Unión Internacional de Telecomunicaciones

UIT-T H.235.2

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

(09/2005)

SERIE H: SISTEMAS AUDIOVISUALES Y MULTIMEDIOS

Infraestructura de los servicios audiovisuales – Aspectos de los sistemas

Marco de seguridad H.323: Perfil de seguridad de firma

Recomendación UIT-T H.235.2

UIT-T

ITU Unión Internacional de Telecomunicaciones

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.349
Arquitectura de servicios de directorio para servicios audiovisuales y multimedios	H.350–H.359
Arquitectura de la calidad de servicio para servicios audiovisuales y multimedios	H.360–H.369
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
SERVICIOS DE BANDA ANCHA Y DE TRÍADA MULTIMEDIOS	
Servicios multimedios de banda ancha sobre VDSL	H.610–H.619

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

Recomendación UIT-T H.235.2

Marco de seguridad H.323: Perfil de seguridad de firma

Resumen

En la presente Recomendación se describe un perfil de seguridad optativo para la utilización de firmas digitales que aseguren la señalización H.225.0.

En versiones anteriores de la subserie H.235 se describió este perfil en el anexo E/H.235. En los apéndices IV, V y VI/H.235.0 se indica la relación entre el texto, las figuras y los cuadros de las versiones 3 y 4 de H.235.

Orígenes

La Recomendación UIT-T H.235.2 fue aprobada el 13 de septiembre de 2005 por la Comisión de Estudio 16 (2005-2008) del UIT-T por el procedimiento de la Recomendación UIT-T A.8.

Palabras clave

Autenticación, certificado, criptación, firma digital, gestión de claves, integridad, perfil de seguridad, seguridad multimedia.

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 H.235.2

Marco de seguridad H.323: Perfil de seguridad de firma

1 Alcance

En la presente Recomendación se describe un perfil de seguridad opcional para la utilización de firmas digitales que aseguren la señalización H.225.0.

2 Referencias

2.1 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.225.0 (2003), *Protocolos de señalización de llamada y paquetización de trenes de medios para sistemas de comunicaciones multimedios por paquetes*.

– Recomendación UIT-T H.235 (1998), *Seguridad y criptado para terminales multimedios de la serie H (basados en las Recomendaciones H.323 y H.245)*.

– Recomendación UIT-T H.235.0 (2005), *Marco de seguridad H.323: Marco de seguridad para sistemas multimedia de la serie H (H.323 y otros basados en H.245)*.

– Recomendación UIT-T H.235.1 (2005), *Marco de seguridad H.323: Perfil de seguridad básico*.

– Recomendación UIT-T H.235.6 (2005), *Marco de seguridad H.323: Perfil de criptación vocal con gestión de claves H.235/H.245 nativa*.

– Recomendación UIT-T H.245 (2005), *Protocolo de control para comunicación multimedia*.

– Recomendación UIT-T H.323 (2003), *Sistemas de comunicación multimedios basados en paquetes*.

– Recomendación UIT-T Q.931 (1998), *Especificación de la capa 3 de la interfaz usuario-red de la red digital de servicios integrados para el control de la llamada básica*.

– Recomendación UIT-T X.509 (2005) | ISO/CEI 9594-8:2005, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Marcos para certificados de claves públicas y de atributos*.

– Recomendación UIT-T X.800 (1991), *Arquitectura de seguridad de la interconexión de sistemas abiertos para aplicaciones del CCITT*.

– Recomendación UIT-T X.803 (1994) | ISO/CEI 10745:1995, *Tecnología de la información – Interconexión de sistemas abiertos – Modelo de seguridad de capas superiores*.

– Recomendación UIT-T X.810 (1995) | ISO/CEI 10181-1:1996, *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos: Visión general*.

– Recomendación UIT-T X.811 (1995) | ISO/CEI 10181-2:1996, *Tecnología de la información – Interconexión de sistemas abiertos –Marcos de seguridad para sistemas abiertos: Marco de autenticación*.

– ISO/CEI 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture*.

– ISO/CEI 9798-3:1998, *Information technology – Security techniques – Entity authentication – Part 3: Mechanisms using digital signature techniques*.

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

2.2 Rerencias informativas

[ISO/CEI 14888-3] ISO/IEC 14888-3:1998, *Information technology – Security techniques – Digital signatures with appendix – Part 3: Certificate-based mechanisms*.

[PKCS] PKCS #1 v2.0: *RSA Cryptography Standard;* RSA Laboratories; October 1, 1998; http://www.rsa.com/rsalabs/pubs/PKCS/index.html.

[PKCS] PKCS #7: *Cryptographic Message Syntax Standard*, An RSA Laboratories Technical Note, version 1.5, Revised November 1, 1993; http://www.rsa.com/rsalabs/pubs/PKCS/index.html

[RFC1321] IETF RFC 1321 (1992), *The MD5 Message-Digest Algorithm.*

[RFC3447] IETF RFC 3447 (2003), *Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1*.

3 Términos y definiciones

A los efectos de la presente Recomendación, se utilizan las definiciones que figuran en las cláusulas 3/H.323, 3/H.225.0 y 3/H.245 junto con las de la presente cláusula. Algunos de los siguientes términos se utilizan como se define en las Recs. UIT-T X.800 | ISO 7498-2, X.803 | ISO/CEI 10745, X.810 | ISO/CEI 10181-1 y X.811 | ISO/CEI 10181-2.

3.1 autoridades de certificación: En el contexto de la firma electrónica, autoridades de certificación (CA, *certification authorities*) que certifican las claves de verificación públicas mediante la expedición de "Certificados".

3.2 depósitos de certificados: Los depósitos de certificados (por ejemplo, un directorio X.500) mantienen los certificados de usuario y las listas de revocación de certificados (CRL, *certificate revocation lists*). Permiten el acceso a esta información, pero no son responsables del contenido y la exactitud de la información que reciben de las CA o las RA.

3.3 firma digital: Transformación criptográfica (que utiliza una técnica criptográfica asimétrica) de la representación numérica de un mensaje de datos, de modo que cualquier persona que tenga el mensaje firmado y la clave pública pertinente puede determinar:

i) que la transformación se creó utilizando la clave privada correspondiente a la clave pública pertinente; y

ii) que el mensaje firmado no ha sido alterado desde que se realizó la transformación criptográfica.

3.4 proveedores de estado de certificado en línea: El protocolo de estado de certificado en línea (OCSP, *on-line certificate status protocol*) permite a las aplicaciones determinar el estado de revocación de un certificado identificado. El OCSP puede utilizarse para satisfacer algunos de los requisitos operacionales de la provisión de información de revocación del modo más oportuno

posible en el tiempo mediante listas CRL. Los proveedores de estado de certificado en línea pueden considerarse una alternativa a la utilización de las CRL fuera de línea.

3.5 apoderado: El apoderado es una entidad H.323 similar a un controlador de acceso. El apoderado puede ser un nodo de red separado o estar cosituado con la funcionalidad de una entidad H.323, como uno de los controladores de acceso. El apoderado puede realizar tareas de seguridad como la verificación de firmas y certificados y el control de acceso.

3.6 autoridades de registro: Las autoridades de registro actúan como intermediarios entre los usuarios y las CA. Reciben peticiones de los usuarios y las transmiten a las CA en forma adecuada.

3.7 autoridades de indicaciones de tiempo: Las autoridades de indicaciones de tiempo son obligatorias para el no repudio en caso de pérdida de la clave o dudas sobre su seguridad. En la práctica estas autoridades proporcionan a cualquiera una contrafirma, incluido un tiempo fiable, sobre un número generador y un identificador de número generador.

3.8 proveedor de servicio de confianza: Entidad que puede ser utilizada por otras entidades como intermediario de confianza en una comunicación o proceso de verificación, o como proveedor de confianza del servicio de información.

En la presente Recomendación se utilizan los siguientes términos para la prestación de servicios de seguridad.

3.9 sólo autenticación: Este servicio de seguridad del perfil de seguridad de firma soporta una forma de autenticación de usuarios en la que el usuario queda autenticado cuando firma digital y correctamente datos con una clave privada. Cabe señalar que este servicio de seguridad no comprende contramedidas contra operaciones arbitrarias de cortar y pegar, la manipulación de mensajes ni los ataques de alteración. El servicio de sólo autenticación puede resultar útil para los apoderados de seguridad que verifican la autenticidad de los mensajes (autenticación del origen de los datos) al reenviar un mensaje a otro destino (por ejemplo, controlador de acceso).

NOTA – El reenvío generalmente modifica algunas partes del mensaje, por lo que no puede lograrse la integridad de extremo a extremo.

No obstante, el sistema de sólo autenticación puede aplicarse también salto por salto. El procedimiento III especifica este servicio de seguridad para los casos de extremo a extremo, mientras que el procedimiento II se aplica al servicio de seguridad salto por salto.

3.10 autenticación e integridad: Se trata de un servicio de seguridad combinado que permite garantizar la integridad del mensaje y autenticar al usuario. El usuario queda autenticado si produce una firma digital correcta para los datos utilizando una clave privada. Además, el mensaje queda protegido contra la alteración. Ambos servicios de seguridad son proporcionados por el mismo mecanismo de seguridad. Es posible combinar la autenticación y la integridad únicamente salto por salto. Este servicio de seguridad está especificado en procedimiento II.

NOTA – Cuando se utilizan firmas digitales, el sistema puede soportar un servicio de seguridad de no repudio; también depende de la configuración de los bits de utilización de claves de la clave de firma en el certificado (véase asimismo RFC 3280).

4 Abreviaturas, siglas o acrónimos

En esta Recomendación se utilizan las siguientes abreviaturas, siglas o acrónimos.

ARQ Petición de admisión (*admission request*)

ASN.1 Notación de sintaxis abstracta uno (*abstract syntax notation one*)

CA Autoridad de certificación (*certification authority*)

CRL Lista de revocación de certificados (*certificate revocation list*)

DH Diffie-Hellman

DNS Servicio de nombres de dominio (*domain name service*)

EP Punto extremo (*endpoint*)

EPID Identificador de punto extremo (*endpoint identifier*)

GK Controlador de acceso (*gatekeeper*)

GKID Identificador de controlador de acceso (*gatekeeper identifier*)

GRQ Petición de controlador de acceso (*gatekeeper request*)

ICV Valor de comprobación de integridad (*integrity check value*)

IP Protocolo Internet (*Internet protocol*)

LDAP Protocolo ligero de acceso al directorio (*light-weight directory access protocol*)

LRQ Petición de localización (*location request*)

MCU Unidad de control multipunto (*multipoint control unit*)

MD5 Message Digest 5

NAT Traducción de dirección de red (*network address translation*)

OCSP Protocolo en línea del estado del certificado (*online certificate status protocol*)

OID Identificador de objeto (*object identifier*)

PKCS Criptosistema de claves públicas (*public-key crypto system*)

RA Autoridad de registro (*registration authority*)

RAS Registro, admisión y estado (*registration, admission and status*)

RSA Rivest, Shamir, Adleman

RTP Protocolo de transporte en tiempo real (*real-time protocol*)

SHA Algoritmo troceado asegurado (*secure hash algorithm*)

UIT Unión Internacional de Telecomunicaciones

URL Localizador de recurso uniforme (*uniform resource locator*)

5 Convenios

En esta Recomendación se utilizan los siguientes convenios en lo relativo al nivel de obligación:

– La obligación firme se expresa con el futuro simple del verbo (futuro de mandato) o expresiones con significado de obligación.

– La conveniencia, es decir, una acción aconsejada pero no obligatoria, se expresa con el condicional del verbo modal "deber" o expresiones que indican conveniencia.

– La opción se expresa mediante el presente de indicativo del verbo "poder" o expresiones de posibilidad.

Si fuera necesario, el perfil de seguridad de firma puede utilizar el **perfil de seguridad de criptación vocal** de H.235.1 para conseguir la confidencialidad de la conversación.

Los procedimientos II y III especifican la forma de implementar los servicios de seguridad para diferentes situaciones, como el método salto por salto y el método de extremo a extremo, mediante diferentes mecanismos de seguridad tales como las técnicas criptográficas asimétricas (firma digital).

El servicio de integridad de mensajes proporciona siempre la autenticación del mensaje, pero no lo contrario. En el modo de autenticación solamente, la integridad se asegura solamente para un

subconjunto determinado de campos del mensaje. Este modelo se aplica a los servicios de integridad realizados por medios asimétricos (por ejemplo, firmas digitales). Con ello, en la práctica, el servicio combinado de autenticación y seguridad utiliza el mismo material de claves sin que con ello introduzca una debilidad en la seguridad.

Además, la información de seguridad salto por salto se introduce en el elemento **CryptoSignedToken**. Esta información se recalcula en cada salto de conformidad con el procedimiento II.

Por otra parte, la información de seguridad de extremo a extremo (posible solamente cuando se utiliza el servidor intermedio H.323 y el procedimiento III) calcula básicamente información similar a la introducida en el **CryptoSignedToken**, pero almacena esta información en un **CryptoToken** independiente del mensaje. Esta información no es modificada en el tránsito. Un identificador de objeto separado permite distinguir entre los **CryptoTokens** de salto por salto y de extremo a extremo.

Las técnicas asimétricas que utilizan firmas digitales pueden aplicarse salto por salto y/o de extremo a extremo.

6 Visión general

Esta Recomendación describe un perfil de firmas, el cual utiliza firmas digitales para asegurar la señalización H.225.0. Las entidades de seguridad H.323 (terminales, controladores de acceso, MCU, etc.) pueden implementar este perfil de seguridad de firma para mejorar la seguridad, o siempre que se desee.

El perfil de seguridad de firma requiere el modelo con encaminamiento por controlador de acceso y está basado en las técnicas de tunelización H.245; el soporte de modelos diferentes del modelo con encaminamiento por controlador de acceso queda en estudio.

El perfil de seguridad de firma es aplicable a la telefonía IP "global" escalable; este perfil de seguridad supera las limitaciones del perfil de seguridad básico simple de H.235.1. Por ejemplo, el perfil de seguridad de firmas no depende de la administración de secretos compartidos mutuos de los saltos en diferentes dominios. Proporciona la tunelización de mensajes H.245 para la integridad de mensajes H.245 y contiene también disposiciones para el no repudio de los mensajes. El perfil de seguridad de firma soporta la seguridad salto por salto y la autenticación de extremo a extremo verdadera, con el uso simultáneo de controladores de acceso intermedios o apoderados H.235.

Estos perfiles proporcionan las siguientes características, para los mensajes RAS, H.225.0 y H.245:

- La autenticación del usuario a una entidad deseada independientemente del número de saltos del nivel de aplicación que el mensaje atraviesa.

  NOTA 1 – "Salto" tiene aquí el sentido de un elemento de red H.235 de confianza (por ejemplo, GK, GW, MCU, apoderado, cortafuegos). Por tanto, la seguridad salto por salto en el nivel de aplicación cuando se utiliza con técnicas simétricas no proporciona una verdadera seguridad de extremo a extremo entre terminales.
- La integridad de todos los mensajes, o porciones (campos) críticas de los mismos, que llegan a una entidad, con independencia del número de saltos del nivel de aplicación que el mensaje atraviesa. La integridad del propio mensaje mediante la generación de un número aleatorio resistente es también facultativa.
- La autenticación, integridad y no repudio del mensaje salto por salto a nivel de aplicación proporciona estos servicios de seguridad para el mensaje completo.
- Se puede proporcionar también el no repudio de mensajes intercambiados entre dos entidades independientemente del número de saltos del nivel de aplicación que el mensaje atraviesa. En particular, el no repudio es proporcionado para porciones (campos) críticas del mensaje. Tal puede ser, por ejemplo, el caso de un EP que envía un mensaje

ESTABLECIMIENTO a su controlador de acceso y ambos (el EP y el controlador de acceso) son divididos por uno o más apoderados.

Mediante la provisión de manera adecuada de los servicios de seguridad anteriores se frustran varios ataques. Estos ataques son:

- Ataques de denegación de servicio: una comprobación rápida de las firmas digitales puede proteger contra tales ataques.
- Ataques por intromisión: la autenticación e integridad de los mensajes salto por salto al nivel de aplicación previene contra tales ataques cuando el punto intermedio se encuentra en un salto del nivel de aplicación, por ejemplo es un encaminador hostil. Cuando el punto de ataque intermedio es una entidad del nivel de aplicación, tales ataques se evitan utilizando la autenticación e integridad de extremo a extremo para porciones seleccionadas del mensaje.
- Ataques de reproducción: estos ataques se evitan mediante la utilización de indicaciones de tiempo y números secuenciales.
- Engaño: la autenticación del usuario evita estos ataques.
- Asalto a la conexión: el uso de la autenticación/integridad para cada mensaje de señalización evita estos ataques.

Este perfil de seguridad es aplicable en entornos en los que puede haber muchos terminales y donde la asignación de claves simétricas/contraseñas no es factible, por ejemplo, en sistemas mundiales o a gran escala. El perfil de seguridad de firma proporciona servicios de seguridad adicionales para el no repudio mediante certificados y firmas digitales. Las firmas digitales pueden utilizar la generación numérica SHA1 o MD5 y proporcionar la autenticación y/o la integridad (véanse los procedimientos II y III).

Las entidades H.323 que utilizan autenticación e integridad, o la autenticación solamente en un modo salto por salto, deberán utilizar el procedimiento II. Las entidades H.323 que utilizan sencillamente la autenticación solamente no implementarían la integridad. Las entidades H.323 con autenticación solamente utilizarán el procedimiento III para la autenticación verdadera de extremo a extremo.

Conforme a esta Recomendación, se puede aplicar protección de integridad de mensaje al mensaje completo. Para los RAS H.225.0, la protección de integridad cubre el mensaje completo RAS; para la señalización de llamada, el mensaje completo de señalización de llamada H.225.0 incluyendo los encabezamientos Q.931.

El perfil de seguridad de firmas permite tunelizar de modo seguro las PDU de control de llamada H.245 dentro de mensajes de facilidad H.225.0. El mecanismo de sincronización y de actualización de claves H.245 necesita la tunelización, de utilidad, por ejemplo, en las llamadas de larga duración.

NOTA 2 – La actualización para la codificación vocal G.711 de seguridad debe producirse a más tardar después de 2^{30} bloques de 64 bits, lo que significa más de 12 días de conversación.

En el cuadro 1, la zona sombreada vertical (azul en la copia electrónica) representa el ámbito del perfil de seguridad de firmas. Cuando se omite la integridad, indicada por la zona sombreada horizontal (verde en la copia electrónica), resulta el perfil de seguridad autenticación solamente. Dentro del perfil de seguridad de firma cabe elegir entre firmas digitales RSA-SHA1 o RSA-MD5. El perfil de seguridad de criptación vocal de H.235.6 (véase 6.1/H.235.6) podría utilizarse facultativamente junto con el perfil de seguridad de firma.

Cuadro 1/H.235.2 – Perfil de seguridad de firma

Servicios de seguridad	Funciones de llamada			
	RAS	H.225.0	H.245 (nota)	RTP
Autenticación	SHA1/ MD5	SHA1/ MD5	SHA1/ MD5	
	Firma digital	Firma digital	Firma digital	
No repudio	SHA1/ MD5	SHA1/ MD5	SHA1/ MD5	
	Firma digital	Firma digital	Firma digital	
Integridad	SHA1/ MD5	SHA1/ MD5	SHA1/ MD5	
	Firma digital	Firma digital	Firma digital	
Confidencialidad				
Control de acceso				
Gestión de claves	Asignación de certificado	Asignación de certificado		
NOTA – H.245 tunelizada o H.245 insertada en conexión rápida H.225.0.				

NOTA 3 – El perfil de seguridad de firma ha de ser soportado también por otras entidades H.235 (por ejemplo, apoderados H.235, controladores de acceso, pasarelas).

NOTA 4 – Los bits de utilización de claves disponibles en el certificado podrían también determinar el servicio de seguridad proporcionado por un terminal (por ejemplo, afirmación del no repudio).

Para la autenticación, el usuario debería utilizar un esquema de firma de claves privadas/públicas. Este esquema proporciona normalmente la mejor integridad y el no repudio de la llamada.

La presente Recomendación **no** describe los procedimientos para:

- El registro, certificación y asignación de certificados desde un centro de confianza y la asignación de claves privadas/públicas, los servicios de directorio, los parámetros de CA específicos, la revocación de certificados, la actualización/recuperación de pares de claves y otros procedimientos operacionales y de gestión de certificados tales como la entrega de certificados o claves públicas/privadas y la instalación de dichos procedimientos en los terminales.

Tales procedimientos pueden aplicarse por medios que no forman parte de la presente Recomendación.

Las entidades de comunicación involucradas son capaces de determinar implícitamente la utilización, bien de los perfiles de seguridad básicos de H.235.1, o bien de este perfil de seguridad de firmas mediante la evaluación de los identificadores de objeto de seguridad señalados en los mensajes (**tokenOID**, y **algorithmOID**; véase también la cláusula 20).

Se describen los siguientes procedimientos para su utilización en este perfil:

El procedimiento II se basa en firmas digitales que utilizan un par de claves privada/pública para garantizar la autenticación, la integridad y el no repudio de mensajes RAS, Q.931 y H.245. Los terminales pueden utilizar este método si se necesita el no repudio y una integridad sofisticada.

Dependiendo de cual sea la política de seguridad, la autenticación puede ser unilateral, o mutua (recíproca) en el caso en que también se aplica la autenticación/integridad en el sentido inverso y se proporciona por tanto una seguridad superior. La política de seguridad de un terminal puede permitir la "autenticación solamente" sin calcular la integridad criptográfica (véase la cláusula 9).

Los controladores de acceso que detectan el fallo de la validación de la autenticación y/o de la integridad en un mensaje RAS/de señalización de llamada recibido de un controlador de acceso

par/terminal responden con un mensaje de rechazo correspondiente que indica un fallo de seguridad mediante la fijación de la causa de rechazo a **securityDenial** u otro error de seguridad adecuado, conforme a 11.1/H.235.0. Dependiendo de la capacidad para reconocer un ataque, y de la manera más adecuada para reaccionar ante él, un controlador de acceso que recibe un **xRQ** seguro con identificadores de objetos no definidos (**tokenOID**, **algorithmOID**) debería responder con un **xRJ** no seguro, o simplemente descartar ese mensaje. El evento de seguridad encontrado debería registrarse. De otra parte, el punto extremo descartará el mensaje no seguro recibido, se desconectará y tratará de nuevo escogiendo diferentes OID. De igual manera, un controlador de acceso que recibe un mensaje SETUP H.225.0 seguro con identificadores de objetos no definidos (**tokenOID**, **algorithmOID**) debería responder con un RELEASE COMPLETE no seguro, indicando como motivo un problema de seguridad (**securityDenied**), o simplemente descartar dicho mensaje. Asimismo, se debería registrar el evento encontrado.

Hay una señalización H.235 implícita para indicar la utilización del procedimiento II y el mecanismo de seguridad aplicado que se basa en el valor de los identificadores de objeto (véase también la cláusula 20) y el relleno de los campos del mensaje. En este texto se hace referencia a los identificadores de objeto mediante letras (por ejemplo, "A").

Este perfil no utiliza los campos ICV H.235; en su lugar, los valores de comprobación de la integridad criptográfica son introducidos en el campo **signature** del **token** en el **cryptoSignedToken**.

6.1 Requisitos H.323

Se supone que las entidades H.323 que implementen este perfil de seguridad soportan las siguientes características:

- Conexión rápida.
- Modelo con encaminamiento por controlador de acceso.

7 Detalles de las firmas digitales con pares de claves privada/clave pública (procedimiento II)

Procedimientos obligatorios cuando se aplica el procedimiento II para la seguridad salto por salto:

- Deben utilizarse SHA1 o MD5 junto con el algoritmo RSA para generar la firma digital. La adhesión a PKCS #1 y PKCS #7 facilita la compatibilidad a este respecto.

  El campo **CryptoH323Token** de cada mensaje RAS/H.225.0 deberá contener los siguientes campos:

  – **nestedCryptoToken** con un **CryptoToken** que a su vez contiene el **cryptoSignedToken** con los siguientes campos:

    - **tokenOID** puesto a:
      - "A", que indica que el cálculo de la autenticación/integridad incluye todos los campos del mensaje RAS o de señalización de llamada H.225.0 (véase la cláusula 11);
      - "B", que indica que el cálculo de la autenticación/integridad incluye solamente un subconjunto de campos (véase la cláusula 10) del mensaje RAS/H.225.0 para autenticación solamente.
    - **token** con los campos:
      – **toBeSigned**, que contiene el **EncodedGeneralToken**, el cual es realmente un **ClearToken** con los siguientes campos fijados:
        - **tokenOID** fijado a "S", que indica que se esta utilizando **ClearToken** la autenticación/integridad/no repudio del mensaje.

- **timeStamp**, que contiene la indicación de tiempo.
- **random**, que contiene un número secuencial monotónicamente creciente.
- **generalID**, que contiene el identificador del receptor (sólo en caso de mensajes de unidifusión).
- **sendersID**, que contiene el identificador del emisor.
- **dhkey**, utilizado para transferir los parámetros Diffie-Hellman especificados en esta Recomendación durante **Setup** a **Connect**:
  - **halfkey**, que contiene la clave pública aleatoria de una parte.
  - **modsize**, que contiene el primo DH (véase el cuadro 4/H.235.6).
  - **generator**, que contiene el grupo DH (véase el cuadro 4/H.235.6).

  NOTA 1 – Cuando el perfil de seguridad de firmas se utiliza sin el perfil de seguridad de criptación vocal, no se enviarán los parámetros Diffie-Hellman y no debería haber **dhkey**; **halfkey**, **modsize** y **generator** pueden fijarse a {'0'B,'0'B,'0'B}.
- **certificate**, que contiene el certificado digital del emisor donde el tipo indica el tipo de certificado ("V" para los certificados MD5-RSA o "W" para los certificados SHA1-RSA) y **certificate** transporta el certificado efectivo (véase la cláusula 14).
- **algorithmOID** puesto a:
  - "V", que indica el empleo de la firma MD5-RSA;
  - "W", que indica el empleo de la firma SHA1-RSA.
- **params** fijado a NULO.
- **signature**, que contiene la firma calculada utilizando SHA1 o MD5 RSA en todos los campos (si **tokenOID** es "A", véase la cláusula 11) o en determinados campos críticos (si **tokenOID** es "B", véase la cláusula 10) del mensaje RAS y mensajes o señalización llamada H.225.0.

Cuando se utiliza el **tokenOID** "A" para la protección de unidades H323-UU-PDUs tunelizadas que incluyen todos los contenidos de mensajes H.245, el cálculo de la firma se realizará sobre el mensaje de señalización de llamada H.225.0 completo con todos los campos, de conformidad con el procedimiento descrito en la cláusula 11. En el caso de que se utilice el **tokenOID** "B", la "autenticación solamente" del **CryptoToken** se alcanza cuando se aplica el procedimiento III (véase la cláusula 10).

- Una entidad (que puede estar alejada uno o más saltos de aplicación) verifica la firma que está destinada a ella.

NOTA 2 – El receptor es capaz de detectar la aplicación del procedimiento II mediante la evaluación del **algorithmOID** dentro del testigo del **cryptoSignedToken** (detectando la presencia de "V" o de "W").

8 Procedimientos para la conferencia multipunto

Las unidades de control multipunto (MCU) deberán soportar la distribución segura de certificados tras la petición efectuada desde los terminales mediante las instrucciones tunelizadas H.245 **ConferenceRequest** y **ConferenceResponse** descritas en 8.8.1/H.235.6. Esto permite a los terminales solicitar certificados desde otros terminales en un entorno de conferencia multipunto y por tanto obtener la certidumbre acerca de la identidad de los demás participantes en la conferencia.

ConferenceRequest transporta la **requestTerminalCertificate**, en la cual se determinan los siguientes campos:

- **terminalLabel**: utilizado como medio de direccionamiento del terminal distante a través de la MCU;
- **certSelectionCriteria**: el emisor sólo puede pedir certificados de tipos específicos;
- **sRandom**: pregunta aleatoria generada por el emisor de la petición.

ConferenceResponse transporta la **terminalCertificateResponse**, en la cual se determinan los siguientes campos:

- **terminalLabel**: permite la asociación entre el certificado devuelto y el terminal.
- **CertificateResponse**: transporta la respuesta procedente de la MCU con los campos puestos a:
  - **terminalLabel**: identificación del terminal distante
  - **certificateResponse**: es de hecho una cadena de octetos codificada en ASN.1 a partir de la **EncodedReturnSig** como:
    - **generalID**: identificación del terminal de destino;
    - **responseRandom**: valor de la pregunta aleatoria generada por la MCU;
    - **requestRandom**: **sRandom** reproducida;
    - **certificate**: transporta el certificado devuelto donde **type** indica el tipo de certificado como OID y **certificate** cursa el certificado digital (véase la cláusula 14).

9 Autenticación de extremo a extremo (procedimiento III)

En la figura 1 se muestra un sistema con servidores intermedios que separan los GK y los EP y donde se utilizan dos CryptoTokens diferentes para la autenticación salto por salto así como para la autenticación de extremo a extremo y/o la integridad salto por salto. El **CryptoToken** utilizado para autenticación salto por salto se aplica solamente a la rama entre dos entidades y debe ser recalculado en cada una de las demás ramas. Por otra parte, el **CryptoToken** utilizado para la autenticación de extremo a extremo es generado una sola vez por el punto extremo de emisión y no es modificado en el tránsito por los nodos intermedios. Los nodos intermedios pueden validar firmas y certificados cursados en **CryptoTokens** de extremo a extremo y deben reenviar el **CryptoToken** en tránsito.

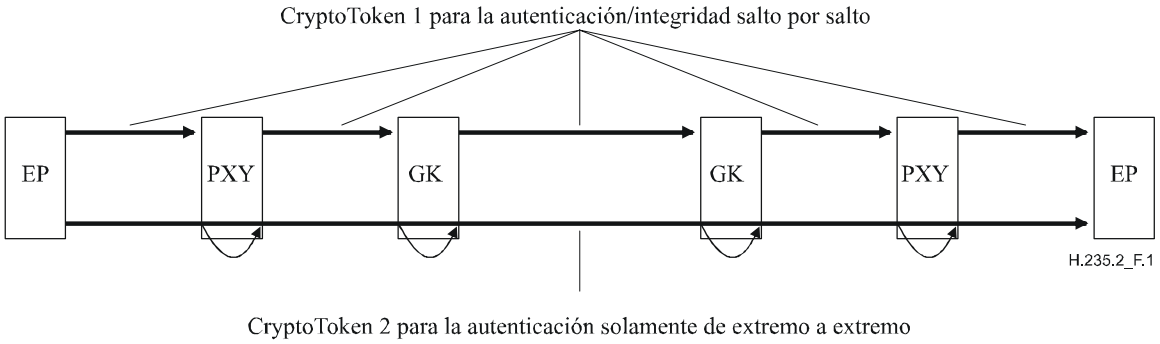

Figura 1/H.235.2 – Utilización simultánea de la seguridad salto por salto y la autenticación de extremo a extremo

NOTA 1 – El apoderado puede ser un nodo de red independiente como muestra la figura 1 o puede estar cosituado con la funcionalidad de una entidad H.323, por ejemplo, como parte de GK.

NOTA 2 – Dependiendo de cual sea el **tokenOID** señalado, el apoderado será capaz de determinar si el **CryptoToken** recibido esta destinado al apoderado ("S") o a algún otro receptor ("R").

NOTA 3 – Debido a que las entidades intermedias modifican el contenido del mensaje de señalización en cada rama, no es posible la integridad de extremo a extremo.

Para la autenticación verdadera de extremo a extremo a través de apoderados H.323 o elementos de red intermedios, el terminal/punto extremo emisor deberá calcular una firma digital como sigue:

El campo **CryptoH323Token** en cada mensaje RAS/H.225.0 deberá contener los siguientes campos:

- **nestedCryptoToken**, con un **CryptoToken** que a su vez contiene el **cryptoSignedToken**, con los siguientes campos:
  - **tokenOID** puesto a:
    - "A", que indica que el cálculo de la autenticación/integridad salto por salto incluye todos los campos del mensaje RAS/H.225.0 (véase la cláusula 11).
    - "B", que indica que el cálculo de la autenticación incluye solamente un subconjunto de campos (véase la cláusula 10) del mensaje RAS o de señalización de llamada H.225.0 para autenticación solamente.
- **token**, que contiene los campos:
  - **toBeSigned**, con el campo **ClearToken** utilizado con los siguientes campos:
    - **tokenOID** puesto a "R", que indica que el **ClearToken** se utiliza para autenticación solamente/no repudio sobre una base de extremo a extremo.

      NOTA 4 – El servicio de seguridad aplicado efectivamente depende también de los bits de utilización de claves del certificado.
    - **random**, que contiene un número secuencial monotónicamente creciente.
    - **timeStamp**, facultativamente, para una seguridad mejorada solamente cuando las entidades extremo de terminación están sincronizadas en el tiempo.
    - **generalID**, que contiene el identificador de punto extremo del receptor (sólo en el caso de unidifusión). En el caso salto por salto, éste es el identificador del salto siguiente; en el caso de extremo a extremo éste es el identificador de punto extremo del extremo lejano.
    - **sendersID**, que contiene el emisor de punto extremo.
    - **certificate**, que contiene el certificado digital del emisor, donde **type** indica el tipo de certificado ("V" para certificados MD5-RSA o "W" para certificados SHA1-RSA) y **certificate** transporta el certificado propiamente dicho (véase la cláusula 14).
    - **dhkey**, utilizado para transferir los parámetros Diffie-Hellman especificados en esta Recomendación durante **Setup** a **Connect**.
      - **halfkey**, que contiene la clave pública aleatoria de una parte.
      - **modsize**, que contiene el primo DH (véase el cuadro 4/H.235.6).
      - **generator**, que contiene el grupo DH (véase el cuadro 4/H.235.6).

NOTA 5 – Cuando el perfil de seguridad de firmas se utiliza sin el perfil de seguridad de criptación vocal no se debería enviar ningún parámetro Diffie-Hellman y no debería haber **dhkey**; **halfkey**, **modsize** y **generator** pueden ser fijados a {'0'B,'0'B,'0'B}.

- **algoritmOID** puesto a:
  - "V", que indica la utilización de la firma MD5-RSA;
  - "W", indicando la utilización de la firma SHA1-RSA.
- **params** puesto a NULO.
- **signature**, que contiene la firma calculada utilizando SHA1-RSA o MD5-RSA en todos los campos (si **tokenOID** es "A") o en determinados campos críticos (si **tokenOID** es "B") del mensaje RAS o de señalización de llamada H.225.0.

El apoderado puede verificar cualquier certificado y/o firma digital obtenidos, y puede descartar el mensaje si no los considera adecuados de acuerdo con la política local o reenviar más adelante el **CryptoToken** recibido. El apoderado deberá generar nuevos elementos de información de señalización H.235 para la seguridad salto por salto de conformidad con los procedimientos II o III.

La entidad que termina la rama (puede ser un terminal) debe verificar la información de seguridad recibida en el **CryptoToken** y, dependiendo de la presencia de elementos de seguridad de extremo a extremo, puede evaluar adicionalmente la información de **CryptoToken** de extremo a extremo. Los procedimientos de verificación exacta en un terminal o en una entidad H.323 intermedia pueden variar de acuerdo con la política local.

10 Solo autenticación

Los terminales pueden decidir implementar la autenticación solamente (utilizando el OID "B"). En este caso, el autenticador es calculado solamente sobre un subconjunto (**ClearToken** dentro de **CryptoToken**) del mensaje RAS/H.225.0. La autenticación solamente puede se útil para la autenticación de extremo a extremo verdadera (véase la cláusula 9). Se utilizan como subconjunto los siguientes campos de la estructura **ClearToken**:

- **tokenOID**: Hay un identificador de objeto de testigo separado (tokenOID "B") para la implementación de la autenticación solamente.
- **random**: El número secuencial monotónicamente creciente.
- **timeStamp**: La indicación de tiempo.
- **generalID**: El identificador del receptor (sólo en el caso de mensajes unidifusión). En el caso salto por salto, es el identificador del salto siguiente; en el caso de extremo a extremo, es el identificador de punto extremo del extremo lejano.
- **sendersID**: El identificador del emisor.
- **dhkey**: Los parámetros Diffie-Hellman. Este campo y subcampos se utilizan durante los mensajes **Setup** a **Connect**.

El autenticador se calcula sobre el **ClearToken** dentro del **EncodedGeneralToken** (es decir, el **ClearToken**) del **token** del **cryptoSignedToken**. La firma digital deberá calcularse sobre la cadena de bits codificada en ASN.1 de **ClearToken**. Antes del cálculo de la firma digital, el **tokenOID** del **ClearToken** deberá ponerse a {0 0}.

11 Autenticación e integridad

El procedimiento aplicado para la autenticación e integridad de mensajes sobre todos los campos del mensaje codificado en ASN.1 (utilizando el OID "A") es el siguiente.

El emisor de un mensaje deberá calcular la firma como sigue:

1) Fijará el valor de firma a un esquema por defecto específico de una longitud fija (por ejemplo 1024 bits). Este paso reservará espacio para la longitud máxima de una firma digital que es posible para un certificado determinado. El esquema exacto de bits no

importa, pero constituye una buena elección un esquema de bits exclusivo que no ocurra en el resto del mensaje.

2) Codificará en ASN.1 el mensaje completo; para RAS, esto incluirá el mensaje completo RAS H.225.0; para la señalización de llamada, el mensaje completo de señalización de llamada H.225.0.

3) Localizará el esquema por defecto en el mensaje codificado; sobrescribirá todo el esquema de bits construido con bits cero.

   NOTA 1 – Esto puede implicar algunos pasos de prueba y error en el caso poco frecuente de que el esquema por defecto aparezca más de una vez en el mensaje.

4) Calculará la firma digital después de la decodificación del mensaje en ASN.1 aplicando el método indicado por **algorithmOID** "V" o "W" (véase la cláusula 12).

5) Sustituirá el esquema por defecto en el mensaje codificado por el valor de firma digital calculado. Si la firma digital es más corta que el espacio reservado, deberán colocarse ceros delanteros antes de los bits más significativos del valor de firma.

El receptor recibe el mensaje y procede como sigue:

1) Decodifica en ASN.1 el mensaje.

2) Extrae el valor de la firma digital recibida y lo guarda en un SV variable local.

3) Busca y localiza el valor de firma SV en el mensaje codificado recibido.

   NOTA 2 – En las ocasiones poco frecuentes en que la subcadena del valor de firma puede aparecer varias veces en el mensaje completo, se han de repetir sucesivamente los pasos 3-6 con una posición de arranque de búsqueda diferente.

4) Sobrescribe el esquema de bits en el mensaje codificado todo con ceros.

5) Calcula la firma digital tras el mensaje codificado aplicando el método indicado por el **algorithmOID** "V" o "W" (véase la cláusula 12).

6) Compara SV con el valor de firma calculado. El mensaje sólo es considerado incorrupto y auténtico si ambos valores de firma son iguales; en este caso la autenticación ha tenido éxito y el procedimiento se detiene.

7) En caso contrario, repite los pasos 3-7 restableciendo SV a la situación anterior y busca otra concordancia. Si ninguna de las concordancias arroja una comparación correcta de los valores de firma, la autenticación ha fracasado y el mensaje ha sido alterado (accidental o deliberadamente) durante el tránsito o por algún otro motivo.

12 Cálculo de la firma digital

El valor de entrada del proceso de generación de firma digital es una cadena de bits codificada en ASN.1 que incluye el resultado del proceso de cálculo resumido del mensaje y la clave privada del firmante. Los detalles de la generación de la firma digital dependen del algoritmo de firma utilizado; el certificado determina el algoritmo de firma que ha de aplicarse; cuando la extensión de utilización de claves en el certificado está presente, el bit **digitalSignature** debe ser fijado para la clave deseable para la firma. El valor de firma generado por el firmante se codifica como una cadena de bits y es cursado en el campo **signature**.

Deberá utilizarse el método descrito en [PKCS #1, sección E.8.1.1] para el cálculo de una firma digital basada en RSA con apéndice (RSASSA-PKCS1-v1_5-SIGN) junto con los procedimientos OS2IP, RSASP1 y I2OSP y el método EMSA-PKCS1-v1_5-ENCODE.

13 Verificación de la firma digital

El valor de entrada del proceso de verificación de firma incluye el resultado del proceso de cálculo resumido del mensaje y la clave pública del firmante. El receptor puede obtener la clave pública correcta para el firmante por cualquier medio, pero el método preferido consiste en la obtención de un certificado a partir del campo **certificate** y la validación posterior utilizando el número generador del certificado del firmante. La validación de la clave pública del firmante puede basarse en el procesamiento del trayecto de certificación (RFC 3280). Los detalles de la verificación de firma dependen del algoritmo de firma empleado.

Deberá utilizarse el método descrito en [PKCS #1, sección E.8.1.2] para la verificación de una firma digital basada en RSA con apéndice (RSASSA-PKCS1-v1_5-VERIFY) junto con los procedimientos OS2IP, RSAVP1 y I2OSP y el método EMSA-PKCS1-v1_5-ENCODE.

14 Tratamiento de los certificados

Para la verificación de las firmas digitales, la entidad receptora debe tener acceso al certificado del emisor que está firmado por una autoridad de certificación (CA, *certification authority*) reconocida. El receptor puede acceder al certificado del emisor de varias formas:

- El certificado está incluido en el intercambio de mensajes como se describe en los procedimientos II y III; en este caso **certificate** contiene el certificado propiamente dicho y **type** contiene el OID "V" o el OID "W".
- El receptor conoce el certificado, que posiblemente se ha almacenado en local desde un intercambio anterior.
- En vez de incluir el certificado propiamente dicho, el emisor proporciona una URL en la cual donde puede hallarse el certificado. A este fin, **certificate** contiene la URL y **type** es fijado al OID "P".
- El receptor obtiene el certificado por otros medios distintos a los de la presente Recomendación (por ejemplo, por consulta al directorio LDAP).

Siempre que se transporte un certificado digital en un mensaje, la entidad receptora (controlador de acceso o punto extremo) verificará si la identidad del remitente (controlador de acceso o punto extremo) coincide con la identidad presente en el certificado, para evitar ataques intermedios.

En el caso de los mensajes con firma digital enviados desde un controlador de acceso hasta un punto extremo, existen varias posibilidades para que éste verifique la identidad de aquél. A saber:

– Si se dispone del hostname, por ejemplo en el atributo de nombre común del campo subject o del campo subjectAltName en el certificado, el punto extremo puede verificar si este hostname coincide con el identificador del controlador de acceso. De igual manera, el punto extremo puede utilizar el DNS para averiguar la dirección IP correspondiente y compararla con la dirección IP del controlador de acceso que ha sido presentada en el mensaje de respuesta firmado por éste.

– Por ejemplo, se puede construir el identificador de controlador de acceso concatenando la dirección IP (representada como un valor de 4 bytes en el orden de bytes de red) con otra información que identifique al controlador de acceso, truncado al valor de la longitud máxima del campo ID del remitente (senders_ID), que transporta la identidad del controlador de acceso. Asimismo, el punto extremo puede verificar si la dirección IP que pertenece al hostname coincide con la presentada en el encabezamiento de IP de la respuesta del controlador de acceso.

  NOTA – Es probable que este método no funcione como se espera cuando se utilicen mecanismos de traducción de dirección de red (NAT, *network address translation*).

– Si no aparece el hostname en el certificado, se tomará directamente la dirección IP que debería ser parte de dicho certificado (*iPAddress subjectAltName*), a fin de efectuar las pruebas antes mencionadas.

Los usuarios deberían estudiar con cuidado el certificado presentado por el controlador de acceso para decidir si satisface sus expectativas. Cuando el punto extremo tenga información externa del tipo de identidad esperada del controlador de acceso, se puede omitir la verificación del hostname. Por ejemplo, puede ocurrir que aunque un punto extremo se esté conectando a un controlador de acceso cuya dirección y hostname sean dinámicos, ya conozca el certificado que éste presentará. En dichos casos, conviene disminuir tanto como se pueda el alcance de los certificados que pueden ser aceptados, a fin de evitar ataques intermedios. En casos especiales, puede ser conveniente que el punto extremo simplemente ignore la identidad del controlador de acceso, aunque esto implique dejar la conexión abierta a ataques activos.

Cuando el hostname no equivalga a la identidad presente en el certificado, los puntos extremos orientados al usuario notificarán a éste (pueden darle la oportunidad de continuar con la conexión en cualquier caso) o terminarán la conexión con un error certificado incorrecto. Los puntos extremos automatizados registrarán el error en un registro auditor (si se dispone de él) adecuado y deberían terminar la conexión (con un error certificado incorrecto).

Si bien los puntos extremos automatizados pueden proporcionar una configuración que inhabilite esta verificación, deberán en todo caso proveer una que la habilite.

De igual manera, se recomienda que el controlador de acceso efectúe una verificación de la de identidad de cualquier mensaje con firma digital que haya recibido del punto extremo. Cómo se efectúa concretamente dicha verificación es asunto local y debería estar sujeto a la implementación de la política de seguridad del controlador de acceso. Por ejemplo, se puede pensar que un nombre de usuario transportado dentro del certificado puede también formar parte del identificador H.323. Más aún, el controlador de acceso puede verificar si dicha información de identidad corresponde con los datos de usuario administrado/configurado localmente, si los hubiere, y puede basar en ello una decisión relacionada con política.

Cuando el controlador de acceso tenga información externa sobre la identidad esperada del punto extremo, se puede omitir la verificación de hostname. Por ejemplo, puede ocurrir que un controlador de acceso se esté conectando a un punto extremo cuyos dirección y hostname sean dinámicos, pero para el que ya conoce el certificado que será presentado. En tales casos, es importante reducir tanto como se pueda el alcance de los certificados aceptables, a fin de evitar ataques intermedios. En casos especiales, puede convenir que el controlador de acceso ignore simplemente la identidad del punto extremo, aunque esto deba implicar que se deja la conexión abierta a ataques activos.

Cuando el hostname no corresponda con la identidad presentada en el certificado, el controlador de acceso registrará el error en un registro cronológico de auditoría adecuado (si lo hubiere) y debería terminar la conexión (con un error certificado incorrecto).

Cuando haya una extensión subjectAltName de tipo dNSName, se la utilizará como identidad. De lo contrario, se utilizará el campo Common Name (más específico) en el campo Subject del certificado. Aunque se acostumbre utilizar el Common Name, no se aconseja y las autoridades de certificación insisten en que debe utilizarse en su lugar el dNSName.

La correspondencia se efectuará conforme a las reglas especificadas en RFC 3280. Cuando haya más de una identidad de un tipo determinado en el certificado (por ejemplo, más de un nombre dNSName), se considera aceptable una correspondencia en cualquiera de los elementos del conjunto. Los nombres pueden incluir el carácter comodín (wildcard) * que se supone corresponde a cualquier nombre único de dominio a cualquier componente o fragmento de componente de nombre único de dominio. Por ejemplo, *.a.com corresponde a foo.a.com, mas no a bar.foo.a.com. De igual manera f*.com corresponde a foo.com, más no a bar.com.

Los procedimientos II y III proporcionan los medios para transportar un certificado digital. En aras de la eficacia, los certificados digitales de las entidades no deberán transmitirse más de una vez, si no están ya disponibles en las entidades por otros medios distintos de los de esta Recomendación. Por tanto, el intercambio de certificados debería producirse solamente al principio del establecimiento de una comunicación: para RAS, esto sucede durante el descubrimiento del controlador de acceso o, si esta fase se omite, durante el registro del controlador de acceso. Ocurre de manera análoga en la conexión rápida, donde el certificado puede ser incluido en los mensajes de señalización de llamada iniciales pero ser omitido sin riesgo en los mensajes de señalización de llamada posteriores.

Para este perfil de seguridad se deberá utilizar el certificado X.509v3 (1997). Otros formatos de certificado quedan en estudio.

15 Ilustración del empleo del procedimiento II

Considérese el caso de la figura 2, donde cada entidad tiene su propio certificado/par de clave pública-clave privada. Una entidad puede tener múltiples pares de claves. En la figura, un apoderado H.323 separa EP1 de GK1.

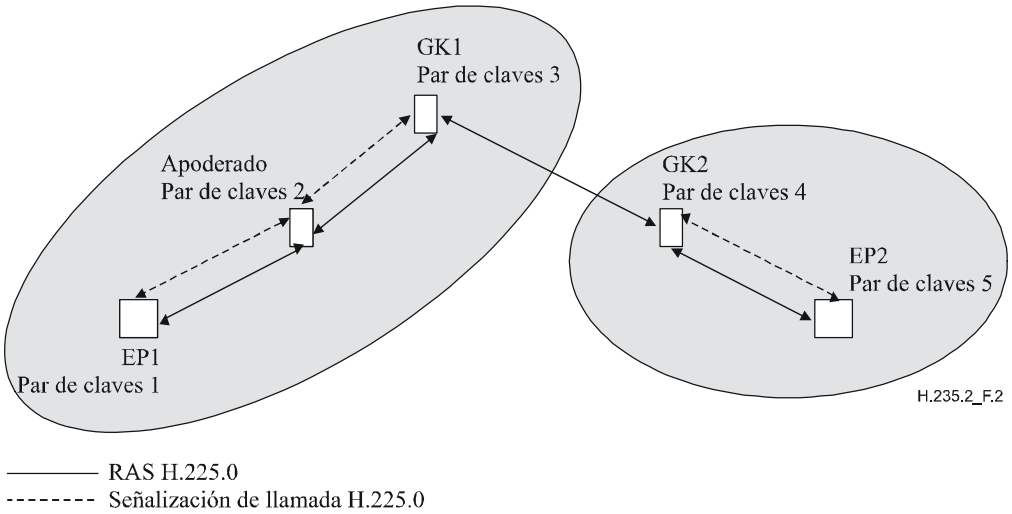

Figura 2/H.235.2 – Ilustración de la utilización de claves públicas en un modelo encaminado por GK-GK

El apoderado H.323 actúa doblemente: Por un lado, el apoderado finaliza la autenticación e integridad de cada una de sus ramas. El apoderado incluye, en tiempo real, la información de autenticación/integridad calculada recientemente en los mensajes RAS de salida, de un modo análogo al descrito en el procedimiento I de H.235.1. Por otro lado, el apoderado permite que la información de seguridad de extremo a extremo pase sin modificación. Sin embargo, el apoderado puede verificar los certificados recibidos y/o las firmas digitales en tránsito.

Más adelante se dan los detalles del procedimiento para la autenticación, integridad y no repudio de mensajes RAS, de señalización de llamada H.225.0 y H.245.

15.1 Autenticación, integridad y no repudio de mensajes RAS

Considérese el caso de una comunicación salto por salto donde EP1 desea enviar un mensaje RAS, por ejemplo, un mensaje **ARQ** a GK1. EP1 genera una indicación de tiempo y un número secuencial y los incluye en los campos **timeStamp** y **random** respectivamente, junto con el alias del apoderado en el campo **generalID** y el **sendersID** de EP1. Estos campos están presentes en el campo **ClearToken** del **EncodedGeneralTokens** presente en el **token** del **cryptoSignedToken** del

campo **CryptoToken** del **cryptoH323Token** del mensaje **ARQ**. Este **cryptoH323Token** es uno de, por lo menos, varios testigos de la secuencia **cryptoTokens**. El **tokenOID** dentro del **cryptoSignedToken** será "A" para indicar que todos los campos del mensaje **ARQ** están firmados. El **token** en **cryptoSignedToken** tiene el **algorithmOID** puesto a "V", indicando que se utiliza MD5-RSA, o el **algorithmOID** puesto a W", indicando que se utiliza SHA1-RSA, y **params** puesto a NULO. EP1 calcula entonces la firma basada en el algoritmo de firma dado utilizando su clave privada. La firma se calcula sobre todos los campos del mensaje **ARQ** cuando el **tokenOID** es "A". EP1 incluye la firma calculada dentro de **signature** en el campo **token** del campo **cryptoSignedToken** del **CryptoToken** presente en el **cryptoH323Token** del mensaje **ARQ** e incluye su certificado en el campo **certificate**.

De manera análoga, en la comunicación de extremo a extremo a través de un apoderado, EP1 genera otro **CryptoToken** con una firma digital que cubre determinados campos críticos (véase la cláusula 9) en el **ClearToken** del mensaje **ARQ**. El **tokenOID** en el **CryptoSignedToken** será "B" para indicar la autenticación solamente de este **ClearToken**; **tokenOID** en el **ClearToken** es "R", indicando la autenticación de extremo a extremo. Asimismo **timeStamp**, **random**, **sendersID**, **generalID** y, en el caso de que éste sea un **SETUP/CONNECT**, también **dhkey**, fijan en **token** los siguientes campos: **algorithmOID** a "V" o "W", indicando el algoritmo de firma, **params** a NULO y **signature** a la firma digital calculada sobre los campos **ClearToken**. El **certificate** transporta el certificado digital de EP1. El mensaje **ARQ** es entonces enviado al apoderado.

Tras la recepción del mensaje **ARQ**, el apoderado verifica la firma de los testigos que están dirigidos a él (en este caso, por ejemplo, los que tienen un **tokenOID** "A"). Esta verificación se basa en varios criterios, que incluyen:

- Actualidad de la identificación de tiempo y unicidad de **random**.
- Identidad del **generalID** e identificador propio.
- Autorizaciones de acceso para los **sendersID**.
- Concordancia de la firma del mensaje **ARQ** con la firma calculada por GK1.
- Verificación de los parámetros Diffie-Hellman, por ejemplo, comprobando si el primo de 1024 bits y el generador son correctos. La comprobación de la seguridad de los parámetros DH se realiza al terminar el proceso, y sólo puede efectuarse cuando la política local lo requiere.
- Verificación del certificado recibido.

Si la verificación de la firma ha tenido éxito, el apoderado calcula una nueva firma para insertarla (sustituirla) en el mensaje **ARQ** antes de reenviar éste al GK1 como sigue. El apoderado sustituye los campos **timeStamp**, **random**, **sendersID** y **generalID** en el campo **ClearToken** (**toBeSigned**) utilizando valores pertinentes a la rama apoderado GK1. El campo **timestamp** contiene la indicación de tiempo actual, el campo **random** contiene el siguiente número secuencial monotónicamente creciente para la rama apoderado GK1, el **sendersID** del apoderado y el campo **generalID** contienen el alias de GK1. El apoderado calcula entonces una nueva firma para este mensaje **ARQ** utilizando su clave privada y el algoritmo de firma, la inserta en **signature** dentro de **token** y añade su **certificate**. El apoderado incluye también el **CryptoToken** de extremo a extremo recibido con su **ClearToken** en el nuevo mensaje saliente y pasa el mensaje **ARQ** al GK1. La firma, calculada por EP1 basándose en campos seleccionados del mensaje **ARQ** (**tokenOID** de "B") y que no estaba destinada al apoderado, se envía también a GK1 sin modificación en el mensaje **ARQ**.

Tras la recepción del mensaje **ARQ**, GK1 verifica las firmas, calcula una nueva firma después de modificar adecuadamente los campos **ClearToken** en el **toBeSigned**, la inserta en el campos **signature**, añade su **certificate** y pasa el mensaje **Setup** al EP2. Nuevamente, GK1 debe enviar cualquier información de extremo a extremo recibida en el **CryptoTokens** separado al par GK2 mediante la inclusión de esta información en un **CryptoToken** separado sin modificar.

15.2 Autenticación solamente de mensajes RAS

Considérese el caso de una comunicación salto por salto donde EP1 desea enviar un mensaje RAS, por ejemplo, un mensaje **ARQ** a GK1. EP1 genera una indicación de tiempo y un número secuencial y los incluye en los campos **timeStamp** y **random** respectivamente, junto con el alias del apoderado en el campo **generalID** y el id de EP en el **sendersID**. Estos campos están presentes en el campo **ClearToken** del **toBeSigned** presente en el **token** de **cryptoSignedToken** del campo **CryptoToken** del **cryptoH323Token** del mensaje **ARQ**. El **tokenOID** dentro del **cryptoSignedToken** será "B" para indicar que solamente los campos del subconjunto especificado en el **ClearToken** están firmados. El **token** en **cryptoSignedToken** tiene el **algorithmOID** puesto a "V", para indicar la utilización de MD5-RSA, o a "W", indicando la utilización del algoritmo de firma SHA1-RSA y **params** puesto a NULO. EP1 calcula entonces la firma basada en el algoritmo de firma utilizando su clave privada. La firma se calcula sobre los campos **ClearToken** especificados del mensaje **ARQ**. EP1 incluye la firma calculada dentro de **signature** en el campo **token** del campo **cryptoSignedToken** del **CryptoToken** presente en el **cryptoH323Token** del mensaje **ARQ** y añade su **certificate**.

De manera análoga, EP1 genera otra firma digital para la autenticación de extremo a extremo que cubre determinados campos **ClearToken** en un **CryptoToken** separado en el mensaje **ARQ**. Se incluye esta firma digital (identificada por el **tokenOID** "V" o "W"). El mensaje **ARQ** es enviado entonces al apoderado.

Tras la recepción del mensaje **ARQ**, el apoderado verifica la firma de los testigos que están dirigidos a él (en este caso, por ejemplo, los que tienen un **tokenOID** "B"). Esta verificación se basa en varios criterios que incluyen:

- Actualidad de la identificación de tiempo y unicidad de **random**.
- Identidad del **generalID** e identificador propio.
- Autorizaciones de acceso para los **sendersID**.
- Concordancia de la firma del mensaje **ARQ** con la firma calculada por GK1.
- Verificación del certificado recibido.

Si la verificación de la firma ha tenido éxito, el apoderado calcula una nueva firma para insertarla (sustituirla) en el mensaje **ARQ** antes de reenviar éste al GK1 como sigue. El apoderado reemplaza los campos **timeStamp**, **random**, **sendersID** y **generalID** en el campo **ClearToken** de **toBeSigned** utilizando valores pertinentes a la rama apoderado GK1. El campo **timeStamp** contiene la indicación de tiempo actual, el campo **random** contiene el siguiente número secuencial monotónicamente creciente para la rama apoderado GK1 y el campo **generalID** contiene el alias de GK1. El apoderado calcula entonces una nueva firma para este **ClearToken** utilizando su clave privada y el algoritmo de firma MD5-RSA o SHA1-RSA (**algorithmOID** = "V" o "W"), la inserta en **signature** dentro de **token** de **cryptoSignedToken**, añade su **certificate** y pasa el mensaje **ARQ** al GK1. La firma calculada por EP1 basándose en campos **ClearToken** seleccionados del mensaje **ARQ** (**tokenOID** de "B") y que no estaba destinada al apoderado, se envía también a GK1 sin modificación en el mensaje **ARQ**.

Tras la recepción del mensaje **ARQ**, GK1 verifica la firma, calcula una nueva firma después de la modificación adecuada de los campos **ClearToken** en **toBeSigned**, la inserta en el campo **signature** y pasa el mensaje **Setup** al EP2. La información de firma de extremo a extremo del EP1 es incluida sin modificación en el mensaje **Setup**.

15.3 Autenticación, integridad y no repudio de mensajes H.225.0

El procedimiento aplicable a los mensajes H.225.0 es idéntico al de los mensajes RAS. La única diferencia estriba en que el conjunto de campos que han de firmarse ha de ser identificado para cada mensaje de señalización de llamada H.225.0 cuando el **tokenOID** está puesto a "B".

15.4 Autenticación e integridad de los mensajes H.245

Considérese el caso en que EP1 desea enviar un mensaje H.245, por ejemplo, un mensaje **TerminalCapabilitySet**, a EP2. EP1 comprueba si se necesita enviar un mensaje H.225.0 al apoderado. En caso afirmativo, el mensaje H.245 es tunelizado dentro de este mensaje H.225.0. Los campos en el mensaje H.225.0 son fijados del modo descrito anteriormente para la transmisión de un mensaje H.225.0. Puesto que el mensaje H.245 es tunelizado, **h323-uu-pdu** en el mensaje **h323-UserInformation** tiene sus campos fijados como sigue:

- en el campo **h323-message-body** se indica el tipo de mensaje H.225.0 que se está transmitiendo.
- **h245Tunnelling** se pone a VERDADERO (TRUE).
- **h245Control** contiene la cadena de octetos PDU H.245.

Sin embargo, si no hay pendiente ninguna transmisión de mensaje H.225.0, se tuneliza el mensaje H.245 dentro de un mensaje **facility** H.225 ad-hoc. La **h323-uu-pdu** en el mensaje **h323-UserInformation** tiene sus campos fijados como sigue:

- en el campo **h323-message-body** se indica **facility** que contiene:
  - **reason** puesto a **undefinedReason**;
  - **tokens** y **cryptoTokens** fijados como para cualquier mensaje H.225.0.
- **h245Tunnelling** puesto a VERDADERO (TRUE).
- **h245Control** contiene la cadena de octetos PDU H.245.

A continuación EP1 transmite el mensaje **facility** al apoderado.

En cualquiera de los dos casos (si está pendiente la transmisión de un mensaje H.225.0 ó si se utiliza un mensaje **facility** H.225.0 ad hoc), el apoderado verifica la firma destinada para él (representada en este caso por el **tokenOID** "A") tras la recepción del mensaje. A continuación, si está pendiente la transmisión de un mensaje H.225.0 para la rama apoderado GK1, el mensaje H.245 es tunelizado dentro de este mensaje; en caso contrario, es tunelizado dentro de un mensaje **facility** H.225.0 ad hoc. Como en el caso de la transmisión de un mensaje de señalización de llamada H.225.0, se calcula una nueva firma para el mensaje H.225.0 antes de su transmisión desde el apoderado al GK1. La firma que fue enviada desde el EP1 al apoderado y que no estaba destinada a este último es transferida del apoderado al GK1 sin modificación.

En esta cláusula se resumen el procedimiento y los métodos que utiliza el perfil de firmas para asegurar los distintos mensajes de señalización H.323.

16 Compatibilidad con la versión 1 de H.235

Si bien estos perfiles de seguridad se han desarrollado pensando en H.235 versión 2 (Rec. UIT-T H.235v2), se pueden también aplicar a H.235 versión 1 (Rec. UIT-T H.235v1] con algunas modificaciones menores. El receptor puede detectar la presencia de la versión de protocolo H.235 del emisor mediante la evaluación de los identificadores de objeto del perfil de seguridad (véase la cláusula 20).

Implementaciones conformes a H.235 versión 1 (Rec. UIT-T H.235v1]:

- no determinar ni analizar el **sendersID** en el **ClearToken**.

17 Comportamiento multidifusión

Los mensajes multidifusión H.225.0, tales como **GRQ** o **LRQ** deberán incluir un **CryptoToken** de conformidad con los procedimientos II y III, donde el **generalID** no está fijado. Cuando tales mensajes son enviados en unidifusión, el mensaje incluirá un **CryptoToken**.

18 Lista de mensajes de señalización seguros

18.1 RAS H.225

Mensaje RAS H.225.0	Campos de señalización H.235	Autenticación solamente	Autenticación e integridad	No repudio
Cualquiera	cryptoTokens	Procedimiento II/III	Procedimiento II/III	Procedimiento II/III

NOTA – Para los mensajes de unidifusión, se deberán aplicar los procedimientos II y III con los campos de seguridad en el **CryptoToken** utilizado.

18.2 Señalización de llamada H.225.0

Mensaje de señalización de llamada H.225.0	Campos de señalización H.235	Autenticación solamente	Autenticación e integridad	No repudio
UUIE Aviso, UUIE Llamada en curso, UUIE Conexión, UUIE Establecimiento, UUIE Facilidad, UUIE Progresión, UUIE Información, UUIE Liberación completa Estado UUIE Indagación de Estado UUIE Acuse de Establecimiento UUIE Notificación UUIE	cryptoTokens	Procedimiento II/III	Procedimiento II/III	Procedimiento II/III

19 Utilización de sendersID y generalID

El **ClearToken** incluye los campos **sendersID** y **generalID**. Cuando se dispone de información de identificación, el **sendersID** será el identificador del controlador de acceso (GKID) para los mensajes iniciados por el controlador de acceso y el identificador de punto extremo (EPID) para los mensajes iniciados por el punto extremo. Cuando se dispone de información de identificación, el **generalID** será el GKID para los mensajes iniciados por el punto extremo y el EPID para los mensajes iniciados por el controlador de acceso. Cuando no se dispone de información de identificación o cuando la radiodifusión/multidifusión es ambigua, no se incluirá el campo o se incluirá con una cadena nula. El cuadro 2 resume la situación:

Cuadro 2/H.235.2 – Utilización de los identificadores sendersID y generalID

Message	sendersID	generalID
GRQ unidifusión	**EPID** si está disponible, en su defecto **NULL**	**GKID**
GRQ multidifusión	**EPID** si está disponible, en su defecto **NULL**	
GCF, GRJ	**GKID**	**EPID** si está disponible, en su defecto **NULL**
RRQ inicial		**GKID**
RCF	**GKID**	**EPID**
RRJ	**GKID**	
URQ, UCF, URJ, BRQ, BCF, BRJ, DRQ, DCF, DRJ, NSM, RIP, SCI, SCR, XRS (EP a GK)	**EPID**	**GKID**
URQ, UCF, URJ, BRQ, BCF, BRJ, DRQ, DCF, DRJ, NSM, RIP, SCI, SCR, XRS (GK a EP)	**GKID**	**EPID**
ARQ, IRQ, RAI	**EPID**	**GKID**
ACF, ARJ, BCF, LCF, LRJ, IRR, IRQ, RAC, LCF, LRJ, IACK, INAK	**GKID**	**EPID**
LRQ unidifusión (EP a GK)	**EPID**	**GKID**
LRQ unidifusión (GK a GK)	**GKID**	**GKID**
LRQ multidifusión	**EPID**	
NOTA – GKID es el identificador del controlador de acceso, EPID es el identificador de punto extremo. Un espacio en blanco equivale una cadena de identificación faltante o nula.		

20 Lista de identificadores de objeto

En el cuadro 3 se presenta una lista de todos los OID referenciados (véase también [OIW] y [WEBOID]). Hay identificadores de objeto para H.235v1 [H.235v1] y para H.235v2 [H.235v2].

Cuadro 3/H.235.2 – Identificadores de objeto

Referencia de identificador de objeto	Valor(es) del identificador de objeto	Descripción
"A"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 1} {itu-t (0) recommendation (0) h (8) 235 version (0) 1 1}	Utilizado en el procedimiento II para el CryptoToken-tokenOID; indica que la firma incluye **todos** los campos del mensaje RAS o de señalización de llamada H.225.0 (autenticación e integridad).
"B"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 2} {itu-t (0) recommendation (0) h (8) 235 version (0) 2 2} {itu-t (0) recommendation (0) h (8) 235 version (0) 1 2}	Utilizado en el procedimiento II para el CryptoToken-tokenOID; indica que la firma incluye un **subconjunto** de campos del mensaje RAS/H.225.0 (ClearToken) para terminales de autenticación solamente sin integridad. Utilizado en el procedimiento IA/H.235.1 del anexo D para el CryptoToken-tokenOID; indica que el número generador incluye un subconjunto de campos en el mensaje RAS/H.225.0 (ClearToken) para terminales con sólo autenticación y sin integridad.
"P"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 4} {itu-t (0) recommendation (0) h (8) 235 version (0) 1 4}	Utilizado en los procedimientos II o III para indicar que el campo **certificate** transporta una URL.
"R"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 3} {itu-t (0) recommendation (0) h (8) 235 version (0) 1 3}	Utilizado en el procedimiento II para el ClearToken-tokenOID; indica que el ClearToken está siendo utilizado para la autenticación/integridad de extremo a extremo.
"S"	{itu-t (0) recommendation (0) h (8) 235 version (0) 2 7} {itu-t (0) recommendation (0) h (8) 235 version (0) 1 7}	Utilizado en el procedimiento II, este OID de testigo indica la autenticación, integridad y no repudio del mensaje.
"V"	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 4}	Utilizado en los procedimientos II o III como OID de algoritmo; indica el empleo de la firma digital MD5 RSA.
"W"	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}	Utilizado en los procedimientos II o III como OID de algoritmo; indica el empleo de la firma digital SHA1 RSA.

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	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
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, comunicaciones de sistemas abiertos y seguridad
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, 2006