Unión Internacional de Telecomunicaciones

UIT-T H.235.4

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: Seguridad de llamada con encaminamiento directo y selectivo

Recomendación UIT-T H.235.4

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.235.4

Marco de seguridad H.323: Seguridad de llamada con encaminamiento directo y selectivo

Resumen

El objetivo de esta Recomendación es recomendar los procedimientos de seguridad necesarios para utilizar la señalización de llamada con encaminamiento directo con los perfiles de seguridad H.235.1 y H.235.3. Es un perfil de seguridad facultativo que puede ser complementario de los perfiles de esas dos Recomendaciones. Asimismo, se suministran detalles relativos a la implementación de la cláusula 8.4/H.235.0 mediante técnicas de gestión de claves simétricas.

En versiones anteriores de la subserie H.235, este perfil se incluía en el anexo I/H.235. En los apéndices IV, V y VI de H.235.0 se indica la correspondencia entre las cláusulas, las figuras y los cuadros de las versiones 3 y 4 de H.235.

Orígenes

La Recomendación UIT-T H.235.4 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, criptación, gestión de claves, integridad, perfil de seguridad, seguridad de multimedia, seguridad de llamada con encaminamiento directo, seguridad de llamada con encaminamiento selectivo.

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

		Página
1	Alcance	1
2	Referencias	1
	2.1 Referencias normativas	1
	2.2 Referencias informativas	2
3	Términos y definiciones	2
4	Símbolos y abreviaturas	2
5	Convenios	2
6	Introducción	3
7	Consideraciones generales	3
8	Limitaciones	4
9	Procedimiento DRC1 (red de empresa)	4
	9.1 Fase GRQ/RRQ	5
	9.2 Fase ARQ	5
	9.3 Fase LRQ	5
	9.4 Fase LCF	5
	9.5 Fase ACF	6
	9.6 Fase de establecimiento (SETUP)	7
10	Procedimiento DRC2 (entre dominios diferentes)	9
	10.1 Fase GRQ/RRQ	10
	10.2 Fase ARQ	10
	10.3 Fase LRQ	10
	10.4 Fase LCF	10
	10.5 Fase ACF	11
	10.6 Fase de establecimiento (SETUP)	13
11	Procedimiento DRC3 (entre dominios diferentes)	15
	11.1 Fase GRQ/RRQ	16
	11.2 Fase ARQ	16
	11.3 Fase LRQ	16
	11.4 Fase LCF	16
	11.5 Fase ACF	17
	11.6 Fase de establecimiento (SETUP)	18
12	Procedimiento de cálculo de clave basado en PRF	19
13	Procedimiento de cálculo de clave basado en FIPS-140	20
14	Lista de identificadores de objeto	20

Recomendación UIT-T H.235.4

Marco de seguridad H.323: Seguridad de llamada con encaminamiento directo y selectivo

1 Alcance

El objetivo de esta Recomendación es recomendar los procedimientos de seguridad necesarios para utilizar la señalización de llamada con encaminamiento directo con los perfiles de seguridad H.235.1 y H.235.3.

Es un perfil de seguridad facultativo que puede ser complementario de los perfiles de esas dos Recomendaciones. Asimismo, se suministran detalles relativos a la implementación de la cláusula 8.4/H.235.0 mediante técnicas de gestión de claves simétricas.

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 llamadas y paquetización de trenes de medios para sistemas de comunicaciones multimedios por paquetes*.

– Recomendación UIT-T H.235 (2003), *Seguridad y criptado para terminales multimedios de la serie H (basados en las Recomendaciones UIT-T H.323 y H.245)*, corrigendum 1 (2005), más erratum 1 (2005).

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

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

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

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

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

– ISO/CEI 10118-3:2004, *Information technology – Security techniques – Hash functions – Part 3: Dedicated hash-functions*.

2.2 Referencias informativas

– Recomendación UIT-T H.235.2 (2005), *Marco de seguridad H.323: Perfil de seguridad de firma*.

– IETF RFC 4120 (2005), *The Kerberos Network Authentication Service (V5)*.

3 Términos y definiciones

A los efectos de esta Recomendación, se aplican las definiciones de esta cláusula junto con las de la cláusula 3 de las Recs. UIT-T H.323, H.225.0, H.235.0 y X.800 | ISO/CEI 7498-2.

4 Símbolos y abreviaturas

En esta Recomendación se utilizan las siguientes abreviaturas y símbolos.

CT	ClearToken
DH	Diffie-Hellman
DRC	Llamada de encaminamiento directo (*direct-routed call*)
EK_{AG}	Clave de criptación compartida entre el EP A y el GK G
EK_{BH}	Clave de criptación compartida entre el EP B y el GK H
EK_{GH}	Clave de criptación compartida entre el GK G y el GK H
$ENC_{K;\,S,\,IV}(M)$	Criptación EOFB de *M* en la que se utiliza la clave secreta *K*, la clave adicional secreta *S* y el vector inicial *IV*
EPID	Identificador de punto extremo (*endpoint identifier*)
GK	Controlador de acceso (*gatekeeper)*
GKID	Identificador de controlador de acceso (*gatekeeper Identifier*)
g^x, g^y	Semiclave Diffie-Hellman de GK G, GK H
K_{AB}	Clave de criptación compartida entre el EP A y el EP B
K_{AG}	Secreto compartido (H.235.1, H.235.3) entre el EP A y el GK G
K_{BH}	Secreto compartido (H.235.1, H.235.3) entre el EP B y el GK H
K_{GH}	Secreto compartido (H.235.1, H.235.3) entre el GK G y el GK H
KS_{AG}	Clave adicional, compartida y secreta entre el EP A y el GK G
KS_{BH}	Clave adicional, compartida y secreta entre el EP B y el GK H
KS_{GH}	Clave adicional, compartida y secreta entre el GK G y el GK H
PRF	Función seudoaleatoria (*pseudo-random function*)

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.

Mientras que en el texto se hace referencia a los identificadores de objeto mediante un símbolo (por ejemplo, "I11"), en la cláusula 14 figuran sus valores numéricos reales, véase también la cláusula 5/H.235.0.

6 Introducción

La Recomendación H.323 se suele implementar utilizando el modelo de encaminamiento por controlador de acceso (pudiéndose soportar así, por ejemplo, una mejor funcionalidad de facturación). Asimismo, el uso difundido del modelo de llamada encaminada por controlador de acceso es el motivo por el cual en la Rec. UIT-T H.235.0 se definen diversos perfiles de seguridad (tales como los de H.235.1, H.235.2, H.235.3) basados precisamente en este modelo de llamada.

No obstante, debido a que se necesita soportar cada vez más canales paralelos, el modelo de encaminamiento directo con un controlador de acceso puede ofrecer ventajas de calidad de funcionamiento y capacidad evolutiva. La ventaja de este modelo es que se utiliza el controlador de acceso para el registro, admisión, resolución de direcciones y control de ancho de banda, mientras que el establecimiento de comunicación se hace directamente entre los puntos extremos como es habitual.

En esta Recomendación se describen las mejoras a los perfiles de seguridad básico H.235.1 e híbrido H.235.3 necesarias para poder soportar llamadas con encaminamiento directo a través de uno o varios controladores de acceso (GK).

7 Consideraciones generales

Tanto el perfil de seguridad básico H.235.1 como el híbrido H.235.3 se sirven de un secreto compartido (tras la primera toma de contacto) para garantizar la autenticación de mensaje y/o la integridad en un modo de funcionamiento salto por salto, utilizando el controlador de acceso como intermediario fiable. En el modelo de llamada con encaminamiento directo no se puede suponer la existencia de un secreto compartido entre dos puntos extremos, ni es práctico utilizar un secreto compartido preestablecido para asegurar la comunicación, puesto que, en tal caso, todos los puntos extremos tendrían que saber por adelantado cuál otro punto extremo será llamado.

En la presente Recomendación se trata el caso mostrado en la figura 1, donde se conectan los puntos extremos a un solo controlador de acceso y se utiliza la señalización de llamada con encaminamiento directo. Se supone que existe una red IP no asegurada en la región del controlador de acceso.

Se supone también que cada punto extremo tiene una relación de comunicación y una asociación de seguridad con su controlador de acceso y que se ha registrado seguramente con él utilizando bien el perfil de seguridad básico o bien el híbrido.

Por tanto, el controlador de acceso del EP de inicio (DRC1) o el del EP de terminación (DRC2) pueden proporcionar un secreto compartido para los puntos extremos que se comunican directamente utilizando un modelo del tipo Kerberos (véase RFC 4120).

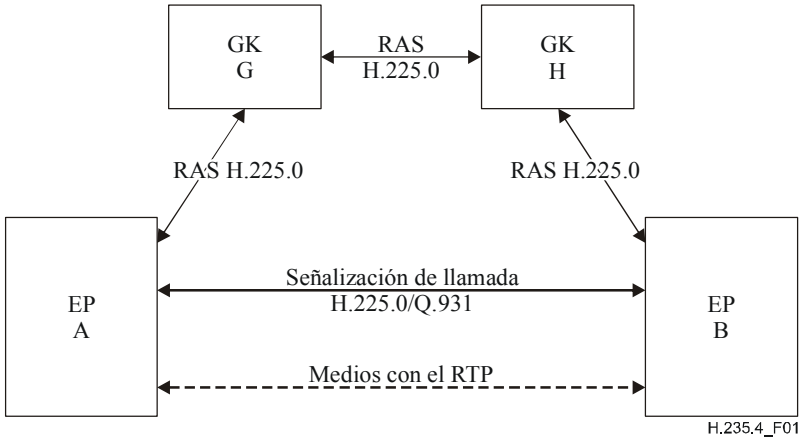

Figura 1/H.235.4 – Caso de una llamada con encaminamiento directo

En esta Recomendación se describen dos procedimientos, a saber DRC1 y DRC2, útiles en entornos diferentes.

El procedimiento DRC1 (véase la cláusula 9) es apropiado para redes de empresas, en las que si bien los GK se encuentran en diferentes sitios (locales), están sujetos a una política común de seguridad. En tales casos, se supone aceptable que el GK G de origen fije la política efectiva de seguridad para una comunicación que se va a establecer; en otras palabras, este GK escoge los parámetros de seguridad que se han de aplicar, los cuales serán aceptados por el GK H de terminación.

Los procedimientos DRC2 (véase la cláusula 10) y DRC3 (cláusula 11) se emplean en los entornos con varios dominios, en los que los GK se encuentran en dominios administrativos diferentes, que probablemente tienen distintas políticas de seguridad.

El procedimiento DRC2 se utiliza cuando el EP llamante o los GK no soportan el algoritmo Diffie-Hellman. En tales casos, se supone aceptable que el GK H de terminación fije la política efectiva de seguridad para una comunicación que se va a establecer; en otras palabras, este GK escoge los parámetros de seguridad que se han de aplicar, los cuales serán aceptados por el GK G de origen.

El procedimiento DRC3 se aplica cuando el EP llamante no soporta el algoritmo de Diffie-Hellman, pero los GK en los dominios llamante y llamado sí lo soportan.

Al inicio del registro de llamada, estos procedimientos suministran los medios de señalización para negociar cuál de ellos, DRC1, DRC2 o DRC3, se debe aplicar.

8 Limitaciones

En esta Recomendación no se tratan los casos de encaminamiento directo en los que no participa ningún GK. Esto queda en estudio.

9 Procedimiento DRC1 (red de empresa)

El DRC1 se aplica en redes de empresas con GK situados en diferentes sitios (locales), pero sujetos a una política empresarial común de seguridad. En tales casos, se supone aceptable que el GK G de origen fije la política efectiva de seguridad para una comunicación que se va a establecer; en otras palabras, este GK escoge los parámetros de seguridad que se han de aplicar, los cuales serán aceptados por el GK H de terminación.

9.1 Fase GRQ/RRQ

Los EP que soporten este perfil de seguridad habrán de indicarlo en **GRQ** y/o **RRQ** incluyendo un ClearToken independiente cuyo **tokenOID** sea "I10"; no conviene utilizar ningún otro campo en dicho ClearToken. Un GK que tenga capacidades H.235.4 y que desee contar con esa funcionalidad deberá responder con **GCF** o **RCF**, que tenga un ClearToken independiente cuyo **tokenOID** sea "I10" y en el que no se use ningún otro campo.

9.2 Fase ARQ

Antes de que un EP A empiece a enviar directamente mensajes de señalización de llamada a otro EP B, uno de los dos deberá solicitar al GK G o H la admisión, utilizando **ARQ**. El EP A tendrá que incluir en el **ARQ** un ClearToken independiente con **tokenOID** igual a "I10" y en el que no se use ningún otro campo.

9.3 Fase LRQ

Este procedimiento comprende tanto el caso de un solo controlador de acceso, común a los puntos extremos, como el caso de múltiples controladores de acceso, en cadena. Cuando intervienen múltiples controladores de acceso, el controlador de acceso G, en cuya zona se origina la llamada, debería localizar al controlador de acceso H utilizando el mecanismo **LRQ** (multidifusión) como se describe en 8.1.6/H.323 "Señalización facultativa de punto extremo llamado". La comunicación entre dos controladores de acceso se protegerá por los procedimientos de H.235.1. Se supone que hay un secreto compartido común K_{GH}. Puesto que **LRQ** entre los controladores de acceso es habitualmente un mensaje multidifusión, en la mayoría de los casos el secreto compartido K_{GH} no puede ser un secreto compartido por pares, sino un secreto colectivo compartido por el grupo potencial de controladores de acceso.

NOTA – Este postulado limita la escalabilidad en el caso general y no permite la autenticación de la fuente. Sin embargo, estas limitaciones de capacidad y seguridad pueden admitirse en redes pertenecientes a compañías con un número pequeño y limitado de controladores de acceso. La protección de la comunicación multidifusión entre controladores de acceso utilizando firmas digitales podría solventar esas limitaciones; no obstante, esto queda en estudio.

Si el mecanismo **LRQ** se utiliza para localizar al controlador de acceso distante, **LRQ** transportará un ClearToken separado que tenga el valor **tokenOID** "I10"; no debe utilizarse ningún otro campo en ese ClearToken. Para el caso multidifusión, el **generalID** en el ClearToken de **LRQ** no se utilizará. La comunicación entre controladores de acceso mediante H.501 y/o H.510 queda en estudio.

9.4 Fase LCF

EK_{BH} es la clave de criptación y KS_{BH} la clave adicional compartidas entre el EP B y el GK H. Como se describe a continuación, ambas entidades calculan separadamente estas claves a partir del secreto compartido K_{BH}, utilizando una PRF.

El GK H generará una solicitación B (Challenge-B) aleatoria, el material de clave de criptación EK_{BH} y el material de clave adicional KS_{BH}, a partir del secreto compartido K_{BH}, utilizando un procedimiento de cálculo de clave basado en una PRF, como se define en la cláusula 12, en donde Challenge-B será el valor de **challenge** y CT_{HG}**→h235Key→secureSharedSecret→keyDerivationOID** incluirá "AnnexI-HMAC-SHA1-PRF", véase la cláusula 14.

EK_{GH} es la clave de criptación y KS_{GH} la clave adicional compartidas entre los GK G y H. El GK H generará un Challenge-G aleatorio. El GK H generará material de clave de criptación EK_{GH} y de clave adicional KS_{GH} a partir del secreto compartido K_{GH}, utilizando el procedimiento de cálculo de clave basado en una PRF que se define en la cláusula 14, donde Challenge-G será el valor de

challenge. CT_{HG}→**challenge** incluirá challenge-G, y se establecerá el ID del EP B en CT_{HG}→**h235Key**→**secureSharedSecret**→**generalID.**

El GK H transmitirá al GK G las claves EK_{BH} y KS_{BH} criptadas. El modo de criptación OFB mejorado (EOFB, *enhanced OFB*) (véase 8.4/H.235.6) se utilizará con la clave adicional secreta y específica del EP, KS_{GH}. Los algoritmos de criptación aplicables son (véase el cuadro 6/H.235.6):

– DES (56 bits) en modo EOFB que utiliza OID "Y1": facultativo.

– 3DES (168 bits) en modo EOFB exterior que utiliza OID "Z1": facultativo.

– AES (128 bits) en modo EOFB que utiliza OID "Z2": algoritmo por defecto y es recomendado.

– Compatible con RC2 (56 bits) en modo EOFB que utiliza OID "X1": facultativo.

En el caso del modo de criptación EOFB, el GK H generará un valor aleatorio inicial, IV, cuya longitud será 64 bits para los OID "X1", "Y1" y "Z1". Este valor se transportará en CT_{HG}→**h235Key**→**secureSharedSecret**→**params**→**iv8**. Cuando se trate de OID "Z2", IV tendrá 128 bits y se transportará en CT_{HG}→**h235Key**→**secureSharedSecret**→**params**→**iv16**.

El GK H incluirá $ENC_{EK_{GH},\ KS_{GH},\ IV}(EK_{BH})$ y $ENC_{EK_{GH},\ KS_{GH},\ IV}(KS_{BH})$ en el ClearToken CT_{HG} con un **tokenOID** puesto a "I13". El texto cifrado que se obtiene, $ENC_{EK_{GH},\ KS_{GH},\ IV}(EK_{BH})$, se transportará en CT_{HG}→**h235Key**→**secureSharedSecret**→**encryptedSessionKey**; el texto cifrado obtenido, $ENC_{EK_{GH},\ KS_{GH},\ IV}(KS_{BH})$, se ha de transportar en CT_{HG}→**h235Key**→**secureSharedSecret**→**encryptedSaltingKey**. En CT_{HG}→**h235Key**→**algorithmOID** ("X1", "Y1", "Z1" o "Z2") se indicará cuál es el algoritmo de criptación. Hay que incluir Challenge-B en CT_{HG}→**h235Key**→**secureSharedSecret**→**clearSaltingKey**. CT_{HG}→**generalID** tendrá el valor del identificador del GK G, mientras que CT_{HG}→**sendersID** tendrá el valor del identificador GK H.

Se transportará Challenge-B hasta el EP B incluyendo una **profileInfo** en el **ClearToken** CT_{HG}→**profileInfo**→**elementID** = 0, que identifique a este elemento particular de perfil.

No se utiliza CT_{HG}→**profileInfo**→**paramS** en tanto que CT_{HG}→**profileInfo**→**element**→**octets** incluirá Challenge-B.

La respuesta **LCF** incluirá el ClearToken CT_{HG}.

9.5 Fase ACF

Al reconocer que los EP A y B soportan esta Recomendación, el GK G generará material de clave y ClearTokens, como se especifica a continuación.

Además de efectuar la **ARQ** normal, el GK es capaz de calcular un secreto compartido, K_{AB}, para la llamada, que se propaga entonces hasta los dos EP mediante ClearTokens. Estos ClearTokens se transportan en el mensaje **ACF** y retornan a la parte llamante.

Se incluirán dos ClearTokens: uno, CT_A, para la parte llamante A y otro, CT_B, para la parte llamada B. Cada **ClearToken** tendrá un OID ("I11" o "I12") en el **tokenOID** que indique si está destinado a quien llama (OID "I11" para CT_A) o a quien recibe la llamada (OID "I12" para CT_B).

Para obtener EK_{BH} y KS_{BH}, el GK G descriptará, respectivamente, CT_{HG}→**h235Key**→**secureSharedSecret**→**encryptedSessionKey** y CT_{HG}→**h235Key**→**secureSharedSecret**→**encryptedSaltingKey**.

Es posible utilizar el **ClearToken,** según se define en esta Recomendación, combinado con otros perfiles de seguridad, por ejemplo H.235.1 o H.235.3, que también empleen ClearTokens, en cuyo caso el ClearToken de esta Recomendación utilizará también los campos de otros **ClearToken**. Por ejemplo, para combinar esta Recomendación con H.235.1 hay que incluir y utilizar los campos

timestamp, **random**, **generalID**, **sendersID** y **dhkey**, conforme a la descripción dada en el perfil de seguridad H.235.1.

El ID del GK (GKID) G se incluirá en CT_A→**sendersID** y CT_B→**sendersID**, en tanto que CT_A→**generalID** tendrá el ID del EP A y CT_B→**generalID** el del EP B.

El GK G generará material de clave adicional, KS_{GH}, y de clave de criptación, EK_{GH}, a partir de K_{GH} utilizando el procedimiento de cálculo de claves basado en una PRF que se define en la cláusula 12, en el que se reemplaza **challenge** por CT_{HG}→**challenge**.

Las claves de criptación EK_{AG} y EK_{BH} para la clave extremo a extremo criptada, K_{AB}, se calcularán a partir del secreto compartido entre el GK y los EP (EK_{AG} o EK_{BH}) utilizando el procedimiento de cálculo de claves basado en una PRF que se define en la cláusula 12. En CT_A→**h235Key**→**secureSharedSecret**→**keyDerivationOID** y en CT_B→**h235Key**→**secureSharedSecret**→**keyDerivationOID** se incluirá "AnnexI-HMAC-SHA1-PRF", véase la cláusula 14 y en CT_A→**challenge** se indicará Challenge-A.

El GK G copiará Challenge-B de CT_{HG}→**h235Key**→**secureSharedSecret**→**clearSaltingKey** en CT_B→**challenge**.

CT_B→**profileInfo** incluirá el elemento de perfil transportado en **profileInfo** del CT_{HG}, de tal manera que al final el EP B obtenga Challenge-B.

Este secreto de sesión, K_{AB}, será criptado por EK_{AG} (para un CT destinado al EP A) o por EK_{BH} (para un CT destinado al EP B) mediante un algoritmo de criptación.

El modo de criptación OFB mejorado (EOFB) (véase 8.4/H.235.6) se utilizará con las claves adicionales secretas específicas de punto extremo, KS_{AG} o KS_{BH}. Los algoritmos de criptación que se pueden emplear son (véase el cuadro 6/H.235.6):

– DES (56 bits) en modo EOFB que utiliza OID "Y1": facultativo.
– 3DES (168 bits) en modo EOFB exterior que utiliza OID "Z1": facultativo.
– AES (128 bits) en modo EOFB que utiliza OID "Z2": algoritmo por defecto y recomendado.
– Compatible con RC2 (56 bits) en modo EOFB que utiliza OID "X1": facultativo.

En el caso del modo de la criptación EOFB, el GK G generará un valor aleatorio inicial, IV, cuya longitud será 64 bits para los OID "X1", "Y1" y "Z1", y que se transportará en CT_A→**h235Key**→**secureSharedSecret**→**params**→**iv8** y CT_B→**h235Key**→**secureSharedSecret**→**params**→**iv8**. Cuando se trate del OID "Z2", IV tendrá 128 bits y se transportará en CT_A→**h235Key**→**secureSharedSecret**→**params**→**iv16** y en CT_B→**h235Key**→**secureSharedSecret**→**params**→**iv16**.

El texto cifrado obtenido, $ENC_{EK_{AG},\ KS_{AG},\ IV}(K_{AB})$, se transportará en CT_A→**h235Key**→**secureSharedSecret**→**encryptedSessionKey**, mientras que $ENC_{EK_{BH},\ KS_{BH},\ IV}(K_{AB})$ irá en CT_B→**h235Key**→**secureSharedSecret**→**encryptedSessionKey**. El algoritmo de criptación se indicará en CT_A→**h235Key**→**secureSharedSecret**→**algorithmOID** y en CT_B→**h235Key**→**secureSharedSecret**→**algorithmOID** ("X1", "Y1", "Z1" o "Z2").

Cuando se trate del ClearToken destinado al EP A, se incluirá el ID del EP B ($EPID_B$) en CT_A→**h235Key**→**secureSharedSecret**→**generalID**. Del mismo modo, para el caso del ClearToken destinado al EP B, el $EPID_A$ se incluirá en CT_B→**h235Key**→**secureSharedSecret**→**generalID**.

No se utilizará **encryptedSaltingKey** con los algoritmos de criptación EOFB.

El GK G incluirá los ClearTokens CT_A y CT_B en el **ACF** hacia el EP A.

9.6 Fase de establecimiento (SETUP)

El EP A identificará el CT_A a partir del **tokenOID** "I11" en el ClearToken.

El EP A verificará si el CT_A obtenido está actualizado, examinado la **timestamp**. Se utilizarán otras pruebas adicionales de seguridad para verificar los **generalID** y **sendersID** del ClearToken y el **generalID** en **V3KeySyncMaterial**. Cuando se haya establecido que el CT_A recibido está actualizado, el EP A extraerá el IV y calculará EK_{AG} y KS_{AG}, siguiendo el mismo procedimiento descrito antes para el caso del GK G. Para obtener K_{AB}, el EP A descriptará la información **encryptedSessionKey** encontrada en el **secureSharedSecret** de CT_A.

Si se ha comprobado que el CT_A está actualizado, el EP A puede enviar al EP B un mensaje SETUP en el que se incluya el CT_B. Este mensaje deberá estar protegido (en lo relativo a la autenticación y/o la integridad) conforme a la Rec. UIT-T H.235.1 o la Rec. UIT-T H.235.3, utilizando K_{AB} como secreto compartido. En este proceso no se podrá emplear el **generalID** incluido en el ClearToken H.235.1 que resulta de la función de troceo (¡diferente del CT_B!), salvo si el EP A ya dispone de un $EPID_B$ (por ejemplo, obtenido por configuración o memorizado tras una comunicación anterior). Si el EP A utiliza un valor $EPID_B$ para el generalID en el SETUP, tendrá que aceptar como el verdadero $EPID_B$ el valor sendersID recibido en el mensaje de señalización de llamada retornado.

El EP B identificará el CT_B inspeccionando el **tokenOID** "I12" en el ClearToken.

El EP B verificará si el CT_B obtenido está actualizado, examinando la **timestamp**. Se utilizarán otras pruebas adicionales de seguridad para verificar el **sendersID** del ClearToken y el **generalID** en **secureSharedSecret**. Cuando se haya establecido que el CT_B recibido está actualizado, el EP B extraerá Challenge-B de CT_{HG}→**profileInfo**→**element**→**octets**, recuperará el IV y calculará EK_{BH} y KS_{BH}, utilizando Challenge-B como valor de **challenge** en la cláusula 12, como se describió *supra* para el caso de un GK. Para obtener K_{AB}, el EP B descriptará la información **encryptedSessionKey** encontrada en el **secureSharedSecret** del CT_B.

Si se comprobó que el CT_B está actualizado, el EP B podrá continuar con la señalización de llamada, respondiendo mediante CALL-PROCEEDING, ALERTING o CONNECT etc., cuando corresponda. Si el CT_B no está actualizado o ha fallado la verificación de seguridad del mensaje SETUP, el EP B responderá con RELEASE-COMPLETE y el **ReleaseCompleteReason** será "error de seguridad", como se define en 11.1/H.235.0.

Si hay que emplear seguridad de medios (véase 6.1/H.235.6), los EP A y B intercambiarán semiclaves Diffie-Hellman, con arreglo a 8.5/H.235.6, y establecerán una clave maestra dinámica para la sesión, a partir de la cual se pueden calcular las claves de sesión propias de cada medio.

El EP B incluirá el **generalID** con el valor $EPID_A$ y el **sendersID** con el valor $EPID_B$ para proteger todo mensaje de señalización de llamada H.225.0 destinado al EP A (por ejemplo, llamada en curso, aviso o conexión).

En la figura 2 se muestra el flujo básico de comunicación:

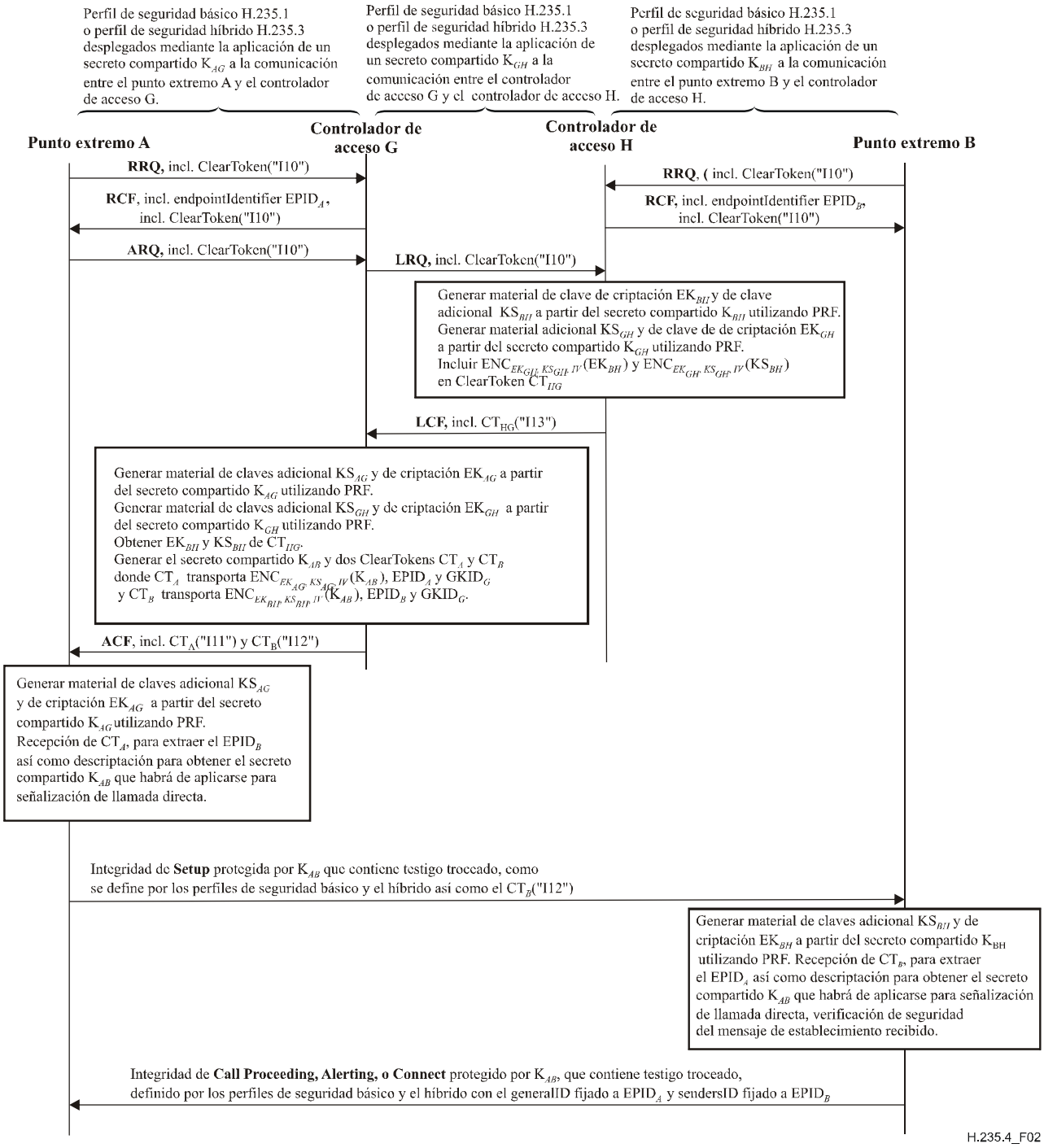

Figura 2/H.235.4 – Flujo básico de comunicación (DRC1)

10 Procedimiento DRC2 (entre dominios diferentes)

Este procedimiento se aplica en entornos en los que hay comunicación entre distintos dominios, con GK ubicados en diferentes dominios administrativos, cada uno de los cuales puede tener su propia política de seguridad. El procedimiento DRC2 se aplica cuando el EP llamante o los GK no soportan el algoritmo Diffie-Hellman.

En tales casos se admite que el GK H de terminación fije la política efectiva de seguridad para una llamada que se va a establecer; en otras palabras, este GK escoge los parámetros de seguridad que se han de aplicar, los cuales serán aceptados por el GK G de origen.

10.1 Fase GRQ/RRQ

Los EP que soporten este perfil de seguridad habrán de indicarlo en **GRQ** y/o **RRQ** incluyendo un ClearToken independiente cuyo **tokenOID** sea "I20"; no conviene utilizar ningún otro campo en dicho ClearToken. Un GK que tenga capacidades H.235.4 y que desee contar con esa funcionalidad deberá responder con **GCF** o **RCF**, incluyendo un ClearToken independiente cuyo **tokenOID** sea "I20" y en el que no se use ningún otro campo.

10.2 Fase ARQ

Antes de que un EP A empiece a enviar directamente mensajes de señalización de llamada a otro EP B, uno de los dos deberá solicitar al GK G o H la admisión, utilizando **ARQ**. El EP A tendrá que incluir en el **ARQ** un ClearToken independiente con **tokenOID** igual a "I20" y en el que no se use ningún otro campo.

10.3 Fase LRQ

Este procedimiento vale para el caso de un solo controlador de acceso, común a los dos puntos extremos, también para el caso de múltiples controladores de acceso en cadena. Cuando intervienen múltiples controladores de acceso, el controlador de acceso G, en cuya zona se origina la llamada, debe localizar el controlador de acceso H utilizando el mecanismo **LRQ** (multidifusión) como se describe en 8.1.6/H.323, "Señalización facultativa de punto extremo llamado". La comunicación entre dos controladores de acceso deberá protegerse conforme a la Rec. UIT-T H.235.1. Se supone que hay un secreto compartido común K_{GH}. Puesto que **LRQ** entre los controladores de acceso es habitualmente un mensaje multidifusión, en la mayoría de los casos, el secreto compartido K_{GH} no puede ser un secreto compartido por pares, sino un secreto colectivo compartido por el grupo potencial de controladores de acceso.

NOTA – Este postulado limita la escalabilidad en el caso general y no permite la autenticación de la fuente. Sin embargo, estas limitaciones de capacidad y seguridad pueden admitirse en redes pertenecientes a compañías con un número pequeño y limitado de controladores de acceso. La protección de la comunicación multidifusión entre controladores de acceso utilizando firmas digitales podría solventar esas limitaciones; no obstante, esto queda en estudio.

Si el mecanismo **LRQ** se utiliza para localizar el controlador de acceso distante, **LRQ** transportará un ClearToken separado cuyo **tokenOID** será "I20"; no debe utilizarse ningún otro campo en ese ClearToken. Para el caso multidifusión, el **generalID** en el ClearToken de **LRQ** no se utilizará. La comunicación entre controladores de acceso mediante H.501 y/o H.510 queda en estudio.

10.4 Fase LCF

Al reconocer que los EP A y B soportan esta Recomendación, el GK H generará material de clave y ClearTokens en **LCF**, como se especifica a continuación.

K_{BH} es el secreto compartido entre el EP B y el GK H. EK_{BH} es la clave de criptación y KS_{BH} la clave adicional compartidas entre el EP B y el GK H. El GK H generará un Challenge-B aleatorio. El GK H generará material de clave de criptación EK_{BH} a partir del secreto compartido K_{BH}, utilizando un procedimiento de cálculo de clave basado en una PRF, como se define en la cláusula 12, utilizando Challenge-B como valor de **challenge**, y CT_B→**h235Key**→**secureSharedSecret**→**keyDerivationOID** incluirá "AnnexI-HMAC-SHA1-PRF", véase la cláusula 14.

El GK H generará una clave adicional, KS_{BH}, a partir K_{BH} utilizando un procedimiento de cálculo de clave basado en una PRF, como se define en la cláusula 12, utilizando Challenge-B como valor de **challenge**.

EK_{GH} es la clave de criptación y KS_{GH} la clave adicional compartidas entre los GK G y H. El GK H generará un Challenge-G aleatorio. El GK H generará material de clave de criptación EK_{GH} a partir del secreto compartido K_{GH}, utilizando el procedimiento de cálculo de clave basado en una PRF que se define en la cláusula 12, utilizando Challenge-G como valor de **challenge**, y CT_{HG}→**h235Key**→**secureSharedSecret**→**keyDerivationOID** incluirá "AnnexI-HMAC-SHA1-PRF", véase la cláusula 14.

El GK H generará KS_{GH} a partir del secreto compartido K_{GH}, utilizando el procedimiento de cálculo de clave basado en una PRF que se define en la cláusula 12, con Challenge-G como valor de **challenge**.

El GK H crea dos ClearTokens en el mensaje **LCF**: uno, el CT_{HG}, para el GK G y otro, CT_B, para la entidad llamada, B. CT_{HG}→**tokenOID** incluirá un OID "I23" mientras que CT_B→**tokenOID** tendrá OID "I12".

Se especificarán: Challenge-G en CT_{HG}→**challenge**, el ID del GK H en CT_{HG}→**sendersID** y el ID del GK G (copiado de **LRQ**) en CT_{HG}→**generalID**.

Se especificarán: Challenge-B en CT_B→**challenge**, el ID del GK H en CT_B→**sendersID** y el ID del EP B en CT_B→**generalID**. Si el **LRQ** tiene el ID del EP A en su campo endpointIdentifier, el GK H lo copiará en CT_B→**h235Key**→**secureSharedSecret**→**generalID** y también en CT_{HG}→**h235Key**→**secureSharedSecret**→**generalID**.

La respuesta **LCF** incluirá los ClearToken CT_{HG} y CT_B si el GK H y el EP B también soportan el DRC2 de esta Recomendación.

Tras haber recibido el mensaje **LCF** del GK H, el GK G verifica los ClearToken CT_B y CT_{HG}. El GK G utiliza Challenge-G como **challenge** y la PRF para calcular KS_{GH} y EK_{GH} a partir de K_{GH} conforme a la cláusula 12 y luego descriptar CT_{HG}→**h235Key**→**secureSharedSecret**→**encryptedSessionKey** y obtener la K_{AB} compartida por los EP A y B.

10.5 Fase ACF

El GK H calcula un secreto, K_{AB}, para la llamada compartida entre los EP A y B, que luego se propaga a ambos EP utilizando ClearTokens. El ClearToken se devuelve inicialmente al GK G de origen, para que entonces éste envíe la información al llamante dentro de un mensaje **ACF**.

El GK H criptará $K_{AB,}$ con EK_{GH}, según el principio $ENC_{EK_{HG,}\ KS_{HG,}\ IV}(K_{AB})$, e incluirá la K_{AB} criptada en CT_{HG}→**h235Key**→**secureSharedSecret**→**encryptedSessionKey**.

El modo de criptación OFB mejorado (EOFB) (véase 8.4/H.235.6) se utilizará con la clave adicional secreta y específica del EP, KS_{GH}. Los algoritmos de criptación aplicables son (véase el cuadro 6 de H.235.6):

– DES (56 bits) en modo EOFB que utiliza OID "Y1": facultativo.
– 3DES (168 bits) en modo EOFB exterior que utiliza OID "Z1": facultativo.
– AES (128 bits) en modo EOFB que utiliza OID "Z2": algoritmo por defecto y recomendado.
– Compatible con RC2 (56 bits) en modo EOFB que utiliza OID "X1": facultativo.

En el caso del modo de criptación EOFB, el GK H generará un valor aleatorio inicial, IV, cuya longitud será 64 bits para los OID "X1", "Y1" y "Z1" y que se transportará en CT_{HG}→**h235Key→secureSharedSecret→ params→iv8**; cuando se trate del OID "Z2", IV tendrá 128 bits y se transportará en CT_{HG}→**h235Key→secureSharedSecret→params→iv16**.

El algoritmo de criptación se indicará en CT_{HG}→**h235Key→secureSharedSecret→algorithmOID** ("X1", "Y1", "Z1" o "Z2"). No se utilizará **encryptedSaltingKey** con los algoritmos de criptación EOFB.

Asimismo, el GK H criptará la K_{AB} con EK_{BH}, según el principio $ENC_{EK_{BH},\ KS_{BH},\ IV}(K_{AB})$, e incluirá la K_{AB} criptada en CT_B→**h235Key→secureSharedSecret→encryptedSessionKey**.

El modo de criptación OFB (mejorado) EOFB (véase 8.4/H.235.6) se utilizará con la clave secreta adicional específica de EP, KS_{BH}, para el EP B (CT_B). Los algoritmos de criptación aplicables son (véase el cuadro 6/H.235.6):

– DES (56 bits) en modo EOFB que utiliza OID "Y1": facultativo.

– 3DES (168 bits) en modo EOFB exterior que utiliza OID "Z1": facultativo.

– AES (128 bits) en modo EOFB que utiliza OID "Z2": algoritmo por defecto y recomendado.

– Compatible con RC2 (56 bits) en modo EOFB que utiliza OID "X1": facultativo.

En el caso del modo de criptación EOFB, el GK H generará un valor aleatorio inicial, IV, cuya longitud será 64 bits para los OID "X1", "Y1" y "Z1" y que se transportará en CT_B→**h235Key→secureSharedSecret→ params→iv8**; cuando se trate del OID "Z2", IV tendrá 128 bits y se transportará en CT_B→**h235Key→secureSharedSecret→params→iv16**.

El algoritmo de criptación se indicará en CT_B→**h235Key→secureSharedSecret→algorithmOID** ("X1", "Y1", "Z1" o "Z2"). No se utilizará **encryptedSaltingKey** con los algoritmos de criptación EOFB.

Para la respuesta **ACF** al EP A, se incluirán dos ClearTokens, a saber CT_A para la parte llamante, A, y CT_B para la parte llamada, B. **ClearToken** CT_A→**tokenOID** contendrá un OID "I11".

El GK G genera un Challenge-A y material de clave de criptación, EK_{AG} a partir del secreto compartido, K_{AG}, utilizando el procedimiento de cálculo de claves basado en una PRF de la cláusula 12, utilizando Challenge-A como **challenge**, y donde CT_A→**h235Key→secureSharedSecret→keyDerivationOID** contendrá "AnnexI-HMAC-SHA1-PRF" (véase la cláusula 14). Para CT_A→**challenge** indicará Challenge-A.

El GK G criptará $K_{AB,}$ con EK_{AG} como $ENC_{EK_{AG},\ KS_{AG},\ IV}(K_{AB})$, utilizando un algoritmo de criptación e incluirá la K_{AB} criptada en CT_A→**h235Key→secureSharedSecret→encryptedSessionKey**.

El modo de criptación OFB mejorado (EOFB) (véase 8.4/H.235.6) se utilizará con la clave secreta adicional específica de EP, KS_{AG}. Los algoritmos de criptación aplicables son (véase el cuadro 6/H.235.6):

– DES (56 bits) en modo EOFB que utiliza OID "Y1": facultativo.

– 3DES (168 bits) en modo EOFB exterior que utiliza OID "Z1": facultativo.

– AES (128 bits) en modo EOFB que utiliza OID "Z2": algoritmo por defecto y recomendado.

– Compatible con RC2 (56 bits) en modo EOFB que utiliza OID "X1": facultativo.

En el caso del modo de criptación EOFB, el GK G generará un valor aleatorio inicial, IV, cuya longitud será 64 bits para los OID "X1", "Y1" y "Z1" y que se transportará en CT_A→**h235Key→secureSharedSecret→params→iv8**; cuando se trate del OID "Z2", IV tendrá 128 bits y se transportará en CT_A→**h235Key→secureSharedSecret→params→iv16**. El algoritmo

de criptación se indicará en CT_A→**h235Key**→**secureSharedSecret**→**algorithmOID** ("X1", "Y1", "Z1" o "Z2").

Se especificarán: el ID del GK G en CT_A→**sendersID** y el ID del EP A en CT_A→**generalID**. Se copiará el ID del EP B de CT_B→**generalID** a CT_A→**h235Key**→**secureSharedSecret**→**generalID**.

Si el GK G no ha rellenado antes el campo endpointIdentifier del **LRQ** con el ID del EP A, deberá hacerlo en CT_B→**h235Key**→**secureSharedSecret**→**generalID**.

No se utilizará **encryptedSaltingKey** con los algoritmos de criptación EOFB.

Es posible utilizar el **ClearToken,** según se define en esta Recomendación, simultáneamente con otros perfiles de seguridad, por ejemplo H.235.1 o H.235.3, que también empleen ClearTokens, en cuyo caso el ClearToken de esta Recomendación utilizará también los los campos de esos otros **ClearToken**. Por ejemplo, para utilizar esta Recomendación y también con la Rec. UIT-T H.235.1, hay que incluir y utilizar los campos **timestamp**, **random**, **generalID**, **sendersID** y **dhkey**, conforme a la descripción dada en el perfil de seguridad H.235.1

Se incluirá en CT_A→**sendersID** se indicará el GKID del GK G, mientras que en CT_A→**generalID** se indicará el ID del EP A.

El EP A identificará el CT_A inspeccionando el CT_A→**tokenOID** "I21". El EP A verificará si el CT_A obtenido está actualizado, examinando la **timestamp**. Se utilizarán otras pruebas adicionales de seguridad para verificar los **generalID** y **sendersID** del ClearToken, y el **generalID** en **secureSharedSecret**. Cuando se haya establecido que el CT_A recibido está actualizado, el EP A extraerá el IV y calculará EK_{AG} y KS_{AG}, siguiendo el mismo procedimiento descrito antes para el caso del GK G, utilizando CT_A→**challenge** con Challenge-A como valor de **challenge** en la cláusula 12. El EP A descifrará CT_A→**h235Key**→**secureSharedSecret**→**encryptedSessionKey** para obtener K_{AB}.

10.6 Fase de establecimiento (SETUP)

El EP A identificará el CT_A a partir del CT_A→**tokenOID** "I11". El EP A verificará si el CT_A obtenido está actualizado, examinando la timestamp. Se utilizarán otras pruebas adicionales de seguridad para verificar los **generalID** y **sendersID** del ClearToken y el **generalID** en **secureSharedSecret**. Cuando se haya establecido que el CT_A recibido está actualizado, el EP A extraerá el IV y calculará EK_{AG} y KS_{AG}, siguiendo el mismo procedimiento descrito antes para el caso del GK G, utilizando CT_A→**challenge** como Challenge-A. El EP A descriptará CT_A→**h235Key**→**secureSharedSecret**→**encryptedSessionKey** para obtener K_{AG}.

Si se ha comprobado que el CT_A está actualizado, el EP A podrá enviar al EP B un mensaje SETUP en el que se incluya el CT_B. Este mensaje deberá estar protegido (en lo relativo a la autenticación y/o la integridad) conforme a las Recs. H.235.1 o H.235.3, utilizando K_{AB} como secreto compartido. En este proceso no se podrá emplear el **generalID** incluido en el ClearToken H.235.1 que resulta de la función de troceo (¡diferente del CT_B!), salvo si el EP A ya dispone de un $EPID_B$ (por ejemplo, obtenido por configuración o memorizado tras una comunicación anterior). Si el EP A utiliza un valor $EPID_B$ para el generalID en el SETUP, tendrá que aceptar como el verdadero $EPID_B$ el valor sendersID recibido en el mensaje de señalización de llamada retornado.

El EP B identificará el CT_B inspeccionando el **tokenOID** "I12" en el ClearToken.

El EP B verificará si el CT_B obtenido está actualizado, examinando la **timestamp**. Se utilizarán otras pruebas adicionales de seguridad para verificar **sendersID** del ClearToken y el **generalID** en **secureSharedSecret**. Cuando se haya establecido que el CT_B recibido está actualizado, el EP B extraerá el IV y calculará EK_{BH} y KS_{BH}, utilizando CT_B→**challenge** con Challenge-B como valor de **challenge** en la cláusula 12, como se describió antes para el GK H. El EP B descifrará CT_B→**h235Key**→**secureSharedSecret**→**encryptedSessionKey** para obtener K_{AB}.

Si se comprobó que el CT_B está actualizado, el EP B podrá continuar con la señalización de llamada, respondiendo mediante CALL-PROCEEDING, ALERTING, CONNECT etc., cuando corresponda. Si el CT_B no se ha renovado o ha fallado la verificación de seguridad del mensaje SETUP, el EP B responderá con RELEASE-COMPLETE y el **ReleaseCompleteReason** será "error de seguridad", como se define en 11.1/H.235.0.

Si hay que utilizar seguridad de medios (véase 6.1/H.235.6), los EP A y B intercambiarán semiclaves Diffie-Hellman, con arreglo a 8.5/H.235.6, y establecerán una clave maestra dinámica para la sesión, a partir de la cual se pueden calcular las claves de sesión propias de cada medio.

El EP B incluirá un **generalID** con el valor $EPID_A$ y un **sendersID** con el valor $EPID_B$ para proteger todo mensaje de señalización de llamada H.225.0 destinado al EP A (por ejemplo, llamada en curso, aviso o conexión).

En la figura 3 se muestra el flujo básico de comunicación:

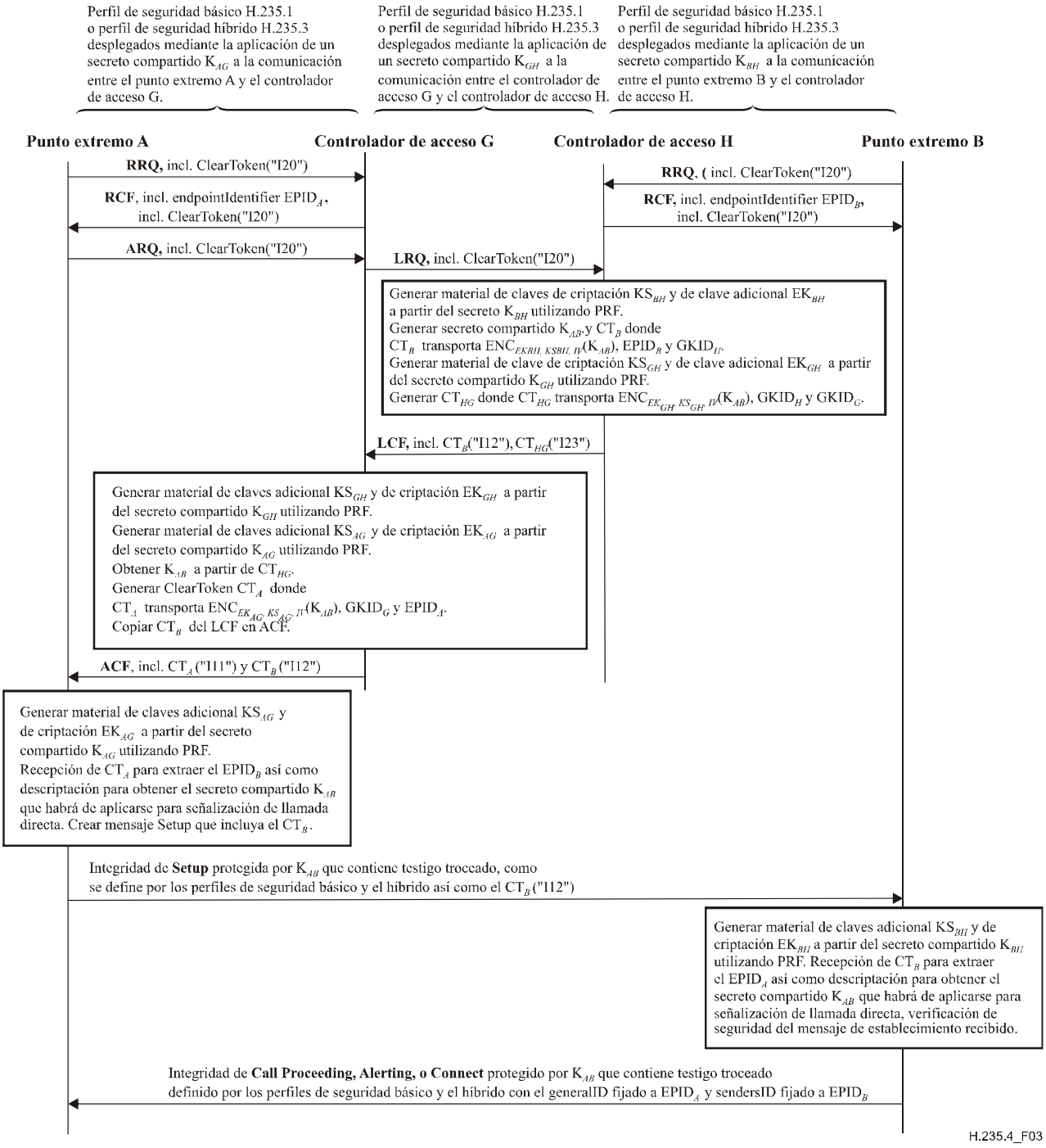

Figura 3/H.235.4 – Flujo básico de comunicación (DRC2)

11 Procedimiento DRC3 (entre dominios diferentes)

Este procedimiento se aplica a entornos en los que hay comunicación entre distintos dominios, en los que el EP llamante no soporta el algoritmo Diffie-Hellman, en tanto que los GK en ambos dominios, llamante y llamado, pueden calcular un intercambio DH. En tales casos, se calcula la clave de sesión intercambiando parámetros DH entre los GK de origen y terminación.

11.1 Fase GRQ/RRQ

En este caso puede haber varios GK en cadena. Los EP que soporten este perfil de seguridad habrán de indicarlo en **GRQ** y/o **RRQ** incluyendo un ClearToken independiente cuyo **tokenOID** sea "I30"; no se utiliza ningún otro campo en dicho ClearToken. Un GK que tenga capacidades H.235.4 y que desee contar con esa funcionalidad deberá responder con **GCF** o **RCF**, incluyendo un ClearToken independiente cuyo **tokenOID** sea "I30" y en el que no se use ningún otro campo.

11.2 Fase ARQ

Antes de que el EP A llame el EP B utilizando DRC3, el EP A envía un mensaje **ARQ** al GK G que contiene un ClearToken independiente cuyo **tokenOID** es "I30" y en el que no se utilizan los demás campos.

11.3 Fase LRQ

Tras recibir el mensaje **ARQ** enviado por el EP A, el GK G envía **LRQ** al GK H solicitando la dirección del EP B, no estando éste en el dominio del GK G. El GK G verifica el ClearToken en el mensaje **ARQ** y encuentra que el **tokenOID** es "I30". Si el GK G soporta el algoritmo DH, aplica ciertas reglas definidas con antelación que determinan que se debería elegir el DRC3.

El GK G genera entonces un mensaje **LRQ** con un ClearToken (en el CryptoHashedToken) cuyo **tokenOID** es "I30", queriendo indicar al GK H que es necesaria una negociación de clave DH. Se rellena el campo **dhkey** del ClearToken con los parámetros DH de la parte llamante (g, p, g^x) generados por el GK G y no se utilizan los demás campos.

Luego, el GK G envía este mensaje **LRQ** al GK H. De tratarse de un conjunto de GK, el GK G envía el mensaje **LRQ** a su GK vecino inmediato, el cual a su vez lo reenvía al siguiente, y así sucesivamente hasta que el mensaje **LCF** llegue al GK H.

En el caso de multidifusión, no se utilizará el **generalID** en el CryptoToken del **LRQ**. Si el GK G no pudo localizar el EP B de extremo lejano, tendrá que retornar un **ARJ** al EP A. Hay que garantizar la seguridad de la comunicación entre los dos GK conforme a la Rec. UIT-T H.235.1.

Cuando el GK G no soporte el perfil, podrá elegir si utiliza DRC2 o retornar ARJ al EP A. Si escoge DRC2, todas las fases subsiguientes, incluida la **LRQ**, serán idénticas a las de DRC2.

11.4 Fase LCF

Tras recibir el mensaje **LRQ** del GK G, el GK H, reconociendo que los EP A y B soportan este procedimiento, generará la clave de sesión, K_{AB}, como se especifica a continuación.

Para comenzar, el GK H produce un Challenge-B aleatorio, que se especificará como CT_B→**challenge** y CT_B→**h235Key**→**secureSharedSecret**→**keyDerivationOID** incluirá "AnnexI-HMAC-SHA1-PRF". Con la clave compartida K_{GH} y el Challenge-B calcula el material de clave EK_{GH} y de clave adicional KS_{GH} utilizando un procedimiento de cálculo de claves basado en una PRF.

Se especificarán: Challenge-B en CT_B→**challenge**, el ID del GK H en CT_B→**sendersID** y el ID del EP B en CT_B→**generalID**. Si el **LRQ** tiene en su campo endpoint Identifier el ID del EP A, el GK H lo copiará en CT_B→**h235Key**→**secureSharedSecret**→**generalID** y también en CT_{HG}→**h235Key**→**secureSharedSecret**→**generalID**.

El GK H incluye, entonces, dos ClearToken en el mensaje **LCF**, a saber el CT_{HG}, para el GK G cuyo **tokenOID** es "I33", y el CT_B, para el EP B cuyo **tokenOID** es "I12". El GK H genera los parámetros DH (g, p, g^y) de la parte llamada. El GK H calculará, utilizando los parámetros DH de la parte llamante obtenidos del mensaje **LRQ**, la clave de sesión $K_{AB} = g^{xy} \bmod p$.

Por último, el GK H criptará K_{AB} utilizando EK_{BH} y KS_{BH}, según el principio $ENC_{EK_{BH},\ KS_{BH},\ IV}(K_{AB})$, e incluirá la K_{AB} criptada en CT_B→**h235Key→secureSharedSecret→encryptedSessionKey** y los parámetros DH de la parte llamada en la **dhkey** del CT_{HG}. Los algoritmos de criptación aplicables son (véase el cuadro 6/H.235.6):

– DES (56 bits) en modo EOFB que utiliza OID "Y1": facultativo.

– 3DES (168 bits) en modo EOFB exterior que utiliza OID "Z1": facultativo.

– AES (128 bits) en modo EOFB que utiliza OID "Z2": algoritmo por defecto y recomendado.

– Compatible con RC2 (56 bits) en modo EOFB que utiliza OID "X1": facultativo.

En el caso del modo de criptación EOFB, el GK H generará un valor aleatorio inicial, IV, cuya longitud será 64 bits para los OID "X1", "Y1" y "Z1" y que se transportará en CT_B→**h235Key→secureSharedSecret→ params→iv8**; cuando se trate del OID "Z2", IV tendrá 128 bits y se transportará en CT_B→**h235Key→secureSharedSecret→params→iv16**.

El algoritmo de criptación se indicará en CT_B→**h235Key→secureSharedSecret→algorithmOID** ("X1", "Y1", "Z1" o "Z2"). No se utilizará **encryptedSaltingKey** con los algoritmos de criptación EOFB.

El GK H envía el mensaje **LCF** al GK G. Si hay un conjunto de GK, se transfiere el mensaje **LCF** por relevos, es decir cada GK lo recibe de su vecino inmediato en sentido ascendente, verifica el **LCF** que contiene el CT_{HG}, y lo reenvía a su vecino inmediato en sentido descendente.

Si el GK H no soporta el algoritmo DH o no se permite la política de seguridad de DRC3, se establecerá en su lugar DRC2. Las fases **LCF** y subsiguientes son, por ende, las del DRC2.

11.5 Fase ACF

Tras recibir el mensaje **LCF**, el GK G, reconociendo que el **tokenOID** en el ClearToken independiente es "I33", obtiene el DH de la parte llamada y crea un ClearToken denominado CT_A cuyo **tokenOID** será "I11", como se especifica a continuación.

En primer lugar, el GK G produce un Challenge-A aleatorio, que será el valor utilizado en CT_A→**challenge** y CT_A→**h235Key→secureSharedSecret→keyDerivationOID** indicará "AnnexI-HMAC-SHA1-PRF". Entonces emplea la clave compartida K_{AG} y el Challenge-A para calcular el material de clave EK_{AG} y el de clave adicional KS_{AG}, utilizando un procedimiento de cálculo de claves basado en una PRF.

Luego, el GK G utiliza los parámetros DH de la parte llamante obtenidos en la fase **LRQ**, combinados con los de la parte llamada, para calcular la clave de sesión $K_{AG} = g^{xy} \bmod p$.

El GK G copia entonces el ClearToken CT_B del mensaje **LCF** en el mensaje **ACF**, cuyo **tokenOID** es "I12".

Por último, el GK G cripta la K_{AB} utilizando EK_{AG} y KS_{AG}, según el principio $ENC_{EK_{AG},\ KS_{AG},\ IV}(K_{AB})$, la incluye en CT_A→**h235Key→secureSharedSecret→encryptedSessionKey** y copia el CT_B del mensaje **LCF** en el mensaje **ACF**.

El modo de criptación OFB mejorado (EOFB) (véase 8.4/H.235.6) se utilizará con la clave secreta adicional específica de EP, KS_{AG}.

Los algoritmos de criptación aplicables son (véase el cuadro 6/H.235.6):

– DES (56 bits) en modo EOFB que utiliza OID "Y1": facultativo.

– 3DES (168 bits) en modo EOFB exterior que utiliza OID "Z1": facultativo.

– AES (128 bits) en modo EOFB que utiliza OID "Z2": algoritmo por defecto y recomendado.

– Compatible con RC2 (56 bits) en modo EOFB que utiliza OID "X1": facultativo.

En el caso del modo de criptación EOFB, el GK G generará un valor aleatorio inicial, IV, cuya longitud será 64 bits para los OID "X1", "Y1" y "Z1" y que se transportará en CT_A→**h235Key→secureSharedSecret→params→iv8**; cuando se trate del OID "Z2", IV tendrá 128 bits y se transportará en CT_A→**h235Key→secureSharedSecret→params→iv16**. El algoritmo de criptación se indicará en CT_A→**h235Key→secureSharedSecret→algorithmOID** ("X1", "Y1", "Z1" o "Z2").

Si se determina que el **tokenOID** del ClearToken (en el **LCF**) es "I23", se concluye que se ha regresado al procedimiento DRC2, y es potestad del GK G decidir si acepta o no la política de seguridad del GK H. Si la acepta, la fase **ACF** y la fase SETUP subsiguiente serán las del DRC2. De lo contrario, se responde con el mensaje de rechazo correspondiente, indicando un fallo de seguridad con el motivo de rechazo securityDenial.

El GK G envía el mensaje **ACF** al EP A.

11.6 Fase de establecimiento (SETUP)

El EP A identificará el CT_A a partir de CT_A →**tokenOID** "I11". El EP A verificará si el CT_A obtenido está actualizado, examinando la **timestamp**. Se utilizarán otras pruebas adicionales de seguridad para verificar **sendersID** y **generalID** del ClearToken y el **generalID** en **secureSharedSecret**. Cuando se haya establecido que el CT_A está actualizado, el EP A extraerá el IV y calculará EK_{AG} y KS_{AG}, como se describió antes para el GK G, utilizando CT_A→**challenge** como Challenge-A. El EP A descriptará CTA→**h235Key→secureSharedSecret→encryptedSessionKey** para obtener KAG.

Si se ha comprobado que el CT_A está actualizado, el EP A podrá enviar al EP B un mensaje SETUP en el que se incluya el CT_B. Este mensaje deberá estar protegido (en lo relativo a la autenticación y/o la integridad) conforme a las Recs. UIT-T H.235.1 o H.235.3, utilizando K_{AB} como secreto compartido. En este proceso no se podrá emplear el **generalID** incluido en el ClearToken H.235.1 que resulta de la función de troceo (¡diferente del CT_B!), salvo si el EP A ya dispone de un $EPID_B$ (por ejemplo, obtenido por configuración o memorizado tras una comunicación anterior). Si el EP A utiliza un valor $EPID_B$ para el **generalID** en el SETUP, tendrá que aceptar como el verdadero $EPID_B$ el valor **sendersID** recibido en el mensaje de señalización de llamada retornado.

El EP B identificará el CT_B inspeccionando el **tokenOID** "I12" en el ClearToken.

El EP B verificará si el CT_B obtenido está actualizado, examinando la timestamp. Se utilizarán otras pruebas adicionales de seguridad para verificar **sendersID** del ClearToken y el **generalID** en **secureSharedSecret**. Cuando se haya establecido que el CT_B recibido está actualizado, el EP B extraerá el IV y calculará EK_{BH} y KS_{BH}, utilizando CT_B→**challenge** como Challenge-B. El EP B descriptará CT_B→**h235Key→secureSharedSecret→encryptedSessionKey** para obtener K_{AB}.

Si se comprobó que el CT_B está actualizado, el EP B podrá continuar con la señalización de llamada, respondiendo mediante CALL-PROCEEDING, ALERTING, CONNECT etc., cuando corresponda. Si el CT_B no se ha renovado o ha fallado la verificación de seguridad del mensaje SETUP, el EP B responderá con RELEASE-COMPLETE y el **ReleaseCompleteReason** será "error de seguridad", como se define en 11.1/H.235.0.

Si hay que utilizar seguridad de medios (véase 6.1/H.235.6), los EP A y B intercambiarán semiclaves Diffie-Hellman, con arreglo a 8.5/H.235.6, y establecerán una clave maestra dinámica para la sesión, a partir de la cual se pueden calcular las claves de sesión propias de cada medio.

El EP B incluirá un **generalID** con el valor $EPID_A$ y un **sendersID** con el valor $EPID_B$ para proteger todo mensaje de señalización de llamada H.225.0 destinado al EP A (por ejemplo, llamada en curso, aviso o conexión).

En la figura 4 se muestra el flujo básico de comunicación:

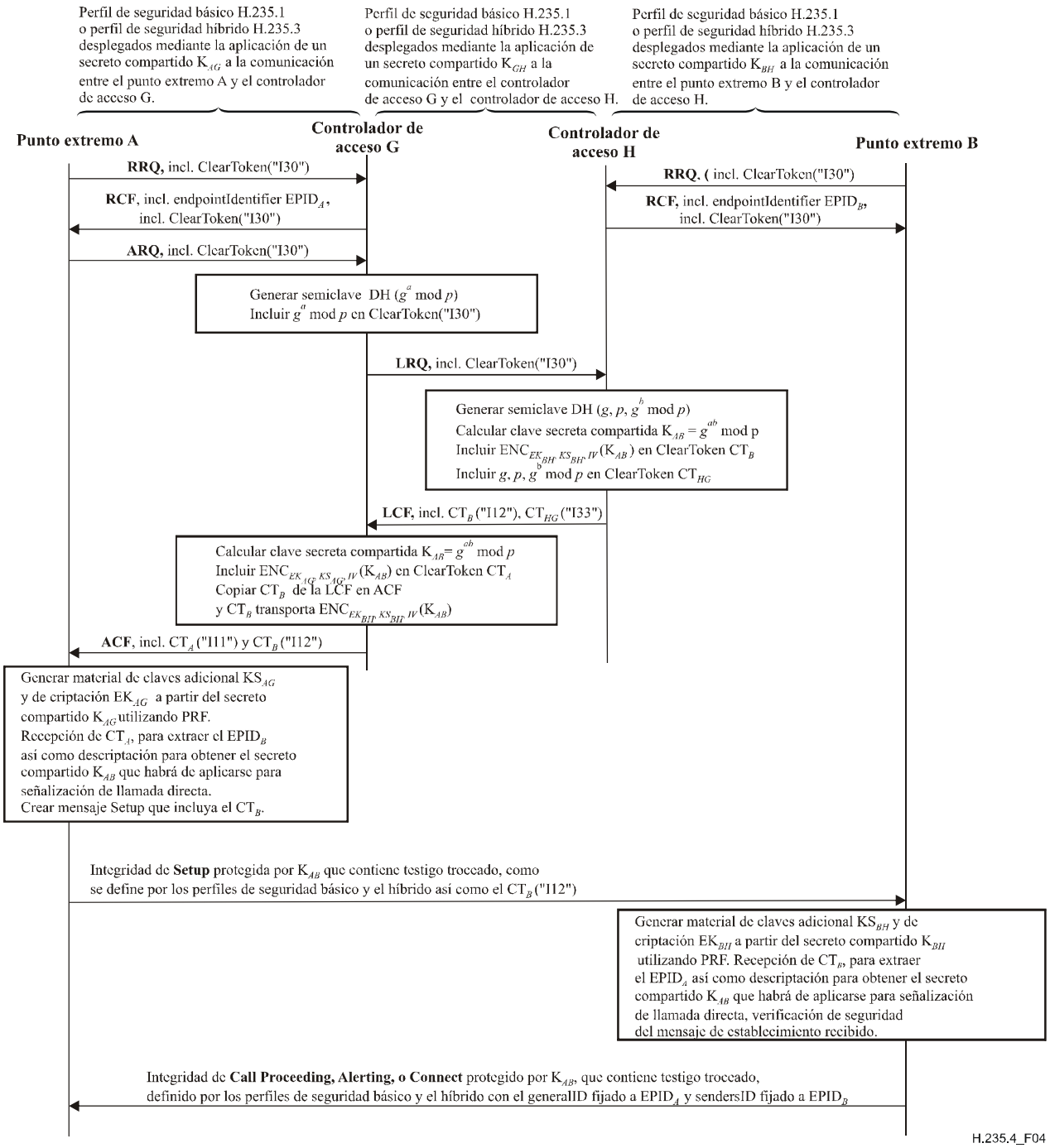

Figura 4/H.235.4 – Flujo de comunicación en el DRC3

12 Procedimiento de cálculo de clave basado en PRF

En esta cláusula se describe un procedimiento para calcular material de clave a partir del secreto compartido y otros parámetros.

Este procedimiento permite calcular una clave de criptación y una adicional a partir de un secreto compartido. El procedimiento es uniforme, sin importar cuál sea el secreto compartido (K_{AG}, K_{BH} o K_{GH}).

Para obtener el material de clave deseado (por ejemplo, EK_{AG}), se utilizará la PRF (véase la cláusula 10/H.235.0) combinada con los parámetros del cuadro 1, donde *inkey* es el secreto

compartido correspondiente (por ejemplo, K_{AG}) y *label* ha de ser la constante correspondiente (por ejemplo, 0x2AD01C64 || **challenge-A)** donde || indica que hay concatenación. El parámetro *outkey_len* será la longitud requerida del material de clave deseado, que depende del algoritmo de criptación que se emplee.

NOTA – Para EK_{AG}, KS_{AG}, EK_{BH} y KS_{BH} los enteros constantes de 32 bits (por ejemplo 0x2AD01C64, etc.) se toman de los decimales de *e* (es decir, 2,71828 ...), y para EK_{GH} y KS_{GH}, los enteros constantes de 32 bits se toman de los decimales de π (es decir, 3,14159 ...). Para EK_{AG}, EK_{BH}, KS_{AG} y KS_{BH}, los enteros de 32 bits provienen de bloques de 9 cifras decimales, respectivamente el primero, segundo, cuarto y séptimo bloques. El valor para EK_{GH} corresponde a las 10 primeras cifras decimales de π, en tanto que KS_{GH} corresponde a las 8 cifras decimales siguientes de π.

Cuadro 1/H.235.4 – Cálculo de las claves de criptación y adicional a partir de un secreto compartido

Clave deseada	*inkey* para la PRF	Constante || solicitación
EK_{AG}	K_{AG}	0x2AD01C64 || **Challenge-A**
KS_{AG}	K_{AG}	0x150533E1 || **Challenge-A**
EK_{BH}	K_{BH}	0x1B5C7973 || **Challenge-B**
KS_{BH}	K_{BH}	0x39A2C14B || **Challenge-B**
EK_{GH}	K_{GH}	0x54655307 || **Challenge-G**
KS_{GH}	K_{GH}	0x35855C60 || **Challenge-G**

13 Procedimiento de cálculo de clave basado en FIPS-140

En esta cláusula se puede describir un procedimiento que defina cómo calcular material de clave a partir del secreto compartido y otros parámetros utilizando el módulo de criptografía, conforme a FIPS-140. Queda en estudio.

14 Lista de identificadores de objeto

Cuadro 2/H.235.4 – Identificadores de objeto utilizados por H.235.4

Referencia de identificador de objeto	Valor de identificador de objeto	Descripción
"I10"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 48}	Utilizado en el procedimiento DRC1 durante GRQ/RRQ y GCF/RCF y ARQ; permite que los EP/GK indiquen soporte de DRC1.
"I11"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 49}	Utilizado en los procedimientos DRC1, DRC2 y DRC3 para el tokenOID del ClearToken; indica que el ClearToken CT_A especifica una clave extremo a extremo para el llamante.
"I12"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 50}	Utilizado en los procedimientos DRC1, DRC2 y DRC3 para el tokenOID del ClearToken; indica que el ClearToken CT_B especifica una clave extremo a extremo para el llamado.

Cuadro 2/H.235.4 – Identificadores de objeto utilizados por H.235.4

Referencia de identificador de objeto	Valor de identificador de objeto	Descripción
"I13"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 52}	Utilizado en el procedimiento DRC1 para el tokenOID del ClearToken entre GK; indica que el ClearToken CT_{HG} especifica una clave de criptación para el GK de origen.
"I20"	{itu-t (0) recommendation (0) h (8) 235 version (0) 4 53}	Utilizado en el procedimiento DRC2 durante GRQ/RRQ y GCF/RCF y ARQ; permite que los EP/GK indiquen soporte de DRC2.
"I23"	{itu-t (0) recommendation (0) h (8) 235 version (0) 4 56}	Utilizado en el procedimiento DRC2 para el tokenOID del ClearToken entre GK; indica que el ClearToken CT_{HG} especifica una clave de criptación para el GK de origen.
"I30"	{itu-t (0) recommendation (0) h (8) 235 version (0) 4 34}	Se utiliza en ClearToken independientes en GRQ/RRQ, GCF/RCF, ARQ para indicar que se soporta DRC3. Se utiliza en ClearToken independientes en LRQ para indicar que se transportan los parámetros DH del llamante.
"I33"	{itu-t (0) recommendation (0) h (8) 235 version (0) 4 37}	Se utiliza en ClearToken independientes en LCF para indicar que se transportan los parámetros DH del llamado.
"Annex I-HMAC-SHA1-PRF"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 51}	Utilizado en los procedimientos DRC1, DRC2 y DRC3 para el keyDerivationOID en V3KeySyncMaterial; indica el método de cálculo de clave aplicado en la cláusula 12 utilizando la función seudoaleatoria HMAC-SHA1.

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