Unión Internacional de Telecomunicaciones

UIT-T H.235.5

(09/2005)

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

SERIE H: SISTEMAS AUDIOVISUALES Y MULTIMEDIOS

Infraestructura de los servicios audiovisuales – Aspectos de los sistemas

Marco de seguridad H.323: Marco para la autenticación segura en RAS utilizando secretos compartidos débiles

Recomendación UIT-T H.235.5

UIT-T

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.235.5

Marco de seguridad H.323: Marco para la autenticación segura en RAS utilizando secretos compartidos débiles

Resumen

Esta Recomendación proporciona el marco para la autenticación mutua de las partes durante intercambios RAS H.255.0. Los métodos "prueba-de-posesión" aquí descritos permiten proteger el uso de secretos compartidos tales como contraseñas que, si se utilizaran solas, no proporcionarían seguridad suficiente.

Se describen también extensiones al marco para permitir la negociación simultánea de parámetros de seguridad de la capa de transporte para la protección de un canal conexo de señalización de llamada.

En las versiones anteriores de la subserie H.235, este perfil figuraba en el anexo H de la Recomendación H.235. En los apéndices IV, V y VI a la H.235.0 figuran las tablas de correspondencia de cláusulas, figuras y cuadros entre las versiones 3 y 4.

Orígenes

La Recomendación UIT-T H.235.5 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, contraseña, seguridad.

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 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

Introducción

En muchas aplicaciones, un punto extremo (o su usuario) y su controlador de acceso pueden compartir solamente un "pequeño" secreto como una contraseña o un número de identificación personal (PIN). Ese secreto (que en adelante se designará por "contraseña"), y toda clave de criptación derivada del mismo, es criptográficamente débil. Los esquemas de autenticación descritos en la cláusula 10 son ejemplos de texto explícito y el correspondiente texto cifrado de la solicitación y la respuesta, que están expuestas a ataques exhaustivos de parte de un observador de la transacción cuando las autenticaciones se introducen por contraseñas simples. Por tanto, el observador puede recuperar la contraseña y o PIN y después hacerse pasar como el punto extremo para obtener el servicio.

Hay varios protocolos del tipo de intercambio de clave criptada, que utilizan un secreto compartido para "oscurecer" un intercambio con clave Diffie-Hellman de tal manera que el atacante tenga que resolver una serie de problemas de logaritmo finito para validar un ataque exhaustivo contra el secreto compartido. En el intercambio de clave criptada (EKE, *encrypted key exchange*) de Bellovin y Merritt [B&M], el secreto compartido se utiliza para criptar las claves públicas Diffie-Hellman con un algoritmo simétrico. En el método de intercambio de clave exponencial con contraseña simple (SPEKE, s*imple password exponential key exchange*) de Jablon [Jab], el secreto compartido se utiliza para elegir un generador diferente del grupo Diffie-Hellman. Estos protocolos combinan la seguridad de un intercambio de claves Diffie-Hellman fuertes con el uso del secreto compartido, de tal manera que un atacante no pueda obtener un texto simple conocido y utilizarlo en un ataque exhaustivo contra el secreto sin haber resuelto el problema de logaritmo finito de Diffie-Hellman. Una ventaja de esos protocolos es que multiplican la fuerza criptográfica del problema Diffie-Hellman por la fuerza de la criptación de la clave secreta (o viceversa). Una desventaja potencial es que están típicamente sujetos a la protección de patentes.

Recomendación UIT-T H.235.5

Marco de seguridad H.323: Marco para la autenticación segura en RAS utilizando secretos compartidos débiles

1 Alcance

Esta Recomendación puede utilizarse en todo controlador de acceso o punto extremo que emplee los protocolos RAS 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 comunicación multimedios por paquetes.*

– 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.245 (2005), *Protocolo de control para comunicación multimedia*.

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

– Federal Information Processing Standard FIPS PUB 180-2, *Secure Hash Standard*, U.S. Department of Commerce, Technology Administration, National Institute of Standards and Technology, 1 de agosto de 2002.

– NIST Special Publication 800-38A 2001, *Recommendation for Block Cipher Modes of Operation – Methods and Techniques*. http://www.csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf.

2.2 Referencias informativas

[AES] IETF RFC 3268 (2002), *Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security*.

[B&M] BELLOVIN (S.), MERRITT (M.): U.S. Patent 5,241,599, 31 de agosto de 1993, 1993, originally assigned to AT&T Bell Laboratories, now assigned to Lucent Technologies.

[Jab] JABLON (D.): Strong Password-Only Authenticated Key Exchange, *Computer Communication Review*, ACM SIGCOMM, Vol. 26, No. 5, pp. 5-26, octubre de 1996.

[NIST SP 800-57] NIST Draft Special Publication 800-57 (2005), *Recommendation for Key Management, Part 1: General Guideline*. http://www.csrc.nist.gov/publications/drafts/draft-800-57-Part1-April2005.pdf

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

[RFC2412] IETF RFC 2412 (1998), *The OAKLEY Key Determination Protocol*.

[RFC2246] IETF RFC 2246 (1999), *The TLS Protocol Version 1.0*.

[RFC3546] IETF RFC 3546 (2003), *Transport Layer Security (TLS) Extensions*.

3 Definiciones

Ninguna.

4 Abreviaturas, siglas o acrónimos

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

ACF Confirmación de admisión (*admission confirm*)

AES Norma de criptación avanzada (*advanced encryption standard*)

ARJ Rechazo de admisión (*admission reject*)

ARQ Petición de admisión (*admission request*)

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

CTR Modo contador (*counter mode*) (véase NIST SP 800-38A)

DH Diffie-Hellman

EKE Intercambio de claves criptadas (e*ncrypted key exchange*)

GCF Confirmación de controlador de acceso (*gatekeeper confirm*)

GK Controlador de acceso (*gatekeeper*)

GRJ Rechazo de controlador de acceso (*gatekeeper reject*)

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

HMAC Código de autenticación de mensaje troceado (*hashed message authentication code*)

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

ID Identificador (*identifier*)

LCF Confirmación de localización (*location confirm*)

LRJ Rechazo de localización (*location reject*)

LRQ Petición de localización (*location request*)

MIM Hombre-en-el-medio (*man-in-the-middle*)

OID Identificador de objeto (*object identifier*)

PIN Número de identificación personal (*personal identification number*)

PRF Función seudoaleatoria (*pseudo-random function*)

RAS Registro, admisiones y estado (*registration, admissions and status*)

RCF Confirmación de registro (*registration confirm*)

RFC Petición de comentarios (*request for comments*)

RRJ Rechazo de registro (*registration reject*)

RRQ Petición de registro (*registration request*)

SHA1 Algoritmo de generación numérica seguro N.º 1 (*secure hash algorithm 1*)

SPEKE Intercambio de clave exponencial de contraseña simple (*simple password exponential key exchange*)

TLS Seguridad de nivel de transporte (*transport level security*)

UDP Protocolo de datagrama de usuario (*user datagram protocol*)

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.

En la cláusula 5/H.235.0 se indican otros convenios.

6 Marco básico

6.1 Capacidades de negociación mejoradas en H.235.0

En la Rec. UIT-T H.235.0 se consigue este marco de seguridad incorporando el siguiente elemento genérico al **ClearToken**:

• **profileInfo** es una secuencia de elementos específicos del perfil, identificados cada uno de ellos por su propio valor entero definido por el perfil específico cuyo OID es transportado en el **ClearToken.tokenOID**.

En las siguientes descripciones se pasan en **profileInfo** varios elementos; para facilitar el análisis, a cada uno de estos elementos se le dará un nombre, en vez de un valor identificador.

6.2 Utilización entre punto extremo y controlador de acceso

No plantea problemas el marco básico, en el cual el solicitante es un punto extremo que desea inscribirse ante un controlador de acceso, y el respondedor es ese controlador de acceso. En adelante se supone implícitamente que cada **ClearToken** mencionado se identifica con el **tokenOID** del perfil de identificación. Se supone que el **ClearToken** está extendido. Los elementos **random** y/o **random2** pueden ser utilizados por un perfil de una de estas dos maneras: pueden ser incluidos en el cálculo de la clave de autenticación, y/o pueden incluirse en un **ClearToken** de perfil en cada mensaje RAS subsiguiente (por ejemplo, RRQ/RCF) para evitar ataques por reproducción. El intercambio de registro de punto extremo se efectúa como sigue:

1) El punto extremo anuncia su intención de participar en uno o más esquemas de negociación y autenticación de claves incluyendo el (los) ID de objeto apropiados para el perfil o perfiles deseados en elementos **authenticationMechanism.keyExch** del elemento **authenticationCapability** de la **G**atekeeper**R**e**Q**uest. Se supone que cada OID específico define completamente un procedimiento de autenticación en términos de un sistema de claves públicas (por ejemplo, Diffie-Hellman o curva elíptica) y un grupo específico (por ejemplo, uno de los grupos OAKLEY de RFC 2412), algoritmo de criptación simétrico (por ejemplo, AES-128-CBC con robo de texto cifrado), función de derivación de clave (por

ejemplo, mediante la función seudoaleatoria de la cláusula 10/H.235.0), código de autenticación de mensajes (por ejemplo, HMAC-SHA1-96 [RFC 2104]), y la secuencia en que se utilizan. El punto extremo incluye también uno o más **ClearToken** de perfil en la GRQ, cada uno de los cuales transporta el OID para el perfil específico ofrecido y el material de clave pública (criptado) en la forma siguiente:

a) **tokenOID** transporta el perfil OID como se ofrece en la **authenticationCapability** de la GRQ encapsulante.

b) **timeStamp** puede utilizarse para asegurar que la transacción está en curso y proteger contra los ataques por reproducción.

c) **password** no se utilizará para la contraseña efectiva.

d) **dhkey** transporta los parámetros de clave Diffie-Hellman, si se utilizan. El elemento **halfkey** encerrado se cripta como se especifica por el perfil seleccionado.

e) **challenge** no se requiere.

f) **random** lo suministra la parte iniciadora y se utiliza para prevenir ataques por reproducción.

g) **certificate** puede utilizarse si el intercambio de certificados forma parte del perfil.

h) **generalID** puede utilizarse si lo requiere el perfil.

i) **eckasdhkey** transporta los parámetros de clave por curva elíptica, si los utiliza el perfil. El elemento **public-key** encerrado debe criptarse como se especifica por el perfil.

j) **sendersID** puede especificarse conforme al perfil.

k) Es posible proporcionar el elemento **profileInfo**, **initVect** junto con el material de clave pública (criptado) (**dhkey** o **eckasdhkey**) si el perfil requiere un vector de inicialización para descriptación.

l) Si el iniciador desea utilizar material de clave derivado de un intercambio anterior, incluirá un elemento **profileInfo**, designado por **sessionID**, que contiene el identificador asignado durante el intercambio anterior. En este caso, **dhkey**, **eckasdhkey** y/o **initVect** no deben incluirse.

m) Si el iniciador desea establecer una sesión TLS para una conexión de señalización de llamada, puede incluir uno o más elementos **profileInfo** que contienen sucesiones cifradas TLS; el mensaje contendrá un solo conjunto de cifrado (la negociada previamente) si **sessionID** está presente.

n) Si el iniciador desea establecer una sesión TLS para señalización de llamada, puede incluir un elemento **profileInfo** que contiene una lista de métodos de compresión; sólo un método de compresión (el negociado previamente) deberá incluirse si **sessionID** está presente.

o) Pueden utilizarse más elementos **profileInfo** para todo parámetro adicional requerido por los procedimientos en el perfil.

2) Al recibir la GRQ, el controlador de acceso selecciona un perfil **AuthenticationMechanism** de la lista ofrecida, genera una clave privada adecuada, calcula la clave pública correspondiente, genera un vector de inicialización si se necesita para criptación simétrica utilizando la contraseña, cripta la clave pública, genera un ID de sesión único, y genera un número aleatorio, todo lo cual se codifica en un **ClearToken**. En función del perfil, los elementos del ClearToken se utilizan como sigue:

a) **tokenOID** transporta el OID de perfil correspondiente al **authenticationMethod** de la GCF encapsulante.

b) **timeStamp** puede utilizarse para asegurarse que la transacción está en curso y proteger contra ataques por reproducción.

c) **password** no se utilizará para la contraseña real.

d) **dhkey** transporta los parámetros Diffie-Hellman, si se utilizan. El elemento **halfkey** incluido se cripta como se especifica según el perfil seleccionado.

e) **challenge** se utiliza para transportar un vector de inicialización, si se requiere para criptación de clave como se especifica por el perfil, o puede utilizarse para transportar una cadena aleatoria que habrá de ser devuelta por el punto extremo para prevenir ataques por reproducción.

f) **random** puede contener el valor único, impredecible, suministrado por el solicitante para prevenir ataques por reproducción.

g) **certificate** puede utilizarse si el intercambio de certificados forma parte del perfil.

h) **generalID** puede utilizarse si lo requiere el perfil.

i) **eckasdhkey** transporta los parámetros de curva elíptica, si los utiliza el perfil. El elemento **public-key** incluido debe criptarse como se especifica según el perfil.

j) **sendersID** puede utilizarse como se especifica según el perfil.

k) **random** (o un elemento **profileInfo** adicional, designado por **random2**, si el perfil requiere que ambos números permanezcan en el intercambio de mensajes) debe contener un valor único, impredecible, suministrado por el respondedor para proteger contra ataques por reproducción.

l) **initVect** se suministra junto con el material de clave pública (criptada) (**dhkey** o **eckasdhkey**) si el perfil requiere un vector de inicialización para descriptación.

m) **sessionID** es un identificador único (para el controlador de acceso) utilizado para identificar esta sesión de registro. En el caso de ciertos perfiles puede utilizarse también como un ID de sesión TLS para establecimiento rápido de un canal de señalización de llamada protegido por TLS.

n) **profileInfo** puede utilizarse para todo parámetro adicional requerido por los procedimientos en el perfil.

El controlador de acceso calcula entonces el secreto compartido o clave maestra utilizando su clave privada y la clave pública (descriptado) a partir de la GCF; a partir de la clave maestra deduce las claves de criptación, las claves de autenticación y todo otro material necesario, de acuerdo con el perfil. El **C**lear**T**oken antes descrito se coloca en el mensaje **G**atekeeper**C**on**F**irm. La GCF debe ser verificada en su integridad y/o autenticada utilizando la clave de autenticación derivada, y después enviada al punto extremo. La autenticación/verificación de integridad puede devolverse de una de varias maneras, como se especifica según el perfil: mediante un elemento **profileInfo** específico del perfil, o mediante uno de los procedimientos especificados en la Rec. UIT-T H.235.1.

3) El punto extremo examina el **authenticationMechanism.keyExch** seleccionado de la GCF y extrae los parámetros del **ClearToken** identificado por el **tokenOID** correspondiente. El punto extremo selecciona entonces su clave privada, calcula la clave pública correspondiente, y selecciona todo otro parámetro requerido por el perfil. El punto extremo calcula después el secreto compartido o la clave maestra utilizando su clave privada y la clave pública (descriptada) a partir de la GCF; a partir de la clave maestra deduce las claves de criptación, claves de autenticación y todo otro material necesario, de acuerdo con el perfil. El punto extremo verificará entonces la integridad de la GCF. Si la verificación de la GCF fracasa, el punto extremo la descartará, junto con todo el material de clave derivado del mismo, y continuará en espera de un mensaje GRQ válido. Una recuperación de RAS estándar conducirá a una retransmisión de la GRQ y, es de suponer, a la recepción de una GCF conforme. Si tras unas pocas retransmisiones no se obtiene una respuesta exitosa, el punto extremo debe abandonar los intentos de registrarse e informar a su usuario que algo ha fallado. Obsérvese que cada GRQ enviada da a un impostor que se está haciendo pasar

por una pasarela una oportunidad más de adivinar la contraseña del usuario y de que su impostura sea validada por la aceptación de la GRQ. Si la verificación de integridad de la GCF tiene éxito, el punto extremo ha validado al controlador de acceso, y puede proceder a registrarse y, en el proceso, a autenticarse a sí mismo ante el controlador de acceso.

4) El punto extremo llena entonces un **ClearToken** con el **tokenOID** de perfil en una forma similar a la empleada por el controlador de acceso, antes descrita. Todo campo del testigo explícito de la GCF que el perfil considere como una solicitación debe incluirse en el **ClearToken**. Si así lo especifica el perfil para evitar ataques por reproducción, el **ClearToken** incluirá **random** y **random2** que se toman de la GCF recibida, como se ha expuesto antes. El **ClearToken** se coloca entonces en una **R**egistration **ReQ**uest que habrá de devolverse al controlador de acceso. El punto extremo debe luego autenticar el mensaje RRQ completo y enviarlo al controlador de acceso. A partir de este momento, el punto extremo no debe aceptar, ni tampoco enviar, mensajes RAS que no hayan sido autenticados por el perfil convenido, utilizando la clave de autenticación derivada del material de clave compartido.

5) El controlador de acceso recibe la RRQ, y utilizará el material de clave compartida para verificar su integridad cotejándola con la autenticación y la verificación de integridad incluidas. Si la verificación de la integridad fracasa, el controlador de acceso no tendrá en cuenta la RRQ recibida, y esperará una RRQ verificable. Si no llega ninguna, el punto extremo abandonará finalmente el intento de registro y volverá a la búsqueda de un controlador de acceso. Si la verificación de integridad tiene éxito, el controlador de acceso preparará un mensaje de confirmación de registro para devolverlo al punto extremo. En función del perfil, este mensaje de RCF podrá contener un **ClearToken** que incluya los elementos **random**, **random2**, y/o **challenge** tomados del **ClearToken** de perfil de autenticación proporcionado en la RRQ. La RCF, y todos los mensajes RAS subsiguientes, contendrán una prueba verificable de autenticación e integridad calculada utilizando la clave de autenticación y el algoritmo negociados.

6) Cuando el punto extremo recibe el mensaje RCF, verifica la integridad mediante el elemento de autenticación y verificación de integridad incluido. Si la verificación fracasa, se descartará la RCF; si se recibe una RCF no válida, incluso después de haberse retransmitido la RRQ, se abandonará la sesión y el punto extremo volverá a la búsqueda de un nuevo controlador de acceso. Si la RCF se verifica, el ID de sesión y la sucesión cifrada seleccionada, si están presentes, pueden extraerse de su **ClearToken** para ulterior utilización en el establecimiento de un canal de señalización de llamada protegido.

6.3 Utilización de perfiles entre controladores de acceso

Esencialmente, se puede utilizar el mismo procedimiento entre controladores de acceso en un intercambio LRQ/LCF. En esta situación, no es posible una selección explícita del perfil; el controlador de acceso iniciador ofrecerá uno o más perfiles incluyendo el o los **ClearToken** apropiados como se ha descrito antes para el mensaje GRQ. El controlador de acceso respondedor puede elegir un perfil ofrecido y debe devolver el correspondiente **ClearToken** como se ha descrito antes con relación al mensaje GCF. Obsérvese que, en este caso, el controlador de acceso iniciador no se autentica a sí mismo ante el controlador de acceso respondedor hasta que establece un canal de señalización de llamada hacia ese controlador de acceso.

Este procedimiento puede emplearse en un modo multidifusión si un grupo de controladores de acceso comparte un secreto único que habrá de utilizarse con este fin. La LRQ multidifusión se basará en ese secreto; los controladores de acceso que respondan con LCF utilizarán la clave para decodificar la clave pública Diffie-Hellman ofrecida, y cada uno de ellos elegirá su propio **nonce** y clave privada Diffie-Hellman para su respuesta. Las claves de sesión resultantes serán únicas para la pareja final de controladores de acceso.

6.4 Criptación y autenticación de canales de señalización

Si el controlador de acceso soporta el encaminamiento por controlador de acceso, el material de clave maestra últimamente negociado y los parámetros criptográficos identificados pueden utilizarse para autenticar y proteger el canal de señalización de llamada, por ejemplo, estableciendo una sesión TLS para señalización de llamada. Si ha de utilizarse TLS, el controlador de acceso incluirá los elementos **cipherSuite** y **compress** seleccionados en el **ClearToken** de perfil devuelto.

7 Perfil de seguridad específico (SP1)

En esta cláusula se especifica un perfil de seguridad normalizado que puede proporcionar un secreto compartido equivalente a un número aleatorio de 80 bits (véase [NIST SP 800-57]). El perfil consta de lo siguiente:

- ID de objeto para este perfil (designado por "SP1") será {itu-t (0) recommendation (0) h (8) 235 version (0) 3 60}.
- Negociación de clave maestra, K_m: intercambio de claves Diffie-Hellman utilizando el conocido grupo 2 de OAKLEY [RFC 2412], seguido de la reducción, por troceado SHA1 [FIPS PUB 180-1] del secreto Diffie-Hellman: K_m = SHA1 (secreto compartido Diffie-Hellman).
- Algoritmo de criptación simétrica: será AES-128 en modo contador segmentado con un discriminador de parte (participante) de 2 octetos, D, un vector de inicialización de 12 octetos, IV, y un campo contador de 2 octetos, C, siendo el contador = D || IV || C y C = 0 inicialmente. Para una descripción del modo CTR, véase [NIST SP 800-38A]. El discriminador de parte, D, se fija a 0x3636 cuando el IV es generado por la parte que emitió la GRQ/RRQ, o LRQ, y se fija a 0x5c5c cuando el IV es generado por la parte que respondió con GCF/RCF, o LCF. Cada parte debe asegurarse de que cada IV que generó es único; puede utilizar su propio método para asegurar esta unicidad.
- Criptación de clave Diffie-Hellman: se utilizará el modo contador segmentado AES-128 para criptar la clave pública Diffie-Hellman (representada por una cadena de octetos en el orden en que se transmiten en la red); el vector de inicialización será transportado en **ClearToken.initVect**, y la clave de 16 octetos, K_p, consistirá en los 128 bits de orden superior del troceado SHA1 de la contraseña del usuario: K_p = Trunc(SHA1(contraseña del usuario), 16), donde Trunc(x,y) trunca la cadena de x octetos a y octetos. Se señala que esta clave suele considerarse débil.
- Prevención de ataques por reproducción: cada parte suministrará un número "aleatorio" ("random") de 32 bits (que puede contener un campo contador para garantizar su unicidad); Los números aleatorios se utilizan explícitamente en el cálculo de claves derivadas, por lo cada número aleatorio sólo hay que transmitirlo una vez.
- Derivación de la clave de autenticación, K_a: utilizando la función PRF de la cláusula 10/H.235.0, que se designa por PRF(*in_key*, *label*, *outkey_len*) con *in_key* = K_m y *label* = "auth_key" || R_e || R_g, donde R_e es un **nonce** obtenido de **ProfileElement** de la GRQ y R_g es un **nonce** obtenido de un **ProfileElement** de la GCF y *outkey_len* = 128.
- Función de autenticación e integridad de mensaje: utilizando un **ClearToken** con **tokenOID** fijado a "SP1" y un **ProfileElement.octets** fijado al valor de troceado HMAC-SHA1-96 calculado sobre el mensaje entero como se describe en la Rec. UIT-T 225.0; este procedimiento se aplicará a todos los mensajes RAS y de señalización de llamada (salvo una GRQ, o LRQ, que no contiene un **sessionID**).
- Clave de criptación de elemento, K_e: elementos seleccionados de mensajes de señalización de llamada (o elementos tunelizados en estos mensajes) pueden ser criptados utilizando AES-128 en modo contador segmentado mediante el uso de la clave K_e = PRF(K_m, "encrypt_key" || R_e || R_g, 128). Por ejemplo, esta clave puede utilizarse para criptar claves

de sesión de medios para distribución en elementos **h235Key** como los utilizados en Fast Connect y/o H.245. Cuando se utilizan de esta manera, "SP1" se emplea como el OID de algoritmo de criptación.

Este perfil utiliza los **ProfileElement** definidos en el cuadro 1. Estos elementos son transportados en una secuencia de elementos **ClearToken.profileInfo** definida en la Rec. UIT-T H.235.0.

Cuadro 1/H.235.5 – Elementos de los perfiles

Nombre del elemento (utilizado en el texto)	Valor del ID del elemento	Característica del elemento (longitud)	Descripción del elemento
initVect	1	Octetos (12)	Vector de inicialización para criptación EKE
nonce	2	Octetos (cualesquiera)	Un valor único, impredecible
cipherSuite	3	Octetos (2)	Un conjunto de cifrado TLS
compression	4	Octetos (1)	Un algoritmo de compresión TLS
sessionID	5	Octetos (1..)	Único, puede concordar con un ID de sesión TLS
integrityCheck	6	Octetos (12)	Valor de comprobación con clave

La secuencia de registro consistirá en lo siguiente:

– El punto extremo enviará GRQ con el elemento **authenticationCapability** y su **AuthenticationMechanism.keyExch** que contiene OID "SP1" y un **ClearToken** correspondiente con **tokenID** = "SP1" y **dhkey** que contiene una clave pública de 1024 bits criptada utilizando **initVect** como el IV y la clave derivada de la contraseña del usuario, y un **nonce** = un número aleatorio de 32 bits seleccionado por el punto extremo.

– El controlador de acceso responderá con GCF con el elemento **authenticationMode** igual a un **AuthenticationMechanism.keyExch** que contiene OID "SP1", y un **ClearToken** con **tokenID** = "SP1" y **dhkey** que contiene una clave pública de 1024 bits no criptada, y un **nonce** = un número aleatorio de 32 bits seleccionado por el controlador de acceso, junto con una **integrityCheck** que contiene el valor de troceado de autenticación calculado utilizando la clave de autenticación, K_a, derivada. Obsérvese que el controlador de acceso no tiene necesidad de criptar su media clave Diffie-Hellman en la GCF, en este perfil, porque él es la primera parte que se autentica a sí misma al demostrar su aptitud para autenticar la GCF utilizando la clave de autenticación derivada. Este modo permite al controlador de acceso reutilizar sus claves Diffie-Hellman con más de un punto extremo. Véase la cláusula 10.5.

– El punto extremo responderá con una RRQ con el valor de autenticación y verificación de integridad en un **ProfileElement** con **elementID** fijado a **integrityCheck**, y **element** fijado al valor calculado utilizando la clave de autenticación, K_a, derivada.

– Los mensajes RAS subsiguientes, incluido el de RCF, serán autenticados y sometidos a verificación de integridad utilizando el mismo procedimiento y clave. Los mensajes de señalización de llamada H.225.0 (y los mensajes H.245 tunelizados, si están presentes) serán autenticados utilizando un **ClearToken**, con **tokenOID** fijado a "SP1", que contiene un **profileInfo ProfileElement** con **elementID** fijado a **integrityCheck** y **element** fijado al valor calculado.

– La clave de criptación, K_e, y el algoritmo de criptación AES-128 en modo contador segmentado pueden ser utilizados por el controlador de acceso y el punto extremo para criptar información seleccionada transportada por RAS, señalización de llamada, y/o

H.245. Por ejemplo, el controlador de acceso puede distribuir claves de criptación de medios protegidas por K_e y el algoritmo de criptación del perfil.

– Si se requiere que un punto extremo se registre de nuevo, y este punto extremo retiene el ID de sesión original y el secreto maestro, debería hacerlo utilizando el ID de sesión original y el secreto maestro, incluyendo explícitamente en su GRQ el ID de sesión (pero no una media clave Diffie-Hellman).

– Este perfil podrá utilizarse entre controladores de acceso (véase 6.3).

8 Perfil de seguridad mejorado (SP2)

En esta cláusula se define un nuevo perfil de seguridad basado en el perfil original SP1, el cual se conoce informalmente con el nombre SP2 y se identifica formalmente con un OID {itu-t (0) recommendation (0) h (8) 235 version (0) 4 62}. Este perfil es idéntico al SP1, con las excepciones que se especifican en las siguientes subcláusulas. Las mejoras específicas con respecto al SP1 son:

– Se ha perfeccionado la numeración de secuencias de los mensajes de señalización de llamada para contrarrestar los ataques por reproducción.

– La generación de un clave de criptación basada en contraseña se completa con un alias del punto extremo para contrarrestar los ataques por diccionario.

– El tamaño de nonce se aumenta y se convierte en variable.

– Se calcula una clave adicional con el vector de inicialización de criptación.

– Se facilita mediante **genericData** un transporte más eficiente del perfil **ClearToken**.

El SP2 utiliza los elementos del perfil que se indican en el cuadro 1, así como los elementos adicionales que figuran en el cuadro 2:

Cuadro 2/H.235.5 – Elementos adicionales del perfil SP2

Nombre del elemento (utilizado en el texto)	Valor del ID del elemento	Característica del elemento (longitud)	Descripción del elemento
seqNumber	7	Octetos (4)	Número de secuencia de 32-bit en el orden de byte de la red
connectID	8	Octetos (2)	Identificador de conexión de señalización. (Facultativo, valor por defecto = 0)
endpointID	9	Octetos (variable)	Dirección alias codificada en ASN.1 correspondiente al punto extremo y su contraseña. (Facultativo)

8.1 Número de secuencia de señalización de llamada

Los mensajes de señalización de llamada H.225.0 no contienen un número de secuencia dado que se transportan por una conexión fiable (TCP) que se encarga de la secuenciación. Sin embargo, la ausencia de un identificador de mensajes único en el nivel de aplicación expone a la señalización de llamada a ataques de reproducción o por reflejo. Este problema puede contrarrestarse añadiendo un número de secuencia y, como opción, un identificador de conexión, a cada mensaje de señalización de llamada. Obsérvese que si bien esta técnica no es infalible contra los ataques de reproducción o por reflejo, reduce considerablemente las posibilidades de éxito de estos ataques.

Los números de secuencia deben ser únicos en cada dirección para evitar el reflejo. En la medida de lo posible, el emisor del mensaje GRQ (punto extremo) o del mensaje LRQ (controlador de acceso) debería empezar el número de secuencia de transmisión de la señalización de llamada en 0 (cero) y su número de secuencia de recepción en 2^{31}, y el controlador de acceso receptor debería actuar de la

misma forma. De este modo puede pasar mucho tiempo antes de que se produzca solapamiento (casi 600 horas a una velocidad bastante inusual de un mensaje por milisegundo). Las sucesivas llamadas que utilicen el mismo ID de sesión deberían transmitir con el siguiente número de secuencia no usado en cada sentido. Para no perder mensajes en las conexiones averiadas, el receptor debería aceptar mensajes dentro de una ventana pequeña (por ejemplo, 5-10) después del último número de secuencia recibido, y continuar a partir de dicho número). Los dispositivos que soporten simultáneamente múltiples conexiones de señalización de llamada con el mismo ID de sesión podrán emplear el **connectID** opcional para determinar espacios de números de secuencia independientes para las llamadas. Si no se especifica lo contrario, el valor de **connectID** se supondrá igual a 0 (cero).

8.2 Generación de claves de criptación débiles a partir de contraseñas

Para contrarrestar los ataques por diccionario en los que se trata de adivinar el PIN que se utilizó para criptar una clave pública D-H, para luego aplicarla sucesivamente a todos los alias del punto extremo conocidos, es conveniente completar la clave de criptación con el propio alias. En particular, podrá calcularse la clave basada en contraseña, K_p, a partir de la contraseña y el **endpointID** suministrado:

$$K_p = \text{Trunc}(\text{SHA1}(\text{contraseña de usuario} \,||\, \textbf{endpointID}), 16)$$

Por regla general, la **AliasAddress** en el **endpointID** será uno de los alias incluidos en el elemento **endpointAlias** de la GRQ, aunque no es obligatorio que así sea. Por ejemplo, el **endpointID** puede identificar a una pasarela que soporta muchos puntos extremos cuyos alias se enumeran en el **endpointType**.

8.3 Tamaño de Nonce

El perfil de seguridad 1 exige que cada parte provea un nonce de 4 octetos (32 bits) como parte del protocolo de negociación de claves. Cuando se suministra durante la negociación de claves inicial, quizás esos 32 bits sean suficientes para asegurar la originalidad en aquellos casos en que el controlador de acceso que responde vuelve a utilizar la misma clave pública Diffie-Hellman pero el solicitante genera una clave original. No obstante, al negociar nuevas claves de sesión a partir de una clave maestra negociada previamente, quizá el total de 64 bits singulares no ofrezca una diferencia suficiente entre los distintos conjuntos de claves calculadas. Se propone que el tamaño de nonce sea variable, con un mínimo de 4 octetos y un máximo de 16.

8.4 Adición de un vector de inicialización

Para mayor seguridad se añade una clave adicional de sesión de 112 bits, K_s, que se calcula a partir de la clave maestra negociada:

$$K_s = \text{PRF}(K_m, \text{"clave\_maestra"} \,||\, R_e \,||\, R_g, 112)$$

Entonces, el contador inicial AES-128-CM para la criptación y descriptación se calcula mediante la siguiente expresión:

Contador = (K_s ^ (D || IV)) || C, siendo C el campo contador de 16 bits, inicialmente cero.

8.5 Codificación del ClearToken

El perfil de seguridad 1 utiliza la secuencia **clearToken** para transportar los parámetros del perfil. Cada mensaje H.225.0 contiene una secuencia de **clearTokens**, salvo la opción **empty** del **h323-message-body**; todos los mensajes transportan **genericData**. La estructura de los procedimientos del SP1 permite que el **ClearToken** tenga una estructura bastante regular, gracias a los cual puede condificarse mediante ASN.1 por anticipado, y transportarse como un parámetro **raw** con **id.standard** puesto a 1 en el elemento **GenericData** determinado por el OID SP2. Esta forma permite identificar el **clearToken** mediante el OID "null" {0,0}. Y lo que es aún más importante,

resulta más facil ubicar el testigo y el valor de verificación que contiene, dado que la forma codificada **ClearToken** se obtiene como parte del proceso normal de codificación y decodificación. Así pues, es más rápido localizar el elemento **integrityCheck** dentro del testigo codificado que dentro del mensaje completo codificado.

9 Extensiones al marco (informativo)

Los siguientes elementos pueden incorporarse en un perfil de seguridad definido dentro de este marco.

9.1 Utilización de la clave maestra para proteger el canal de señalización de llamada mediante TLS

El material de clave negociado durante el intercambio de RAS puede utilizarse para derivar claves de sesión destinadas a la protección del canal de señalización de llamada en el protocolo de transporte TLS ([RFC 2246], [RFC 3546]). En efecto, la negociación de RAS reemplaza al protocolo de toma de contacto TLS inicial. Desde luego, esto sólo tiene sentido si la señalización de llamada va a ser encaminada por un controlador de acceso. Es especialmente conveniente para autenticación por controlador de acceso y señalización mediante intercambio de LRQ/LCF. En este caso, no hay un tercer mensaje RAS por el cual el controlador de acceso llamante pueda autenticarse a sí mismo ante el controlador de acceso llamado utilizando el material de clave negociado, pero el llamante puede autenticarse implícitamente por su aptitud para establecer el canal de señalización de llamada con los parámetros de sesión TLS correctos. La figura 1 ilustra el consiguiente flujo de información: se utiliza RAS para negociar la clave maestra de sesión, se comunican al software TLS el ID de sesión y el correspondiente secreto anterior a la clave maestra, y la capa de señalización de llamada utiliza el ID de sesión para establecer el canal de señalización de llamada por TLS. La forma de transferencia del secreto depende de la implementación y está fuera del ámbito de esta Recomendación. Obsérvese que esta Recomendación especifica el puerto 1300 como el puerto de escucha TLS por defecto para la señalización de llamada. Ahora bien, el punto extremo tiene que utilizar una de las direcciones de transporte de señalización de llamada suministradas por el controlador de acceso.

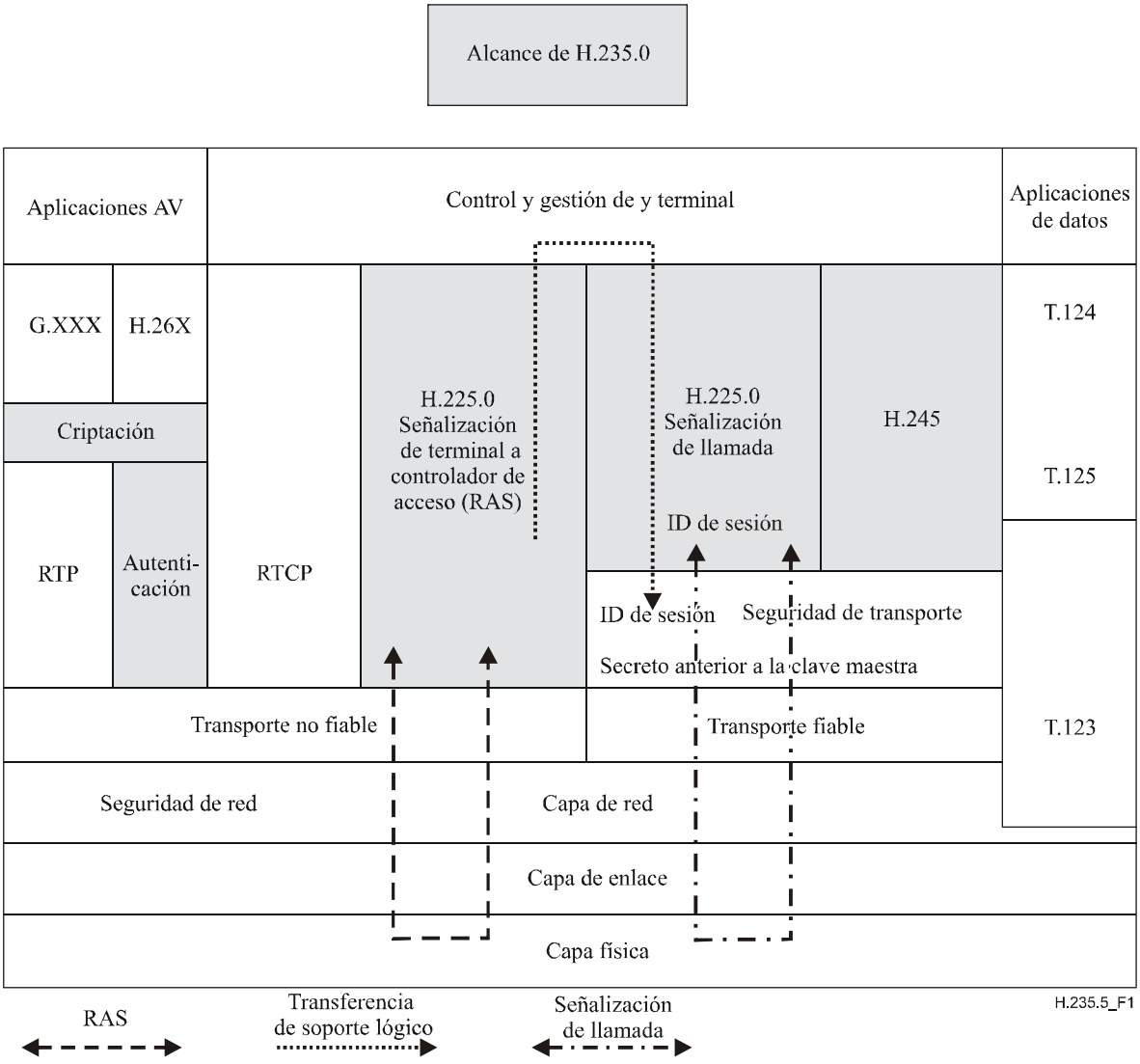

Figura 1/H.235.5 – Flujo de información para perfil de seguridad y TLS

En la siguiente descripción se hace referencia a los pasos dentro del marco básico de la figura 1.

9.1.1 Registro de punto extremo

Un punto extremo puede probar la aptitud de un controlador de acceso para soportar la señalización de llamada con protección TLS incluyendo uno o más elementos **cipherSuite** y uno o más elementos **compression** en el **ClearToken** de perfil en el mensaje GRQ enviado en la primera de estas acciones. Si el punto extremo desea utilizar una sesión negociada previamente, incluirá también el **sessionID** en el **ClearToken** (y especificará solamente el único conjunto de cifrado y el único método de compresión que concuerdan con la sesión solicitada). Si la negociación ha de basarse en una sesión TLS existente, no se requiere material criptográfico en el **ClearToken de perfil**, salvo **nonce**.

Si la sesión que se solicita no existe, el controlador de acceso seleccionará otro perfil de autenticación (si se ha ofrecido) o devolverá un GRJ con **GatekeeperRejectReason.resourceUnavailable**. Si la sesión solicitada no existe, el material de clave maestra se obtiene de la sesión TLS, y se utiliza (junto con **random** tomado de la GRQ y **random2** generado por el controlador de acceso) para calcular la clave de autenticación con miras al intercambio RAS. El **sessionID**, el **cipherSuite**, el método **compress**, y el **nonce** del controlador de acceso se devolverán en el **ClearToken** del perfil de una GCF.

Si el controlador de acceso puede soportar la negociación de sesión TLS, calculará el material de clave maestra como se especifica según el perfil, asignará un nuevo ID de sesión y lo devolverá en el **ClearToken** de perfil, en el **sessionID**. El **ClearToken** de perfil contendrá también los parámetros de seguridad requeridos del paso 2 anterior, un solo **cipherSuite** seleccionado, un solo método **compress** seleccionado, y el **sessionID** diferente de cero. Obsérvese que el método de intercambio de claves del conjunto de cifrado seleccionado es intrascendente. Si el controlador de acceso acepta la protección TLS de señalización de llamada, todas las direcciones de transporte de señalización de llamada intercambiadas en los subsiguientes mensajes RRQ/RCF o ARQ/ACF serán compatibles con los procedimientos TLS.

Si la negociación TLS y/o el encaminamiento por el controlador de acceso no son soportados por el controlador de acceso, no se devolverá ningún parámetro TLS, pero los procedimientos de autenticación podrán continuar a partir del paso 3, como se ha descrito antes. El punto extremo decidirá si prosigue sin la protección TLS de la señalización de llamada; puede optar por hacer esto y, además, utilizar el perfil de autenticación. Tras una finalización exitosa de la secuencia de registro, la sesión TLS está disponible para uso en establecimiento rápido de una o más conexiones de señalización al controlador de acceso, sin necesidad de renegociar material de clave mediante métodos de clave pública.

Las sesiones TLS tienen un periodo de validez. Por tanto, puede que un punto extremo tenga que renegociar parámetros de sesión y obtener un nuevo ID de sesión, y puede hacerlo intercambiado los elementos **ClearToken** necesarios, como se ha descrito antes, en una secuencia de registro simplificada (de actualización). Tal secuencia no afectará a la clave de autenticación RAS.

9.2 Utilización de certificados para autenticar el controlador de acceso

Aunque puede no ser viable en la práctica intercambiar cadenas de certificados verificables en RAS (debido a limitaciones del tamaño de los paquetes UDP), es posible hacer que un servidor se identifique a sí mismo ante el punto extremo si éste puede obtener una copia de confianza de la clave pública del servidor por otros medios. El servidor puede simplemente incluir, en el mensaje GCF, un **CryptoH323Token.cryptoGKCert** que tenga como **ClearToken.tokenOID** el OID del perfil de seguridad seleccionado.

9.3 Utilización de otros mecanismos de seguridad de la señalización

Los parámetros negociados como parte de un perfil de seguridad en el contexto de esta Recomendación pueden emplearse en mecanismos de seguridad en el nivel de transporte y/o de aplicación como esté determinado por el perfil específico. La secuencia **profileInfo** añadida al **ClearToken** H.235 ha sido prevista para tal utilización, si fuera necesario.

10 Amenazas (informativo)

10.1 Ataque pasivo

Actualmente este esquema no es vulnerable a un ataque pasivo, siempre que la negociación Diffie-Hellman tampoco lo sea.

10.2 Ataques por denegación de servicio

Este esquema está expuesto a un ataque, activo por denegación de servicio, en el cual un tercero responde a la GRQ con un GRJ espurio. Este tipo de ataque puede o no ser identificable: si el controlador de acceso que lo rechaza es legítimo y conoce el secreto compartido (por ejemplo, es el controlador de acceso del punto extremo y la **rejectReason** es **resourceUnavailable**), entonces el controlador de acceso podría completar la negociación de la clave y autenticar el GRJ devolviendo, en el GRJ, los mismos elementos descritos para la GCF (salvo que el OID devuelto en

authenticationMode de la GCF sería devuelto en un elemento **ClearToken.profileInfo** del GRJ). Esto se deja como parte de la definición de un perfil específico.

Si el GRJ no está autenticado, podría provenir de un atacante. Antes de reaccionar al GRJ (por ejemplo, buscando otro posible controlador de acceso), el punto extremo debería esperar la posible recepción de otro GRJ o una GCF autenticada del mismo controlador de acceso. En otro caso, el punto extremo debería probar con cada controlador de acceso sugerido en cualquier **altGKInfo** recibida en todos los GRJ (uno de los cuales, cabe suponer, es legítimo). De todas formas, sólo el controlador de acceso legítimo (que conoce el secreto compartido) puede devolver una GCF autenticada.

10.3 Ataques de intromisión [ataques MIM (*man-in-the-middle*)]

Parece evidente la solución de realizar el intercambio con una clave Diffie-Hellman no criptada y después utiliza la contraseña o el PIN para calcular claves de sesión a partir del secreto Diffie-Hellman. Sin embargo, esta forma de intercambio es vulnerable al ataque de intromisión (MIM), que puede utilizarse para descubrir el "pequeño" secreto compartido mediante una acción exhaustiva, utilizando el valor de verificación de integridad proporcionado por el controlador de acceso legítimo en el mensaje GCF.

Desde luego, cualquier MIM puede manipular cualquier mensaje RAS autenticado para asegurarse de que el mensaje será descartado debido un fallo de la verificación de integridad. Si todos los mensajes pueden ser manipulados, el servicio puede ser denegado.

10.4 Ataques por intentos de adivinar

Un atacante puede hacerse pasar por un punto extremo legítimo, por un controlador de acceso legítimo, o por los dos (intromisión), y tratar de adivinar el secreto compartido por el método de intentos-fracasos sucesivos. Por ejemplo, el atacante (que se supone que conoce los detalles del perfil de autenticación, pero no el secreto compartido) puede tratar de adivinar el secreto compartido y tratar de obtener el registro enviando una GRQ con esa suposición. En general, el controlador de acceso responde a este intento con una GCF que contiene la clave pública del controlador de acceso (criptada utilizando el secreto compartido real), y un ICV calculado utilizando la clave derivada que depende de la descriptación, por el controlador de acceso, de la clave pública criptada del atacante. El atacante puede utilizar esta información para verificar su intento de adivinar el secreto compartido. Si su suposición confirma el ICV de la GCF, entonces probablemente es igual al secreto compartido real; esto puede confirmarse continuando con la secuencia de registro. Si esta suposición no permite reproducir el ICV de la GCF, el atacante tiene que hacer un nuevo intento de adivinar. Cuando el espacio de las claves para el secreto compartido es pequeño, es realizable intentarlo repetidamente para hacer esta búsqueda exhaustiva. Este ataque requiere la participación activa del controlador de acceso (o del punto extremo si el atacante se está haciendo pasar por el controlador de acceso). El método tradicional para contrarrestar tal ataque es vigilar los intentos infructuosos, contarlos y, cuando su número alcanza cierto umbral, tratar todos los intentos subsiguientes como no válidos (al menos durante un periodo especificado) y señalizar una alarma, pero esos procedimientos dependen de la implementación.

10.5 Media clave del controlador de acceso no criptada

Como se ha expresado antes, el intercambio EKE puede mantenerse protegido, en ciertas condiciones, si el controlador de acceso respondedor no cripta su media clave Diffie-Hellman. En particular, el controlador de acceso tiene que ser la primera parte que demuestre su conocimiento del secreto compartido (PIN) mediante el ICV. Si no fuera así, el controlador de acceso (o un intruso que se hiciera pasar por el controlador de acceso) podría, simplemente, realizar intentos con todos los PIN posibles para descriptar la media clave D-H del punto extremo, calcular el secreto compartido D-H resultante, derivar la clave de autenticación, y cotejarla con el ICV suministrado por el punto extremo. Esto no es posible si el punto extremo puede verificar el ICV suministrado

inicialmente por el controlador de acceso y rechazar la continuación del registro si el ICV no es el esperado.

La utilización de una media clave no criptada ofrece ventajas a un controlador de acceso ya que éste puede reutilizar su correspondiente clave privada con múltiples puntos extremos. Esto no sería posible si la misma clave se distribuyera criptada para múltiples secretos compartidos o PIN. Un tercero podría observar distintos casos de media clave criptada, por ejemplo, según dos PIN diferentes, después de lo cual podría recorrer todas las combinaciones posibles de dos PIN para determinar qué pareja produjo la misma media clave al efectuarse la decriptación. Si hay, por ejemplo, 10^8 PIN posibles, habrá que tratar solamente 10^{16} combinaciones posibles. Este es un problema equivalente al que se plantea en la búsqueda de un número aleatorio de 54 bits, que no es insoluble en lo absoluto. Incluso si se encontrara más de una solución posible, la correcta podría determinarse rápidamente efectuando una tercera observación.

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