de configuración de módem de cable, el módem de cable recibe fijaciones de configuración pertinentes a la verificación de mejora de código. Dichas fijaciones NO DEBEN ser utilizadas sino hasta que el CMTS haya registrado el CM de manera satisfactoria.

El fichero de configuración DEBERÍA incluir siempre el CVC más actualizado aplicable al módem de cable de destino; pero, cuando el fichero de configuración se utiliza para iniciar una mejora de código, DEBE incluir un certificado de verificación de código (CVC) para inicializar el módem de cable de modo que acepte ficheros de código de acuerdo con la presente Recomendación. Con independencia de si se requiere o no una mejora de código, un CVC del fichero de configuración DEBE ser procesado por el módem de cable.

Un fichero de configuración PUEDE contener:

- ningún CVC;
- un CVC de fabricante solamente;
- un CVC de co-firmante (operador de cable) solamente;
- tanto un CVC de fabricante como un CVC de co-firmante.

Antes de que el CM ponga a punto su capacidad de mejorar ficheros de código en la red, DEBE recibir un CVC válido en un fichero de configuración y registrarse de manera satisfactoria en el CMTS. Además, cuando el fichero de configuración del módem de cable no contiene un CVC válido, y su capacidad de mejorar ficheros de código ha sido inhabilitada, el CM DEBE rechazar cualquier información que figure en un CVC entregado subsiguientemente vía SNMP.

Cuando el fichero de configuración del módem de cable contiene solamente un CVC de fabricante válido, el módem de cable sólo requerirá una signatura del fabricante en los ficheros de código. En este caso, el CM NO DEBE aceptar ficheros de código que hayan sido co-firmados.

Cuando el fichero de configuración del módem de cable contiene el CVC de un co-firmante, se utiliza para inicializar el módem de cable con un agente co-firmante. Una vez validado, el nombre de organizationName del asunto del CVC pasará a ser el agente co-firmante del código asignado al módem de cable. Para que un CM acepte subsiguientemente una configuración de código, el co-firmante, además del fabricante del módem de cable, DEBE haber firmado el fichero de código.

El nombre de organización del fabricante del módem de cable y los valores de control variables con el tiempo del fabricante DEBEN estar siempre presentes en el módem de cable. Si se inicializa el módem de cable para aceptar un código co-firmado por un agente co-firmante adicional, el nombre de la organización y sus correspondientes valores de control variables con el tiempo DEBEN ser almacenados y mantenidos mientras sean operativos. Se DEBE asignar espacio en la memoria del módem de cable para los valores de control del co-firmante siguientes:

1) nombre de organización del agente co-firmante;
2) valores de control variables con el tiempo del co-firmante:
    a) cvcAccessStart (comienzo de acceso a CVC);
    b) codeAccessStart (comienzo de acceso a código).

El conjunto de estos valores del fabricante se DEBE almacenar en la memoria no volátil del CM y no deberá perderse cuando se elimine la alimentación de energía eléctrica del CM o durante un proceso de reiniciación. Cuando se asigna un co-firmante al CM, el conjunto de estos valores del co-firmante DEBEN almacenarse en la memoria del CM. El CM PUEDE mantener estos valores en su memoria no volátil y no se deben perder cuando se elimine la alimentación del CM o durante el proceso de reiniciación del CM. Sin embargo, cuando se asigna al CM un agente co-firmante, el CVC está siempre en el fichero de configuración. Por tanto, el CM siempre recibirá los valores de control del co-firmante durante la fase de reiniciación y no precisa almacenar los valores de control variables con el tiempo del co-firmante cuando se pierda la alimentación de energía eléctrica o durante un proceso de reiniciación.

B.3.3.2.1 Procesamiento de CVC de fichero de configuración

Cuando se incluye un CVC en el fichero de configuración DOCSIS 1.1 o DOCSIS 2.0, el CM DEBE verificar el CVC antes de aceptar cualquiera de las fijaciones de mejora de código que contiene. Al recibir el CVC en el fichero de configuración, el CM DEBE efectuar los pasos de validación y procedimiento que se indican a continuación. Si cualquiera de las comprobaciones de verificación siguientes falla, el CM DEBE detener inmediatamente el proceso de verificación del CVC y registrar cronológicamente el error, si procede. Si el fichero de configuración del CM no incluye un CVC cuya validación sea ratificadora, el CM NO DEBE efectuar telecargas de ficheros de código de mejora, ya sean provocadas por el fichero de configuración de CM o vía una MIB de SNMP. Además, si los ficheros de configuración del CM no incluyen un CVC que se valide adecuadamente, no es necesario que el CM procese un CVC entregado a continuación por conducto de una MIB de SNMP, y NO DEBE aceptar información procedente de un CVC entregado seguidamente por ese mismo conducto.

Al recibir el CVC en un fichero de configuración, y después de que el CM se haya registrado de manera satisfactoria en el CMTS, el CM DEBE:

1) Verificar que la extensión utilización de clave ampliada figura en el CVC tal como se define en B.3.1.1.2.

2) Comprobar el nombre de organización de asunto del CVC:

   Si el CVC es un CVC de fabricante (tipo 32), entonces:

   a) SI el organizationName es idéntico al nombre del fabricante del módem de cable, se trata ENTONCES del CVC del fabricante. En este caso, el CM DEBE verificar que el tiempo de comienzo de la validez del CVC del fabricante es superior o igual al valor de cvcAccessStart del fabricante retenido a la sazón en el CM.

   b) SI el organizationName no es idéntico al nombre del fabricante del módem de cable, ENTONCES DEBE rechazarse ese CVC y el error debe ser registrado cronológicamente.

   Si el CVC es un CVC de co-firmante(tipo 33), entonces:

   a) SI el organizationName es idéntico al agente co-firmante de código actual del módem de cable, se trata ENTONCES del CVC del co-firmante actual y el CM DEBE verificar que el tiempo de comienzo de la validez es superior o igual al valor de cvcAccessStart del co-firmante retenido a la sazón en el CM.

   b) SI el organizationName no es idéntico al nombre del fabricante o del agente co-firmante del código actual, una vez que el CVC haya sido validado (y se haya completado el registro), este nombre de organización de asunto pasará a ser ENTONCES el nuevo agente co-firmante de código del CM. El CM NO DEBE aceptar un fichero de código a menos que haya sido firmado por el fabricante, y co-firmado por este agente co-firmante de código.

3) Validar la signatura o firma del certificado utilizando la clave raíz DOCSIS retenida por el CM. La verificación de la signatura del CM autenticará la fuente y validará la confianza en los parámetros del CVC.

4) Actualizar los valores de cvcAccessStart y codeAccessStart actuales del CM correspondientes al organizationName de asunto del CVC (es decir, el fabricante o el agente co-firmante del código) con el valor de tiempo de comienzo de validez del CVC validado. Si el valor de tiempo de comienzo de validez es mayor que el valor actual del CM en codeAccessStart, se actualizará el valor del codeAccessStart del CM con el valor de tiempo de comienzo de validez. El CM DEBERÍA descartar cualquier remanente del CVC.

B.3.3.2.2 Procesamiento de CVC del SNMP

El CM DEBE procesar los CVC entregados por el SNMP cuando esté habilitado para mejorar ficheros de código; de otro modo, todos los CVC entregados vía SNMP DEBEN ser rechazados. Cuando se valide el CVC entregado vía SNMP, el CM DEBE efectuar los pasos de validación y procedimientos que se indican a continuación. Si cualquiera de las comprobaciones de verificación siguientes falla, el CM DEBE detener inmediatamente el proceso de verificación del CVC, registrar cronológicamente el error, si procede, y eliminar todos los remanentes del proceso hasta ese paso.

El CM DEBE:

1) Verificar que la extensión utilización de clave ampliada figura en el CVC tal como se define en B.3.1.1.2.

2) Comprobar el nombre de organización de asunto del CVC.

   a) SI el organizationName es idéntico al nombre del fabricante, del módem, se trata ENTONCES del CVC del fabricante. En este caso, el CM DEBE verificar que el

tiempo de comienzo de la validez del CVC del fabricante es superior o igual al valor de cvcAccessStart del fabricante retenido a la sazón en el CM.

b) SI el organizationName es idéntico al agente co-firmante de código actual del módem de cable, se trata ENTONCES del CVC del co-firmante actual y el tiempo de comienzo de la validez DEBE ser superior o igual al valor de cvcAccessStart del co-firmante retenido a la sazón en el CM.

c) SI el organizationName no es idéntico al nombre del fabricante del módem de cable o del agente co-firmante de código actual, ENTONCES el CM DEBE rechazar de inmediato ese CVC.

3) Validar la signatura o firma del certificado utilizando la clave raíz DOCSIS retenida por el CM. La verificación de la signatura autenticará el certificado y confirmará la confianza en el tiempo de comienzo de validez del CVC.

4) Actualizar los valores de cvcAccessStart y codeAccessStart actuales del asunto con el valor de tiempo de comienzo de validez del CVC validado. Si el valor de tiempo de comienzo de validez es mayor que el valor actual del CM en codeAccessStart, se actualizará el valor del codeAccessStart del CM con el valor de tiempo de comienzo de validez. Todos los parámetros del certificado, EXCEPTO el tiempo de comienzo de validez, ya no se necesitan y DEBERÍAN ser descartados.

B.3.4 Requisitos de firma de código

Cuando se firmen ficheros de código, DEBEN seguirse los procedimientos que se indican a continuación.

B.3.4.1 Requisitos de autoridad de certificación (CA)

Además del certificado DOCSIS de fabricante expedido a un fabricante, que se describe con anterioridad en la presente Recomendación, la CA raíz DOCSIS expedirá certificados de firma de código llamados certificados de verificación de código (CVC).

El certificado de verificación de código (CVC) lo proporciona la CA DOCSIS y se firma con la clave raíz (DRK) DOCSIS. Los CVC firmados por la CA DOCSIS DEBEN ser exactamente tal como se especifica en B.3.1.1.2 y utilizados solamente como respaldo de las signaturas de código de módem de cable DOCSIS. La CA DOCSIS no DEBE firmar ningún CVC a menos que sea idéntico al formato especificado en esa cláusula. Antes de firmar un CVC, la CA DOCSIS DEBE verificar que el agente que firma el código es auténtico y es un agente válido a tal fin.

La CA DOCSIS será responsable del registro de nombres de agentes firmantes de código autorizados. Entre los agentes firmantes de código figuran los fabricantes de CM y los operadores de cable que co-firmarán las configuraciones de código de módem de cable. Corresponde a la CA DOCSIS garantizar que el nombre de organización de cada agente firmante de código es diferente. Cuando se asignan nombres de organización para co-firmantes de código se DEBEN aplicar las directrices que siguen:

- El nombre de organización utilizado para identificarse como el agente co-firmante de código en un CVC DEBE ser asignado por DOCSIS.
- El nombre DEBE ser una cadena imprimible de ocho dígitos hexadecimales que distinga de manera exclusiva a un agente firmante de código de todos los demás.
- Cada dígito hexadecimal del nombre DEBE elegirse del conjunto de caracteres 0-9 (0x30-0x39) o A-F (0x41-0x46).
- La cadena formada por ocho dígitos 0 no está permitida y NO DEBE ser utilizada en un CVC.

B.3.4.2 Requisitos de fabricación

Para firmar sus ficheros de código, el fabricante DEBE obtener un CVC válido de la CA DOCSIS. Todas las configuraciones de código de fabricante proporcionadas a un operador de cable para la mejora a distancia de un CM de una red HFC DOCSIS DEBEN ser firmadas de acuerdo con los requisitos definidos en la presente Recomendación.

Cuando el fabricante firma un fichero de código, PUEDE optar por no actualizar el valor de signingTime de [PKCS #7] en la información de firma del fabricante. Esta especificación requiere que el valor de signingTime de [PKCS #7] sea igual o superior al tiempo de comienzo de validez del CVC. Si el fabricante utiliza un signingTime igual al tiempo de comienzo de validez del CVC cuando firma una serie de ficheros de código, esos ficheros pueden ser utilizados y reutilizados. De esta manera, un operador de cable puede utilizar el fichero de código para aumentar o rebajar la categoría de la versión del código de los módems de cable de aquel fabricante. Esos ficheros de código serán válidos hasta que se genere un nuevo CVC y sea recibido por el módem de cable. Se recomienda que el fabricante firme sus ficheros de código de esta manera cuando DOCSIS y su política de seguridad así lo permitan (véase B.4).

Para conservar espacio de almacenamiento, el CM PUEDE representar internamente el nombre del agente co-firmante de código en un formato alternativo en tanto en cuanto se mantenga toda la información y el formato original pueda ser reproducido; por ejemplo, un entero no cero de 32 bits, con un valor entero de 0 representando la ausencia de agente firmante de código.

B.3.4.3 Requisitos de operador de cable

Un operador de cable DOCSIS recibirá ficheros de código de mejora de soporte lógico procedentes del fabricante. Utilizando la clave pública raíz DOCSIS, el operador de cable deberá confirmar que esa configuración de código ha sido elaborada por el fabricante fiduciado. El operador de cable puede verificar de nuevo el fichero de código, en cualquier momento, repitiendo el proceso.

El operador de cable tiene la opción de co-firmar la configuración de código destinada a un módem de cable de su red. Para ello, el operador co-firma el contenido del fichero de acuerdo con la norma de signatura [PKCS #7], e incluye su CVC firmado por DOCSIS. DOCSIS no requiere que un operador de cable co-firme ficheros de código; pero cuando el operador de cable sigue todas las reglas definidas en la presente especificación para la preparación de un fichero de código, el módem de cable DEBE aceptarlo.

Todas las configuraciones de código telecargadas en un CM a través de la red HFC DOCSIS DEBEN ser firmadas de acuerdo con los requisitos definidos en esta Recomendación.

B.3.5 Requisitos de verificación de código

NO DEBE instalarse un código de mejora a menos que se compruebe que el código está fiduciado de acuerdo con el proceso de verificación descrito en la presente Recomendación.

El CM DEBE poder procesar una signatura o firma digital de la norma [PKCS #7] y un certificado DOCSIS X.509 según lo definido en esta especificación. No es preciso que el CM soporta la gama completa de las especificaciones [PKCS #7] y X.509.

B.3.5.1 Pasos de la verificación de código de módem de cable

Cuando el CM telecarga un código, DEBE efectuar los pasos que se describen en esta cláusula. Si falla cualquiera de las comprobaciones de verificación, o si se rechaza cualquier subcláusula del fichero de código debido a un formato no válido, el CM DEBE detener inmediatamente el proceso de telecarga, registrar cronológicamente el error, si procede, eliminar todos los remanentes del proceso hasta ese paso, y continuar funcionando con el código existente. Las comprobaciones de verificación se pueden realizar en cualquier orden, siempre que se realicen todas las comprobaciones pertinentes que figuran en esta cláusula.

1) El CM DEBE validar la información de signatura o firma del fabricante verificando que:
   a) el valor de signingTime de [PKCS #7] es igual o superior al valor de codeAccessStart del fabricante retenido a la sazón en el CM;
   b) el valor de signingTime de [PKCS #7] es igual o superior al tiempo de comienzo de validez del CVC del fabricante;
   c) el valor de signingTime de [PKCS #7] es menor o igual que el tiempo de final de validez del CVC del fabricante.
2) El CM DEBE validar el CVC del fabricante verificando que:
   a) el organizationName del asunto del CVC es idéntico al nombre del fabricante almacenado a la sazón en la memoria del CM;
   b) el tiempo de comienzo de validez del CVC es igual o superior al valor de cvcAccessStart del fabricante retenido a la sazón en el CM;
   c) la extensión utilización de clave ampliada figura en el CVC tal como se define en B.3.1.1.2.
3) El CM DEBE validar la signatura o firma del certificado utilizando la clave raíz DOCSIS retenida por el CM. La verificación de la signatura autenticará la fuente de la clave de verificación de código (CVK) pública y confirmará la confianza en la clave. Una vez establecida la confianza en la CVK del fabricante, los parámetros del certificado restantes, EXCEPTO el tiempo de comienzo de validez, ya no se necesitan y DEBERÍAN ser descartados.
4) El CM DEBE verificar la signatura o firma del fichero de código del fabricante:
   a) el CM DEBE realizar un nuevo troceo SHA-1 en SignedContent. Si el valor de messageDigest no concuerda con el nuevo troceo, el CM DEBE considerar la signatura del fichero de código como no valida.
   b) si la signatura no pasa la prueba de verificación, todos los componentes del fichero de código (incluida la configuración de código), y cualesquiera valores obtenidos a partir del proceso de verificación DEBEN ser rechazados y DEBERÍAN ser descartados inmediatamente.
5) Si la signatura del fabricante pasa la prueba de verificación y se requiere la signatura del agente co-firmante:
   a) el CM DEBE validar la información de la signatura del co-firmante verificando que:
      1) la información de signatura del co-firmante está incluida en el fichero de código;
      2) el valor de signingTime de la norma [PKCS #7] es igual o superior al valor de codeAccessStart correspondiente retenido a la sazón en el CM;
      3) el valor de signingTime de [PKCS #7] es igual o superior al tiempo de comienzo de validez del CVC correspondiente;
      4) el valor de signingTime de [PKCS #7] es menor o igual que el tiempo de final de validez del CVC correspondiente.

b) el CM DEBE validar el CVC del co-firmante, verificando que:

1) el organizationName del asunto del CVC es idéntico al nombre de organización del co-firmante almacenado a la sazón en la memoria del CM;

2) el tiempo de comienzo de validez del CVC es igual o superior al valor de cvcAccessStart retenido a la sazón en el CM para el organizationName del asunto correspondiente;

3) la extensión utilización de clave ampliada figura en el CVC tal como se define en B.3.1.1.2.

c) el CM DEBE validar la signatura o firma del certificado utilizando la clave raíz DOCSIS retenida por el CM. La verificación de la signatura autenticará la fuente de la clave de verificación de código (CVK) pública del co-firmante y confirmará la confianza en la clave. Una vez establecida la confianza en la CVK del co-firmante, los parámetros del certificado restantes, EXCEPTO el tiempo de comienzo de validez, ya no se necesitan y DEBERÍAN ser descartados.

d) el CM DEBE verificar la signatura de fichero de código del co-firmante.

e) el CM DEBE realizar un nuevo troceo SHA-1 en SignedContent. Si el valor de messageDigest no concuerda con el nuevo troceo, el CM DEBE considerar la signatura del fichero de código como no valida.

f) Si la signatura no pasa la prueba de verificación, todos los componentes del fichero de código (incluida la configuración de código), y cualesquiera valores obtenidos a partir del proceso de verificación, DEBEN ser rechazados y DEBERÍAN ser descartados inmediatamente.

6) Si se verifica la signatura del fabricante, y facultativamente la del co-firmante, y pasa la prueba de verificación, la configuración de código puede ser fiduciada y la instalación puede proseguir. Antes de instalar la configuración de código, todos los demás componentes del fichero de código y cualesquiera valores obtenidos a partir del proceso de verificación, excepto los valores de signingTime de [PKCS #7] y el tiempo de comienzo de validez del CVC, DEBERÍAN ser descartados inmediatamente.

7) El CM puede mejorar su soporte lógico instalando el fichero de código de acuerdo con [J.112-B].

8) Si la instalación del código no tiene éxito, el CM DEBE rechazar los valores de signingTime de [PKCS #7] y los valores de tiempo de comienzo de validez del CVC que acaba de recibir en el fichero de código. Deberán seguirse los pasos indicados en la [J.112-B] para el tratamiento de esta condición de fallo.

9) Cuando la instalación del código tiene éxito, el CM DEBE actualizar los controles variables con el tiempo del fabricante con los valores obtenidos de la información de signatura del fabricante y el CVC:

a) actualizar el valor actual de codeAccessStart con el valor de signingTime de [PKCS #7];

b) actualizar el valor actual de cvcAccessStart con el valor de comienzo de validez del CVC.

10) Cuando la instalación del código tiene éxito, SI el fichero está co-firmado, el CM DEBE actualizar los controles variables con el tiempo del co-firmante con los valores obtenidos de la información de signatura del co-firmante y el CVC:

a) actualizar el valor actual de codeAccessStart con el valor de signingTime de [PKCS #7];

b) actualizar el valor actual de cvcAccessStart con el valor de comienzo de validez del CVC.

B.3.6 Interoperabilidad de DOCSIS 1.0

Los módems de cable DOCSIS 1.1 ó 2.0 DEBEN verificar las mejoras de código de acuerdo con esta especificación incluso cuando funcionen con un entorno DOCSIS.

Los ficheros de configuración de DOCSIS 1.0 destinados a módems de cable DOCSIS 1.1 ó 2.0 DEBEN soportar los requisitos de fichero de configuración definidos en la presente Recomendación.

Los módems de cable DOCSIS 1.1 ó 2.0 DEBEN recibir ficheros de código conforme a DOCSIS 1.1 ó 2.0. Los ficheros de mejora pasan a través del sistema DOCSIS 1.0 inalterados, y no precisarán modificación alguna de los requisitos de tratamiento de ficheros de código de DOCSIS 1.0.

En un entorno DOCSIS 1.0 en donde módems de clave de DOCSIS 1.1 ó 2.0 están recibiendo ficheros de mejora de código, el gestor SNMP DEBERÍA soportar las bases de información de gestión (MIB) definidas para la verificación de códigos de DOCSIS 1.1 ó 2.0. La disponibilidad de esta capacidad MIB es muy importante a efectos del funcionamiento y la seguridad adecuados del proceso de mejora de códigos de DOCSIS 1.1 ó 2.0.

B.3.7 Códigos de error

Se definen códigos de error para reflejar posibles estados de fallo durante el proceso de verificación del código. En el apéndice H a [SCTE23-3] o en el anexo D a [SCTE79-2] se pueden encontrar la descripción y las directrices de uso de estos códigos de error.

1) Controles de ficheros de código inadecuado:
   a) El organizationName del asunto del CVC del fabricante no concuerda con el nombre de fabricante del CM.
   b) El organizationName del asunto del CVC para el agente co-firmante del código no concuerda con el agente co-firmante de código actual del CM.
   c) El valor de signingTime de PKCS #7 del fabricante es inferior al valor de codeAccessStart retenido a la sazón en el CM.
   d) El valor de tiempo de comienzo de validez de PKCS #7 del fabricante es inferior al valor de cvcAccessStart retenido a la sazón en el CM.
   e) El tiempo de comienzo de validez del CVC del fabricante es inferior al valor de cvcAccessStart retenido a la sazón en el CM.
   f) El valor de signingTime de PKCS #7 del fabricante es inferior al tiempo de comienzo de validez del CVC.
   g) Falta o es inapropiada la extensión utilización de cable ampliada en el CVC del fabricante.
   h) El valor de signingTime de PKCS #7 del co-firmante es inferior al valor de codeAccessStart retenido a la sazón en el CM.
   i) El valor de tiempo de comienzo de validez de PKCS #7 del co-firmante es inferior al valor de cvcAccessStart retenido a la sazón en el CM.
   j) El tiempo de comienzo de validez del CVC del co-firmante es inferior al valor de cvcAccessStart retenido a la sazón en el CM.
   k) El valor de signingTime de PKCS #7 del co-firmante es inferior al tiempo de comienzo de validez del CVC.
   l) Falta o es inapropiada la extensión utilización de clave ampliada en el CVC del co-firmante.

2) Fallo de validación de CVC del fabricante del fichero de código.
3) Fallo de validación de CVS del fabricante del fichero de código.
4) Fallo de validación de CVC del co-firmante del fichero de código.
5) Fallo de validación de CVS del co-firmante del fichero de código.
6) Formato de CVC de fichero de configuración inapropiado:
   a) El atributo de utilización de clave falta o es inapropiado.
7) Fallo de validación de CVC de fichero de configuración.
8) Formato de CVC de SNMP inapropiado:
   a) El organizationName del asunto del CVC para el fabricante no concuerda con el nombre del fabricante del CM.
   b) El organizationName del asunto del CVC para el agente co-firmante del código no concuerda con el agente co-firmante de código actual del CM.
   c) El tiempo de comienzo de validez del CVC es inferior o igual al valor de cvcAccessStart del asunto correspondiente retenido a la sazón en el CM.
   d) El atributo de utilización de clave falta o es inapropiado.
9) Fallo de validación de CVC de SNMP.

B.4 Consideraciones relativas a la seguridad (informativo)

La protección dada a las claves privadas constituye un factor fundamental para el mantenimiento de la seguridad. Los usuarios autorizados a firmar códigos, tales como los fabricantes y operadores a los que la autoridad de certificación raíz DOCSIS ha enviado certificados de verificación de firma de código (CVC), deben proteger sus claves privadas. Un atacante con acceso a la clave privada de un usuario firmante de código autorizado puede crear, a su capricho, ficheros de código potencialmente aceptables por un gran número de módems de cable (CM).

La defensa contra ese tipo de ataques consiste en que el operador revoque el certificado cuya clave privada de firma de código asociada ha sido descubierta por el atacante. Para revocar un certificado, el operador debe entregar a cada CM afectado un CVC actualizado con un tiempo de comienzo de validez más reciente que el del certificado o los certificados que se revocan. El CVC nuevo puede ser entregado por conducto de cualquiera de los mecanismos soportados: fichero de configuración, fichero de código o MIB de SNMP. El CVC nuevo revoca implícitamente todos los certificados cuyo tiempo de comienzo de validez es anterior al del CVC nuevo.

Para reducir la vulnerabilidad a este tipo de ataques, es importante que los operadores actualicen periódicamente el CVC de cada CM, con una frecuencia comparable a la de sus actualizaciones de la lista de revocación de certificados (CRL), si se dispusiera de una. Las actualizaciones periódicas ayudan a controlar el intervalo de tiempo durante el cual un atacante puede utilizar una clave de firma de código comprometida. Con independencia de si se está en el ciclo de actualización de los CVC, éstos deberían actualizarse también cuando se sospeche que una clave de firma de código ha quedado comprometida. Para actualizar un CVC, el usuario necesita otro CVC expedido por la CA DOCSIS cuyo tiempo de comienzo de validez sea posterior al del CVC del CM. Esto significa que la CA raíz DOCSIS debe enviar periódicamente CVC nuevos a todos los fabricantes y operadores firmantes de códigos autorizados, para facilitar la actualización de los CVC. Es probable que DOCSIS establezca una estrategia respecto al programa de expedición de nuevos CVC, y seguramente los operadores deseen coordinar sus políticas de actualización con ese programa.

Cuando un CM está tratando de registrarse en la red por primera vez, o si ha estado fuera de línea durante un cierto periodo de tiempo, es importante que reciba un CVC fiduciado tan pronto como sea posible. Así se da al CM la oportunidad de recibir el CVC más actualizado de que se disponga y se le impide el acceso a los CVC que tuvieron que ser revocados desde la última inicialización del

CM. La primera oportunidad que tiene el CM de recibir un CVC fiduciado está en su fichero de configuración. Si el fichero de configuración no incluye un CVC válido, el CM no pedirá o no podrá mejorar a distancia ficheros de código. Además, el CM no aceptará los CVC entregados subsiguientemente vía una MIB de SNMP.

Para reducir la posibilidad de que un CM reciba un fichero de código anterior como consecuencia de un ataque de tipo reproducción, los ficheros de código incluyen un valor de tiempo de firma en la estructura [PKCS #7] que se puede utilizar para indicar el momento en que se firmó la configuración de código. Cuando el CM recibe un fichero de código cuyo tiempo de firma es posterior al tiempo de firma que hubiera recibido en último lugar, actualizará su memoria interna con ese valor. El CM no aceptará ficheros de código con un tiempo de firma anteriores al valor almacenado internamente. Para mejorar la categoría de un CM con un fichero de código nuevo sin denegar el acceso a ficheros de código pasados, el firmante puede optar por no actualizar el tiempo de firma. De esta manera, múltiples ficheros de código con el mismo tiempo de firma de código permiten a un operador rebajar de categoría libremente la configuración de código de un CM a una versión anterior (es decir, hasta que el CVC sea actualizado). Esta manera de actuar presenta varias ventajas para el operador, pero esas ventajas deberían ponderarse frente a la posibilidad de un ataque del tipo reproducción de fichero de código.

Sin un mecanismo fiable que permita retornar a una versión de código buena y conocida, cualquier esquema de actualización de códigos, incluido el de la presente Recomendación, tiene el inconveniente de que una sola actualización impuesta y exitosa de una configuración de código no válida por parte de un CM puede inutilizar el CM. Incluso peor, una configuración de código no válida puede provocar que el CM se comporte de forma dañina y perjudicial para la red. Ese CM podría no ser reparable por medio de una actualización de código a distancia, ya que la configuración de código no válida no admite el esquema de actualización.

Anexo C

Interoperabilidad BPI/BPI+

La privacidad de referencia plus constituye un perfeccionamiento de los requisitos originales de la privacidad básica. La especificación ha introducido las mejoras necesarias para aumentar la seguridad del sistema y tener en cuenta los recelos derivados de la especificación original a propósito de la calidad de funcionamiento. La arquitectura y el diseño originales de la privacidad básica se han mantenido donde ha sido posible.

La evolución de las características de DOCSIS 1.1 ó 2.0 y de la privacidad básica plus no tenía por objeto la obsolescencia inmediata de los sistemas DOCSIS 1.0, ni que dejara de utilizarse la privacidad básica. La transición de los sistemas DOCSIS hacia la conformidad con DOCSIS 1.1 ó 2.0 puede hacerse de forma escalonada. Mientras tanto, las unidades de privacidad básica de DOCSIS 1.0 y las de privacidad básica plus de DOCSIS 1.1 ó 2.0 pueden coexistir dentro de un sistema DOCSIS.

C.1 Interoperabilidad de DOCSIS v1.0/v1.1/v2.0

Los requisitos de interoperabilidad BPI/BPI+ son un subconjunto de los requisitos de interoperabilidad global de DOCSIS v1.0/v1.1/v2.0 definidos en el anexo G de [J.112-B] o [J.122]. Deberán cumplirse los requisitos de interoperabilidad relativos a aprovisionamiento y registro definidos por [J.112-B] o [J.122].

C.2 Requisitos de interoperabilidad BPI/BPI+ de DOCSIS

Los requisitos de interoperabilidad BPI/BPI+ se resumen en el cuadro C.1. Un sistema de privacidad de referencia plus DEBERÍA ser retrocompatible con la privacidad básica de acuerdo con ese cuadro. Hay cuatro capacidades unidad definidas aquí a partir de la especificación de la privacidad básica y soportadas por estos requisitos de interoperabilidad.

1) Sistema de terminación de módem de cable:
   a) CMTS BPI: privacidad básica con DES de 56 bits, y aceptará un módulo de clave pública tanto de 768 bits como de 1024 bits.
   b) CMTS BPI – 40 bits: privacidad básica con DES de 40 bits, y aceptará un módulo de clave pública tanto de 768 bits como de 1024 bits. DES sólo puede funcionar en el modo 40 bits.
2) Módem de cable:
   a) CM BPI: privacidad básica con DES de 56 bits, y un módulo de clave pública de 768 bits o 1024 bits.
   b) CM BPI – 40 bits: privacidad básica con DES de 40 bits, y un módulo de clave pública de 768 bits o 1024 bits. DES sólo puede funcionar en el modo 40 bits.

Como se define en esta Recomendación, la privacidad de referencia plus introduce dos tipos de unidad adicionales.

1) CMTS BPI+: privacidad de referencia plus con DES de 56 bits, y aceptará un módulo de clave pública tanto de 768 bits como de 1024 bits.
2) CM BPI+: privacidad de referencia plus con DES de 56 bits, y un módulo de clave pública de 1024 bits.

El CMTS y el CM negocian el modo compatible BPI/BPI+ utilizando la capacidad TLV (tipo 5.6) de módem con soporte de privacidad en los mensajes REG-REQ y REG-RSP. Los requisitos para la interoperabilidad BPI/BPI+ son como sigue:

a) Un CMTS DEBE aceptar claves públicas con un módulo tanto de 768 bits como de 1024 bits procedente de un CM durante la autorización.

b) Si un CM con privacidad de referencia plus (CM BPI+) dispone de un fichero de configuración de estilo DOCSIS 1.0, el CM fija la capacidad de módem de soporte de privacidad TLV (tipo 5.6) a soporte (0) de BPI o soporte (1) de BPI+ en función de su capacidad en dicha situación (véase la cláusula B.G.2.1 de [J.112-B] o la cláusula G.1.1 de [J.122]).

c) Cuando un CMTS con privacidad de referencia plus (CMTS BPI+) recibe un conjunto TLV de capacidad de módem con soporte de privacidad (tipo 5.6, valor 0) o ningún TLV de tipo 5.6 en el mensaje REG-REQ proveniente de un CM, el CMTS DEBE replegarse a un modo de funcionamiento compatible con la privacidad básica [SCTE22-2] para las comunicaciones con ese CM.

d) Cuando un CMTS con privacidad de referencia plus funcione en un sistema que soporte módems de cable (CM) tanto de BPI como de BPI+, el servidor TFTP DEBE incluir dos tipos de ficheros de configuración:
   - Fichero de configuración con todos los parámetros BPI (tipo 17.1 hasta 17.7) para los CM dispuestos para funcionar en el modo BPI; y
   - Fichero de configuración con todos o parte de los parámetros BPI+ para los CM dispuestos para funcionar en el modo BPI+.

e) Cuando un CM con privacidad de referencia plus (CM BPI+) recibe un conjunto TLV de capacidad de módem con soporte de privacidad (tipo 5.6, valor 0) o ningún TLV de tipo 5.6 en el mensaje REG-RSP proveniente de un CMTS, el CM DEBE replegarse a un modo de

funcionamiento compatible con la privacidad básica [SCTE22-2] para las comunicaciones con ese CMTS.

NOTA – Como se especifica en el anexo B, el CM DOCSIS 1.1 ó 2.0 siempre certifica el soporte lógico con independencia de la fijación de soporte de privacidad (tipo 5.6) en el mensaje REG-RSP y de la fijación de habilitación de privacidad (tipo 4.7 ó 29) en el fichero de configuración de CM.

Cuadro C.1/J.125 – Matriz de interoperabilidad BPI/BPI+

	CM BPI	**CM BPI -40 bits**	**CM BPI+**
CMTS BPI	Configuración BPI nacional. Módulo RSA de 768 ó 1024 bits	Módulo RSA de 768 ó 1024 bits. El soporte lógico del CMTS pone a cero los bits de la TEK hasta la norma de 40 bits	El CM se repliega al modo BPI con módulo RSA de 1024 bits
CMTS BPI 40 bits	Módulo RSA de 768 ó 1024 bits. El soporte lógico del CMTS pone a cero los bits de la TEK hasta la norma de 40 bits	Módulo RSA de 768 ó 1024 bits. Toda la compatibilidad a 40 bits manejada por microplaquetas MAC	El CM se repliega al modo BPI con módulo RSA de 1024 bits. El soporte lógico del CMTS pone a cero bits de TEK hasta la norma de 40 bits
CMTS BPI+	El CMTS se repliega al modo BPI. Módulo RSA de 768 ó 1024 bits	Módulo RSA de 768 ó 1024 bits. El soporte lógico del CMTS pone a cero los bits de la TEK hasta la norma de 40 bits	Configuración BPI+ o BPI completa en función del fichero de configuración y de la fijación de CMTS. Módulo RSA de 1024 bits

C.3 Consideraciones relativas al modo exportación DES de 40 bits de BPI

La especificación de la privacidad de referencia plus es retrocompatible con el modo exportación DES de 40 bits de privacidad básica. La carga de la conformidad se sitúa en el CMTS. No todos los vendedores de equipos DOCSIS necesitarán funcionar alguna vez en sistemas con unidades BPI con capacidad de DES de 40 bits. Por ello, la conformidad se deja a criterio de cada fabricante de CMTS. Un CMTS DEBERÍA soportar la retrocompatibilidad con la privacidad básica de DES de 40 bits. Si la soporta, DEBE hacerlo de acuerdo con la presente Recomendación.

a) Cuando un CMTS envía o recibe datos criptados que circulan entre él mismo y un CM que utiliza DES de 40 bits, el CMTS DEBE poner a cero los bits apropiados de sus TEK antes de criptar o descriptar los datos de tráfico correspondientes. Los bits apropiados de la TEK DEBEN ser puestos a cero de acuerdo con el requisito de TEK de 40 bits de la privacidad básica.

b) Cuando se ha de pasar tráfico criptado entre un CMTS con capacidad de DES de 40 bits solamente y un CM con capacidad de DES de 56 bits, el CMTS DEBE proporcionar una TEK conforme de 40 bits en el mensaje respuesta de clave enviado al CM.

El método que utiliza un CMTS para reconocer los CM de un sistema con capacidad de DES de 56 bits o sólo DES de 40 bits se deja que lo decida cada operador de sistema y cada vendedor de CMTS, de la forma que se acomode lo mejor posible a su propia situación. Una manera de obtener esta información sería conseguirla de los vendedores de CM, en base a los números de serie de los CM, las direcciones MAC, las fechas de fabricación o algún otro mecanismo que permita efectuar el seguimiento del dispositivo. Una vez recogida la información, debería incorporarse a la base de datos del CMTS de información almacenada en cada uno de los CM.

Una manera alternativa de obtener esa información es mediante una base de información de gestión (MIB) de BPI DOCSIS definida a tal fin.

C.4 Funcionamiento del sistema

C.4.1 CMTS con capacidad BPI

Un CMTS con capacidad BPI aprovisionará siempre los módems de cable (CM) utilizando ficheros de configuración TFTP según DOCSIS 1.0 y fijaciones de configuración de BPI. Los CM tanto de BPI como de BPI+ recibirán las fijaciones BPI y cada CM sólo tratará de registrarse como un CM DOCSIS 1.0 con capacidad de BPI. Si un CM indica una capacidad de módem BPI+ en la petición de registro, el CMTS responderá con esa capacidad eliminada y forzará la compatibilidad del CM con BPI.

C.4.2 CMTS con capacidad BPI+

Un CMTS con capacidad BPI+ DOCSIS 1.1 ó 2.0 DEBE poder funcionar en modos compatibles con BPI y con BPI+ y ajustarse de acuerdo con la capacidad de cada CM cliente. Cuando el CMTS tiene capacidad BPI+ y el sistema soporta simultáneamente módems de cable (CM) de BPI y BPI+, DEBEN estar disponibles los ficheros de configuración tanto DOCSIS 1.0 y DOCSIS 1.1 como DOCSIS 2.0 para la entrega de fijaciones de configuración BPI+ y BPI a los CM apropiados. Un CM con capacidad BPI recibirá un fichero de configuración DOCSIS 1.0 con fijaciones BPI. A continuación se registrará con capacidad de módem BPI.

Anexo D

Mejora de BPI a BPI+

D.1 Módem de cable híbrido con BPI+

Algunos diseños de CM DOCSIS 1.0 pueden ser capaces de soportar características BPI+ mediante una mejora del soporte lógico. Para facilitar estos "CM híbridos DOCSIS 1.0", [J.112-B] o [J.122] proporciona las codificaciones de capacidades de módem que puede introducir el CM híbrido en el mensaje de petición de registro para negociar sus características DOCSIS 1.1 ó DOCSIS 2.0 con el CMTS.

Un módem de cable híbrido DOCSIS 1.0 PUEDE poner a 1 la fijación de capacidades de módem con soporte de privacidad (soporte BPI+), si el CM cumple en su totalidad la BPI+, salvo en los puntos siguientes.

- soporte de DES de 56 bits, si el CM soporta sólo DES de 40 bits,
- soporte de la clave RAS de 1024 bits, si el CM soporta la clave RAS de 768 bits,
- memoria permanente de una sola lectura para los certificados de CM emitidos por el fabricante,
- criptación de los paquetes concatenados, si está fijada a 0 (desactivada) la codificación de capacidades de módem con soporte de concatenación,
- criptación de los paquetes de fragmentación, si está fijada a 0 (desactivada) la codificación de capacidades de módem con soporte de fragmentación,
- criptación de los paquetes de PHS (supresión de encabezamiento de cabida útil), si está fijada a 0 (desactivada) la codificación de capacidades de módem con soporte de supresión de encabezamiento de cabida útil.

El CM híbrido con BPI+ podrá funcionar tanto con CMTS BPI+ como con CMTS BPI de acuerdo con las DES de 56 y de 40 bits. Además del anexo C, el requisito para el interfuncionamiento BPI/BPI+ es:

a) Si el CM híbrido con BPI+ soporta únicamente la DES de 40 bits y funciona en el modo BPI+, DEBE enviar un mensaje de petición de autorización con el atributo capacidades de seguridad para especificar la DES de 40 y el CMTS DEBE funcionar con el CM en el modo DES de 40 bits especificado en 10.1.

D.2 Procedimiento de mejora

Las características BPI+ PUEDEN ser telecargadas en el CM DOCSIS 1.0 mediante los procedimientos siguientes.

1) Telecargar la configuración de soporte lógico con características MIB BPI+ y BPI+ en el CM utilizando la función de telecarga de soporte lógico definida en la especificación DOCSIS 1.0. El certificado de CA de fabricante firmado por la clave privada raíz DOCSIS está insertado en esa configuración de código de soporte lógico.

2) Fijar el certificado de CM firmado por la clave privada del fabricante y por la clave privada de CA raíz DOCSIS al CM utilizando MIB BPI+, si el CM no dispone todavía de esta información. Los detalles sobre estos objetos MIB BPI+ para esta operación se definirán en [DOCSIS8].

NOTA – El CM no puede ni funcionar en el modo BPI+ ni fijar a 1 la fijación de capacidades de módem con soporte de privacidad (soporte BPI plus) hasta que el certificado de CM y la clave pública del CA raíz DOCSIS sean establecidos por el CM.

Apéndice I

Ejemplos de mensajes, certificados y PDU

Este apéndice presenta ejemplos numéricos que pueden ser de utilidad para los implementadores de la presente Recomendación. Los ejemplos se desarrollan a través de un intercambio de claves típico: información de autorización, petición de autorización, respuesta de autorización, petición de clave y respuesta de clave. En cada paso se dan detalles sobre los cálculos criptográficos, y se incluyen ejemplos de certificados. Los ejemplos incluyen asimismo varias PDU paquete, criptadas utilizando el material de aplicación de claves obtenido en el intercambio de claves del ejemplo.

El presente apéndice es de carácter informativo solamente y no forma parte de la Recomendación.

I.1 Notación

En el ejemplo que sigue, los paquetes se representan como trenes de octetos, cada octeto en notación hexadecimal, a veces con una anotación de texto. El orden de transmisión de los octetos es de izquierda a derecha y de arriba abajo. Considérese, por ejemplo la representación siguiente de un paquete:

00 01 02 03	Descripción #1
04 05	
06 07 08	Descripción #2

El paquete consta de 9 octetos, representados en notación hexadecimal como "00", "01", ..., "08". El octeto representado por "00" es el que se transmite primero, y el octeto representado por "08" se transmite el último.

En el análisis de los ejemplos, los valores enteros se representan en notación hexadecimal utilizando un prefijo "0x" o en notación decimal sin prefijo. Por ejemplo, la notación hexadecimal 0x12345 y la notación decimal 74565 representan el mismo valor entero. Todos los valores enteros son valores no negativos. Así por ejemplo, 0xff representa el entero que tiene el valor 255, es decir, un valor no negativo.

El protocolo BPKM genera y distribuye claves DES de 8 octetos y claves DES triple de 16 octetos, sin corregir el bit menos significativo de cada octeto para paridad. Las implementaciones extraen una clave de 56 bits de una clave de 8 octetos y una clave de 112 bits de una clave de 16 octetos ignorando el valor del bit menos significativo de cada octeto. En los ejemplos que aquí se dan, las claves se representan sin corrección de paridad.

I.2 Información de autorización

El CM envía el mensaje información de autorización siguiente:

0c 01 02 94	Encabezamiento de información de autorización
11 02 91	Encabezamiento de certificado de CA
30 82 02 8d 30 82 01 f6 . . . 81 87 19 61 72 20 19 1e	Certificado de CA

El campo código tiene el valor 0x0c, lo que identifica esto como un mensaje información de autenticación. El campo longitud tiene el valor 0x294 (660), que es el número de octetos que siguen al campo longitud.

El único atributo es el certificado de CA. A continuación se dan detalles del certificado.

I.2.1 Detalles del certificado de CA

Los campos del certificado de CA del mensaje información de autorización anterior se descomponen como sigue:

30 82 02 8d	encabezamiento de certificado
30 82 01 f6	encabezamiento de tbsCertificate
a0 03 02 01 02	versión
02 08 01 02 03 04 05 06 07 08	número de serie
30 0d 06 09 2a 86 48 86 f7 0d 01 01 05 05 00	signatura
30 81 88	encabezamiento de expedidor
31 0b 30 09 06 03 55 04 06 13 02 55 53	nombre de país
31 0f 30 0d 06 03 55 04 0a 13 06 4e 6f 72 74 65 6c	nombre de organización
31 0f 30 0d 06 03 55 04 0b 13 06 44 4f 43 53 49 53	nombre de unidad organizacional
31 1f 30 1d 06 03 55 04 0b 13 16 42 75 69 6c 64 69 6e 67 20 31 2c 20 41 6e 64 6f 76 65 72 20 4d 41	nombre de unidad organizacional
31 36 30 34 06 03 55 04 03 13 2d 4e 6f 72 74 65 6c 20 43 61 62 6c 65 20 4d 6f 64 65 6d 20 52 6f 6f 74 20 43 65 72 74 69 66 69 63 61 74 65 20 41 75 74 68 6f 72 69 74 79	nombre común

30 1e	encabezamiento de validez
17 0d 39 39 30 31 32 30 31 36 30 35 30 30 5a	no antes
17 0d 34 39 31 32 33 31 32 33 35 39 35 35 5a	no después
30 81 88	encabezamiento de asunto
31 0b 30 09 06 03 55 04 06 13 02 55 53	nombre de país
31 0f 30 0d 06 03 55 04 0a 13 06 4e 6f 72 74 65 6c	nombre de organización
31 0f 30 0d 06 03 55 04 0b 13 06 44 4f 43 53 49 53	nombre de unidad organizacional
31 1f 30 1d 06 03 55 04 0b 13 16 42 75 69 6c 64 69 6e 67 20 31 2c 20 41 6e 64 6f 76 65 72 20 4d 41	nombre de unidad organizacional
31 36 30 34 06 03 55 04 03 13 2d 4e 6f 72 74 65 6c 20 43 61 62 6c 65 20 4d 6f 64 65 6d 20 52 6f 6f 74 20 43 65 72 74 69 66 69 63 61 74 65 20 41 75 74 68 6f 72 69 74 79	nombre común
30 81 9f	encabezamiento de información de clave pública de asunto
30 0d 06 09 2a 86 48 86 f7 0d 01 01 01 05 00	tipo de algoritmo de clave pública
03 81 8d 00 30 81 89	encabezamiento de clave pública
02 81 81 00 af d1 86 c8 17 45 02 bc e5 59 b4 15 ac 95 87 7b 89 f5 8b f8 3b 8a 8b ef 67 cf 9e 00 47 d5 f1 06 42 55 36 a1 d1 8c dc cb 81 bb 31 8d 35 f7 6d 11 a0 91 9b 31 3d b9 71 38 46 15 c8 81 c4 51 06 7b d7 8a 70 be c1 28 0d 78 80 3c 44 a6 5e 35 5f 6e 46 2f 80 41 28 78 63 6c 86 cc d0 b3 58 ca bc 07 d5 19 3e 8a a2 1c 7e ff 0d 16 2b 0f bd a5 5e 60 93 64 09 80 24 76 ed e4 a9 e3 81 26 0c de 8a 89	módulo de clave pública
02 03 01 00 01	exponente de clave pública
30 0d 06 09 2a 86 48 86 f7 0d 01 01 05 05 00	algoritmo de signatura
03 81 81 00 81 4d db 31 e2 31 d2 6c f5 21 29 93 4a ce cb 6c fb 8b fc 3d ef 4b e8 4a 8a db f7 d8 e3 70 1d 3c ff ba 71 70 c4 82 24 9f 12 b5 d4 3e 3a 4d 20 64 2f ab 8b 05 27 9a 34 24 33 24 d4 7e bc 41 07 34 7a a6 51 12 29 55 e7 9b 5b e5 6b 79 bb 31 04 2f d1 c6 d3 7f 32 a2 b5 cc 99 23 09 97 1a 21 44 fa 25 3b f4 4b d6 00 cf e9 1b a9 be 9b 88 f8 90 fd 59 77 80 41 7d cb ca bf 81 87 19 61 72 20 19 1e	valor de signatura

Algunos de los campos de este ejemplo son los mismos en todos los certificados de CA. Dichos campos son:

- versión: v3;
- signatura: SHA-1 con RSA, parámetros nulos;
- primer nombre de unidad organizacional del asunto: "DOCSIS";
- tipo de algoritmo de clave pública: encriptación RSA, parámetros nulos;
- exponente de clave pública: entero de 3 octetos de valor 0x10001;
- algoritmo de signatura: SHA-1 con RSA, parámetros nulos.

Éste es un ejemplo de certificado de CA auto-firmado. El nombre del expedidor y los nombres del asunto son idénticos. En este ejemplo, los campos nombre concordantes son:

- nombre de país: "US";
- nombre de organización: "Nortel";
- primer nombre de unidad organizacional: "DOCSIS";
- segundo nombre de unidad organizacional: "Building 1, Andover MA";
- nombre común: "Nortel Cable Modem Root Certificate Authority".

Los otros campos son ejemplos de valores. Algunos de éstos son:

- número de serie: entero de 8 octetos cuyo valor es 0x0102030405060708. Otros certificados de CA pueden utilizar una longitud diferente;
- no antes: 1999-01-20 16:05:00 GMT;
- no después: 2049-12-31 23:59:55 GMT;
- módulo de clave pública: entero de 1024 bits cuyo valor es 0x00afd1...8a89 (otros certificados de CA pueden utilizar una longitud de entero de 1024 a 2048 bits, inclusive);
- valor de signatura: cadena de bits de 1024 bits de longitud que representa el valor entero 0x00814d...191e (otros certificados de CA pueden utilizar una cadena de bits de longitud 1024 a 2048 bits, inclusive; la longitud concuerda con la del módulo del expedidor. La signatura se calcula en la porción del certificado que comienza con el encabezamiento de tbsCertificate y termina con el exponente de clave pública, inclusive).

I.3 Petición de autorización

El CM envía la petición de autorización siguiente:

04 72 03 40	Encabezamiento de petición de autorización
05 00 ad	Encabezamiento de identificación de CM
01 00 0c 30 30 30 30 30 30 31 32 33 34 35 36	Número de serie
02 00 03 00 00 ca	ID de fabricante
03 00 06 00 00 ca 01 04 01	Dirección MAC
04 00 8c 30 81 89 02 81 81 00 e0 e0 6c 8d be b2 8b c9 f3 a6 3d a1 12 ea f7 99 f7 3d 3e fa a3 b1 e2 42 95 71 b5 71 d2 32 7a da 10 40 e2 5b 09 74 69 08 78 46 37 71 34 3e 69 a7 37 6d f8 70 1d aa a5 34 b0 33 a3 43 ac 4d eb 41 5e 0a 8a fd a6 0a 4b 09 7f 5a 18 f2 9e c2 22 a6 6b 9a 69 73 22 d5 37 c9 63 b0 88 f5 60 5d 99 16 33 54 53 30 ed 35 de 0c 87 3b 54 ba 59 22 3e b2 79 90 96 61 db f3 4a 37 18 4c 7f a8 ca ee d6 31 02 03 01 00 01	Clave pública RSA
12 02 7a	Encabezamiento de certificado de CM
30 82 02 76 30 82 01 df . . . 19 c9 f1 dc 30 b8 d3 d5	Certificado de CM
13 00 0b	Encabezamiento de capacidades de seguridad
15 00 04 01 00 02 00	Lista de series criptográficas
16 00 01 01	Versión de BPI
0c 00 02 22 60	SAID

El campo código tiene el valor 0x04, lo que identifica esto como un paquete petición de autorización. El campo identificador tiene el valor 0x72; se trata de un valor de ejemplo. El campo longitud tiene el valor 0x0340 (832), que es el número de octetos que siguen al campo longitud.

El primer atributo es la identificación de CM. Es un atributo compuesto formado por los subatributos siguientes: número de serie, ID de fabricante, dirección MAC y clave pública RSA. Se muestran ejemplos de valores de estos tres subatributos.

La clave pública RSA se codifica según las DER y es similar al ejemplo de la sección 2.2 de [RSA2]. El módulo es un entero de 1024 bits que se representa utilizando 0x81 (129) octetos. En este ejemplo, el valor del módulo es:

```
0x00e0e06c8d ... caeed631.
```

Se señala que 0x00 es el octeto más significativo del módulo y 0x31 el menos significativo. El exponente es un entero formado por 3 octetos y cuyo valor es 0x010001.

El atributo siguiente es el certificado de CM. Más adelante se dan detalles del certificado.

NOTA – Algunos campos del certificado de CM deben concordar con subatributos de la identificación de CM; esos subatributos son la dirección MAC y la clave pública RSA.

El siguiente atributo es el atributo capacidades de seguridad. Es un atributo compuesto formado por la lista de series criptográficas y la versión de BPI. En este ejemplo se indican dos series criptográficas: DES de 56 bits sin autenticación y DES de 40 bits sin autenticación. La versión de BPI es BPI+.

El atributo final es el SAID primario del CM, cuyo valor es igual a su SID primario. En este ejemplo, el SAID primario tiene el valor 0x2260.

I.3.1 Detalles del certificado de CM

Los campos del certificado de CM del mensaje información de autorización anterior se descomponen como sigue:

30 82 02 76	encabezamiento de certificado
30 82 01 df	encabezamiento de tbsCertificate
a0 03 02 01 02	versión
02 08 01 01 01 01 01 01 01 01	número de serie
30 0d 06 09 2a 86 48 86 f7 0d 01 01 05 05 00	signatura
30 81 88	encabezamiento de expedidor
31 0b 30 09 06 03 55 04 06 13 02 55 53	nombre de país
31 0f 30 0d 06 03 55 04 0a 13 06 4e 6f 72 74 65 6c	nombre de organización
31 0f 30 0d 06 03 55 04 0b 13 06 44 4f 43 53 49 53	nombre de unidad organizacional
31 1f 30 1d 06 03 55 04 0b 13 16 42 75 69 6c 64 69 6e 67 20 31 2c 20 41 6e 64 6f 76 65 72 20 4d 41	nombre de unidad organizacional
31 36 30 34 06 03 55 04 03 13 2d 4e 6f 72 74 65 6c 20 43 61 62 6c 65 20 4d 6f 64 65 6d 20 52 6f 6f 74 20 43 65 72 74 69 66 69 63 61 74 65 20 41 75 74 68 6f 72 69 74 79	nombre común
30 1e	encabezamiento de validez

17 0d 39 39 30 33 32 33 31 36 35 38 33 34 5a	no antes
17 0d 34 39 31 32 33 31 32 33 35 39 35 30 5a	no después
30 72	encabezamiento de asunto
31 0b 30 09 06 03 55 04 06 13 02 55 53	nombre de país
31 0f 30 0d 06 03 55 04 0a 13 06 4e 6f 72 74 65 6c	nombre de organización
31 1f 30 1d 06 03 55 04 0b 13 16 42 75 69 6c 64 69 6e 67 20 31 2c 20 41 6e 64 6f 76 65 72 20 4d 41	nombre de unidad organizacional
31 15 30 13 06 03 55 04 03 13 0c 30 30 30 30 30 30 31 32 33 34 35 36	nombre común (número de serie)
31 1a 30 18 06 03 55 04 03 13 11 30 30 3a 30 30 3a 43 41 3a 30 31 3a 30 34 3a 30 31	nombre común (dirección MAC)
30 81 9f	encabezamiento de información de clave pública de asunto
30 0d 06 09 2a 86 48 86 f7 0d 01 01 01 05 00	tipo de algoritmo de clave pública
03 81 8d 00 30 81 89	encabezamiento de clave pública
02 81 81 00 e0 e0 6c 8d be b2 8b c9 f3 a6 3d a1 12 ea f7 99 f7 3d 3e fa a3 b1 e2 42 95 71 b5 71 d2 32 7a da 10 40 e2 5b 09 74 69 08 78 46 37 71 34 3e 69 a7 37 6d f8 70 1d aa a5 34 b0 33 a3 43 ac 4d eb 41 5e 0a 8a fd a6 0a 4b 09 7f 5a 18 f2 9e c2 22 a6 6b 9a 69 73 22 d5 37 c9 63 b0 88 f5 60 5d 99 16 33 54 53 30 ed 35 de 0c 87 3b 54 ba 59 22 3e b2 79 90 96 61 db f3 4a 37 18 4c 7f a8 ca ee d6 31	módulo de clave pública
02 03 01 00 01	exponente de clave pública
30 0d 06 09 2a 86 48 86 f7 0d 01 01 05 05 00	algoritmo de signatura
03 81 81 00 19 b0 2b e5 2c 37 4a af 34 cb c9 59 62 68 88 05 8a 91 5b d4 c6 fa 2e 19 ab 98 42 33 68 9d fc e4 76 23 84 8d 4a be ff bf 34 cf e0 fb 93 96 01 8b 89 d9 86 42 5e cf 6d e6 68 2e 44 99 56 6a cc f1 2c b9 5b 30 21 08 22 f5 11 b1 38 ba 6e b5 62 f0 3a dc f1 2e c4 61 95 2f 16 c8 27 63 b6 e8 69 a6 1c e1 4f 1a 8c 65 cb 57 5e 13 ce db 7f 27 f9 c1 6e bf 2f 75 77 9e a9 87 19 c9 f1 dc 30 b8 d3 d5	valor de signatura

Algunos de los campos de este ejemplo son los mismos en todos los certificados de CM.

Dichos campos son:

- versión: v3;
- signatura: SHA-1 con RSA, parámetros nulos;
- primer nombre de unidad organizacional del expedidor: " DOCSIS";
- tipo de algoritmo de clave pública: criptación RSA, parámetros nulos;
- exponente de clave pública: entero de 3 octetos de valor 0x10001;
- algoritmo de signatura: SHA-1 con RSA, parámetros nulos.

El nombre del expedidor del certificado de CM concuerda con el nombre del asunto del certificado de CA. En este ejemplo, los campos nombre de expedidor concordantes son:

- nombre de país: "US";

- nombre de organización: "Nortel";
- primer nombre de unidad organizacional: "DOCSIS";
- segundo nombre de unidad organizacional: "Building 1, Andover MA";
- nombre común: "Nortel Cable Modem Root Certificate Authority".

Los otros campos son ejemplos de valores. Algunos de éstos son:

- número de serie: entero de 8 octetos de valor 0x0101010101010101 (otros certificados de CM pueden utilizar una longitud diferente);
- no antes: 1999-03-23 16:58:34 GMT;
- no después: 2049-12-31 23.59.50 GMT;
- nombre de país del asunto: "US";
- nombre de organización del asunto: "Nortel";
- nombre de unidad organizacional del asunto: "Building 1, Andover MA";
- nombre común del asunto (número de serie): "000000123456" (otros certificados de CM pueden utilizar una cadena de longitud diferente. El valor concuerda con el atributo número de serie del mensaje petición de autorización);
- segundo nombre común del asunto (dirección MAC): "00:00:CA:01:04:01". (Todos los certificados de CM utilizan una cadena de esta longitud. El valor concuerda con el atributo dirección MAC del mensaje petición de autorización);
- módulo de clave pública: entero de 1024 bits de longitud y valor 0x00e0e0 ... d631 (otros certificados de CM pueden utilizar un entero de longitud 768 ó 1024 bits);
- valor de signatura: cadena de bits de 1024 bits de longitud que representa el valor entero 0x0019b0 ... d3d5. (Otros certificados de CM pueden utilizar una cadena de bits de 1024 a 2048 bits de longitud, inclusive; la longitud concuerda con la del módulo del expedidor. La signatura se calcula en la porción del certificado que comienza con el encabezamiento de tbsCertificate y termina con el exponente de clave pública, inclusive.)

I.4 Respuesta de autorización

El CMTS envía la respuesta de autorización siguiente:

05 72 00 9f	Encabezamiento de respuesta de autorización
07 00 80 a2 cb ad c8 34 27 71 47 06 d5 10 0c 07 94 90 bf e6 44 1b 0c 90 0d b4 ed 9c 39 aa 05 a0 c1 ef 54 4b cc fb 3a 7a 22 81 c0 dc c6 6e 39 a4 91 1c ba bf b0 ed 47 10 f2 f4 13 f9 09 33 c6 ae a3 45 67 c8 38 0f c3 9a 12 be d5 27 27 39 77 fb 98 03 39 50 39 99 f5 b6 ad b5 85 f9 16 d0 ff c6 2a ff 9f 38 73 6f 35 44 21 ad 9e e1 a5 91 4d 34 06 1d bb c9 b6 8f 8a 17 9e be c6 c9 40 eb 81 f0 62 d8 18	Clave de autorización
09 00 04 00 09 3a 80	Tiempo de vida de la clave
0a 00 01 07	Número de secuencia de clave
17 00 0e	Encabezamiento de descriptor de SA
0c 00 02 22 60	SAID
18 00 01 00	Tipo de SA
14 00 02 01 00	Serie criptográfica

El campo código tiene el valor 0x05, lo que identifica esto como un paquete respuesta de autorización. El campo identificador tiene el valor 0x72, que concuerda con el campo identificador de la petición de autorización. El campo longitud tiene el valor 0x009f (159), que es el número de octetos que siguen al campo longitud.

El primer atributo es la clave de autorización. Este atributo contiene una clave de autorización que ha sido criptada según RSA utilizando la clave pública del mensaje petición de autorización. La clave de autorización criptada según RSA es un entero formado por 0x80 (128) octetos. En este ejemplo, el valor de la clave de autorización criptada según RSA es:

0xa2cbadc8 ... f062d818.

Se señala que 0xa2 es el octeto más significativo de la clave de autorización con criptación RSA y 0x18 es el octeto menos significativo. Más adelante se dan detalles relativos al cálculo de la criptación RSA.

El segundo atributo es el tiempo de vida de la clave. En este ejemplo, su valor es 0x00093a80 (604800) segundos, o 7 días.

El tercer atributo es el número de secuencia de clave. En este ejemplo, su valor es 0x07.

Los atributos restantes son descriptores de SA. Cada descriptor de SA es un atributo compuesto formado por los subatributos siguientes: SAID, tipo de SA y serie criptográfica. En este ejemplo se incluye sólo un descriptor de SA, correspondiente al SAID de la petición de autorización. El tipo de SA es primario, y la serie criptográfica es DES de 56 bits sin autenticación.

El CM y el CMTS obtienen, cada uno de ellos, una clave de criptación de claves y dos claves de autenticación de mensajes a partir de la clave de autorización, utilizando el proceso de troceo. Más adelante se dan detalles a propósito de los cálculos del troceo. Los valores de las claves de este ejemplo son como sigue:

Clave de autorización	`4e 85 27 ff c4 12 72 8e 61 84 de c9 20 b6 e0 64 f0 bc 0b 75`
Clave de criptación de claves	`76 b4 d4 2f 14 98 59 6a ab fe 72 94 15 7c 7d 62`
Clave de autenticación de mensajes, sentido ascendente	`fe b9 f1 e2 46 a7 6d 7c a7 7b 5e b0 98 25 fd 0b 57 ca 90 c7`
Clave de autenticación de mensajes, sentido descendente	`93 d3 9d 70 c3 b6 f5 92 c4 6b d3 92 76 46 f4 f1 90 3a 52 fd`

I.4.1 Detalles de la criptación según RSA

El CMTS genera una clave de autorización aleatoria de 20 octetos. En este ejemplo, el valor de la clave de autorización es:

```
4e 85 27 ff c4 12 72 8e 61 84 de c9 20 b6 e0 64 f0 bc 0b 75
```

La clave de autorización se cripta utilizando el esquema RSAES-OAEP de [RSA3]. En esta cláusula se dan detalles del esquema aplicado en el presente ejemplo. El esquema utiliza una función generadora de máscaras (MGF, *mask-generation function*) que se basa en el troceo; en una cláusula posterior se dan detalles al respecto.

La clave de autorización se inserta en un bloque DB de 107 octetos:

```
DB =
da 39 a3 ee 5e 6b 4b 0d 32 55 bf ef 95 60 18 90 af d8 07 09 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 01 42 85 27 ff c4 12 72 8e 61 84 de c9 20 b6 e0 64 f0 bc ob 75
```

Para formar DB la clave de autorización se prologa con un octeto de valor 1, y el resultado se coloca en los 21 últimos octetos del bloque. Los 20 primeros octetos del bloque son el resultado de efectuar una operación de troceo en una cadena de longitud 0; estos 20 octetos tienen el mismo valor en cada respuesta de autorización y no son exclusivos del presente ejemplo. Los 66 octetos restantes del bloque se fijan a 0.

El CMTS genera una cadena aleatoria de 20 octetos llamada SEED (semilla). La SEED se genera de manera independiente para cada respuesta de autorización. En este ejemplo, la SEED tiene el valor siguiente:

```
SEED =
ad 9c af 8d f8 26 fe af b5 df fd 95 de 7e 97 cc e9 4b 6d 6d
```

La SEED es la entrada a la MGF para generar DB_MASK, un bloque de 107 octetos:

```
DB_MASK =
de 10 c9 59 41 c9 ea 72 a4 35 68 79 d2 53 85 db 13 7b a6 3b 37 ac 86 06 7c b5 ec
97 d2 d0 9e 01 30 2b 10 91 3a ec 3f d9 a1 2f c4 e9 8d 18 88 95 f6 9c ea 17 23 9f
5d d5 f1 4d 25 8e 9e 6d 7d 3c ca 55 fe 0e ee 2d 0d 7e 5b 64 b6 79 44 76 c 3f 6e
ac 99 3a ae 14 3e 9a 8e df 3c 36 79 58 b2 fa 13 72 58 4c ca 04 a1 af c7 c4 62
```

A DB y DB_MASK se les aplica conjuntamente el operador lógico OR exclusivo para producir MASKED_DB, que tiene 107 octetos:

```
MASKED_DB =
04 29 6a b7 1f a2 a1 7f 96 60 d7 96 47 33 9d 2d bc a3 a1 32 37 ac 86 06 7c b5 ec
97 d2 d0 9e 01 30 2b 10 91 3a ec 3f d9 a1 2f c4 e9 8d 18 88 95 f6 9c ea 17 23 9f
5d d5 f1 4d 25 8e 9e 6d 7d 3c ca 55 fe 0e ee 2d 0d 7e 5b 64 b6 79 44 76 cc 3f 6e
ac 99 3a ae 14 3f d4 0b f8 c3 f2 6b 2a 3c 9b 97 ac 91 6c 7c e4 c5 5f 7b cf 17
```

MASKED_DB la entrada a la MGF para generar SEED_MASK, un bloque de 20 octetos:

```
SEED_MASK =
b4 b6 f1 bf a6 b3 a1 7e 95 82 d3 b8 93 71 b6 7f 45 31 9e 82
```

A SEED y SEED_MASK se les aplica conjuntamente el operador lógico OR exclusivo para producir MASKED_SEED, que tiene 20 octetos:

```
MASKED_SEED =
19 2a 5e 32 5e 95 5f d1 20 5d 2e 2d 4d 0f 21 b3 ac 7a f3 ef
```

MASKED_SEED y MASKED_DB están concatenadas, y el resultado se prolonga con un solo octeto de valor 0. Con ello se obtiene un bloque de 128 octetos llamado EM:

```
EM =
00 19 2a 5e 32 5e 95 5f d1 20 5d 2e 2d 4d 0f 21 b3 ac 7a f3 ef 04 29 6a b7 1f a2
a1 7f 96 60 d7 96 47 33 9d 2d bc a3 a1 32 37 ac 86 06 7c b5 ec 97 d2 d0 9e 01 30
2b 10 91 3a ec 3f d9 a1 2f c4 e9 8d 18 88 95 f6 9c ea 17 23 9f 5d d5 f1 4d 25 8e
9e 6d 7d 3c ca 55 fe 0e ee 2d 0d 7e 5b 64 b6 79 44 76 cc 3f 6e ac 99 3a ae 14 3f
d4 0b f8 c3 f2 6b 2a 3c 9b 97 ac 91 6c 7c e4 c5 5f 7b cf 17
```

Para efectuar la criptación según RSA, EM se interpreta como el valor entero:

0x00192a5e32 ... 5f7bcf17 .

Se señala que 0x00 es el octeto más significativo y 0x17 es el octeto menos significativo.

La criptación RSA se efectúa como la operación $Y = M^E$ módulo N, donde:

M es el valor entero del bloque EM (0x00192a5e32 ... 5f7bcf17); E es el valor entero del exponente de la clave pública RSA (0x010001); N es el valor entero del módulo de la clave pública RSA (oxe0e06c8d ... caeed631), e Y es el valor entero de la clave de autorización criptada según RSA (0xa2cbadc8 ... f062d818).

I.4.2 Detalles de la descriptación según RSA

El cuadro I.1 contiene la lista de parámetros de clave privada que concuerdan con los de la clave pública RSA en el mensaje petición de autorización del ejemplo:

Cuadro I.1/J.125 – Parámetros de clave privada

Parámetro	Propiedad	Valor
D (exponente privado)	M^{DE} módulo N = M	6b 1f 1d 36 ec 77 7b 15 a9 c6 30 27 71 ae 92 62 3a 9f 67 47 d8 00 9d ca a0 0b f9 a6 0d be 54 3d 5a 6e be 25 25 bc d9 67 da 7b 80 5f a1 c6 75 67 dd 84 ba 4b 16 26 ba e9 fd 61 ab cd 49 e0 18 47 37 9f 56 08 2d d9 16 81 ff 7d d0 7e 01 8f d4 84 d3 e8 eb 27 48 c3 6c dc a9 01 b7 e5 24 28 d1 6c 67 03 a7 63 fb fa 79 d8 08 6a e1 de 3d 12 7a 36 20 25 01 d1 08 11 0c cd 80 44 3c fd c5 c4 db d1
P (factor primo)	N = PQ	f1 6b dd 2f dd d8 df 80 30 e6 9c d3 4e 46 5e 9f 42 62 b1 66 86 57 1b ca 87 9c cf fd 1c b6 26 76 95 35 bf 0b fb 51 af 0f 46 1c 5e cb 82 a0 83 bf 46 c9 3b d6 4e 7a 5d bf 03 05 69 27 31 6d 65 bd
Q (factor primo)	N = PQ	ee 74 cb a3 d0 90 2d 8a e9 e7 10 dd b4 65 2e 91 22 09 52 72 ab bd 32 31 4e d7 d0 2b 4b 13 57 20 6b f9 a4 57 b1 47 59 67 86 a6 8c 2c c1 f3 8b ba 8a 6b b1 62 5d 43 5a 71 db d0 33 43 97 99 17 85
D_p (exponente del CRT)	D_p = D módulo (P – 1)	a6 35 dc d2 57 aa 38 35 c9 74 fc 03 7e a0 74 04 b1 6f c1 33 14 ca 64 17 cb c5 ea 6c 18 98 4f 62 d4 d7 6b f0 93 d6 68 ef db 15 2d 2e 6f 80 93 33 dd 48 2e 2a 1d 5d a1 ad 20 27 59 7d e2 49 af 01
D_q (exponente del CRT)	D_q = D módulo (Q – 1)	cf f1 9c 30 33 cd b7 59 7f 96 57 f7 ee bb 99 bb 48 a2 36 7a f7 57 1a f1 32 df 32 92 be 7a 94 2d 1a db ed bb e7 45 e0 2a 4e 9a e8 7c 93 7a 4e 2c 93 4f 4c b6 09 bc 95 9f da df 9a 04 e4 ab c5 7d
U_p (Constante del CRT)	PU_p módulo Q = 1	08 17 0c 11 bc aa 2f 96 80 8b 31 95 6d 2e b8 3c ee 2e 05 88 ab 9e fc 53 24 c4 04 b8 7e 1d 01 db 2d f2 2c 06 b0 cd 04 6b 1c 14 d8 d0 4f c9 a0 ae 1b c9 80 88 be 42 0a 52 4a ef 62 3c 8b dd c5 37

Cada valor del cuadro I.1 representa los octetos de un entero, mostrándose en primer lugar el octeto más significativo. Por ejemplo, el exponente privado D tiene el valor entero:

0x6b1f1d36 ... c5c4dbd1.

El CM puede descriptar la clave de autorización utilizando o no el teorema del resto chino (CRT, *chinese remainder theorem*). La descriptación con el CRT es más complicada, pero puede resultar una operación más rápida.

Para descriptar sin utilizar el CRT, el CM efectúa la operación $M = Y^D$ módulo N. D es el exponente privado del cuadro, e Y y N se describen en la cláusula precedente. El valor resultante concuerda con el valor de M de la cláusula precedente, es decir, es el valor entero del bloque EM formado por el CMTS. El CM decodifica la clave de autorización a partir del EM invirtiendo el procedimiento utilizado por el CMTS para formar el EM, como se describe en [RSA3].

Para descriptar utilizando el CRT, el CM calcula primero dos cantidades intermedias:

$$A = Y^{Dp} \text{ mod } P;$$

$$B = Y^{Dq} \text{ mod } Q.$$

P y Q son los factores primos del módulo, y D_p y D_q son exponentes privados relacionados con esos factores, todos ellos con los valores mostrados en el cuadro. El CM calcula el valor de M de la manera siguiente:

$$M = A + ((B – A)U_p \text{ módulo } Q)P$$

U_p es una constante derivada de los factores primos, cuyo valor se muestra en el cuadro. El valor resultante de M concuerda con el valor que se hubiera calculado utilizando la fórmula $M = Y^D$ módulo N.

I.4.3 Detalles del troceo

La clave de autorización se trocea utilizando el algoritmo SHA-1 [FIPS-180-2] para producir la clave de criptación de claves (KEK), la clave de autenticación de mensajes para el sentido ascendente y la clave de autenticación de mensajes para el sentido descendente.

En el análisis que aquí se hace se representa un cálculo de troceo utilizando un cuadro que muestra la entrada a la función de troceo y el valor de troceo resultante. A continuación se muestra, para referencia, un cuadro que describe el ejemplo del apéndice B de [FIPS-180-2]:

Entrada al troceo	61 62 63 64 62 63 64 65 63 64 65 66 64 65 66 67 65 66 67 68 66 67 68 69 67 68 69 6a 68 69 6a 6b 69 6a 6b 6c 6a 6b 6c 6d 6b 6c 6d 6e 6c 6d 6e 6f 6d 6e 6f 70 6e 6f 70 71
Valor del troceo	84 98 3e 44 1c 3b d2 6e ba ae 4a a1 f9 51 29 e5 e5 46 70 f1

I.4.3.1 KEK

La KEK se computa aplicando el cálculo de troceo siguiente:

Entrada al troceo	53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 5 3 53 53 53 53 53 53 53 53 53 53 53 53 53 53 4e 85 27 ff c4 12 72 8e 61 84 de c9 20 b6 e0 64 f0 bc 0b 75
Valor del troceo	76 b4 d4 2f 14 98 59 6a ab fe 72 94 15 7c 7d 62 b0 df e6 3b

La entrada es el octeto 0x53, repetido 64 veces, seguido por los 20 octetos de la clave de autorización. El orden en que los octetos de la clave de autorización son compendiados es el mismo en que aparecen en el bloque de criptación EM.

El valor del troceo tiene una longitud de 20 bytes. Los 16 primeros bytes son la KEK.

I.4.3.2 Claves de autenticación de mensajes

La clave de autenticación de mensajes en sentido ascendente se computa aplicando el cálculo de troceo siguiente:

Entrada al troceo	5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 5c 4e 85 27 ff c4 12 72 8e 61 84 de c9 20 b6 e0 64 f0 bc 0b 75
Valor del troceo	fe b9 f1 e2 46 a7 6d 7c a7 7b 5e b0 98 25 fd 0b 57 ca 90 c7

La entrada es el octeto 0x5c, repetido 64 veces, seguido por los 20 octetos de la clave de autorización. El orden en que los octetos de la clave de autorización son compendiados es el mismo que en el cálculo de la KEK.

El valor del troceo tiene una longitud de 20 octetos. Los 20 octetos forman la clave de autenticación de mensajes en sentido ascendente.

La clave de autenticación de mensajes en sentido descendente se computa aplicando el cálculo de troceo siguiente:

Entrada al troceo	3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 4e 85 27 ff c4 12 72 8e 61 84 de c9 20 b6 e0 64 f0 bc 0b 75
Valor del troceo	93 d3 9d 70 c3 b6 f5 92 c4 6b d3 92 76 46 f4 f1 90 3a 52 fd

Esto es similar al cálculo en el caso del sentido ascendente, con la salvedad de que el valor 0x3a sustituye al valor 0x5c.

I.4.3.3 Función de generación de máscaras

La función de generación de máscaras (MGF) se construye a partir de las operaciones de troceo de SHA-1. Cada operación de troceo genera 20 octetos de datos de máscara. El número de operaciones de troceo efectuadas depende del tamaño de la máscara que se necesite.

La cantidad SEED_MASK se forma aplicando la MGF a MASKED_DB. Puesto que SEED_MASK tiene una longitud de 20 octetos, sólo se necesita una función de troceo:

Entrada al troceo	04 29 6a b7 1f a2 a1 7f 96 60 d7 96 47 33 9d 2d bc a3 a1 32 37 ac 86 06 7c b5 ec 97 d2 d0 9e 01 30 2b 10 91 3a ec 3f d9 a1 2f c4 e9 8d 18 88 95 f6 9c ea 17 23 9f 5d d5 f1 4d 25 8e 9e 6d 7d 3c ca 55 fe 0e ee 2d 0d 7e 5b 64 b6 79 44 76 cc 3f 6e ac 99 3a ae 14 3f d4 0b f8 c3 f2 6b 2a 3c 9b 97 ac 91 6c 7c e4 c5 5f 7b cf 17 00 00 00 00
Valor del troceo	b4 b6 f1 bf a6 b3 a1 7e 95 82 d3 b8 93 71 b6 7f 45 31 9e 82

Los datos de entrada a la operación de troceo son el MASKED_DB de 107 octetos seguido por 4 octetos de valor 0. La salida de la operación de troceo es el valor de SEED_MASK.

La cantidad DB_MASK se forma aplicando la MGF a SEED. Puesto que DB_MASK tiene una longitud de 107 octetos, hacen falta seis operaciones de troceo:

Entrada al troceo	ad 9c af 8d f8 26 fe af b5 df fd 95 de 7e 97 cc e9 4b 6d 6d 00 00 00 00
Valor del troceo	de 10 c9 59 41 c9 ea 72 a4 35 68 79 d2 53 85 bd 13 7b a6 3b

Entrada al troceo	ad 9c af 8d f8 26 fe af b5 df fd 95 de 7e 97 cc e9 4b 6d 6d 00 00 00 01
Valor del troceo	37 ac 86 06 7c b5 ec 97 d2 d0 9e 01 30 2b 10 91 3a ec 3f d9

Entrada al troceo	ad 9c af 8d f8 26 fe af b5 df fd 95 de 7e 97 cc e9 4b 6d 6d 00 00 00 02
Valor del troceo	a1 2f c4 e9 8d 18 88 95 f6 9c ea 17 23 9f 5d d5 f1 4d 25 8e

Entrada al troceo	ad 9c af 8d f8 26 fe af b5 df fd 95 de 7e 97 cc e9 4b 6d 6d 00 00 00 03
Valor del troceo	9e 6d 7d 3c ca 55 fe 0e ee 2d 0d 7e 5b 64 b6 79 44 76 cc 3f

Entrada al troceo	ad 9c af 8d f8 26 fe af b5 df fd 95 de 7e 97 cc e9 4b 6d 6d 00 00 00 04
Valor del troceo	6e ac 99 3a ae 14 3e 9a 8e df 3c 36 79 58 b2 fa 13 72 58 4c

Entrada al troceo	ad 9c af 8d f8 26 fe af b5 df fd 95 de 7e 97 cc e9 4b 6d 6d 00 00 00 05
Valor del troceo	ca 04 a1 af c7 c4 62 3a df 6f 33 ec e2 cd 2c 7f b7 7e 48 19

Los datos de entrada a cada operación de troceo son los 20 octetos de SEED seguidos por un valor de cuatro octetos. El valor de cuatro octetos cuenta los valores enteros 0, 1, 2, 3, 4, 5 en operaciones de troceo sucesivas. Las salidas de las seis operaciones de troceo se concatenan en un resultado de 120 octetos, y los primeros 107 octetos del resultado constituyen DB_MASK.

I.5 Petición de clave

El CM envía la petición de clave siguiente:

07 73 00 d0	Encabezamiento de petición de clave
05 00 ad	Encabezamiento de identificación de CM
01 00 0c 30 30 30 30 30 30 31 32 33 34 35 36	Número de serie
02 00 03 25 53 41	ID de fabricante
03 00 06 00 00 ca 01 04 01	Dirección MAC
04 00 8c 30 81 89 02 81 81 00 e0 e0 6c 8d be b2 8b c9 f3 a6 3d a1 12 ea f7 99 f7 3d 3e fa a3 b1 e2 42 95 71 b5 71 d2 32 7a da 10 40 e2 5b 09 74 69 08 78 46 37 71 34 3e 69 a7 37 6d f8 70 1d aa a5 34 b0 33 a3 43 ac 4d eb 41 5e 0a 8a fd a6 0a 4b 09 7f 5a 18 f2 9e c2 22 a6 6b 9a 69 73 22 d5 37 c9 63 b0 88 f5 60 5d 99 16 33 54 53 30 ed 35 de 0c 87 3b 54 ba 59 22 3e b2 79 90 96 61 db f3 4a 37 18 4c 7f a8 ca ee d6 31 02 03 01 00 01	Clave pública RSA
0a 00 01 07	Número de secuencia de clave
0c 00 02 22 60	SAID
0b 00 14 86 b8 33 b7 48 9c 4b a1 51 67 44 d7 a6 e6 ca 21 33 f5 22 9e	Compendio de HMAC

El campo código tiene el valor 0x07, lo que identifica esto como un paquete petición de clave. El campo identificador tiene el valor 0x73; se trata de un valor de ejemplo, obtenido incrementando el valor del identificador de la petición de autorización. El campo longitud tiene el valor 0x00d0 (208), que es el número de octetos que siguen al campo longitud.

El primer atributo es la identificación de CM. Es un atributo compuesto, idéntico al de la petición de autorización.

El segundo atributo es el número de secuencia de clave, que identifica la clave de autorización. El valor es idéntico al de la respuesta de autorización.

El tercer atributo es el SAID para el que se está pidiendo una clave. Este valor de SAID estaba contenido en la respuesta de autorización.

El atributo final es el compendio de HMAC. El compendio consta de 20 octetos. Se calcula utilizando la clave de autenticación de mensajes en sentido ascendente. El compendio se efectúa con todos los octetos del paquete petición de clave, excluyendo los 23 octetos del propio atributo compendio de HMAC. A continuación se dan detalles del cálculo del compendio.

I.5.1 Detalles del compendio de HMAC

El compendio de HMAC se calcula utilizando el método de autenticación de HMAC definido en [RFC2104], con SHA-1 como función de troceo. En [RFC2202] se presentan ejemplos de cálculo de HMAC utilizando SHA-1.

En el análisis que aquí se hace se representa un cálculo de HMAC utilizando un cuadro que muestra la clave, la entrada a la función HMAC y el compendio de HMAC resultante. A continuación se muestra, para referencia, un cuadro que describe el caso de prueba #2 de los ejemplos de HMAC-SHA-1 en [RFC2202]:

Clave	4a 65 66 65
Entrada a HMAC	77 68 61 74 20 64 6f 20 79 61 20 77 61 6e 74 20 66 6f 72 20 6e 6f 74 68 69 6e 67 3f
Compendio de HMAC	ef fc df 6a e5 eb 2f a2 d2 74 16 d5 f1 84 df 9c 25 9a 7c 79

El compendio de HMAC del paquete petición de clave se computa aplicando el cálculo de HMAC siguiente:

Clave	fe b9 f1 e2 46 a7 6d 7c a7 7b 5e b0 98 25 fd 0b 57 ca 90 c7
Entrada a HMAC	07 73 00 d0 05 00 ad 01 00 0c 30 30 30 30 30 30 31 32 33 34 35 36 02 00 03 25 53 41 03 00 06 00 00 ca 01 04 01 04 00 8c 30 81 89 02 81 81 00 e0 e0 6c 8d be b2 8b c9 f3 a6 3d a1 12 ea f7 99 f7 3d 3e fa a3 b1 e2 42 95 71 b5 71 d2 32 7a da 10 40 e2 5b 09 74 69 08 78 46 37 71 34 3e 69 a7 37 6d f8 70 1d aa a5 34 b0 33 a3 43 ac 4d eb 41 5e 0a 8a fd a6 0a 4b 09 7f 5a 18 f2 9e c2 22 a6 6b 9a 69 73 22 d5 37 c9 63 b0 88 f5 60 5d 99 16 33 54 53 30 ed 35 de 0c 87 3b 54 ba 59 22 3e b2 79 90 96 61 db f3 4a 37 18 4c 7f a8 ca ee d6 31 02 03 01 00 01 0a 00 01 07 0c 00 02 22 60
Compendio de HMAC	86 b8 33 b7 48 9c 4b a1 51 67 44 d7 a6 e6 ca 21 33 f5 22 9e

La clave es la clave de autenticación de mensajes en sentido ascendente. La entrada consta de todos los octetos del paquete petición de clave, excluyendo el atributo compendio de HMAC. Los octetos del compendio son el contenido del atributo compendio de HMAC.

I.6 Respuesta de clave

El CMTS envía la respuesta de clave siguiente:

08 73 00 68	Encabezamiento de respuesta de clave
0a 00 01 07	Número de secuencia de clave (clave de autorización)
0c 00 02 22 60	SAID
0d 00 21	Encabezamiento de parámetros de TEK
08 00 08 b6 4d 54 8c 3f 6b 25 69	Clave de TEK
09 00 04 00 00 a8 c0	Tiempo de vida de la clave
0a 00 01 02	Número de secuencia de clave (TEK)
0f 00 08 81 0e 52 8e 1c 5f da 1a	IV CBC DES
0d 00 21	Encabezamiento de parámetros de TEK
08 00 08 5e bd 03 aa 5e d5 e2 94	Clave TEK
09 00 04 00 01 51 80	Tiempo de vida de la clave
0a 00 01 03	Número de secuencia de clave (TEK)
0f 00 08 25 35 67 c3 09 21 8c 2c	IV CBC DES
0b 00 14 a5 e3 33 25 ea 72 f8 50 1c 2a b6 65 45 6b cc de 8b 4f 22 02	Compendio de HMAC

El campo código tiene el valor 0x08, lo que identifica esto como un paquete respuesta de clave. El identificador tiene el valor 0x73, que concuerda con el valor de la petición de clave. El campo longitud tiene el valor 0x68 (104), que es el número de octetos que siguen al campo longitud.

El atributo número de secuencia de clave identifica la clave de autorización. Concuerda con el valor de la petición de clave.

El atributo SAID identifica el SAID para el que se está suministrando una TEK. Concuerda con el valor de la petición de clave.

Se incluyen dos atributos parámetros de TEK, el primero para la generación más antigua de parámetros de clave y el segundo para la más reciente. Cada atributo parámetros de TEK es un atributo compuesto formado por los subatributos siguientes: clave TEK, tiempo de vida de la clave, número de secuencia de clave y vector de inicialización (IV) de encadenamiento de bloques cifrados (CBC) de DES.

La clave TEK consta de 8 octetos. Contiene la TEK, criptada utilizando ECB de DES triple con la KEK obtenida a partir de la clave de autorización. Más adelante se dan detalles sobre el cálculo de ECB de DES triple.

El subatributo tiempo de vida de la clave se refiere a la TEK. En este ejemplo, el valor para la TEK más antigua es 0x0000a8c0 (43200) segundos, o 12 horas, y el valor para la TEK más reciente es 0x00015180 (86400) segundos, o 24 horas.

El subatributo número de secuencia de clave identifica la TEK. En este ejemplo, el valor para la TEK más antigua es 0x02, y el valor para la TEK más reciente es 0x03.

El subatributo IV CBC DES (vector de inicialización del encadenamiento de bloques cifrados de la norma DES) consta de 8 octetos. Especifica el vector de inicialización que se ha de utilizar con la TEK.

El atributo final es el compendio de HMAC. Consta de 20 octetos. Se calcula de manera similar a la de la respuesta de clave, con la salvedad de que se utiliza la clave de autenticación de mensajes en sentido descendente en vez de la clave en sentido ascendente. Más adelante se dan detalles sobre el cálculo de HMAC.

Una vez que el CM ha procesado el paquete respuesta de clave, el CM y el CMTS comparten dos generaciones de TEK e IV. Los valores de estos parámetros para el presente ejemplo son como sigue:

TEK más antigua	`e6 60 0f d8 85 2e f5 ab`
IV más antiguo	`81 0e 52 8e 1c 5f da 1a`
TEK más reciente	`b1 d7 4f c9 64 68 f7 58`
IV más reciente	`25 35 67 c3 09 21 8c 2c`

I.6.1 Detalles de la criptación de EK

El CMTS genera una TEK aleatoria de 8 octetos. En este ejemplo, el valor de la TEK es:

`e6 60 0f d8 85 2e f5 ab.`

Ésta es la primera TEK del mensaje respuesta de clave.

La TEK se cripta utilizando criptación DES-ECB triple. La clave de criptación es la KEK:

`76 b4 d4 2f 14 98 59 6a ab fe 72 94 15 7c 7d 62.`

La criptación DES-ECB triple se describe aquí en términos de varias iteraciones de criptación o descriptación DES-ECB. DES-ECB se define en [FIPS-81].

En el análisis que aquí se hace se representa una operación de criptación o descriptación DES-ECB utilizando un cuadro que muestra la clave, la entrada y la salida. A continuación se muestran, para referencia, los cuadros que describen el ejemplo del cuadro B1 de [FIPS-81]:

Modo	Criptación ECB
Clave	`01 23 45 67 89 ab cd ef`
Entrada a DES	`4e 6f 77 20 69 73 20 74`
Salida de DES	`3f a4 0e 8a 98 4d 48 15`

Modo	Descriptación ECB
Clave	`01 23 45 67 89 ab cd ef`
Entrada a DES	`3f a4 0e 8a 98 4d 48 15`
Salida de DES	`4e 6f 77 20 69 73 20 74`

NOTA – En [FIP-81] se pide que el bit menos significativo de cada octeto de la clave se ajuste de manera que el octeto tenga paridad impar. Esto es evidente en la clave del ejemplo anterior. El protocolo BPKM no precisa paridad impar. BPKM genera y distribuye claves DES de 8 octetos de paridad arbitraria, y requiere que las implementaciones ignoren el valor del bit menos significativo de cada octeto.

La TEK se cripta según DES-ECB triple utilizando las tres operaciones DES-ECB siguientes:

Modo	Criptación ECB
Clave	76 b4 d4 2f 14 98 59 6a
Entrada a DES	e6 60 0f d8 85 2e f5 ab
Salida de DES	c3 94 31 f5 8d f9 1d bf

Modo	Descriptación ECB
Clave	ab fe 72 94 15 7c 7d 62
Entrada a DES	c3 94 31 f5 8d f9 1d bf
Salida de DES	44 b0 94 4e ab 04 4c 23

Modo	Criptación ECB
Clave	76 b4 d4 2f 14 98 59 6a
Entrada a DES	44 b0 94 4e ab 04 4c 23
Salida de DES	b6 4d 54 8c 3f 6b 25 69

La primera y tercera operaciones son criptación DES-ECB; la clave para cada una de ellas son los ocho primeros octetos de la KEK. La segunda operación es descriptación DES-ECB; la clave son los últimos ocho octetos de la KEK. La entrada a la primera operación es la TEK que ha de ser criptada. La entrada a la segunda operación es la salida de la primera, y la entrada a la tercera es la salida de la segunda. La salida de la tercera operación es la TEK criptada; esto se lleva en el subatributo clave TEK del mensaje respuesta de clave.

I.6.2 Detalles del HMAC

El compendio de HMAC del paquete respuesta de clave se calcula aplicando un método similar al del paquete petición de clave. La clave es la clave de autenticación de mensajes en sentido descendente. A continuación se indican los detalles del cálculo de HMAC:

Clave	93 d3 9d 70 c3 b6 f5 92 c4 6b d3 92 76 46 f4 f1 90 3a 52 fd
Entrada a HMAC	08 73 00 68 0a 00 01 07 0c 00 02 22 60 0d 00 21 08 00 08 b6 4d 54 8c 3f 6b 25 69 09 00 04 00 00 a8 c0 0a 00 01 02 0f 00 08 81 0e 52 8e 1c 5f da 1a 0d 00 21 08 00 08 5e bd 03 aa 5e d5 e2 94 09 00 04 00 01 51 80 0a 00 01 03 0f 00 08 25 35 67 c3 09 21 8c 2c
Compendio de HMAC	a5 e3 33 25 ea 72 f8 50 1c 2a b6 65 45 6b cc de 8b 4f 22 02

I.7 Criptación de PDU paquete

Los 12 primeros octetos de la PDU paquete, que contienen las direcciones de destino y origen (DA/SA, *destination and source addresses*) Ethernet/802.3, no son criptados. Los restantes octetos de la PDU paquete se criptan utilizando el modo DES-CBC con un tratamiento especial de los bloques de terminación residuales que tienen menos de 64 bits. La combinación DES-CBC y procesamiento de bloques residuales garantiza el que la criptación no cambie la longitud del paquete. La clave de criptación es la TEK correspondiente al número de secuencia de clave del encabezamiento ampliado de privacidad del paquete.

La especificación describe el procesamiento del bloque residual como sigue:

"Dado un bloque final que tiene n bits, siendo n inferior a 64, el penúltimo bloque de texto cifrado se cripta aplicando DES una segunda vez, el modo ECB, y a los n bits menos significativos del resultado se les aplica el operador lógico OR exclusivo con los n bits finales de la cabida útil para generar el bloque cifrado final corto. ... En el caso especial de que la cabida útil de la PDU datos por paquetes sea inferior a 64 bits, el vector de inicialización se cripta aplicando DES, y a los n bits situados más a la izquierda del texto cifrado resultante, correspondientes al número de bits de la cabida útil, se les aplica el operador lógico OR exclusivo con los n bits de la cabida útil para generar el bloque cifrado corto."

Una descripción alternativa de este procedimiento, que equivale a la descripción de la especificación, es como sigue:

Dado un bloque final que tiene n bits, siendo n inferior a 64, se añaden bits de relleno a los n bits hasta formar un bloque de 64 bits agregando 64-n bits de un valor cualquiera a la derecha de los n bits de la cabida útil. El bloque resultante se cripta según DES utilizando el modo CFB64, en donde el penúltimo bloque de texto cifrado actúa como vector de inicialización de la operación CFB64. Los n bits situados más a la izquierda del texto cifrado resultante se utilizan como bloque cifrado corto. ... En el caso especial de que la cabida útil de la PDU datos por paquetes sea inferior a 64 bits, el procedimiento es el mismo que para un bloque final corto, con el vector de inicialización proporcionado sirviendo como vector de inicialización de la operación DES-CFB64.

La descripción alternativa produce el mismo texto cifrado que la descripción de la especificación. En la descripción alternativa, no obstante, no se menciona la combinación de criptación ECB con la aplicación de un operador lógico OR exclusivo. Estas operaciones son operaciones internas de CFB64, al igual que lo son de CBC. La descripción alternativa conviene aquí porque permite que el procesamiento del bloque residual se ilustre utilizando ejemplos de CFB64 de [FIPS-81].

La PDU paquete incluye la dirección de destino (DA), la dirección de origen (SA) y los campos tipo/longitud. En los ejemplos que se presentan aquí no se hace ningún esfuerzo por utilizar valores correctos para esos campos. Como resultado de ello, los ejemplos no son paquetes válidos, adecuados para la transmisión. El propósito de los ejemplos es ilustrar los detalles de la criptación solamente.

En estos ejemplos, la TEK y el IV se toman del ejemplo de paquete respuesta de clave descrito más arriba.

I.7.1 CBC solamente

Cuando el número de octetos que se han de criptar es un múltiplo de 8, el modo de criptación es el DES-CBC definido en [FIPS-81]. La clave de criptación y el IV se llevan en el paquete respuesta de clave.

En el análisis que aquí se hace se representa una criptación DES-CBC utilizando un cuadro que muestra la clave, el IV, la entrada de texto en claro y la salida de texto cifrado. A continuación se muestra, para referencia, un cuadro que describe el ejemplo del cuadro C1 de [FIPS-81]:

Modo	CBC
Clave	`01 23 45 67 89 ab cd ef`
IV	`12 34 56 78 90 ab cd ef`
Texto en claro	`4e 6f 77 20 69 73 20 74 68 65 20 74 69 6d 65 20`
Texto cifrado	`e5 c7 cd de 87 2b f2 7c 43 e9 34 00 8c 38 9c 0f`

Supóngase que la PDU paquete, antes de la criptación, es como sigue:

DA	01 02 03 04 05 06
SA	f1 f2 f3 f4 f5 f6
Tipo/longitud	00 01
Datos de usuario	02 03 04 05 06 07 08 09 0a 0b
CRC	88 41 65 06

La criptación DES-CBC se efectúa como sigue:

Modo	CBC
Clave	e6 60 0f d8 85 2e f5 ab
IV	81 0e 52 8e 1c 5f da 1a
Texto en claro	00 01 02 03 04 05 06 07 08 09 0a 0b 88 41 65 06
Texto cifrado	0d da 5a cb d0 5e 55 67 9f 04 d1 b6 41 3d 4e ed

La PDU paquete, después de la criptación, tiene el aspecto siguiente:

DA	01 02 03 04 05 06
SA	f1 f2 f3 f4 f5 f6
Tipo/longitud	0d da
Datos de usuario	5a cb d0 5e 55 67 9f 04 d1 b6
CRC	41 3d 4e ed

I.7.2 CBC con procesamiento de bloque residual

Cuando el número de octetos que se han de criptar es superior a 8 y no es un múltiplo de 8, el modo de criptación es una combinación de DES-CBC y DES-CFB64.

La criptación empieza en el modo DES-CBC. El modo DES-CBC se utiliza para procesar todos los bloques DES completos que estén presentes. La clave de criptación y el IV se llevan en el paquete respuesta de clave.

Después de la criptación DES-CBC, hay 1 a 7 octetos que no han sido criptados. Estos octetos se criptan utilizando el modo DES-CFB64. El modo DES-CFB64 es "el modo realimentación de cifrado de 64 bits", definido en [FIPS-81]. La clave de criptación está en el paquete respuesta de clave. El vector de inicialización (IV) son los 8 últimos octetos del texto cifrado producido por el procesamiento DES-CBC.

En el análisis que aquí se hace se representa una criptación DES-CFB64 utilizando un cuadro que muestra la clave, el IV, la entrada de texto en claro y la salida de texto cifrado. A continuación se presenta, para referencia, un cuadro que describe el ejemplo del cuadro D3 [FIPS-81]:

Modo	CFB64
Clave	01 23 45 67 89 ab cd ef
IV	12 34 56 78 90 ab cd ef
Texto en claro	4e 6f 77 20 69 73 20 74 68 65 20 74 69 6d 65 20
Texto cifrado	f3 09 62 49 c7 f4 6e 51 a6 9e 83 9b 1a 92 f7 84

Supóngase que la PDU paquete, antes de la criptación, es como sigue:

DA	01 02 03 04 05 06
SA	f1 f2 f3 f4 f5 f6
Tipo/longitud	00 01
Datos de usuario	02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e
CRC	91 d2 d1 9f

El número total de octetos que se han de criptar es 19. Los 16 primeros octetos se procesan utilizando criptación DES-CBC, y los 3 últimos octetos utilizando criptación DES-CFB64.

La criptación DES-CBD se efectúa como sigue:

Modo	CBC
Clave	e6 60 0f d8 85 2e f5 ab
IV	81 0e 52 8e 1c 5f da 1a
Texto en claro	00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 91
Texto cifrado	0d da 5a cb d0 5e 55 67 51 47 46 86 8a 71 e5 77

La criptación DES-CFB64 se efectúa como sigue:

Modo	CFB64
Clave	e6 60 0f d8 85 2e f5 ab
IV	51 47 46 86 8a 71 e5 77
Texto en claro	d2 d1 9f 00 00 00 00 00
Texto cifrado	ef ac 88 e8 ee 80 33 14

La clave es la misma que se utiliza para la operación criptación DES-CBC. El IV son los 8 últimos octetos del texto cifrado generado por la operación DES-CBC.

Se señala que se han agregado 5 octetos de valor 0 a los 3 octetos de texto en claro. Los valores de estos octetos de texto en claro agregados no afectan a los valores de los tres primeros octetos de texto cifrado, que son los únicos octetos de texto cifrado que interesan. Se pueden utilizar cualesquiera otros valores en vez de 0 para los octetos de texto en claro agregados.

La PDU paquete, después de la criptación, tiene el aspecto siguiente:

DA	01 02 03 04 05 06
SA	f1 f2 f3 f4 f5 f6
Tipo/Longitud	0d da
Datos de usuario	5a cb d0 5e 55 67 51 47 46 86 8a 71 e5
CRC	77 ef ac 88

I.7.3 Trama runt

Cuando el número de octetos que se han de criptar es inferior a 8, el modo de criptación es DES-CFB64. La clave de criptación y el IV se llevan en el paquete respuesta de clave.

Supóngase que la PDU paquete, antes de la criptación, es como sigue:

DA	01 02 03 04 05 06
SA	f1 f2 f3 f4 f5 f6
Tipo/longitud	00 01
Datos de usuario	02
CRC	88 ee 59 7e

La criptación DES-CFB64 se efectúa como sigue:

Modo	CFB64
Clave	e6 60 0f d8 85 2e f5 ab
IV	81 0e 52 8e 1c 5f da 1a
Texto claro	00 01 02 88 ee 59 7e 00
Texto cifrado	17 86 a8 03 a0 85 75 01

Se señala que se ha agregado 1 octeto de valor 0 a los 7 octetos de texto en claro. El valor de este octeto de texto en claro agregado no afecta a los valores de los 7 primeros octetos de texto cifrado, que son los únicos octetos de texto cifrado que interesan. Se puede utilizar cualquier otro valor en vez de 0 para el octeto de texto en claro agregado.

La PDU paquete, después de la criptación, tiene el aspecto siguiente:

DA	01 02 03 04 05 06
SA	f1 f2 f3 f4 f5 f6
Tipo/longitud	17 86
Datos de usuario	a8
CRC	03 a0 85 75

I.7.4 Clave de 40 bits

El protocolo BPKM genera y distribuye siempre claves DES de 56 bits. Cuando se requiere criptación de 40 bits, la clave DES de 56 bits se convierte, dentro de una implementación, en una clave de 40 bits enmascarando (a cero) 16 de los 56 bits de una TEK.

La TEK tiene 8 octetos, cada uno de los cuales contiene 7 bits de clave y 1 bit de paridad. El procedimiento de conversión de una TEK en una clave de 40 bits es como sigue:

- los dos primeros octetos de la TEK se fijan a 0;
- los dos bits más significativos del tercer octeto de la TEK se fijan a 0;
- los cinco octetos restantes de la TEK permanecen inalterados.

Por ejemplo, si la TEK distribuida por el protocolo BPKM es:

`ff ff ff ff ff ff ff ff,`

la conversión a 40 bits genera la TEK

`00 00 3f ff ff ff ff ff.`

Excepto por lo que se refiere a esta conversión del valor de la TEK, el procedimiento de criptación de 40 bits de una PDU paquete es idéntico al caso de criptación de 40 bits.

Para ilustrar la criptación de 40 bits, se repite aquí un ejemplo previo de PDU paquete, con la TEK convertida a 40 bits.

Supóngase que la PDU paquete, antes de la criptación, es como sigue:

DA	01 02 03 04 05 06
SA	f1 f2 f3 f4 f5 f6
Tipo/longitud	00 01
Datos de usuario	02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e
CRC	91 d2 d1 9f

El número total de octetos que se han de criptar es 19. Los 16 primeros octetos se procesan utilizando criptación DES-CBC, y los tres últimos octetos utilizando criptación DES-CFB64.

La criptación DES-CBD se efectúa como sigue:

Modo	CBC
Clave	00 00 0f d8 85 2e f5 ab
IV	81 0e 52 8e 1c 5f da 1a
Texto en claro	00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 91
Texto cifrado	44 c8 4a 41 14 67 56 a2 dc 64 8f b0 dc 1e 1e 86

La clave es la TEK llevada en el mensaje respuesta de clave, convertida en una clave de 40 bits. El IV es tal como se lleva en el mensaje respuesta de clave.

La criptación DES-CFB64 se efectúa como sigue:

Modo	CFB64
Clave	00 00 0f d8 85 2e f5 ab
IV	dc 64 8f b0 dc 1e 1e 86
Texto en claro	d2 d1 9f 00 00 00 00 00
Texto cifrado	f1 42 aa a3 e4 9b eb 29

La clave es la misma que se utiliza para la operación criptación DES-CBC. El IV son los últimos 8 octetos del texto cifrado generado por la operación DES-CBC.

La PDU paquete, después de la criptación, tiene el aspecto siguiente:

DA	01 02 03 04 05 06
SA	f1 f2 f3 f4 f5 f6
Tipo/Longitud	44 c8
Datos de usuario	4a 41 14 67 56 a2 dc 64 8f b0 dc 1e 1e
CRC	86 f1 42 aa

I.8 Criptación de PDU paquete con supresión de encabezamiento de cabida útil

Estos ejemplos muestran cómo se efectúa la criptación de una PDU paquete cuando se aplica supresión de encabezamiento de cabida útil (PHS). El ejemplo utiliza la cabida útil del protocolo de transmisión de la voz por Internet con RTP. En los ejemplos que aquí se presentan no se hace ningún esfuerzo por utilizar valores correctos para los campos de la PDU paquete. Como resultado

de ello, los ejemplos no son paquetes válidos, adecuados para la transmisión. El objetivo de los ejemplos es ilustrar los detalles de la criptación solamente.

I.8.1 Sentido descendente

Supóngase que la PDU paquete, después de la PHS y antes de la criptación, es como sigue:

DA	01 02 03 04 05 06
SA	f1 f2 f3 f4 f5 f6
Encabezamiento de RTP	21 22 23 24 25 26 27 28 29 2a 2b 2c
Datos de voz	31 32 33 34 35 36 37 38 39 3a
CRC	93 86 b3 b9

La PHS ha suprimido los campos tipo/longitud que, de otro modo, estarían incluidos en el encabezamiento Ethernet/802.3. Los datos de usuario consisten en el encabezamiento de RTP y los datos de voz. La criptación se aplica empezando con el primer octeto del encabezamiento de RTP y terminando con el último octeto de la CRC, como sigue:

Modo	CBC
Clave	e6 60 0f d8 85 2e f5 ab
IV	81 0e 52 8e 1c 5f da 1a
Texto en claro	21 22 23 24 25 26 27 28 29 2a 2b 2c 31 32 33 34 35 36 37 38 39 3a 93 86
Texto cifrado	b4 55 da c8 39 1e 0c ed 15 cf b5 79 0a c3 24 5e cf 0f 52 c0 69 f5 f6 6e

Modo	CFB64
Clave	e6 60 0f d8 85 2e f5 ab
IV	cf 0f 52 c0 69 f5 f6 6e
Texto en claro	b3 b9 00 00 00 00 00 00
Texto cifrado	3e 31 de ea 96 6a 88 6b

La PDU paquete, después de la criptación, tiene el aspecto siguiente:

DA	01 02 03 04 05 06
SA	f1 f2 f3 f4 f5 f6
Encabezamiento de RTP	b4 55 da c8 39 1e 0c ed 15 cf b5 79
Datos de voz	0a c3 24 5e cf 0f 52 c0 69 f5
CRC	f6 6e 3e 31

I.8.2 Sentido ascendente

Supóngase que la PDU paquete, después de la PHS y antes de la criptación, es como sigue:

Encabezamiento de RTP	21 22 23 24 25 26 27 28 29 2a 2b 2c
Datos de voz	31 32 33 34 35 36 37 38 39 3a
CRC	65 cf fe 89

La PHS ha suprimido la DA, la SA y los campos tipo/longitud que, de otro modo, estarían incluidos en el encabezamiento Ethernet/802.3. Los datos de usuario consisten en el encabezamiento de RTP y los datos de voz. Los primeros 12 octetos de los datos de usuario no son criptados. La criptación se aplica empezando con el primer octeto de los datos de voz y terminando con el último octeto de la CRC, como sigue:

Modo	CBC
Clave	e6 60 0f d8 85 2e f5 ab
IV	81 0e 52 8e 1c 5f da 1a
Texto en claro	31 32 33 34 35 36 37 38
Texto cifrado	d6 88 87 66 1f 66 04 79

Modo	CFB64
Clave	e6 60 0f d8 85 2e f5 ab
IV	d6 88 87 66 1f 66 04 79
Texto en claro	39 3a 65 cf fe 89 00 00
Texto cifrado	c0 07 20 8e 3b 0b b1 b9

La PDU paquete, después de la criptación, tiene el aspecto siguiente:

Encabezamiento de RTP	21 22 23 24 25 26 27 28 29 2a 2b 2c
Datos de voz	d6 88 87 66 1f 66 04 79 c0 07
CRC	20 8e 3b 0b

I.9 Criptación de paquete fragmentado

Cuando se fragmenta un paquete, cada fragmento se cripta independientemente utilizando DES-CBC con procesamiento del bloque residual. La TEK y el IV de cada fragmento son los mismos TEK e IV utilizados para criptar una PDU paquete no fragmentado. Se criptan todos los octetos de un fragmento, incluidos los 12 octetos que llevan las direcciones de destino y origen (DA/SA) Ethernet/802.3 de la PDU paquete.

En el ejemplo que aquí se presenta, no se hace ningún esfuerzo por utilizar valores significativos de los campos del paquete. Como resultado de ello, el ejemplo no es un paquete válido, adecuado para la transmisión. El objetivo del ejemplo es ilustrar los detalles de la criptación solamente.

En este ejemplo, la TEK y el IV se toman del ejemplo de paquete respuesta de clave descrito anteriormente.

Supóngase que el paquete se divide en dos fragmentos, como sigue:

Cabida útil del fragmento 1	01 02 03 04 05 06 f1 f2 f3 f4 f5 f6 00 01 02 03 04 05
CRC del fragmento 1	b4 2b 6d d4

Cabida útil del fragmento 2	06 07 08 09 0a 0b 0c 0d
CRC del fragmento 2	48 34 45 36

El primer fragmento se cripta utilizando DES-CBC y DES-CFB64, como sigue:

Modo	CBC
Clave	e6 60 0f d8 85 2e f5 ab
IV	81 0e 52 8e 1c 5f da 1a
Texto en claro	01 02 03 04 05 06 f1 f2 f3 f4 f5 f6 00 01 02 03
Texto cifrado	47 41 0f 4f fd 78 47 6e c8 1a 67 4e 26 0c 20 c5

Modo	CFB64
Clave	e6 60 0f d8 85 2e f5 ab
IV	c8 1a 67 4e 26 0c 20 c5
Texto en claro	04 05 b4 2b 6d d4 00 00
Texto cifrado	56 6d 5c 58 2f 56 dc 39

El primer fragmento, después de la criptación, tiene el aspecto siguiente:

Cabida útil del fragmento 1	47 41 0f 4f fd 78 47 6e c8 1a 67 4e 26 0c 20 c5 56 6d
CRC del fragmento 1	5c 58 2f 56

El segundo fragmento se cripta utilizando DES-CBC y DES-CFB64, como sigue:

Modo	CBC
Clave	e6 60 0f d8 85 2e f5 ab
IV	81 0e 52 8e 1c 5f da 1a
Texto en claro	06 07 08 09 0a 0b 0c 0d
Texto cifrado	d8 55 0f 59 9d 19 d9 c6

Modo	CFB64
Clave	e6 60 0f d8 85 2e f5 ab
IV	d8 55 0f 59 9d 19 d9 c6
Texto en claro	48 34 45 36 00 00 00 00
Texto cifrado	b4 5f 3e 95 0e e4 d7 df

El segundo fragmento, después de la criptación, tiene el aspecto siguiente:

Cabida útil del fragmento 2	d8 55 0f 59 9d 19 d9 c6
CRC de fragmento 2	b4 5f 3e 95

BIBLIOGRAFÍA

[IEEE1] IEEE Standard 802-1990, *IEEE Standards for Local and Metropolitan Area Networks: Overview and Architecture*, diciembre de 1990.

[RFC1750] EASTLAKE (D.), CROCKER (S.), SCHILLER (J.), *Randomness Recommendations for Security*, *IETF RFC 1750*, diciembre de 1994.

[RFC2202] CHENG (P.), GLENN (R.), *Test Cases for HMAC-MD5 and HMAC-SHA-1*, *IETF RFC 2202*, septiembre de 1997.

[SCHNEIER] SCHNEIER (B.), *Applied Cryptography*, Second Edition, John Wiley, New York, 1996.

[SET Book 2] *SET, Secure Electronic Transaction Specification* – Book 2: Programmer's Guide, Version 1.0, 31 mayo de 1997.

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios generales de tarificación
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedios
Serie I	Red digital de servicios integrados
Serie J	**Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedios**
Serie K	Protección contra las interferencias
Serie L	Construcción, instalación y protección de los cables y otros elementos de planta exterior
Serie M	RGT y mantenimiento de redes: sistemas de transmisión, circuitos telefónicos, telegrafía, facsímil y circuitos arrendados internacionales
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de transmisión telefónica, instalaciones telefónicas y redes locales
Serie Q	Conmutación y señalización
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	Redes de datos y comunicación entre sistemas abiertos
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet y Redes de la próxima generación
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2005