UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T H.234

(11/2002)

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

SERIE H: SISTEMAS AUDIOVISUALES Y MULTIMEDIOS

Infraestructura de los servicios audiovisuales – Aspectos de los sistemas

Sistema de autenticación y de gestión de las claves de criptación para los servicios audiovisuales

Recomendación UIT-T H.234

RECOMENDACIONES UIT-T DE LA SERIE H

SISTEMAS AUDIOVISUALES Y MULTIMEDIOS

CARACTERÍSTICAS DE LOS SISTEMAS VIDEOTELEFÓNICOS	H.100–H.199
INFRAESTRUCTURA DE LOS SERVICIOS AUDIOVISUALES	
Generalidades	H.200–H.219
Multiplexación y sincronización en transmisión	H.220–H.229
Aspectos de los sistemas	**H.230–H.239**
Procedimientos de comunicación	H.240–H.259
Codificación de imágenes vídeo en movimiento	H.260–H.279
Aspectos relacionados con los sistemas	H.280–H.299
SISTEMAS Y EQUIPOS TERMINALES PARA LOS SERVICIOS AUDIOVISUALES	H.300–H.399
SERVICIOS SUPLEMENTARIOS PARA MULTIMEDIOS	H.450–H.499
PROCEDIMIENTOS DE MOVILIDAD Y DE COLABORACIÓN	
Visión de conjunto de la movilidad y de la colaboración, definiciones, protocolos y procedimientos	H.500–H.509
Movilidad para los sistemas y servicios multimedios de la serie H	H.510–H.519
Aplicaciones y servicios de colaboración en móviles multimedios	H.520–H.529
Seguridad para los sistemas y servicios móviles multimedios	H.530–H.539
Seguridad para las aplicaciones y los servicios de colaboración en móviles multimedios	H.540–H.549
Procedimientos de interfuncionamiento de la movilidad	H.550–H.559
Procedimientos de interfuncionamiento de colaboración en móviles multimedios	H.560–H.569

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T H.234

Sistema de autenticación y de gestión de las claves de criptación para los servicios audiovisuales

Resumen

Esta Recomendación describe tres métodos de gestión de claves de criptación:

– ISO 8732;

– Diffie-Hellman; y

– RSA.

Los métodos se aplican a la criptación de señales audiovisuales transmitidas digitalmente con la estructura de trama H.221. Los mensajes de gestión descritos se transmiten por el canal de señal de control H.221, cuya estructura y utilización se definen en la Rec. UIT-T H.233.

Esta revisión de la Recomendación mejora la redacción del texto, suprime las ambigüedades de algunos aspectos relativos al intercambio de claves de longitud asimétrica y suprime las referencias a la criptación MLP de las Recomendaciones de la serie T.120, ya que el tema queda en estudio. Además, se han actualizado las referencias a ASN.1 de acuerdo con la versión más reciente de su especificación.

Orígenes

La Recomendación UIT-T H.234, revisada por la Comisión de Estudio 16 (2001-2004) del UIT-T, fue aprobada por el procedimiento de la Resolución 1 de la AMNT el 29 de noviembre de 2002.

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.

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 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 H.234

Sistema de autenticación y de gestión de las claves de criptación para los servicios audiovisuales

1 Generalidades

Un sistema de privacidad consta de dos partes: el mecanismo de confidencialidad, o proceso de criptación de los datos, y un subsistema de gestión de claves. Esta Recomendación describe los métodos de autenticación y gestión de claves de un sistema de privacidad adecuado para utilizarlo en los servicios audiovisuales de banda estrecha conforme con las Recomendaciones UIT-T H.221, H.230 y H.242. La especificación de la confidencialidad es independiente y figura en la Rec. UIT-T H.233.

La privacidad se consigue utilizando *claves secretas*. Las claves se cargan en la parte confidencialidad del sistema de privacidad y controlan la manera según la cual se criptan y descriptan los datos transmitidos. Si un tercero consigue acceder a las claves que están siendo utilizadas, el sistema de privacidad deja de ser seguro.

El mantenimiento de claves por los usuarios constituye, pues, parte importante del sistema de privacidad. En esta Recomendación se especifican tres métodos prácticos alternativos de gestión de claves. En los casos en que no sea posible la gestión de claves automatizada puede utilizarse una alternativa no especificada, por ejemplo la gestión de claves manual.

El primer método se identifica como ISO 8732. Se basa en claves instaladas manualmente en sistemas que atribuyen físicamente a estas claves un alto grado de protección y a continuación en intercambios automatizados de claves criptadas según las claves distribuidas manualmente. Normalmente, el algoritmo utilizado para criptar las claves distribuidas automáticamente es el mismo que para criptar la propia comunicación. La seguridad de las claves distribuidas automáticamente depende, por tanto, de la seguridad de las claves distribuidas manualmente.

Las claves distribuidas automáticamente pueden utilizarse para una única sesión o para múltiples sesiones en un periodo de tiempo determinado (por ejemplo, un mes). El método ISO 8732 contiene no sólo protocolos para el intercambio automatizado de información entre los dos terminales, sino también protocolos físicos con los que se garantiza asimismo la seguridad de las claves de distribución manual.

Hay dos entornos diferentes: el entorno directo punto a punto (dos capas), en el que los dos terminales comparten una clave común, y el entorno de tres capas, en el que los dos terminales que desean comunicar no comparten una clave común, pero utilizan las facilidades de un tercer participante con el que cada uno de ellos comparte una llave común. Las interfaces con ese tercer participante quedan fuera del alcance de esta Recomendación, pero es preciso distinguir entre ambos entornos.

Se señala que el intercambio de claves de sesión especificado en 3.3.2 está duplicado funcionalmente en X9.17, en el sentido de que las claves distribuidas automáticamente en X9.17 son lo bastante fuertes como para ser utilizadas como claves de sesión. No obstante, para seguir el modelo de esta Recomendación, se utilizará como *clave*, la *clave* de claves de 3.3.2.

El segundo método es un método sencillo, aunque seguro, conocido como método "Diffie-Hellman ampliado", que genera e intercambia claves automáticamente por conducto del propio sistema (este intercambio de claves está él mismo criptado). No requiere acción alguna de los usuarios hasta que se hayan intercambiado las claves; a los usuarios se les dice a continuación que confirmen *verbalmente* que en cada terminal está disponible la misma secuencia de comprobación. El método es muy adecuado para evitar, por ejemplo, que personas no autorizadas a participar en una comunicación audiovisual efectuada por canal de satélite la escuchen. Para burlar el sistema el

intruso tiene que interceptar toda la comunicación bidireccional antes de activar la criptación e intercambiar claves con ambos participantes, simulando ser, ante cada uno de ellos, el otro participante legítimo. El método no proporciona autenticación.

El tercer método es más complejo y proporciona un mayor grado de privacidad y también la *autenticación* de entidades de servicios audiovisuales [terminales, unidades de control multipunto (MCU, *multipoint control units*) etc.]. El "método RSA" es muy similar al de claves públicas especificado en la Rec. UIT-T X.509 y utiliza el algoritmo RSA. Este método requiere el establecimiento de un entidad de seguridad disponible para todo el colectivo de entidades que necesitan interconectabilidad: la certificación es externa o "fuera de línea" y se basa en la integridad de la entidad. Este mecanismo de autenticación hace posible que los participantes en una comunicación conferencia sean identificados ante otros de manera segura y puede utilizarse tanto en llamadas multipunto como en llamadas punto a punto.

Todos los métodos precisan la utilización de un canal asociado, despejado y libre de errores. Se señala que ninguno de estos métodos proporciona control de acceso, integridad y no rechazo.

En esta Recomendación se hace referencia a un cuarto método, el de "intercambio de claves manual".

El intercambio de claves manual se define como la introducción por los usuarios de claves de criptación de claves directamente en los terminales, sin intercambio de mensajes H.234. La misma clave se introduce en ambas ubicaciones. La longitud de las claves depende del algoritmo de criptación. El orden de los bits de las claves es: bit más significativo (MSB, *most significant bit*) primero y bit menos significativo (LSB, *least significant bit*) último. El mecanismo real de introducción de las claves en el terminal depende del terminal y queda fuera del alcance de esta Recomendación.

A continuación se dan algunos ejemplos:

- usar un teclado telefónico para introducir: (MSB) 00111010...01110100 (LSB);
- descargar lo mismo desde un computador;
- usar un teclado para introducir lo mismo como caracteres hexadecimales: (MSB) 3A...74 (LSB).

La introducción manual puede efectuarse antes de iniciar la llamada o durante la misma. En este segundo caso, los participantes pueden optar por invocar la criptación mientras están en una conferencia, introducir una clave utilizando la interfaz proporcionada por el terminal e iniciar seguidamente la criptación a través de la interfaz de usuario del terminal. Cuando se solicita la criptación a través de la interfaz de usuario, se envía el código de señal de asignación de velocidad binaria (BAS, *bit rate allocation signal*), "Encrypt-on" (criptación activada), se abre el canal de señal de control de criptación (ECS, *encryption control signal*), se seleccionan los algoritmos de criptación, se acuerda el modo manual de gestión de claves y se intercambian las claves de sesión.

Para que un sistema de criptación se considere privado, todos los conferenciantes deben estar al corriente de quién o qué tiene acceso a datos no criptados, ya sean otros conferenciantes o equipos, como MCU o facilidades de conversión. Para ello, se necesita un periodo de establecimiento inicial, antes de que comience la conferencia, de modo que las entidades puedan autenticarse entre sí. De este modo, todas las entidades que tienen acceso a datos no criptados son identificadas de manera segura por todas las demás entidades antes del comienzo de la conferencia. El marco de autenticación proporciona también información a cualquier proveedor de red, por ejemplo la relativa a la facturación de una llamada de MCU.

Si se dispone de datos no criptados en la MCU (denominada "MCU confiable") el equipo deberá formar parte de cualquier marco de autenticación. Además, los usuarios tienen que saber que en la red hay una MCU confiable.

En la cláusula 3 se examinan aspectos comunes a todos los métodos, mientras que las cláusulas 4, 5 y 6 se ocupan, respectivamente, de los métodos ISO 8732, Diffie-Hellman y RSA.

Abreviaturas y definiciones

AVSE Entitidad de servicio audiovisual (terminales, MCU, etc.) (*audiovisual service entity*)

clave clave de criptación de claves (*key-encrypting key*)

2 Referencias 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.

– Recomendación UIT-T H.221 (1999), *Estructura de trama para un canal de 64 a 1920 kbit/s en teleservicios audiovisuales*.

– Recomendación UIT-T H.230 (1999), *Señales de control e indicación con sincronismo de trama para sistemas audiovisuales*.

– Recomendación UIT-T H.233 (2002), *Sistemas con confidencialidad para servicios audiovisuales*.

– Recomendación UIT-T H.242 (1999), *Sistemas para el establecimiento de comunicaciones entre terminales audiovisuales con utilización de canales digitales de hasta 2 Mbit/s*.

– Recomendación UIT-T X.509 (2000), *Tecnología de la información – Interconexión de sistemas abiertos – El directorio*: *Marcos para certificados de claves públicas y de atributos*.

– Recomendación UIT-T X.690 (2002), *Tecnología de la información – Reglas de codificación de notación de sintaxis abstracta uno*: *Especificación de las reglas de codificación básica, de las reglas de codificación canónica y de las reglas de codificación distinguida*.

– ISO 8732:1988, *Banking – Key Management* (*wholesale*).

– IETF RFC 2412 (1998), *The Oakley Key Determination Protocol*.

3 Sistema de mensajes e intercambio de claves

3.1 Canal de mensajes

El sistema que se describe a continuación se compone de varios mensajes definidos, que se transmiten en secuencia entre los dos extremos del enlace. El canal sin errores requerido a tal efecto se describe en la Rec. UIT-T H.233, donde se hace referencia a los bloques de intercambio de sesión (SE, *session exchange*).

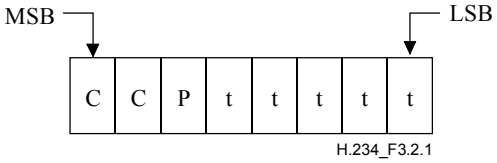
3.2 Formatos de mensaje

Los mensajes utilizados por el sistema de criptación para la distribución y autenticación de claves se formatean en la forma identificador, longitud, contenido (ILC, *identifier, length, content*) nidificada que se describe en la Rec. UIT-T X.690. La longitud puede codificarse en forma corta o forma larga. No se utilizará la forma indefinida indicada en la Rec. UIT-T X.690.

A continuación se da una breve descripción de algunas de las definiciones de la Rec. UIT-T X.690 utilizadas en esta Recomendación.

3.2.1 Identificador

Un identificador es un octeto con la siguiente estructura:



Los dos bits CC, "clase de rótulo", definen el tipo de identificador, que es 10 (específico del contexto) para los identificadores definidos en esta Recomendación.

El bit primitiva/constructor (P) indica si el contenido es una primitiva o si se compone de elementos anidados.

El rótulo de 5-bits (ttttt) define de manera exclusiva al identificador (de acuerdo con su clase).

Así pues, todos los identificadores de esta Recomendación tienen la forma de octeto 1 0 P t_1 t_2 t_3 t_4 t_5.

3.2.2 Longitud

La longitud especifica el largo del contenido en octetos y es en sí misma de longitud variable.

La forma corta tiene un octeto de longitud y se la preferirá a la forma larga cuando L es menor que 128. El bit 8 tiene el valor cero y los bits 7 a 1 codifican L como un número binario sin signo, cuyos MSB y LSB son el bit 7 y el bit 1, respectivamente.

La forma larga tiene una longitud de 2 a 127 octetos si se utiliza cuando L es superior o igual a 128 y menor que 2 a la potencia 1008. El bit 8 del primer octeto tiene el valor uno. Los bits 7 a 1 del primer octeto codifican un número inferior en una unidad al tamaño de la longitud en octetos, como número binario sin signo, cuyos MSB y LSB son el bit 7 y el bit 1, respectivamente. El propio L se codifica como un número binario sin signo, cuyos MSB y LSB son el bit 8 del segundo octeto y el bit 1 del último octeto, respectivamente. Este número binario se codificará con el menor número posible de octetos, sin octetos delanteros que contengan el valor 0.

3.2.3 Cadena de bits

Una cadena de bits primitiva tiene los bits empaquetados en ocho por octeto y va precedida por un octeto que codifica el número de bits no utilizados en el octeto final del contenido de cero a siete como número binario sin signo. Estos MSB y LSB son el bit 8 y el bit 1, respectivamente.

3.3 Arranque del sistema de privacidad

El sistema necesita tres mensajes para arrancar, P0, P1 y P2, que se detallan más adelante. El sistema de privacidad se invoca enviando un mensaje (desde cualquier extremo) de tipo (P0). El mensaje (P0) incluye bits que describen los mecanismos, ISO 8732 y/o Diffie-Hellman y/o RSA, que el emisor puede manejar. El receptor de ese mensaje determina el mecanismo que se debe utilizar y responde con un mensaje de tipo (P0) o de tipo (P1), según el resultado.

Si los dos envían el mensaje (P0) al mismo tiempo, todavía es posible efectuar la elección comparando los campos de bits intercambiados:

– si ambos extremos soportan el mismo mecanismo, ése es el que se utiliza; si soportan más de un mecanismo, el orden de preferencia es ISO 8732, seguido de Diffie-Hellman, seguido de RSA/X.509 y, por último, la opción no especificada a la que se hace referencia en esta Recomendación como opción "manual";

– si no hay ninguna capacidad común, el enlace no se puede criptar.

3.3.1 Mensajes de arranque

Nombre de mensaje:	Petición de sistema de privacidad (P0).
Identificador de mensaje:	1 0 P t_1 t_2 t_3 t_4 t_5 = 1000 0000
Significado:	El emisor del mensaje desea utilizar un sistema de criptación. Este mensaje se puede utilizar para iniciar la criptación o en respuesta a otro mensaje P0.
Contenido:	Un octeto primitivo como se muestra a continuación. El campo de bits dentro del contenido muestra el tipo de mecanismo que se puede utilizar. (MSB) 0000XDRM (LSB). X se pone a '1' si se soporta ISO 8732, o a '0' si no se soporta. D se pone a '1' si se soporta Diffie-Hellman, o a '0' si no se soporta. R se pone a '1' si se soporta RSA, o a '0' si no se soporta. M se pone a '1' si hay un sistema de gestión de claves no especificado, como el de introducción de claves manual, o a '0' si no lo hay.
En la "notación de sintaxis abstracta" ASN.1 de la Rec. UIT-T X.690:	RequestEncryptionSystem ::= [0] IMPLICIT OCTET STRING
	En este mensaje, el contenido tiene siempre una longitud de un octeto.

Nombre de mensaje:	No se puede criptar (P1).
Significado:	Enviado en respuesta al (P0). El emisor de este mensaje no utilizará un sistema de criptación.
Identificador de mensaje	1 0 P t_1 t_2 t_3 t_4 t_5 = 1000 0001
Contenido:	Este mensaje no tiene contenido.

Nombre de mensaje:	No arranca el sistema de criptación (P2).
Significado:	El emisor de este mensaje no ha arrancado su sistema de criptación. Esto puede deberse a un fallo del intercambio de claves pero, por razones de seguridad, no se da ninguna indicación de la causa del fallo en el mensaje.
Identificador de mensaje:	1 0 P t_1 t_2 t_3 t_4 t_5 = 1000 0010
Contenido:	Este mensaje no tiene contenido.

3.3.2 Intercambio de claves de sesión

Las claves de sesión utilizadas para criptar la información se obtienen del intercambio de claves de sesión. El mensaje que contienen las claves de sesión está formateado como aquí se describe, y criptado utilizando una clave de criptación de claves (abreviada *clave* en esta Recomendación) derivada del protocolo de autenticación o de distribución de *clave*. Conviene insistir en la diferencia entre estos dos tipos de clave. Las claves de sesión se utilizan en la criptación/descriptación de la señal audiovisual en su trama H.221, mientras que *clave* sólo se utiliza en la criptación y descriptación del intercambio de claves de sesión.

El mecanismo de criptación consiste en claves de N bits de longitud. Las dos partes establecen una *clave* común, cuya longitud es también de N bits; en el caso del RSA, hay una #clave# de autenticación adicional, utilizada para obtener la *clave*.

La *clave* común se utiliza para criptar cuatro claves de N bits descritas en esta subcláusula (veáse la figura 1). El método de criptación es el mismo que el elegido para la criptación de la señal audiovisual, lo que se indica mediante la transmisión del mensaje P9, definido a tal efecto en la Rec. UIT-T H.233.

El mensaje de intercambio de claves de sesión entre dos terminales Ta y Tb consta de un identificador de mensaje de 8 bits, un vector de inicialización con corrección de errores y un valor aleatorio de 2(Na + Nb) bits. Cada extremo envía ese valor y deduce de él el conjunto de cuatro claves de sesión. La longitud de cada una de las claves es de Na y Nb bits, según el valor de Na y Nb del algoritmo de criptación que se usa (por ejemplo, en el caso de B-crypt, utilizado de Ta a Tb, Na = 56).

Los números aleatorios transmitidos y recibidos se procesan según se indica en la figura 1:

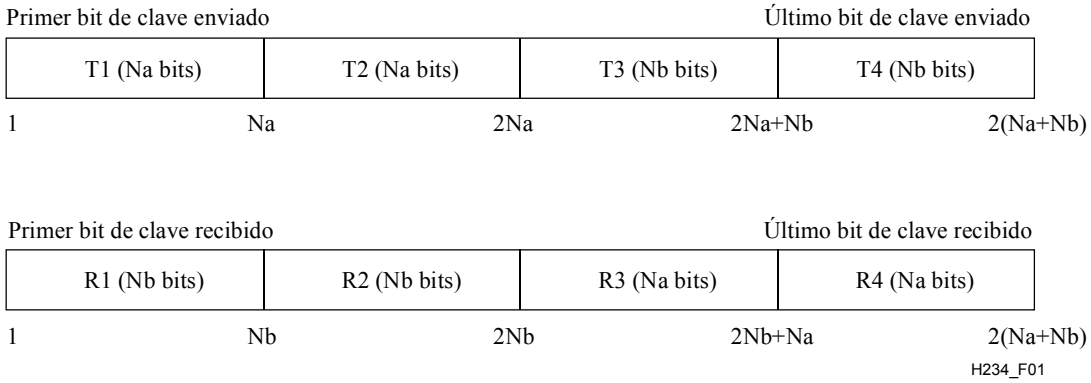


Figura 1/H.234 – Ordenación de los bits en el intercambio de claves de sesión

Cada una de las cuatro claves se forma mediante la operación O exclusiva aplicada bit por bit a un bloque transmitido y a un bloque recibido, manteniendo la ordenación de los bits, esto es, el bit más significativo de la clave, es decir, el bit más significativo del primer byte o palabra de datos de clave cargada en el dispositivo de criptación está formado por los dos primeros bits de los dos bloques. Con la ordenación de bits de la figura 1 se obtienen las cuatro claves así:

"Enviar clave de criptación #1" formada por el bloque T1, la O exclusiva y el boque R3

"Enviar clave de criptación #2" formada por el bloque T2, la O exclusiva y el boque R4

"Recibir clave de criptación #1" formada por el bloque T3, la O exclusiva y el boque R1

"Recibir clave de criptación #2" formada por el bloque T4, la O exclusiva y el boque R2

La clave de criptación #1 se utiliza para la criptación del contenido de la señal tramada "Encryp-on" (criptación activada) especificada en A.3/H.221.

Es posible que el algoritmo elegido requiera paridad en las claves. Esto es un asunto local y no forma parte de la transmisión.

La única comprobación se efectúa en el conjunto 2(Na + Nb) bits. Si el resultado de la operación "O exclusiva" en la totalidad de 2(Na + Nb) bits es cero [es decir, todas las claves de 2(Na + Nb) bits son cero], no se cargan las claves y no se invoca el sistema de privacidad.

Mensaje de intercambio de claves de sesión (P6)

El mensaje consta de un identificador de mensaje, un vector de inicialización, que incluye por defecto bits de corrección de errores, y un número aleatorio de 2(Na + Nb) bits.

Nombre de mensaje:	Aquí se da la información de clave de sesión (P6).
Identificador de mensaje:	1 0 P t_1 t_2 t_3 t_4 t_5 = 1010 0110
Significado:	El emisor de este mensaje está intercambiando información de clave de sesión.
Contenido:	Constructor que contiene el vector de inicialización (no criptado) utilizado para la criptación de los datos de clave de sesión y la información de clave de sesión criptada con el formato mostrado en la figura 1.
En la "notación de sintaxis abstracta" de la Rec. UIT-T X.690:	SessionKeyInformation ::= [6] IMPLICIT SEQUENCE { initialization-vector [0] IMPLICIT BIT STRING, session-key-information [1] IMPLICIT BIT STRING }

4 Gestión de claves ISO 8732

4.1 Introducción

La norma ISO 8732 proporciona un proceso uniforme de protección e intercambio de claves criptográficas para la autenticación y la criptación. Define la gestión manual y automatizada del material de generación de claves:

- El control durante la vida útil del material de generación de claves para evitar la revelación no autorizada de las mismas, su modificación o su sustitución.
- La distribución del material de generación de claves para permitir el interfuncionamiento entre equipos o facilidades de criptografía.
- La seguridad de la integridad del material de generación de claves durante todas las fases de su vida útil: generación, distribución, almacenamiento, introducción, utilización y destrucción.
- La recuperación en caso de fallo del proceso de gestión de claves o cuando se cuestione la integridad del material de generación de claves.

El algoritmo que se usa en la criptación de las claves distribuidas automáticamente suele ser el mismo que el utilizado para criptar la propia comunicación, y se puede negociar mediante intercambios de mensajes P8. Cuando se utiliza un algoritmo distinto del DES, el sistema de gestión de claves no es estrictamente conforme con ISO 8732, pero la única diferencia es este aspecto.

4.2 Arquitectura de la gestión de claves

En ISO 8732, se da una lista de requisitos del par de comunicantes. Hay una arquitectura de dos capas y una arquitectura de tres capas. Cualquiera de ellas se puede utilizar en el intercambio de claves.

4.3 Entornos de la gestión de claves

Existen tres entornos de distribución de claves:

– punto a punto;

– centro de distribución de claves (CKD, *key distribution centre*); y

– centro de traducción de claves (CKT, *key translation centre*).

En ISO 8732 pueden encontrarse los detalles relativos a estos entornos.

Punto a punto es un entorno de dos capas, en el que dos terminales comparten una clave común. Se supone que esta clave común ha sido distribuida manualmente con protocolos seguros y protección física, según se indica en ISO 8732. El intercambio automático de claves especificado en ISO 8732 garantiza que un terminal genera una *clave* común, que se pasa al otro terminal de manera segura y que es la clave utilizada en la creación de las claves de sesión especificadas en 3.3.2.

La diferencia entre centro de distribución de claves (CKD) y centro de traducción de claves (CKT) no es pertinente a los efectos de esta Recomendación, pero se especifica que la clave compartida por cada terminal con la tercera parte o centro (CKD o CKT) es una clave de longitud doble. La manera según la cual uno de los terminales, por ejemplo el terminal A, interconecta con el centro queda también fuera de la especificación de esta Recomendación, pero al concluir el intercambio con el centro, el terminal A posee no sólo una *clave* clara sino, también, una *clave* criptada con la clave de longitud doble (véase la especificación del algoritmo en ISO 8732) del terminal B. La envía a través del bloque SE a través del ECS al terminal B, donde seguidamente se la convierte en una *clave* clara, y el protocolo de intercambio de sesión puede comenzar.

4.4 Intercambios de mensajes de servicio criptográfico

ISO 8732 emplea texto para intercambiar mensajes. El orden y las circunstancias en que se envía los mensajes se dan en ISO 8732. El siguiente mensaje (P11) proporciona el mecanismo de envío de un mensaje de servicio criptográfico (CSM, *cryptographic service message*) de ISO 8732. Cada byte representa un carácter de texto.

La ordenación de bits es tal que se transmite primero el bit más significativo.

Nombre de mensaje:	Mensaje de servicio criptográfico (P11).
Identificador de mensaje:	1 0 P t_1 t_2 t_3 t_4 t_5 = 1010 1011
Significado:	El emisor de este mensaje envía un solo mensaje de servicio criptográfico.
Contenido:	Cadena de texto primitiva.
En la "notación de sintaxis abstracta" de la Rec. UIT-T X.690:	CryptographicServiceMessage := [11] IMPLICIT VisibleString

Se supone que la interfaz de usuario del terminal proporciona protocolos para identificar por su nombre las claves apropiadas y otros identificadores implícitos en el protocolo de ISO 8732. Por ejemplo, en una red privada, cada par de comunicantes en un entorno de dos capas puede tener una clave con nombre y compartida insertada en la unidad criptográfica del sistema, que el mecanismo para efectuar la llamada puede identificar automáticamente ante subsistema criptográfico.

En ISO 8732 se especifican mensajes de servicio para condiciones de error y respuestas erróneas. Si dos terminales, que soportan ISO 8732, tratan de comunicar de manera ad hoc, cuando, de hecho, no se corresponden mutuamente en ninguno de los tres entornos, los protocolos (que implican identificadores o nombres de claves, contadores, centros, etc., conocidos comúnmente) dejarán de funcionar y el intento de sesión criptográfica terminará con una notificación a los operadores de los terminales. Para completar una llamada que requiera criptación, los usuarios de los dos terminales deberán usar otro mecanismo de intercambio de gestión de claves o establecerse ellos mismos en uno de los tres entornos (utilizando muy probablemente una tercera parte o centro).

4.5 Ejemplo de intercambio de mensajes de ISO 8732

La figura 2 muestra un flujo de mensajes normal. El primer mensaje que se envía es petición de servicio (RSI, *request service*). En la subcláusula 8.4 de ISO 8732 se describe el formato de mensaje CSM [*cryptographic service message*] [mensaje de servicio criptográfico], cuya forma es:

CSM(MCL/...)

donde todos los caracteres son ASCII, los paréntesis indican el comienzo y fin del mensaje y la barra (/) se utiliza para separar los rótulos de los campos del contenido de los mismos.

En este caso, el contenido de los campos MCL es RSI, con lo que el texto efectivamente enviado es:

CSM(MCL/RSI...)

El orden de los campos del mensaje RSI se indica en el cuadro III de ISO 8732. Dicho orden es MCL RCV ORG SVR EDC (opcional). En este ejemplo se omite el EDC opcional.

En el cuadro II de ISO 8732 se define con más detalle cada uno de los campos. Así pues, el mensaje enviado es:

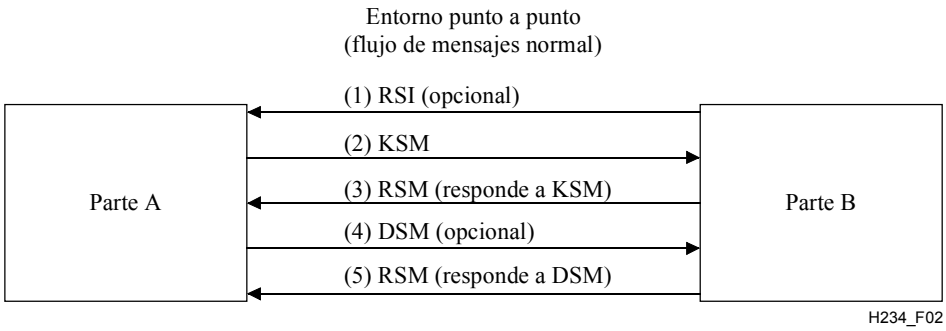
CMS (MCL/RSI"RCV/A"ORG/B"SVR/KK.KD.IV)

donde:

–	Espacio utilizado como separador de campos
A	El destinatario
B	El emisor
.	Separador de subcampos
SVR	Petición de servicio
KK	Petición de *clave*
KD	Petición de dos claves de sesión
IV	Petición de vector de inicialización (IV, *initialization vector*)
MCL	Clase de mensaje
RCV	Receptor
ORG	Originador

En la subcláusula 9.7 de ISO 8732 se describe con más detalle el mensaje RSI.

El segundo mensaje es mensaje de servicio de clave (KSM, *key service message*), el tercero es mensaje de servicio de respuesta (RSM, *response service message*), el cuarto es mensaje de servicio desconectado (DSM, *disconnected service message*) y el quinto es otra vez RSM.



NOTA – La parte A o la parte B puede iniciar el proceso de desconexión (DSM); se muestra el inicio por la parte A.

Figura 2/H.234 – Flujo de mensaje normal

5 Distribución de clave Diffie-Hellman ampliada

5.1 Introducción

El intercambio se basa en el método Diffie-Hellman, pero ampliado para aprovechar las propiedades del enlace audiovisual a fin de proporcionar un elemento de protección contra la intrusión en líneas activas. El resultado del intercambio es un valor secreto compartido, que se usa tanto para verificar la línea como para intercambiar claves de sesión.

El funcionamiento es como sigue (véase [1]):

1) el protocolo de distribución de *clave* intercambia datos de acuerdo con el protocolo aquí descrito;
2) los datos de (1) se utilizan para intercambiar claves de sesión, que se emplean a continuación para criptar el enlace;
3) los datos de (1) se utilizan para verificar el enlace.

5.2 El protocolo básico

El protocolo básico consiste en un intercambio inicial de datos, seguido de un intercambio bidireccional de los resultados intermedios, de los que se obtienen los datos compartidos.

5.2.1 Método de intercambio de *clave*

El método utilizado es una versión doble del método Diffie-Hellman básico. El intercambio doble se utiliza para que la *clave* resultante no se base enteramente en un primo y una raíz primitiva elegidos en un solo terminal.

Considérense dos AVSE: A y B.

A envía a B: el primo p_A,

la raíz primitiva probabilística a_A,

el valor $c_1 = \{a_A^{a1} \bmod p_A\}$, donde a_1 es un número aleatorio conocido solamente por A.

B envía a A: el primo p_B,

la raíz primitiva probabilística a_B,

el valor $c_2 = \{a_B^{b1} \bmod p_B\}$, donde b_1 es un número aleatorio conocido solamente por B.

A envía a B: el valor $c_3 = \{a_B^{a2} \text{mod } p_B\}$, donde a_2 es un número aleatorio conocido solamente por A.

B envía a A: el valor $c_4 = \{a_A^{b2} \text{mod } p_A\}$, donde b_2 es un número aleatorio conocido solamente por B.

Calcúlese un par de resultados r_1 y r_2 para A y luego para B.

AVSE A forma: $r_1 = c_4^{a1} \text{mod } p_A$ y $r_2 = c_2^{a2} \text{mod } p_B$

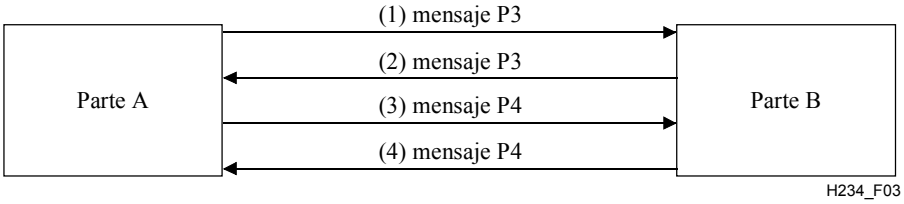
AVSE B forma: $r_1 = c_1^{b2} \text{mod } p_A$ y $r_2 = c_3^{b1} \text{mod } p_B$

Tanto A como B tienen ahora los mismos valores de resultados $r_1 = a_A^{a1.b2} \text{mod } p_A$ y $r_2 = a_B^{a2.b1} \text{mod } p_B$.

El resultado final R_{12} se obtiene mediante la aplicación de "O exclusiva" bit por bit a r_1 y r_2. Si r_1 y r_2 no tienen la misma longitud, y L denota la longitud del más corto, la operación O exclusiva es:

{(bits L menos significativos de r_1). O exclusiva. (bits L menos significativos de r_2)}

El intercambio Diffie-Hellman doble se ilustra en la figura 3.



(1) p_A, a_A, (a_A^{a1} mod p_A) por mensaje {P3}
(2) p_B, a_B, (a_B^{b1} mod p_B) por mensaje {P3}
(3) a_B^{a2} mod p_B por mensaje {P4}
(3) a_a^{b2} mod p_A por mensaje {P4}

Figura 3/H.234 – Intercambio Diffie-Hellman doble

Se recomienda usar cualquier valor primo 512 bits para el algoritmo DES, un valor primo 1024 bits para los algoritmos triple DES y AES (cuando se necesita seguridad alta), y un valor primo 1536 bits para los algoritmos triple DES y AES (cuando se necesita seguridad muy alta). En el caso de los valores primos 1024 y 1536 bits, se recomienda además utilizar los valores verificados indicados en el apéndice E de RFC 2412.

5.2.2 Obtención de la *clave*

Como se expone más arriba, A y B forman $r_1 = a_A^{a1.b2} \text{mod } p_A$) y $r_2 = (a_B^{a1.b2} \text{mod } p_B)$, y a continuación se forma R_{12} mediante "O exclusiva" bit por bit de estos valores. Tanto A como B comprueban el valor del resultado y, si todos los bits son 0, se envía el mensaje "Fallo en el sistema de criptación" (P2) a la otra entidad.

R_{12} es un valor de K bits disponible en cada extremo del enlace. Se emplea para obtener el código de comprobación y la *clave* utilizada para la criptación de las claves de sesión. En un mecanismo de confidencialidad de N bits, con un código de comprobación de M bits, los N bits menos significativos constituyen el código de comprobación y los siguientes N bits constituyen la *clave*. Esto se muestra en la figura 4. El valor de M es 64 bits. El valor de N es la longitud de la *clave* y lo determina el algoritmo de criptación aplicado.

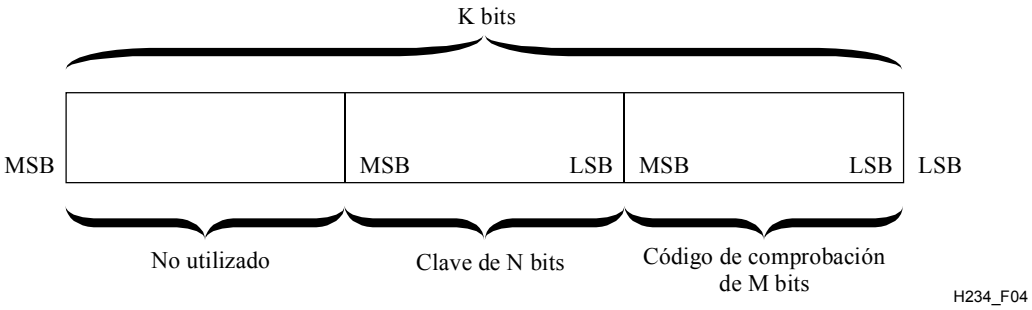


Figura 4/H.234 – Interpretación de los resultados de la distribución de claves

Obsérvese que K debe ser más largo que M + N bits. En el caso de un algoritmo de criptación de 64 bits y un código de comprobación de 64 bits, K debe rebasar 128 bits. En la práctica, K será bastante más largo que eso.

5.3 Mensajes Diffie-Hellman

En esta cláusula se describe el contenido de los mensajes necesarios para arrancar el sistema de criptación y para el intercambio de *clave* Diffie-Hellman.

5.3.1 Información de intercambio de *clave*

Nombre de mensaje:	Aquí se da la información de intercambio de *clave* (P3).
Identificador de mensaje:	1 0 P t_1 t_2 t_3 t_4 t_5 = 1010 0011
Significado:	El emisor de este mensaje envía la información de intercambio de *clave* contenida como parte de un intercambio Diffie-Hellman doble.
Contenido:	Un constructor constituido por las primitivas: raíz primitiva, primo y resultado intermedio, como se muestra más adelante. Se señala que el término raíz primitiva no tiene relación con el término primitiva utilizado en las definiciones de mensaje.
En notación ASN.1:	keyExchangeInformation ::= [3] IMPLICIT SEQUENCE { primitive root [0] IMPLICIT BIT STRING, prime [1] IMPLICIT BIT STRING, intermediate result [2] IMPLICIT BIT STRING } El contenido de Primitive Root (raíz primitiva) es una cadena de bits primitiva. El contenido de Prime (primo) es una cadena de bit primitiva. El contenido de Intermediate Result (resultado intermedio) es una cadena de bits primitiva que contiene uno de los resultados intermedios para el intercambio Diffie-Hellman.

5.3.2 Información intermedia de intercambio de *clave*

Nombre de mensaje:	Información intermedia de intercambio de *clave* (P4).
Identificador de mensaje:	1 0 P t_1 t_2 t_3 t_4 t_5 = 1000 0100
Significado:	El emisor de este mensaje envía la información de intercambio de la *clave* contenida como parte de un intercambio Diffie-Hellman doble.
Contenido:	Una cadena de bits primitiva que contiene el resultado intermedio.

En la notación de ASN.1:	IntermediateKeyExchangeInformation ::= [4] IMPLICIT BIT STRING
	La cadena de bits del resultado intermedio contiene uno de los resultados intermedios del intercambio Diffie-Hellman. Los mensajes P3 y P4 constituyen un intercambio Diffie-Hellman doble, de modo que la *clave* Diffie-Hellman final viene determinada por los dos extremos del enlace.

5.3.3 Información de código de comprobación enviada por MCU

Nombre de mensaje:	Aquí se da la información de código de comprobación enviada por MCU (P5).
Identificador de mensaje:	1 0 P t_1 t_2 t_3 t_4 t_5 = 1010 0101
Significado:	Una MCU envía la información de código de comprobación contenida resultante de los intercambios Diffie-Hellman.
Contenido:	Un constructor para identificador de enlace y código de comprobación.
En notación ASN.1:	Link check code information ::= [5] IMPLICIT SEQUENCE { link identifier [0] IMPLICIT BIT STRING, check code [1] IMPLICIT BIT STRING }

Una MCU enviará un mensaje (P5) por cada uno de los enlaces que haya completado el intercambio de *clave* Diffie-Hellman.

Obsérvese que el identificador de enlace se utiliza para identificar el enlace de la MCU con el que está relacionado el código de comprobación. Para interpretar este identificador es preciso conocer la configuración de la MCU. (Véase también la nota de 5.4.)

5.4 Extensión para comprobación de línea

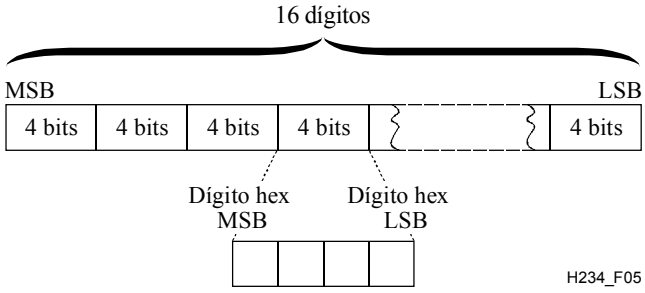
En 5.2 se obtuvo un código de comprobación de 64 bits. Dicho código será presentado por el terminal como la totalidad o parte de un número hexadecimal de 16 dígitos, cuya ordenación de bits se muestra en la figura 5 con la terminología de la figura 4.

El valor se presenta a cada usuario tal como se muestra, es decir, el dígito situado más a la izquierda se obtiene del extremo MSB del código de comprobación. No es necesario presentar todos los dígitos; es probable que baste con presentar los cuatro situados más a la izquierda, pues con esta presentación, la probabilidad de no detectar un problema en la línea es de 1 en 2^{16}. El valor presentado lo transfiere verbalmente un usuario al otro por el canal audiovisual criptado; el otro usuario debe comprobar que corresponde al valor visualizado en su terminal.

NOTA – Se sugiere que la comprobación verbal se haga antes de criptar el audio; además, conviene que la temporización de este proceso y la del proceso alternativo para la situación multipunto descrita en 5.3.3 sea la misma.

6 Funcionamiento basado en RSA

NOTA – Todas las referencias de esta cláusula a "clave" tienen el significado de #clave# mencionado en 3.3.2.



NOTA – Cada bloque de 4 bits del código de comprobación constituye un dígito hexadecimal que se presenta visualmente al usuario.

Figura 5/H.234 – Ordenación de los bits para comprobación de línea

6.1 Introducción

6.1.1 Consideraciones generales

En esta subcláusula se describe un marco de autenticación basado en RSA para los servicios audiovisuales que tienen conexiones punto a punto y multipunto.

Los procedimientos y las funciones de autenticación se basan en la Rec. UIT-T X.509. En esta Recomendación, la autenticación se establece con la utilización de uno o más niveles de las llamadas autoridades de certificación. Una autoridad de certificación (CA, *certification authority*) firma certificados fuera de linea a entidades u otras CA, que esas entidades o CA pueden utilizar para autenticarse ellas mismas ante otras entidades y CA. En el caso de los servicios audiovisuales, las entidades pueden ser terminales de usuario o MCU confiables.

El marco de autenticación específico que aquí se describe utiliza dos niveles de CA. En el nivel más bajo, cada dominio de red, por ejemplo, un país o una empresa, tendrá su propia CA. Para hacer posibles los servicios audiovisuales entre dominios autenticados, las CA tendrán una CA común en un nivel superior que las autentique. Esta CA común tiene que ser un punto de confianza común para los usuarios.

Si esto no se consigue, hay un esquema alternativo, más complicado, descrito brevemente en 6.5.

Hay que confiar en que las CA de nivel dominio de red no repetirán los nombres de identificación en los certificados. Se supone que la propia autenticación se establece en un entorno no fiable. Además, una vez que una entidad ha sido autenticada, se confía en ella (hasta que termine la llamada).

6.1.2 Abreviaturas

CA Autoridad de certificación (*certification authority*)

CCA Autoridad de certificación de país (*country certification authority*)

GCA Autoridad de certificación general (*general certification authority*)

h[*] Resultado de la función h aplicada a *

X<<Y>> Certificado de Y generado por X

Xp Clave RSA pública de la entidad X

Xs Clave RSA secreta de la entidad X

Xp[*] Criptación/descriptación de [*] con Xp. En el caso de RSA, se efectúan por exponenciación.

Xs[*] Criptación/descriptación de [*] con Xs. En el caso de RSA, se efectúan por exponenciación.

6.2 Configuración del sistema

El sistema que aquí se especifica tiene una jerarquía de tres niveles. En el nivel más bajo están las entidades de servicio audiovisual, AVSE. Cada una tiene relación con una sola CA de nivel medio cuando comunica con otra AVSE. Las CA de este nivel sirven como autoridades de certificación de un grupo de entidades (normalmente todas están dentro del mismo país o dominio de red). Estas CA, llamadas autoridades de certificación de país (CCA, *country certification authorities*) otorgan certificados a las entidades con las que están relacionadas. En el nivel más elevado hay una sola CA, llamada autoridad de certificación general (GCA, *general certification authority*). La GCA emite certificados a todas las CA. En la figura 6 se muestra la jerarquía.

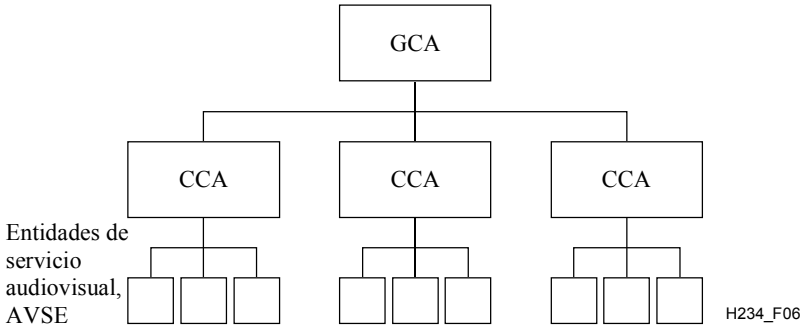


Figura 6/H.234 – Jerarquía de las autoridades de certificación

El marco de autenticación utiliza el algoritmo criptográfico RSA. Se trata de un algoritmo de clave pública, en el que las claves de criptación y descriptación son diferentes. Una de estas claves se puede hacer pública, mientras que la otra se mantiene secreta. Se las denomina *clave pública* y *clave secreta*, respectivamente.

La autenticación utiliza además una función de cálculo de troceo h(*), que hace corresponder una secuencia de caracteres de longitud arbitraria en una secuencia de caracteres de longitud limitada, no superior a la del módulo RSA utilizado. La función h(*) no se especifica en esta Recomendación, pero la autoridad de certificación debe especificarla. En [3] se da un ejemplo de dicha función de troceo disponible públicamente.

6.3 Generación y distribución de las claves de autenticación

Una clave de autenticación se compone de un par de claves secreta/pública con algoritmo RSA. Cada CA y cada entidad AVS tiene su propio par de autenticación.

La GCA genera su propia clave de autenticación, formada por una clave secreta, GCA, y una clave pública, GCAp.

Cada CCA genera su propia clave de autenticación, formada por una clave secreta, GCA y una clave pública, CCAp. La CCA pone la CCAp a disposición de la GCA, que certifica esta clave.

La clave de autenticación de AVSE U, formada por una clave secreta Us y una clave pública Up, la genera su CCA. La Up y la Us se ponen a disposición de AVSE. La CCA certifica la Up.

Se tiene que lograr el consenso internacional para la generación de la clave de autenticación GCA y para la generación y distribución de las claves de autenticación CCA.

NOTA – La interfaz física entre autoridades de certificación y entidades de servicio audiovisual queda fuera del alcance de esta Recomendación.

6.4 Certificación

La GCA certifica una clave pública CCAp mediante el cálculo de un certificado, denotado como GCA<<CCA>>, que consta de la siguiente información:

GCA<<CCA>>: GCA,CCA,CCAp,T1,GCAs[h(GCA,CCA,CCAp,T1)]

donde:

GCA es la identidad de GCA

CCA es la identidad de CCA

CCAp es la clave pública de CCA

T1 es la fecha de principio y fin de la validez del certificado

GCAs[*] es la criptación de * con la clave GCA

NOTA – Se ha incluido la identidad de la GCA a efectos de conformidad con la Rec. UIT-T X.509, pero en el sistema descrito la identidad de la GCA se determina de manera exclusiva.

La CCA certifica una clave pública Xp de una AVSE X mediante el cálculo de un certificado, denotado como CCA<<X>>, que consta de la siguiente información:

CCA<<X>>: CCA,X,Xp,T2,CCAs[h(CCA,X,Xp,T2)]

donde:

CCA es la identidad de CCA

X es la identidad de X

Xp es la clave pública de X

T2 es la fecha de principio y fin de la validez del certificado

CCAs[*] es la criptación de * con la clave CCA

GCAp, GCA<<CCA>> y CCA<<X>> se ponen, junto con X, a disposición de la entidad X, por ejemplo, en forma de tarjeta o módulo incorporado en el soporte físico. X debe tener también una copia impresa de las GCAp, que servirá de referencia si hay dudas sobre la integridad de la GCA.

Verificación de los certificados

GCA<<CCA>> se puede verificar mediante el cálculo de h(GCA,CCA,CCAp,T1) utilizando la GCAp y comparándolo con GCA[GCAs[h(GCA,CCA,CCAp,T1)]]; ambos valores deben ser iguales. CCA<<X>> se puede verificar mediante el cálculo de h(CCA,X,Xp,T2) utilizando la CCAp y comparándolo con CCAp[CCAs[h(CCA,X,Xp,T2)]]; ambos valores deben ser iguales.

El esquema descrito en 6.4 se presenta de forma resumida en la figura 7 para las AVSE X e Y con autoridades de certificación CA1 y CA2, respectivamente.

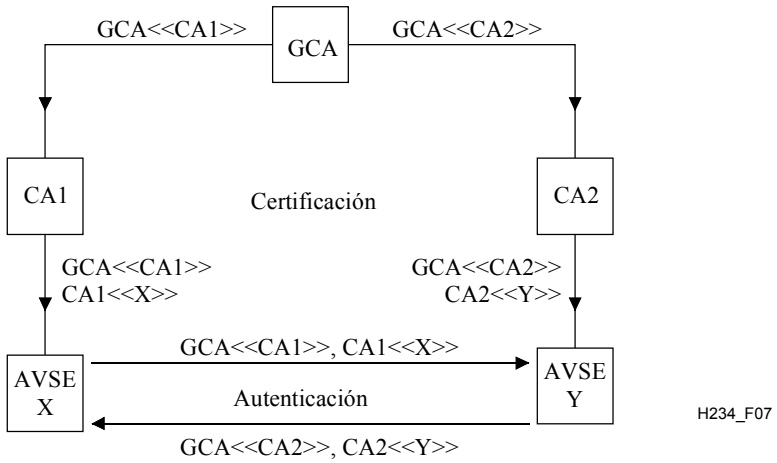


Figura 7/H.234 – Resumen del procedimiento de certificación

6.5 Solución alternativa para la certificación sin GCA

Si dos operadores de red o compañías desean que sus AVSE se autentiquen mutuamente, sus autoridades de certificación CA1 y CA2 deben certificarse mutuamente mediante el intercambio de los certificados CA1<<CA2>> y CA2<<CA1>>. Este sistema funciona de manera compleja, ya que las AVSE X e Y podrían tener que entrar en un directorio externo para obtener CA1<<CA2>> o CA2<<CA1>> y tener también que intercambiar de antemano las identidades de sus autoridades de certificación. Esto es lo que se detalla en la figura 8.

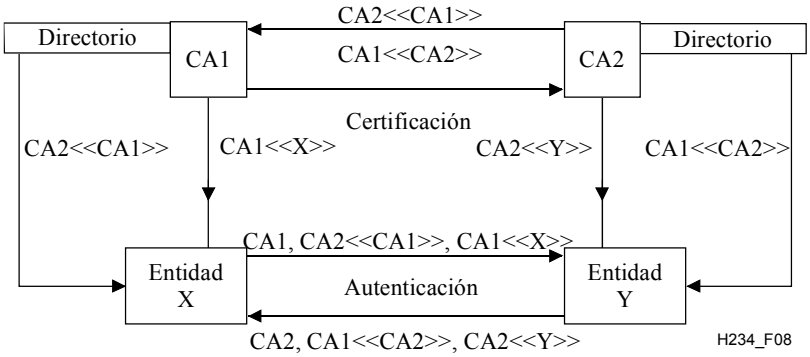


Figura 8/H.234 – Certificación sin una autoridad de certificación superior

6.6 Autenticación de entidades

A continuación, se detalla el procedimiento de autenticación, que es aplicable en todas las conexiones posibles, es decir, MCU-MCU, terminal-MCU, MCU-terminal y terminal-terminal.

El procedimiento de autenticación entre dos entidades durante el establecimiento de la comunicación consta de cuatro mensajes:

– RSA.P1 – Inicio de autenticación;

– RSA.P2 – Respuesta de autenticación;

– RSA.P3 – Autenticación completa;

– RSA.P4 – Autenticación fallada.

RSA.P1 y RSA.P3 los envía la entidad iniciadora, denotada por X; el RSA.P2, la entidad llamada, denotada por Y. Las CCA de X e Y se denotan por CX y CY, respectivamente.

El contenido de RSA.P1 es:

GCA<<CX>>,CX<<X>>,RX,Y,Xs[h(RX,Y)]

donde RX es un número aleatorio generado por X.

Y, ahora:

1) obtiene Xp de RSA.P1 y comprueba Xp utilizando los certificados con GCAp como punto de confianza;
2) comprueba la integridad del mensaje calculando h(RX,Y) y comparándolo con Xp[Xs[h(RX,Y)]]; ambos valores deben ser iguales;
3) comprueba las fechas de expiración de los certificados;
4) comprueba la integridad de X.

El contenido de RSA.P2 es:

GCA<<CY>>,CY<<Y>>,RY,X,RX,Xp[KY],Ys[h(RY,X,RX,KY)]

donde RY es un número aleatorio y KY es datos de clave (véase 3.3.2), ambos generados por Y.

X, ahora:

1) obtiene Yp de RSA.P2 y comprueba Yp utilizando los certificados con GCAp como punto de confianza;
2) descripta Xp[KY], obtiene KY;
3) comprueba la integridad del mensaje calculando h(RY,X,RX,KY) y comparándolo con Yp[Ys[h(RY,X,RX,KY)]]; ambos valores deben ser iguales;
4) comprueba las fechas de expiración de los certificados;
5) comprueba que RX es igual al enviado en RSA.P1;
6) comprueba la integridad de Y.

El contenido de RSA.P3 es:

RY,Y,Yp[KX],Xs[h(RY,Y,KX)],

donde KX es datos de clave generado por X.

Y, ahora:

1) descripta Yp[KX], obtiene KX;
2) comprueba la integridad del mensaje calculando h(RY,Y,KX) y comparándolo con Xp[Xs[h(RY,Y,KX)]]; ambos valores deben ser iguales;
3) comprueba que RY es el mismo que el enviado en RSA.P2;
4) comprueba la integridad de X.

Si falla cualquiera de las comprobaciones efectuadas en RSA.P1, RSA.P2 o RSA.P3 se interrumpe el establecimiento de la comunicación enviando un mensaje RSA.P4: autenticación fallada. RSA.P4 lo puede enviar tanto X como Y, después de RSA.P1, RSA.P2 o RSA.P3. El envío de RSA.P4 invoca la terminación del procedimiento de establecimiento de la comunicación.

NOTA 1 – Se puede acelerar los cálculos de RSA si se eligen parámetros públicos específicos.

NOTA 2 – Este esquema difiere de la especificación X.509 original en que KX se envía en RSA.P3 y no en RSA.P1. Esto tiene la ventaja de que X no tiene que obtener Yp de un directorio. Tanto para X como para Y, GCAp es el único punto de confianza: mientras se confíe en esta clave y se tenga confianza en que la información secreta de una entidad no va a ser sustraída, X e Y no necesitan acceder a directorios. Además, en RSA.P3 se añade la identidad de Y por motivos de seguridad, y en RSA.P2 y RSA.P3, la firma va en datos de clave no criptados KY y KX, respectivamente.

6.6.1 Transmisión simultánea de mensajes RSA.P1

Si la entidad X envía a la entidad Y un mensaje iniciador:

RSA.P1(X–>Y): GCA<<CX>>,CX<<X>>,RX,Y,Xs[h(RX,Y)]

y, antes de recibir RSA.P2(Y–>X), Y envía a X un mensaje iniciador:

RSA.P1(Y–>X): GCA<<CY>>,CY<<Y>>,RY,X,Ys[h(RY,X)]

entonces X e Y resolverán esta situación, *comparando RX y RY*.

Si RX>RY, el mensaje RSA.P1(Y–>X) debe ser desechado e Y debe responder con un mensaje RSA.P2.

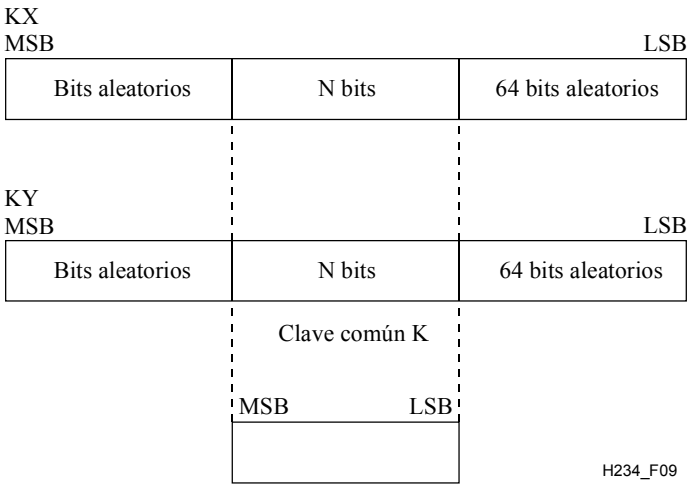
Si RY>RX, el mensaje RSA.P1(X–>Y) debe ser desechado y X debe responder con un mensaje RSA.P2.

Si se da la coincidencia de que RX = RY, se desechan ambos mensajes RSA.P1 y se termina el procedimiento de autenticación con el envío de un mensaje RSA.P4 (autenticación fallada).

6.7 Generación de la clave para la criptación de claves de sesión

Los datos de clave KY y KX transmitidos en los mensajes RSA.P2 y RSA.P3 se utilizan para establecer la *clave* común K, que se utilizará para criptar los mensajes de intercambio de claves de sesión, como se describe en 3.3.2. (De estos mensajes se obtiene un conjunto de cuatro claves de sesión.) Si N representa la longitud de K, la clave K se forma tomando la suma en módulo 2 de los bits 64 a 64 + N – 1 de KX y de 64 a 64 + N – 1 de KY (el bit cero indica aquí el bit menos significativo de KX y KY). El bit 64 de KX y el bit 64 de KY generan juntos el bit 0 de K. El valor de N es la longitud de la *clave* y lo determina el algoritmo de criptación aplicado.

Los bits no utilizados de KX y KY (índice 0 a 63 y 64 + N y superior) se rellenan con información aleatoria. La generación de la clave K común a partir de KX y KY se muestra en forma de diagrama en la figura 9.



NOTA – Los bloques de N bits de KX y KY se suman en módulo 2 para formar la clave común K.

Figura 9/H.234 – Generación de la *clave* común

6.8 Mensajes RSA

En esta cláusula se detalla el contenido de los mensajes del esquema de autenticación con RSA que se describe en 6.6. Las descripciones se basan en la Rec. UIT-T X.690. En 3.2 se describen brevemente algunas definiciones X.690 utilizadas en esta cláusula.

6.8.1 Inicio de autenticación

Nombre de mensaje:	Inicio de autenticación (RSA.P1).
Identificador de mensaje:	1 0 P t_1 t_2 t_3 t_4 t_5 = 1010 0111
Significado:	El emisor de estos mensajes desea iniciar un procedimiento de autenticación con el destinatario y envía la información necesaria para arrancar el procedimiento.
Contenido:	Un constructor, que consta de dos constructores para los certificados GCA<<CX>> y CX<<X>> y tres primitivas: número aleatorio RX, identidad de Y e información de troceo calculado criptada Xs[h(RX,Y)].
Notación en ASN.1:	RSA.P1 ::= [7] IMPLICIT SEQUENCE { GCA-certificate-for-CCA [0] IMPLICIT GCA-Certificate, CCA-certificate-for-entity [1] IMPLICIT CCA-Certificate, calling-entity-random-number [2] IMPLICIT BIT STRING, called-entity-identity [3] IMPLICIT BIT STRING, hashed-information-in-calling-secret-key [4] IMPLICIT BIT STRING }

El contenido de Calling-Entity-Random-number (número aleatorio de entidad llamante) es una cadena de bits primitiva.

El contenido de Called-Entity-Identity (identidad de la entidad llamada) es una cadena de bits primitiva.

El contenido de Hashed-Information-In-Calling-Secret-Key (información de troceo calculado en clave secreta de llamante) es una cadena de bits primitiva.

Contenido de GCA-Certificate-For-CCA (certificado de GCA para CCA): un constructor, que consta de cinco primitivas: identidad de GCA, identidad de CCA, clave pública CCAp, gama de fechas de validez T1 e información de troceo calculado criptada GCAs[h(GCA,CCA,CCAp,T1)].

En notación ASN.1:

GCA-Certificate::= SEQUENCE{GCA-identity [0] IMPLICIT BIT STRING,

CCA-identity [1] IMPLICIT BIT STRING,

CCA-public-key [2] IMPLICIT BIT STRING,

certificate-valid-date-range [3] IMPLICIT BIT STRING,

hashed-information-in-GCA-secret-key [4] IMPLICIT BIT STRING}

El contenido de GCA-Identity (identidad de GCA) es una cadena de bits primitiva.

El contenido de CCA-Identity (identidad de CCA) es una cadena de bits primitiva.

El contenido de CCA-Public-Key (clave pública de CCA) es una cadena de bits primitiva.

El contenido de Certificate-Valid-Date-Range (gama de fechas de validez del certificado) es una cadena de bits primitiva.

El contenido de Hashed-Information-In-GCA-Secret-Key (información de troceo calculado criptada en clave secreta de GCA) es una cadena de bits primitiva.

Contenido de CCA-Certificate-For-Entity (certificado de CCA para entidad): un constructor, que consta de cinco primitivas: identidad de CCA, identidad de entidad X, clave pública Xp, gama de fechas de validez T2 y la información de troceo calculado criptada CCAs[h(CCA,X,Xp,T2)].

En notación ASN.1:

```
CCA-Certificate::= SEQUENCE{CCA-identity [0] IMPLICIT BIT STRING,
                            entity-identity [1] IMPLICIT BIT STRING,
                            entity-public-key [2] IMPLICIT BIT STRING,
                            certificate-valid-date-range [3] IMPLICIT BIT STRING,
                            hashed-information-in-CCA-secret-key [4] IMPLICIT BIT STRING}
```

El contenido de CCA-Identity es una cadena de bits primitiva.

El contenido de Entity-Identity es una cadena de bits primitiva.

El contenido de Entity-Public-Key es una cadena de bit primitiva.

El contenido de Certificate-Valid-Date-Range es una cadena de bits primitiva.

El contenido de Hashed-Information-In-CCA-Secret-Key es una cadena de bits primitiva.

6.8.2 Respuesta de autenticación

Nombre de mensaje:	Respuesta de autenticación (RSA.P2).
Identificador de mensaje:	1 0 P t_1 t_2 t_3 t_4 t_5 = 1010 1000
Significado:	El emisor de este mensaje responde a un inicio de autenticación y envía la información necesaria para el procedimiento de autenticación.
Contenido:	Un constructor, que consta de dos constructores para los certificados GCA<<CY>> y CY<<Y>> y cinco primitivas: número aleatorio RY, entidad de X, número aleatorio RX, información de clave criptada Xp[KY] e información de troceo calculado criptada Ys[h(RY,X,RX,KY)].
Notación en ASN.1:	RSA.P2 ::= [8] IMPLICIT SEQUENCE { GCA-certificate-for-CCA [0] IMPLICIT GCA-Certificate, CCA-certificate-for-entity [1] IMPLICIT CCA-Certificate, called-entity-random-number [2] IMPLICIT BIT STRING, calling-entity-identity [3] IMPLICIT BIT STRING, calling-entity-random-number [4] IMPLICIT BIT STRING, key-information-in-calling-public-key [5] IMPLICIT BIT STRING, hashed-information-in-called-secret-key [6] IMPLICIT BIT STRING }

El contenido de Called-Entity-Random-Number es una cadena de bits primitiva.

El contenido de Calling-Entity-Identity es una cadena de bits primitiva.

El contenido de Calling-Entity-Random-Number es una cadena de bits primitiva.

El contenido de Key-Information-In-Calling-Public-Key es una cadena de bits primitiva.

El contenido de Hashed-Information-In-Called-Secret-Key es una cadena de bits primitiva.

Los contenidos de GCA-Certificate-For-CCA y CCA-Certificate-For-Entity son similares a las descripciones dadas en 6.8.1.

6.8.3 Autenticación completa

Nombre de mensaje:	Autenticación completa (RSA.P3).
Identificador de mensaje:	1 0 P t_1 t_2 t_3 t_4 t_5 = 1010 1001
Significado:	El emisor de este mensaje, que es el iniciador del procedimiento de autenticación, envía la información necesaria para completar el procedimiento de autenticación.
Contenido:	Un constructor, que consta de cuatro primitivas: número aleatorio RY, entidad de Y, información de clave criptada Yp[KX] e información de troceo calculado criptada Xs[h(RY,Y,KX)].
Notación en ASN.1:	RSA.P3 ::= [9] IMPLICIT SEQUENCE { called-entity-random-number [0] IMPLICIT BIT STRING, called-entity-identity [1] IMPLICIT BIT STRING, key-information-in-called-public-key [2] IMPLICIT BIT STRING, hashed-information-in-calling-secret-key [3] IMPLICIT BIT STRING }

El contenido de Called-Entity-Random-Number es una cadena de bits primitiva.

El contenido de Called-Entity-Identity es una cadena de bits primitiva.

El contenido de Key-Information-In-Called-Public-Key es una cadena de bits primitiva.

El contenido de Hashed-Information-In-Calling-Secret-Key es una cadena de bits primitiva.

6.8.4 Autenticación fallada

Nombre de mensaje:	Autenticación fallada (RSA.P4).
Identificador de mensaje:	1 0 P t_1 t_2 t_3 t_4 t_5 = 1000 1010
Significado:	El emisor de este mensaje indica que algo ha fallado durante el procedimiento de autenticación y que se va a terminar dicho procedimiento. El envío o la recepción de este mensaje debe invocar la terminación del procedimiento de establecimiento de la comunicación.
Contenido:	Este mensaje no tiene contenido.

7 Operación de la MCU

En el caso de una "MCU confiable" (en la que todas las señales se descriptan en las entradas de la MCU y, por consiguiente, la MCU debe estar en un sitio seguro), las comunicaciones entre cada terminal audiovisual y la MCU se criptan como se describe en esta Recomendación para un enlace punto a punto. Evidentemente, este método no es aplicable a la conexión de terminales telefónicos a la conferencia por medio de la red telefónica analógica.

Esta Recomendación no estipula el funcionamiento de una MCU sin esa descriptación.

Bibliografía

[1] DIFFIE (W.), HELLMAN (M.): New directions in cryptography, *IEEE Transactions IT-22*, 6, pp. 644-654, (noviembre de 1976).

[2] RIVEST (R. L.), SHAMIR (A.), ADLEMAN (L.): A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, *Communications of the ACM*, 21, 2, pp. 120-126, (febrero de 1978).

[3] The MD4 Message Digest Algorithm, *RSA Data Security Inc.*, Redwood City, California 94065.

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie B	Medios de expresión: definiciones, símbolos, clasificación
Serie C	Estadísticas generales de telecomunicaciones
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 y aspectos del protocolo Internet
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2003