Unión Internacional de Telecomunicaciones

UIT-T H.235.9

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: Soporte de pasarela de seguridad para H.323

Recomendación UIT-T H.235.9

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.235.9

Marco de seguridad H.323:
Soporte de pasarela de seguridad para H.323

Resumen

En la presente Recomendación se define un método para la detección de pasarelas de seguridad que se encuentren en el trayecto de señalización entre entidades H.323 comunicantes y para intercambiar información de seguridad entre un controlador de acceso y las pasarelas de seguridad a fin de preservar la integridad y la privacidad de la señalización.

Orígenes

La Recomendación UIT-T H.235.9 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

Pasarela, seguridad, señalización.

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

Introducción

La utilización de cortafuegos y de dispositivos de traducción de direcciones de red para proteger el tráfico entre regiones de red que pertenecen a diferentes controles administrativos plantea problemas con los protocolos de señalización de telefonía que deben intercambiar direcciones de red a efectos de señalización e intercambio de medios.

En la Rec. UIT-T H.235.5 se describe un marco mediante el cual un punto extremo y su controlador de acceso, o dos controladores de acceso, pueden utilizar los mensajes RAS iniciales para negociar un conjunto de secretos fuertemente compartidos entre ellos, y utilizar dichos secretos para criptar determinadas partes de los mensajes RAS y de señalización de llamada subsiguientes y para autenticar dichos mensajes. Dicho método se aplica únicamente a la señalización encaminada a través de controladores de acceso. En las Recs. UIT-T H.235.1, H.235.2 y H.235.3 se definen métodos y perfiles de seguridad similares. Estos mecanismos de seguridad pueden entrar en conflicto con las pasarelas de nivel de aplicación (ALG) que interconectan dominios de red diferentes y manipulan la señalización y las direcciones de transporte de medios que se transportan en los mensajes RAS H.225.0 y en los de señalización de llamada. Esta modificación de los mensajes puede ocasionar el fallo de la verificación de la autenticación del mensaje en el destino.

En la presente Recomendación se describe un mecanismo sencillo para informar al controlador de acceso de las ALG que se encuentran en el trayecto de señalización e intercambiar con dichas ALG la clave de autenticación de señalización negociada. Gracias a este procedimiento, las ALG podrán modificar datos no privados, en particular direcciones de transporte, de los mensajes de señalización y autenticar el resultado antes de retransmitir los mensajes modificados hacia su destino. En el texto que figura a continuación estos dispositivos se denominan pasarelas de seguridad (SG). Esta técnica permite mantener la privacidad de extremo a extremo de todo elemento criptado que intervenga en la señalización.

Recomendación UIT-T H.235.9

Marco de seguridad H.323: Soporte de pasarela de seguridad para H.323

1 Alcance

La presente Recomendación puede aplicarse a todo controlador de acceso y punto extremo que utilice los protocolos RAS H.225.0 y en el que intervengan una o varias pasarelas de seguridad con el funcionamiento descrito anteriormente.

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.235.2 (2005), *Marco de seguridad H.323: Perfil de seguridad de firma*.

– Recomendación UIT-T H.235.3 (2005), *Marco de seguridad H.323: Perfil de seguridad híbrido*.

– Recomendación UIT-T H.235.5 (2005), *Marco de seguridad H.323: Marco para la autenticación segura en RAS utilizando secretos compartidos débiles*.

– 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*.

2.2 Referencias informativas

– IETF RFC 2246 (1999), *The TLS Protocol Version 1.0*.

– IETF RFC 3546 (2003), *Transport Layer Security (TLS) Extensions*.

– IETF RFC 2401 (1998), *Security Architecture for the Internet Protocol*.

3 Definiciones

En esta Recomendación se definen los términos siguientes.

3.1 pasarela de capa de aplicación: Dispositivo sensible al protocolo que interconecta dos o más regiones de red y que es capaz de interpretar y modificar los protocolos de capa de aplicación para traducir direcciones de transporte y realizar otras funciones. Las ALG pueden realizar funciones de NAT (traductor de direcciones de red) y de cortafuegos a nivel de transporte, funciones que puede integrar internamente o controlarlos desde el exterior.

3.2 dirección local: Dirección de transporte dentro de un dominio local de direcciones.

3.3 pasarela de medios: Dispositivo que interconecta dos o más dominios de red y que puede ser controlado a su vez por otro dispositivo (por ejemplo, una pasarela de seguridad) para controlar los flujos de medios entre dominios. La MG es efectivamente un traductor de direcciones de red (NAT) o cortafuegos programable que funciona en la capa de transporte y en las inferiores.

3.4 traducción de direcciones de red: Operación que consiste en establecer una correspondencia entre las direcciones de transporte de red de un dominio de red y las de otro.

3.5 válvula: Mecanismo que regula el flujo a través de una pasarela de seguridad (o pasarela de medios controlada por ésta) por el que está autorizado el paso de paquetes o mensajes de un dominio a otro. Una válvula se caracteriza normalmente por cuatro direcciones de transporte (la dirección origen en el dominio A, la dirección de la pasarela de seguridad en el dominio A, la dirección de la pasarela de seguridad en el dominio B y la dirección de destino en el dominio B) y por otras características tales como el protocolo de transporte y la direccionalidad. La dirección de origen no tiene por qué especificarse cuando se trata, por ejemplo, de un puerto de escucha.

3.6 dominio: Región de red que comparte un espacio de direcciones de red común; se sobreentiende que cada dominio diferente utiliza un espacio de direcciones incompatible, contradictorio o privado.

3.7 pasarela de seguridad: Dispositivo que se instala entre dos o más regiones de red IP para realizar funciones de seguridad, tales como la validación o restricción de los flujos de paquetes y la traducción de direcciones de transporte entre regiones de red. En esta Recomendación se sobreentiende que la pasarela de seguridad es una ALG sensible a los protocolos de señalización H.323.

4 Abreviaturas, siglas o acrónimos

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

ALG Pasarela de capa de aplicación (*application layer gateway*)

GCF Confirmación del controlador de acceso (*gatekeeperconfirm*)

GK Controlador de acceso (*gatekeeper*)

GRJ Rechazo del controlador de acceso (*gatekeeperreject*)

LCF Confirmación de localización (*locationconfirm*)

LRQ Petición de localización (*locationrequest*)

MG Pasarela de medios (*media gateway*)

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

OID Identificador de objeto (*object identifier*)

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

SG Pasarela de seguridad (*security gateway*)

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

5 Convenios

En la presente Recomendación se definen varios identificadores de objeto (OID) para la señalización de capacidades de seguridad, procedimientos y algoritmos de seguridad. Estos OID forman un árbol jerárquico de valores asignados que puede proceder de fuentes externas o ser parte del árbol de OID que gestiona el UIT-T. Los OID que están específicamente relacionados con la Rec. UIT-T H.235 aparecen en el texto con el siguiente formato:

"OID" = {itu-t (0) recommendation (0) h (8) 235 version (0) **V N**}, donde **V** representa simbólicamente una sola cifra decimal que indica la correspondiente versión de la Rec. UIT-T H.235, por ejemplo 1, 2, 3 ó 4. **N** representa simbólicamente un número decimal que identifica de manera exclusiva el ejemplar del OID y, por consiguiente, el procedimiento, algoritmo o capacidad de seguridad.

Así pues, el OID codificado en ASN.1 consta de una secuencia de números. Por razones prácticas, se utiliza una notación nemotécnica de cadenas de caracteres abreviadas para cada OID del texto tal como "OID". Se establece una correspondencia que relaciona cada cadena OID con la secuencia de números ASN.1. Las implementaciones que sean conformes con la Rec. UIT-T H.235 utilizarán únicamente los números codificados ASN.1.

Hipótesis básicas

En la presente Recomendación se examina un modelo de red IP en el que varias regiones de red, denominadas dominios, están interconectadas mediante dispositivos denominados pasarelas de seguridad (SG, *security gateways*) que son sensibles al protocolo H.323 y se han diseñado para controlar los flujos de información entre los dominios de red que interconectan. Las SG deben examinar los mensajes de señalización que fluyen entre dominios, verificar su validez y extraer la información de direcciones de transporte intercambiada, que se utilizará para construir los trayectos de flujo adecuados entre los dominios y para modificar las direcciones de transporte de acuerdo con el dominio al que se retransmita el mensaje. Obviamente, las SG deben garantizar el flujo de señalización a través de sí mismas, y además controlar otros dispositivos de soporte de los flujos de medios establecidos. En esta Recomendación no se especifica el protocolo de control entre la pasarela de seguridad y las "pasarelas de medios".

Para facilitar los servicios de un controlador de acceso de un dominio a puntos extremos o controladores de acceso de otro dominio, la SG puede proporcionar una dirección de detección del controlador de acceso para cada dominio que atienda y del que no se conozca el controlador de acceso. La SG podría enviar luego cualquier mensaje de detección recibido a una de esas direcciones hacia el controlador de acceso real después de realizar el correspondiente procesamiento del mensaje H.323. En la figura 1 se ilustra un ejemplo de configuración en la que un controlador de acceso atiende varios puntos extremos de varios dominios de red.

En efecto, las pasarelas de seguridad deben representar al controlador de acceso en cada uno de los dominios que atiendan (salvo, obviamente, el dominio en que resida el controlador de acceso, por ejemplo, el dominio A para el controlador de acceso A en el diagrama). La SG B proporciona direcciones de detección para los dos controladores de acceso de la figura y, por consiguiente, ofrece un trayecto entre los controladores de acceso para la señalización LRQ/LCF. Obsérvese asimismo que no es necesario que las SG proporcionen acceso a todos los controladores de acceso de cada dominio. Por ejemplo, en la figura 1, la SG A puede estar configurada para suministrar una dirección de detección en el dominio B para el controlador de acceso A únicamente.

Se supone que cada controlador de acceso conoce un nombre unívoco para cada SG del sistema, y que el controlador de acceso y cada SG comparten además un secreto criptográficamente fuerte que puede utilizarse para establecer comunicaciones seguras entre ellos. Aunque no sea el tema

principal de esta Recomendación, a continuación se describe la manera en que se negocian o intercambian estas identidades y las correspondientes claves. Los secretos compartidos deben ser únicos para cada par SG/controlador de acceso. Se supone que las SG modifican las direcciones RAS y de señalización de llamada que se intercambian para asegurar que el tráfico RAS y de señalización de llamada circula a través de ellos.

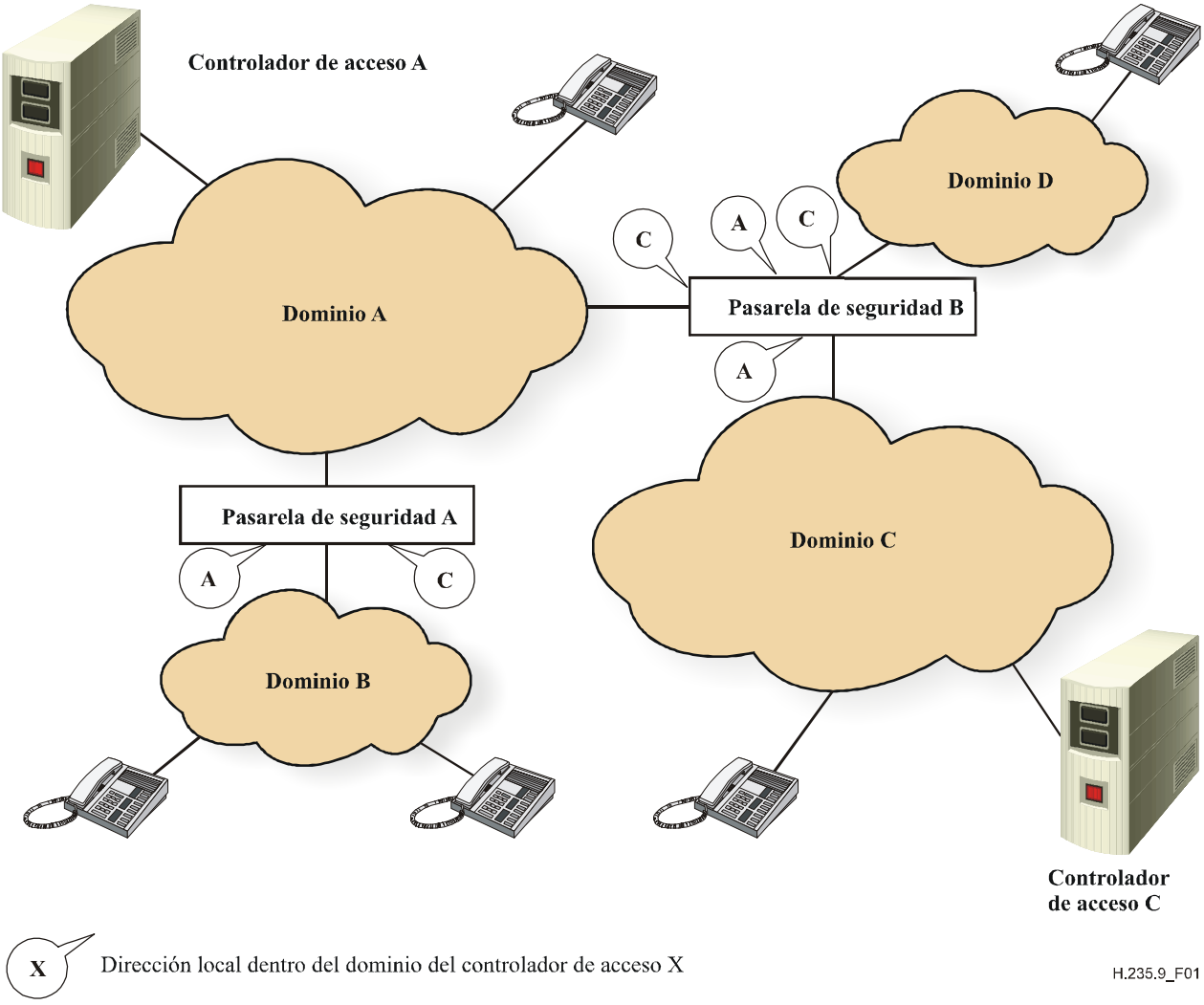


Figura 1/H.235.9 – Configuración de la pasarela de seguridad

Aunque tampoco sea el tema principal de esta Recomendación, a continuación se describen los mecanismos por los que se establece el encaminamiento y/o la traducción de direcciones en el proceso de detección inicial. Se supone que el establecimiento de direcciones subsiguiente, así como las traducciones necesarias, forman parte del funcionamiento de las SG.

6 Funcionamiento básico

En la siguiente descripción se supone que cada SG del sistema se ha registrado en cada controlador de acceso al que va a atender. Los mecanismos que pueden emplearse para ello se describen más adelante. En el modo de funcionamiento básico, se supone que la propia SG ha identificado a cada controlador de acceso, comparte un secreto fuerte único con cada uno de ellos y proporciona una o varias direcciones "locales" de detección para cada controlador de acceso. El procedimiento de registro de la SG se describe más adelante en esta cláusula. A continuación se describe el mecanismo mediante el cual las SG participan en el registro del punto extremo con el fin de acceder

a las claves de autenticación de extremo a extremo negociadas entre el controlador de acceso y el punto extremo.

6.1 Detección del controlador de acceso del punto extremo

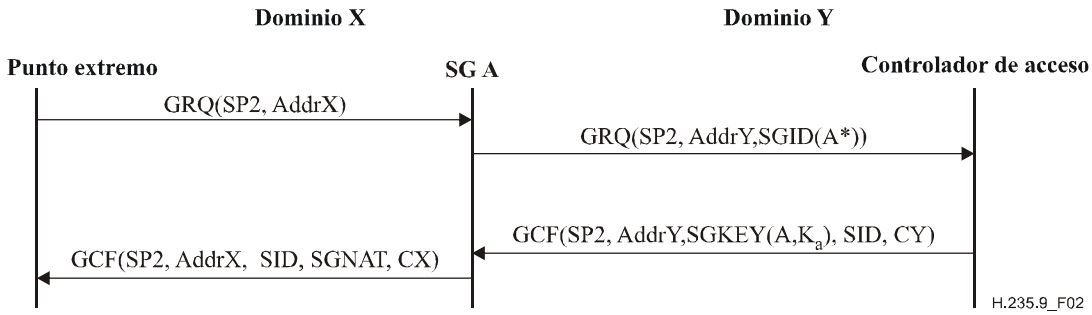
Cuando un punto extremo envía una GRQ a una dirección de detección de controlador de acceso, y la GRQ atraviesa una SG que encamina uno o más controladores de acceso, la SG puede añadir un **ClearToken** al elemento GRQ.**token** al modificar las direcciones que contiene la GRQ. Este **ClearToken** se identificará como testigo de identificación de la SG (mediante su **tokenOID**) y contendrá una cadena que identifique de modo exclusivo la SG. La SG debería suprimir del perfil **authenticationCapability** de la GRQ todo **AuthenticationMechanism** concreto (por ejemplo, TLS en RFC 2246 y RFC 3546 o IPsec en RFC 2401) cuyo procedimiento de autenticación de mensajes no pueda soportar. De este modo se garantiza que el controlador de acceso seleccionará un perfil compatible con la SG. La primera SG que reciba la GRQ deberá incluir un elemento que identifique la dirección de detección en la que recibió la GRQ procedente del punto extremo.

Se sobreentiende que cada SG modificará todos los campos de dirección de señalización de la GRQ y los subsiguientes mensajes RAS para garantizar que se procesarán las direcciones de todos los mensajes de señalización que pasen a su través.

6.2 Distribución de claves de autenticación del punto extremo

Cuando la GRQ llega al controlador de acceso (GK), éste la procesará, incluido el testigo de identificación de la SG. Suponiendo que se comporta como un controlador de acceso del punto extremo, el GK se preparará para devolver una GCF al punto extremo. El GK incluirá en este mensaje GCF el **AuthenticationMechanism** seleccionado junto con un **ClearToken** de clave de la SG (identificado por su **tokenOID**), para la SG identificada por el testigo de identificación de la SG recibido. Este testigo de clave incluirá la identificación de la SG, la identificación del GK, un vector de inicialización y la clave de autenticación de sesión criptada mediante dicho vector y el secreto compartido entre la SG y el controlador de acceso. El algoritmo de criptación se negociará durante el registro de la SG, o estará preconfigurado.

Al recorrer el trayecto inverso hacia el punto extremo, la GCF pasará de nuevo por la SG que suministró el testigo de id de la SG. La SG analizará la sintaxis del mensaje para obtener el ID de la sesión y su propio testigo de clave. Seguidamente deberá descriptar la clave de autenticación de sesión y utilizarla para autenticar el mensaje recibido. Si el mensaje es auténtico, la SG gestionará las direcciones de transporte como corresponda y reconstruirá el mensaje sin su propio testigo de clave SG, insertará un testigo NAT de la SG si no lo hubiera, y luego autenticará y enviará el mensaje reconstruido. La ID de sesión y la clave de autenticación deberá conservarse para los mensajes RAS y de señalización de llamada subsiguientes de dicha sesión. En la figura 2 se ilustra la secuencia básica a través de una misma SG. Obsérvese asimismo que la SG debe preparar las válvulas de acuerdo con lo inferido de la GCF (por ejemplo, una válvula RAS y válvulas de direcciones del GK alternativas).

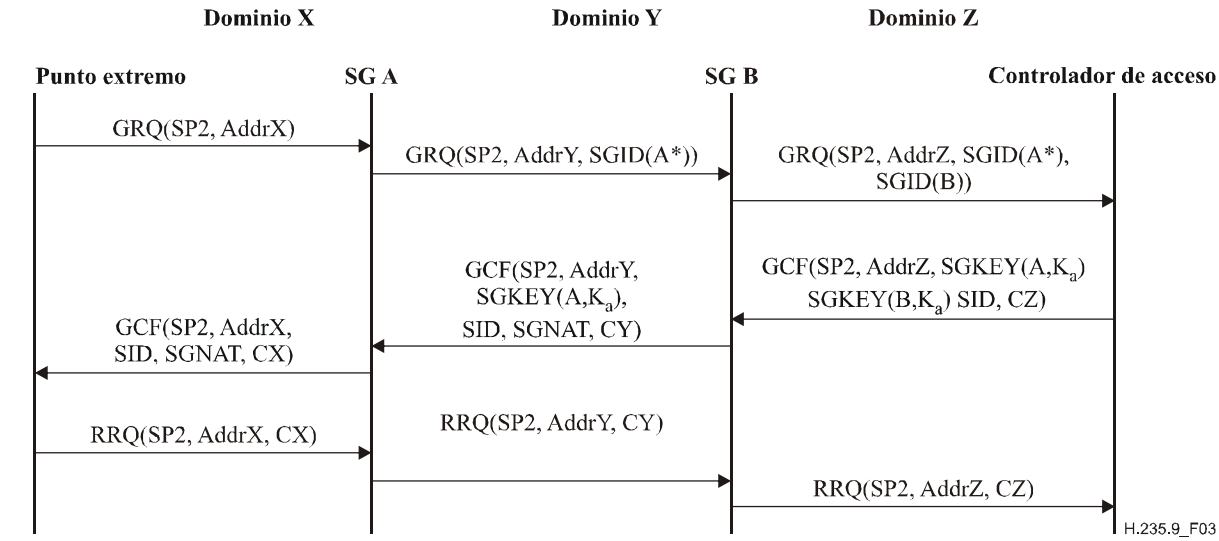


SP2 = perfil de seguridad H.235.5
Addrx = direcciones en el dominio x
SGID(A*) = ClearToken de identificación de la SG que identifica la presencia de la SG A
(* indica que el ID de la SG incluye la dirección de detección utilizada por la GRQ)
SID = ID de sesión (asignado por el controlador de acceso)
K_a = clave de autenticación del mensaje para SID
SGKEY (A, K_a) = ClearToken de clave de la SG, estando K_a criptado con la clave secreta de A
SGNAT = ClearToken NAT de la SG
Cx = verificación de suma de comprobación del mensaje (calculando mediante el K_a negociado) en el dominio x

Figura 2/H.235.9 – Intercambio básico a través de una SG

Este diagrama puede generalizarse fácilmente al caso de varias SG entre el punto extremo y el controlador de acceso. Cada SG añade su propio ClearToken a la GRQ cuando pasa a través de ella y saca su propio ClearToken de respuesta cuando la GCF recorre el camino inverso desde el controlador del acceso hacia el punto extremo. La primera SG que se encuentre en el trayecto inverso hacia el punto extremo deberá insertar en la GCF el testigo NAT de la SG. En la figura 3 se ilustra este caso. El procesamiento de los siguientes mensajes RAS se ilustra mediante la transformación de direcciones de transporte en un mensaje RRQ y la suma de verificación nuevamente calculada.

En el caso de un intercambio de LRQ/LCF es posible llevar a cabo una secuencia similar, utilizando los mismos elementos del mensaje, y los resultados pueden utilizarse para procesar y autenticar los mensajes de señalización subsiguientes para esa sesión.



SP2 = perfil de seguridad H.235.5
Addrx = direcciones en el dominio x
SGUD(A*) = ClearToken de identificación de la SG que identifica la presencia de la SG A
(* indica que el ID de la SG incluye la dirección de detección utilizada por la GRQ)
SID = ID de sesión (asignada por el controlador de acceso)
K_a= clave de autenticación del mensaje para SID
SGKEY (A, K_a) = ClearToken de clave de la SG, estando K_a criptado con la clave secreta de A
SGNAT = ClearToken NAT de la SG
Cx = verificación del mensaje en el dominio x

Figura 3/H.235.9 – Intercambio a través de una SG para el caso de dos niveles

6.3 Manipulación de direcciones

A medida que cada mensaje de señalización H.225.0 o H.245 pasa a través de ella, la SG debe examinar y sustituir todas las direcciones de transporte que éste contenga a fin de que sean válidas dentro del siguiente dominio por el que vaya a circular el mensaje. Para ello puede ser necesario que la SG cree nuevas válvulas que regulen los correspondientes flujos de señalización y de medios que creen esas direcciones. Obsérvese que algunas direcciones representan puertos de escucha que deben abrirse "por si acaso"; es decir, se creará una válvula totalmente especificada cuando llegue un paquete al puerto de escucha.

Cada SG puede examinar cada una de las direcciones de transporte de destino recibidas para comprobar si representa en realidad una dirección de destino en esa SG. Considérese el ejemplo de la configuración de dominio y trayectos de medios de la figura 4. El tren de medios que circula desde el punto de extremo en el dominio B hacia el punto de extremo en el dominio C debe fluir a través de las SG B y C, como se indica mediante el flujo "1". Si la SG B no realiza un procesamiento especial, los trenes de medios que circulan entre dos puntos extremos en el dominio B seguirían un trayecto equivalente hacia el dominio A y de regreso al dominio B, como se ilustra mediante el flujo "2". Sin embargo, si la SG B reconoce que las direcciones de origen y destino indicadas para el flujo en el dominio A corresponden en realidad a direcciones de la SG B, podrá "cortocircuitar" el flujo entre los dos sentidos: es decir, podrá encaminar el flujo internamente como se ilustra mediante el flujo "3" (que para mayor claridad se ilustra en la SG C); o si por el contrario reconoce que ambos puntos extremos residen en el dominio B, podrá sustituir las direcciones del punto extremo del dominio B para reencaminar el flujo directamente entre los puntos extremos como se ilustra mediante el flujo "4". Obsérvese que las direcciones "del punto extremo" desde el punto de vista de la SG B pueden corresponder en realidad a direcciones de una SG (por ejemplo D) que interconecta otro dominio. Una vez que la SG D haya modificado las direcciones para realizar el encaminamiento "directo" entre las direcciones de la SG D, ésta puede cortocircuitar los flujos del mismo modo.

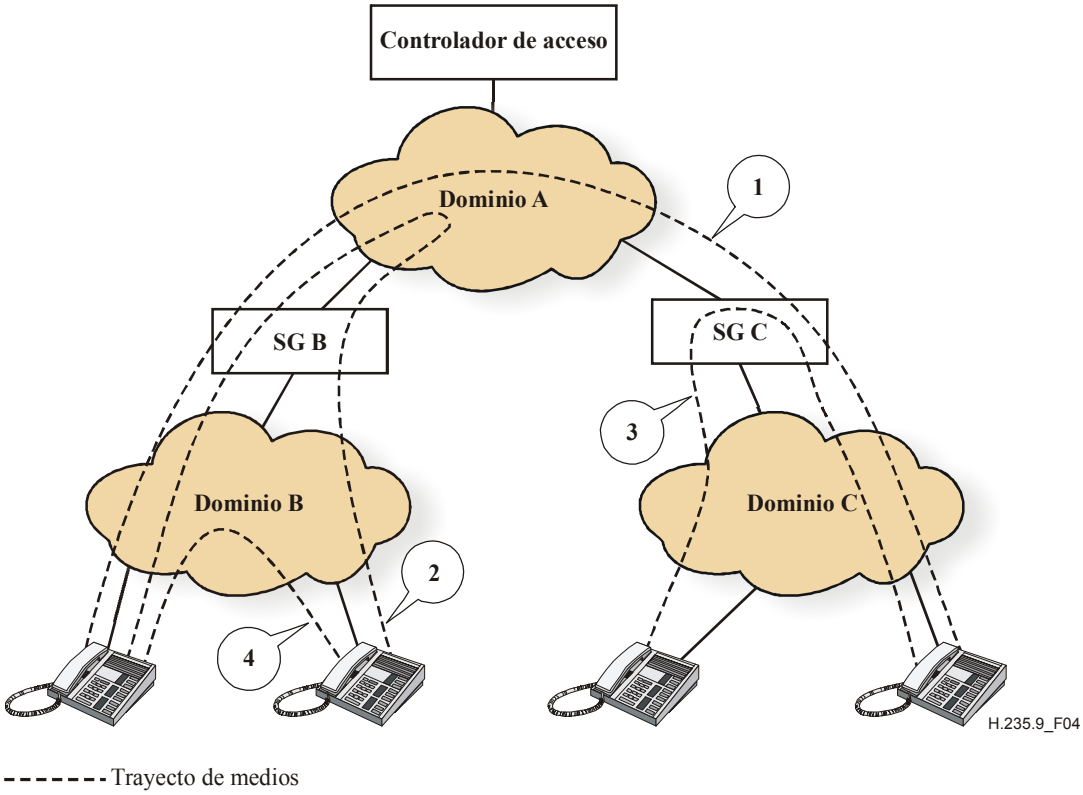


Figura 4/H.235.9 – Trayectos de medios

Una configuración que no contempla este diagrama es el caso en el que una región obtiene acceso a otra a través de más de una SG. Si el punto extremo se registra y emite señales a través de una SG y otro punto extremo en la misma región emite señales hacia una segunda SG, será difícil para ambas SG detectar que los dos puntos extremos pertenecen al mismo dominio o conocer las direcciones que ha de utilizar para el punto extremo cuyas señales pasan por la otra SG. Para evitar este problema, resulta conveniente emplear una sola SG que sea capaz de procesar el nivel previsto de señalización; es posible relegar el procesamiento de los flujos de medios a pasarelas de medios independientes controladas por la SG.

7 Información de señalización

El soporte de esta capacidad se identifica más claramente mediante un identificador de objetos normal (OID) en los testigos de liberación aplicables. En adelante, estos testigos se denominarán testigos SG. Ello permite que los controladores de acceso receptores (o las pasarelas intermedias u otros dispositivos que no participen) hagan caso omiso de esta información. El OID asignado se utilizará para identificar los **ClearToken** que transporten los elementos siguientes:

- **tokenOID** – cuyo valor sea igual al OID asignado a esta función, por ejemplo "SG1", véase la cláusula 11.
- **generalID** – cuyo valor, de estar presente, sea el nombre de la SG a la que va dirigida este **ClearToken** (utilizado en el testigo de claves SG).
- **sendersID** – cuyo valor sea el nombre de la SG que creó este **ClearToken** (utilizado en el testigo de ID de la SG).
- **profileInfo** – contiene la información específica que transporta este **ClearToken**, según se indica en el cuadro 1.

Cuadro 1/H.235.9 – Elementos de perfil para la detección de la SG

Nombre de elemento	Valor del ID del elemento	Tipo de elemento (longitud)	Descripción del elemento
Tipo de testigo	1	entero	0 = testigo de id de la SG 1 = testigo de clave de la SG 2 = testigo NAT de la SG 3 = testigo de registro de la SG
Clave cifrada	2	octetos (16 para SP2)	Clave de autenticación de sesión de acuerdo con el perfil de seguridad indicado, criptada mediante el secreto compartido entre la SG especificada y el GK. Se envía en el testigo de clave SG. El vector de inicialización necesario para descriptarla se especifica en ProfileElement.paramS.
Dominio atendido	3	nombre	Nombre del dominio en el que la SG puede/debe proporcionar una dirección de detección del controlador de acceso

8 Consideraciones relativas a la configuración de la SG

Los procedimientos descritos en esta Recomendación dependen en cierto modo de que las SG de la red detecten los trayectos hacia los controladores de acceso cuyos servicios se desea hacer accesibles a usuarios que se encuentran en otros dominios de la red. Cada SG debe ser capaz de contactar a su controlador o controladores de acceso de un dominio y facilitar el acceso a los mismos desde los puntos extremos (u otros controladores de acceso) que residen en el otro dominio. Por ejemplo, en la figura 3, la SG B accede al controlador de acceso del dominio Z, el cual puede facilitar a los elementos que pertenecen al dominio Y el acceso al controlador de acceso. Así pues, la SG A puede acceder al controlador de acceso a través de la SG B. Una vez que la SG B ha accedido al controlador de acceso, puede facilitar acceso a las partes que pertenecen al dominio X. De lo anterior se desprende que las SG deben utilizar un protocolo de detección, tal como el RAS. Estos procedimientos podrían utilizarse asimismo para identificar todas las SG a las que pueda acceder un controlador de acceso, y negociar (un conjunto de) claves para proteger los intercambios de señalización del usuario.

8.1 Registro de la SG

Una SG puede representar dentro de un dominio a un controlador de acceso de otro dominio accesible por esa SG. Por ejemplo, en la figura 1 la SG A puede representar en el dominio B (mediante una dirección detección) al controlador de acceso del dominio A, una vez conocida la dirección detección de dicho controlador de acceso en el dominio A. Esta técnica puede ampliarse a varios niveles de SG, es decir, cada vez que una SG detecta un controlador de acceso (o un representante) puede proporcionar una dirección de detección para dicho controlador de acceso en uno o más dominios nuevos, tras lo cual, las SG conectadas a ese dominio pueden detectar esas nuevas direcciones.

Las SG deberán utilizar los procedimientos RAS H.225.0 para detectar los controladores de acceso, y registrarse en los mismos, para todo dominio en el que vayan a actuar como pasarelas de seguridad. La SG deberá autoidentificarse como tipo de punto extremo **gateway**. La SG puede especificar el protocolo de soporte H.323 si desea especificar los prefijos y/o las limitaciones de anchura de banda que soporta, aunque no es obligatorio. Deberán utilizarse los procedimientos de seguridad normales, tales como los que se describen en las Recs. UIT-T H.235.1, H.235.2, H.235.3

y H.235.5 para autenticar la SG en el controlador de acceso y negociar los secretos compartidos de seguridad que se utilizarán en los procedimientos que se describen a continuación. Los procedimientos H.235.1, H.235.2, H.235.3 y H.235.5 pueden atravesar otras pasarelas de seguridad que sean compatibles con esta Recomendación. La SG también debe incluir un ClearToken de registro de SG en la RRQ que envía hacia el controlador de acceso. Este testigo sirve para indicar que la pasarela es una SG y deberá incorporar un elemento **ServedRealm** para cada nuevo dominio que atienda. Cada elemento representa una posible nueva dirección de detección de controlador de acceso en su correspondiente dominio. Cada SG puede configurarse para limitar los dominios en los que proporciona direcciones de detección para un controlador de acceso. Por ejemplo, la SG B de la figura 1 podría configurarse para no proporcionar una dirección de detección al controlador de acceso C en el dominio D, lo que obliga a los puntos extremos del dominio D a registrarse en el controlador de acceso A. Siempre que no haga ni reciba llamadas, la SG no necesita proporcionar una dirección de señalización de llamada al registrarse; esto es, puede proporcionar una SEQUENCE vacía en el campo **callSignalAddress** de la RRQ. El controlador de acceso deberá responder del mismo modo en **callSignalAddress** de la RCF.

El controlador de acceso deberá indicar el dominio o dominios para los que la SG puede prestar servicios, para lo cual devolverá en la RCF un testigo de registro de SG que contenga uno o más de los elementos **ServedRealm** incluidos en la RRQ de la SG. Una vez registrada, la SG deberá abrir un zócalo de escucha para cada dirección de detección de controlador de acceso en cada dominio indicado. Para anunciar esta dirección de detección dentro del dominio pueden utilizarse mecanismos distintos de los descritos en esta Recomendación. El controlador de acceso puede optar por utilizar las direcciones de detección facilitadas por la SG en una lista de direcciones alternativas.

Podrá emplearse cualquier perfil de seguridad RAS, siempre que las SG estén autorizadas a leer y modificar las direcciones de señalización y de transporte de los medios intercambiadas y puedan reautenticar el mensaje.

El controlador de acceso puede utilizar la información del dominio de la SG para hacer corresponder las regiones y la conectividad de la red y autenticar la SG. El controlador de acceso debe devolver a la SG la siguiente información:

- Las credenciales del controlador de acceso.
- La dirección o direcciones de registro que puede utilizar la SG para retransmitir las peticiones RAS desde los puntos extremos de la región o regiones que atiende (es decir, el GK puede rehusar atender a puntos extremos de una o varias regiones atendidas por la SG).

Una vez registrada correctamente la SG, debería obtenerse como resultado una clave fuertemente secreta que compartan la SG y el controlador de acceso, y que sirva para obtener las claves de criptación y/o autenticación. La clave de autenticación puede resultar útil para autenticar el mecanismo de registro de la SG, y la clave de criptación debe emplearse durante el registro de los puntos extremos para criptar la clave de autenticación de sesión del punto extremo a fin de distribuirla a la SG, como se ha descrito anteriormente.

8.2 Credenciales de autenticación

Con independencia del número de puntos extremos, el número de SG en una red multirregión será en principio relativamente pequeño. En la mayor parte de los casos, se prevé que el servicio se preste por suscripción u otro tipo de acuerdo contractual y, por consiguiente, el controlador de acceso se configurará con información que identifique a las SG que puedan registrarse en el mismo. En el caso más sencillo, podrían asignarse contraseñas a las SG y emplearse los procedimientos de autenticación H.235.1, H.235.2, H.235.3, H.235.5 o de pregunta-respuesta. Evidentemente, la utilización de secretos compartidos con antelación hace necesario un mecanismo seguro fuera de banda para su distribución.

También podría emplearse un mecanismo basado en certificados de claves públicas. Mediante un procedimiento fiable, podrían guardarse en las SG copias de los certificados del controlador de acceso (o del certificado que pertenece a la autoridad que firma el certificado del controlador de acceso). La utilización de métodos de certificado queda pendiente de estudio.

9 Consideraciones relativas a la seguridad

Los protocolos de este tipo, en los que se permite modificar un mensaje en circulación, están expuestos a ataques por relajación de protección. Por ejemplo, si un punto extremo ofrece capacidades de transporte de medios criptados y no criptados, una SG malintencionada podría suprimir la criptación y suministrar sólo los no criptados, logrando de este modo que los trenes de medios no estén criptados. Para protegerse de este tipo de ataques, los puntos extremos (y el controlador de acceso) ofrecerán únicamente las capacidades que sean aceptables de acuerdo con su propia política de seguridad. En última instancia, es responsabilidad de los puntos extremos y de sus usuarios garantizar que se establece y mantiene el nivel de seguridad adecuado. Consideraciones similares son aplicables a la selección de los perfiles de seguridad durante el registro: si un punto extremo exige una autenticación fuerte, debe especificarlo en su GRQ y no debe aceptar un nivel de autenticación más débil del controlador de acceso.

10 Aplicabilidad

Este plan será aplicable a otros perfiles de seguridad H.235.1, H.235.2 y H.235.3 además de a los descritos en la Rec. UIT-T H.235.5. Se podrían soportar los perfiles de seguridad que proporcionen negociación/cálculo de claves de autenticación adecuadas. Las SG deben examinar los elementos de las GRQ/GCF (por ejemplo, **authenticationCapability** y/o **authenticationMode**) para averiguar si pueden utilizar el mecanismo de seguridad o de autenticación de mensajes negociados.

11 Identificador de objeto

OID	Valor del identificador de objeto	Descripción
"SG1"	{ itu-t (0) recommendation (0) h (8) 235 version (0) 4 65 }	ClearToken que transportan elementos de perfil para la detección de SG.

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