

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

H.235

Corrigendum 1
(01/2005)

SERIE H: SISTEMAS AUDIOVISUALES Y MULTIMEDIOS

Infraestructura de los servicios audiovisuales – Aspectos
de los sistemas

Seguridad y criptado para terminales multimedia
de la serie H (basados en las
Recomendaciones UIT-T H.323 y H.245)

Corrigendum 1

Recomendación UIT-T H.235 (2003) – Corrigendum 1

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

Seguridad y criptado para terminales multimedia de la serie H (basados en las Recomendaciones UIT-T H.323 y H.245)

Corrigendum 1

Resumen

La versión 3 de la Rec. UIT-T H.235 sustituye a la versión 2 con las siguientes mejoras: un procedimiento para señales DTMF criptadas, unos identificadores de objeto para el algoritmo de criptación AES a efectos de criptación de cabida útil de medios, el modo de criptación para el cifrado de trenes OFB mejorado (EOFB) para la criptación de trenes de medios, una opción de sólo autenticación para el paso sin problemas a través de un NAT/cortafuegos, presentada en el anexo D, un procedimiento de distribución de claves en el canal RAS, algunos procedimientos para el transporte más seguro de claves de sesión y una distribución y actualización de claves más robustas, unos procedimientos para proporcionar seguridad a trenes de cabida útil múltiple, un mejor soporte de seguridad para las llamadas con encaminamiento directo en un nuevo anexo I, unos medios de señalización que permitan informes de error más flexibles, algunas aclaraciones y mejoras de la eficacia con el fin de lograr seguridad en el arranque rápido y para la señalización Diffie-Hellman, junto con parámetros Diffie-Hellman más largos y ciertos cambios provenientes de la guía del implementador de la Rec. UIT-T H.323

La enmienda 1 permitió ampliar la versión 3 de la Rec. UIT-T H.235 al incluir el nuevo anexo H y ampliar la funcionalidad del anexo I. Se han introducido modificaciones en la ASN.1 para mejorar el anexo H. Pueden utilizarse para cualquier otro fin identificado por el elemento **profileInfo** de ClearToken. Esta enmienda contiene también algunas correcciones y actualiza el texto de la versión 3 de la Rec. UIT-T H.235.

El corrigendum 1 permitió alinear la especificación de la función pseudoaleatoria que se define en B.7 con la función pseudoaleatoria definida a su vez en la norma RFC 3830, corregir los errores de redacción en las figuras F.2 y F.3 y corregir también un par de defectos en el anexo I.

Orígenes

El corrigendum 1 a la Recomendación UIT-T H.235 (2003) fue aprobado el 8 de enero de 2005 por la Comisión de Estudio 16 (2005-2008) del UIT-T por el procedimiento de la Recomendación UIT-T A.8.

PREFACIO

La UIT (Unión Internacional de Telecomunicaciones) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones. El UIT-T (Sector de Normalización de las Telecomunicaciones de la UIT) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB.

© UIT 2005

Reservados todos los derechos. Ninguna parte de esta publicación puede reproducirse por ningún procedimiento sin previa autorización escrita por parte de la UIT.

ÍNDICE

	Página
2 Referencias	1
Anexo B – Aspectos específicos de H.323	1
B.7 Función pseudoaleatoria (PRF)	1
Anexo F – Perfil de seguridad híbrido	2
F.10 Ejemplos ilustrativos	2
Anexo I – Soporte de llamadas con encaminamiento directo	7
I.5 Símbolos y abreviaturas	7
I.9 Procedimiento DRC.....	7
I.10 Procedimiento de cálculo de clave basado en PRF	13
I.11 Procedimiento de cálculo de clave basado en FIPS-140	14
I.12 Lista de identificadores de objeto	15

Recomendación UIT-T H.235

Seguridad y criptado para terminales multimedios de la serie H (basados en las Recomendaciones UIT-T H.323 y H.245)

Corrigendum 1

...

2 Referencias

...

– IETF RFC 3830 (2004), MIKEY: Multimedia Internet KEYing.

...

Anexo B

Aspectos específicos de H.323

...

B.7 Función pseudoaleatoria (PRF)

En esta cláusula se define una función pseudoaleatoria (PRF, *pseudo-random function*) para calcular claves dinámicas a partir de material de clave estática y un valor aleatorio.

NOTA – Esta PRF es idéntica a la PRF MIKEY (véase [MIKEY]/ sección 4.1.2 de RFC ~~xxxx~~3830).

El método de cálculo de clave tiene los siguientes parámetros de entrada:

- *inkey*: la clave de entrada para la función de cálculo.
- *inkey_len*: la longitud en bits de la clave de entrada.
- *label*: una etiqueta específica, que depende del tipo de clave que se debe calcular y del valor aleatorio **challenge**.
- *outkey_len*: longitud deseada en bits de la clave de salida.

La función pseudoaleatoria tiene el siguiente resultado:

- *outkey*: la clave de salida de longitud deseada.

~~Esta PRF será la que se define en la sección 4.1.2 de RFC 3830. Sea HMAC (véase [RFC 2104]) la función de autenticación de mensaje basada en SHA1 (véase [ISO/CEI 10118-3]). Como en RFC 2246 se define:~~

$$\begin{aligned} P(s, label, m) = & \text{HMAC}(s, A_1 || label) || \\ & \text{HMAC}(s, A_2 || label) || \dots \\ & \text{HMAC}(s, A_{\#} || label) \end{aligned}$$

~~donde:~~

$$\text{A}_0 = label,$$

~~————— $A_i = \text{HMAC}(s, A_{i-1})$.~~

~~Mientras que se suele utilizar SHA1 [ISO/CEI 10118-3], se puede también utilizar HMAC con otras funciones generadoras; esto queda en estudio.~~

~~A continuación se describe un procedimiento para obtener una función pseudoaleatoria, denominada $\text{PRF}(\text{inkey}, \text{label})$, que se aplica para computar la clave de salida, outkey :~~

- ~~• sea $s_{\#} = \text{inkey_len}/512$, aproximada al entero más cercano~~
- ~~• sepárese inkey en n bloques, $\text{inkey} = s_1 || \dots || s_{\#}$, donde todos los s_i , salvo probablemente $s_{\#}$, tienen 512 bits~~
- ~~• sea $m = \text{outkey_len}/160$, aproximada al entero más cercano.~~

~~Se obtiene entonces la clave de salida, outkey , como los outkey_len bits más significativos de~~

~~————— $\text{PRF}(\text{inkey}, \text{label}) = P(s_1, \text{label}, m) \text{ XOR } P(s_2, \text{label}, m) \text{ XOR } \dots \text{ XOR } P(s_{\#}, \text{label}, m)$.~~

...

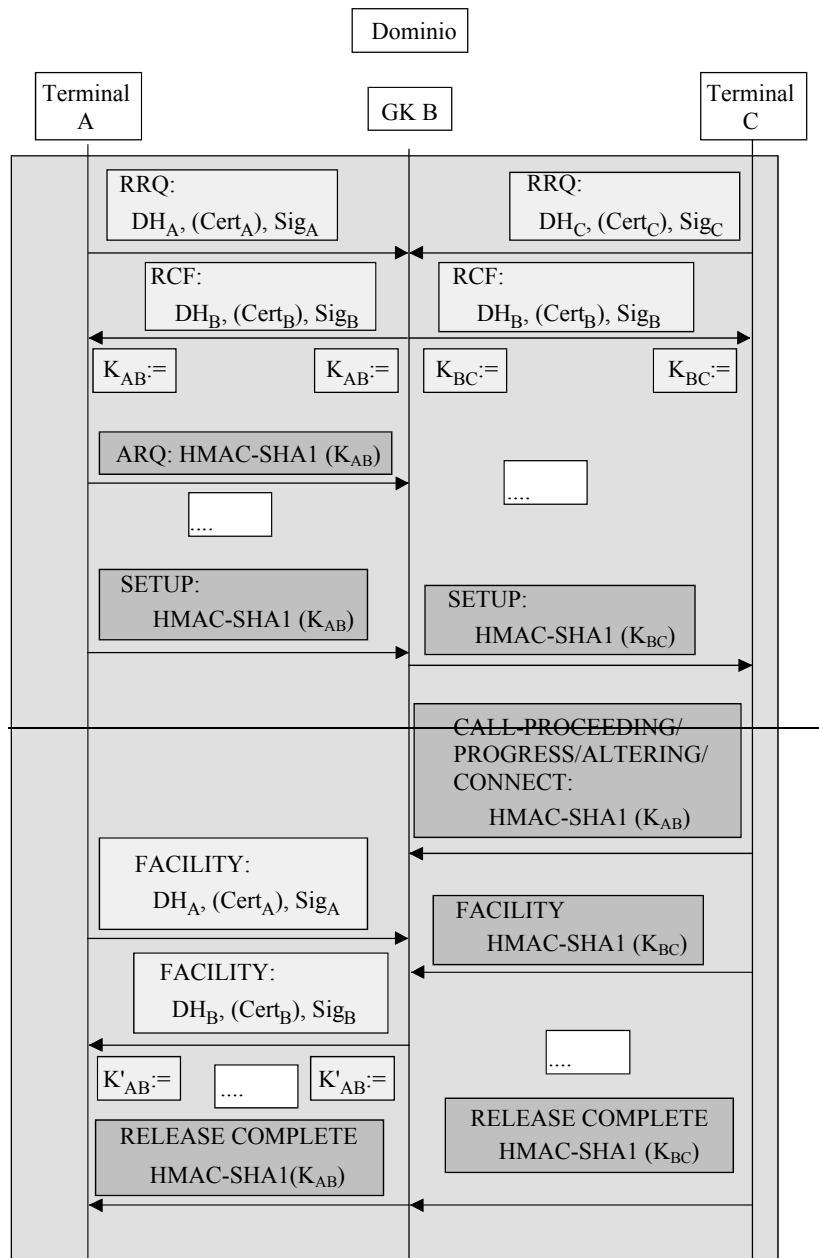
Anexo F

Perfil de seguridad híbrido

...

F.10 Ejemplos ilustrativos

...



T1610350-02

Cert	Certificado de usuario	K, K'	Clave de enlace simétrica
DH_A	Testigo Diffie-Hellman $g^a \bmod p$	Sig	Firma digital
DH_B	Testigo Diffie-Hellman $g^b \bmod p$		
EP	Punto extremo (Terminal)		
GK	Controlador de acceso		

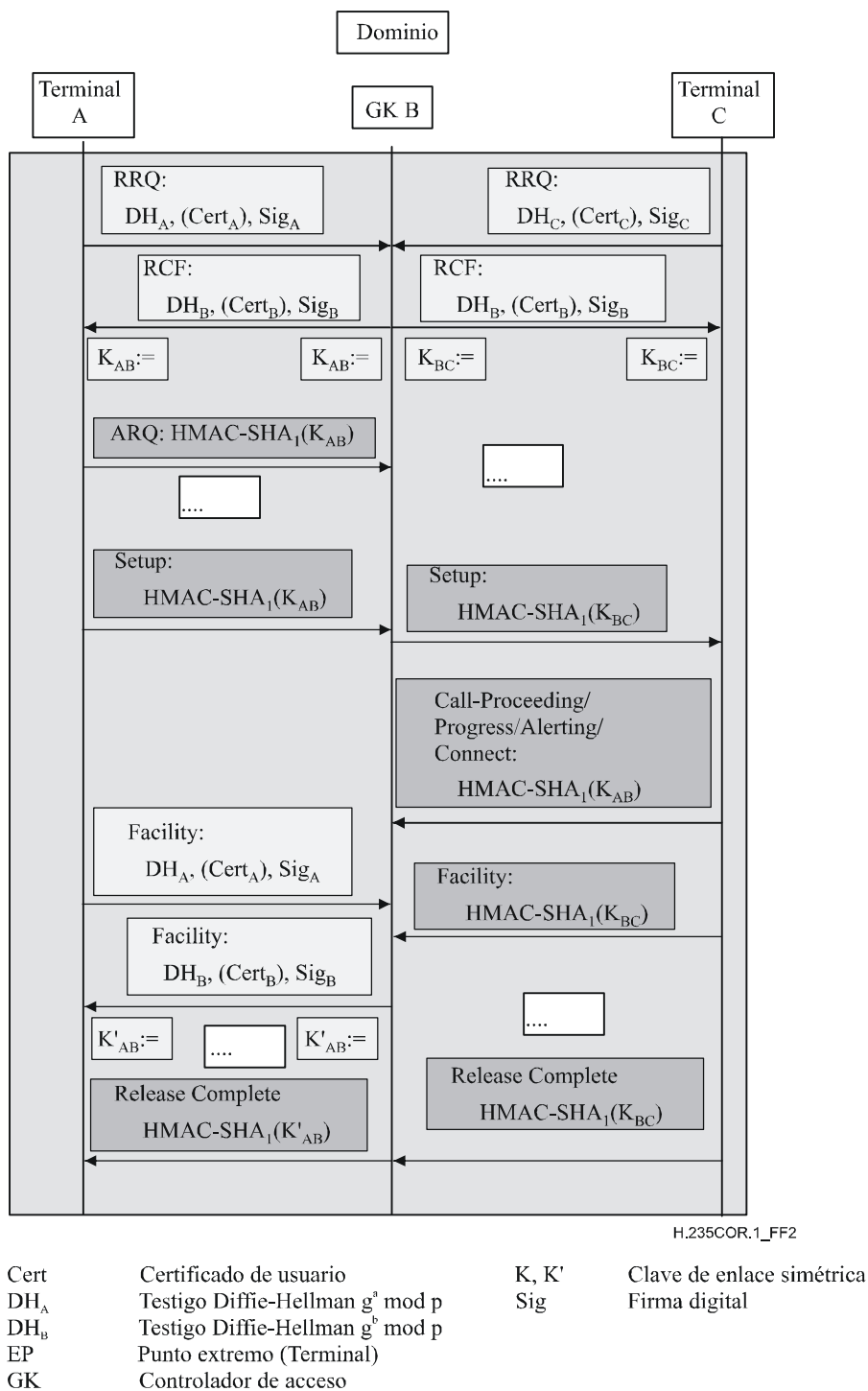
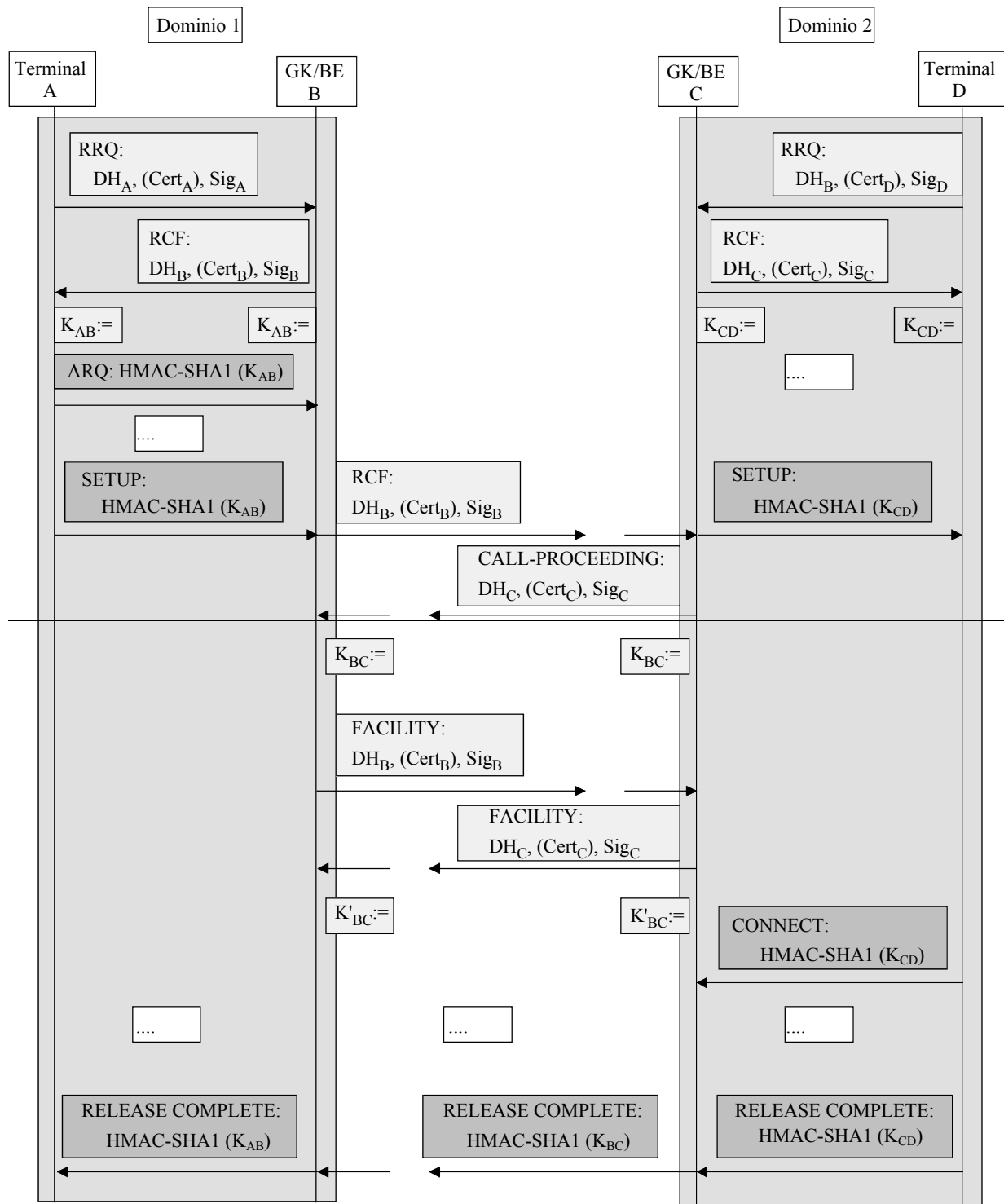


Figura F.2/H.235 – Diagrama de flujo en un dominio administrativo simple

...



T1610360-02

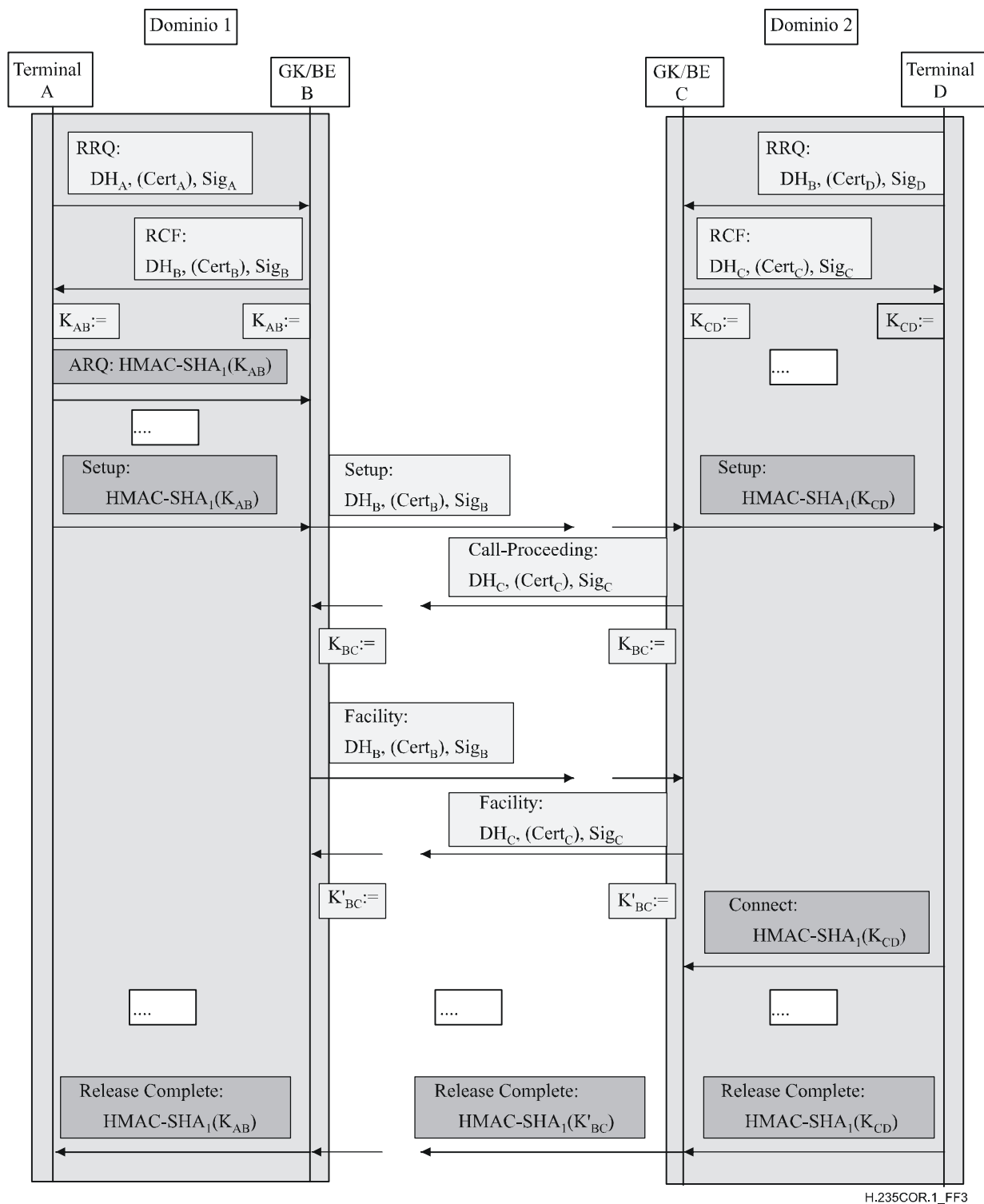


Figura F.3/H.235 – Diagrama de flujo en un dominio administrativo múltiple

...

Anexo I

Soporte de llamadas con encaminamiento directo

...

I.5 Símbolos y abreviaturas

En este anexo se usan las siguientes abreviaturas.

$ENC_{K;S,IV}(M)$	Criptación EOFB de M que utiliza claves secretas K y adicional secreta S , además de vector inicial IV
CT	Testigo despejado (<i>ClearToken</i>)
DRC	Llamada con encaminamiento directo (<i>direct-routed call</i>)
EPID	Identificador de punto extremo (<i>endpoint identifier</i>)
GKID	Identificador de controlador de acceso (<i>gatekeeper identifier</i>)
K_{AG}	Secreto compartido (anexo D, anexo F) entre el punto extremo A y el controlador de acceso G
K_{BH}	Secreto compartido (anexo D, anexo F) entre el punto extremo B y el controlador de acceso H
K_{GH}	Secreto compartido (anexo D, anexo F) entre el controlador de acceso G y el controlador de acceso H
KS_{AG}	Clave adicional compartida secreta entre el punto extremo A y el controlador de acceso G
KS_{BH}	Clave adicional compartida secreta entre el punto extremo B y el controlador de acceso H
KS_{GH}	<u>Clave adicional compartida secreta entre el controlador de acceso G y el controlador de acceso H</u>
EK_{AG}	La clave de criptación compartida entre el punto extremo A y el controlador de acceso G
EK_{BH}	La clave de criptación compartida entre el punto extremo B y el controlador de acceso H
EK_{GH}	<u>La clave de criptación compartida entre el controlador de acceso G y el controlador de acceso H</u>
K_{AB}	La clave de criptación compartida entre el punto extremo A y el punto extremo B
PRF	<u>Función pseudoaleatoria</u>

...

I.9 Procedimiento DRC

Los puntos extremos que puedan soportar este perfil de seguridad lo indicarán durante **GRQ** y/o **RRQ** incluyendo un ClearToken independiente con **tokenOID** puesto a "I0"; no se debería utilizar ningún otro campo en este ClearToken. El controlador de acceso que tenga las capacidades de este anexo I y desee proporcionar esta funcionalidad responderá con **GCF** ~~respuesta a o~~ **RCF** con un ClearToken aparte que tenga **tokenOID** puesto a "I0", todos los demás campos en ese ClearToken inutilizados.

Antes de que un punto extremo A empiece a enviar mensajes de señalización de llamada a otro punto extremo B directamente, uno de los dos solicitará admisión en el controlador de acceso G o H utilizando **ARQ**. El punto extremo A incluirá dentro de **ARQ** un ClearToken independiente con **tokenOID** puesto a "I0" y todos los demás campos en ese ClearToken inutilizados.

Este procedimiento comprende tanto el caso de un solo controlador de acceso, común a los dos 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 – debe 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 será securizada de acuerdo con el anexo D. Para esto, se supone que está disponible un secreto compartido común K_{GH} . Puesto que **LRQ** entre los controladores de acceso es típicamente un mensaje multidifusión, el secreto compartido K_{GH} no puede usualmente ser un secreto compartido por parejas, sino que se supone que es en realidad un secreto compartido en base a un grupo dentro de la nube potencial de controladores de acceso.

NOTA – Este supuesto limita la escalabilidad en el caso general y no permite la autenticación de la fuente. Sin embargo, se cree que en redes pertenecientes a compañías con un número pequeño, limitado, de controladores de acceso, esa restricción y las limitaciones de seguridad, son aún aceptables. La securización 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 con **tokenOID** fijado a "I0"; no debe utilizarse ningún otro campo en ese ClearToken. Para el caso multidifusión, el **generalID** en el ~~Crypto~~ClearToken de **LRQ** no se utilizará. La comunicación entre controladores de acceso mediante H.501 y/o H.510 queda en estudio.

EK_{BH} designa la clave de criptación y KS_{BH} la clave adicional que es son compartidas entre el punto extremo B y el controlador de acceso H. Como se describe más adelante, el controlador de acceso H y el punto extremo B calculan por separado este material de claves a partir del secreto compartido K_{BH} utilizando una función PRF.

El controlador de acceso H generará un Challenge-B aleatorio, material de clave de criptación EK_{BH} y material de clave adicional KS_{BH} a partir del secreto compartido K_{BH} utilizando el procedimiento de derivación de clave basada en PRF como se define en I.10 donde Challenge-B se sustituye con challenge y $CT_{HG} \rightarrow h235Key \rightarrow V3KeySyncMaterial \rightarrow secureSharedSecret \rightarrow keyDerivationOID$ en ~~V3KeySyncMaterial~~ mantendrá "AnnexI-HMAC-SHA1-PRF"; véase I.12.

EK_{GH} designa la clave de criptación y KS_{GH} la clave adicional que son compartidas entre el controlador de acceso G y el controlador de acceso H. Este último generará un Challenge-G aleatorio. El controlador de acceso H generará material de clave de criptación EK_{GH} y material de clave adicional KS_{GH} a partir del secreto compartido K_{GH} utilizando el procedimiento de deducción de clave basado en PRF como se define en la cláusula 11 donde Challenge-G se sustituye con challenge. $CT_{HG} \rightarrow challenge$ mantendrá challenge-G y el ID del punto extremo B se fijará a $CT_{HG} \rightarrow h235Key \rightarrow V3KeySyncMaterial \rightarrow secureSharedSecret \rightarrow generalID$.

El controlador de acceso H transmitirá la EK_{BH} criptada al controlador de acceso G. El modo de criptación OFB realzada (EOFB) (véase B.2.5) se utilizará con la clave adicional específica del punto extremo, secreta, KS_{GH} . Son algoritmos de criptación aplicables (véase D.11):

- 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": por defecto y es recomendado.
- RC2-compatible (56 bits) en modo EOFB que utiliza OID "X1": facultativo.

Para el modo de criptación EOFB, el controlador de acceso H generará un valor inicial IV aleatorio. Para OID "X1", OID "Y1" y OID "Z1", el valor inicial aleatorio (IV) tiene 64 bits y será transportado Para el modo de criptación EOFB, el controlador de acceso H generará un valor inicial aleatorio IV. Para OID "X1", OID "Y1" y OID "Z1", el valor inicial aleatorio IV tiene 64 bits y será transportado dentro de **iv8** de **params** dentro de **V3KeySyncMaterial**; en tanto que el IV tiene 128 bits para OID "Z2" y será transportado dentro de **iv16** de **params** dentro de **V3KeySyncMaterial**.

El controlador de acceso H incluirá $ENC_{K_{GH}, K_{SGH}, IV}(EK_{BH})$ en ClearToken CT_{HG} con **tokenOID** fijado a "I3". El texto cifrado obtenido $ENC_{K_{GH}, K_{SGH}, IV}(EK_{BH})$ será transportado en la estructura de datos **h235key** como parte de **secureSharedSecret** donde se colocará dentro de **encryptedSessionKey** de la estructura de datos **secureSharedSecret**. El algoritmo de criptación será el indicado en **algorithmOID** ("X1", "Y1", "Z1" o "Z2") dentro de **V3KeySyncMaterial**. La respuesta **LCF** contendrá el ClearToken CT_{HG} . Para el modo de criptación EOFB, el controlador de acceso H generará un valor inicial IV aleatorio. Para OID "X1", OID "Y1" y OID "Z1", el valor inicial aleatorio IV tiene 64 bits y será transportado dentro de $CT_{HG} \rightarrow \mathbf{h235Key} \rightarrow \mathbf{V3KeySyncMaterial} \rightarrow \mathbf{secureSharedSecret} \rightarrow \mathbf{params} \rightarrow \mathbf{iv8}$; mientras que para el OID "Z2" el IV tiene 128 bits y será transportado dentro de $CT_{HG} \rightarrow \mathbf{h235Key} \rightarrow \mathbf{V3KeySyncMaterial} \rightarrow \mathbf{secureSharedSecret} \rightarrow \mathbf{params} \rightarrow \mathbf{iv16}$.

El controlador de acceso H incluirá $ENC_{EK_{GH}, K_{SGH}, IV}(EK_{BH})$ en el ClearToken CT_{HG} con **tokenOID** fijado a "I3". El texto cifrado obtenido $ENC_{EK_{GH}, K_{SGH}, IV}(EK_{BH})$ será transportado en $CT_{HG} \rightarrow \mathbf{h235Key} \rightarrow \mathbf{V3KeySyncMaterial} \rightarrow \mathbf{secureSharedSecret} \rightarrow \mathbf{encryptedSessionKey}$. El algoritmo de criptación será indicado en $CT_{HG} \rightarrow \mathbf{h235Key} \rightarrow \mathbf{V3KeySyncMaterial} \rightarrow \mathbf{algorithmOID}$ ("X1", "Y1", "Z1" o "Z2"). El Challenge-B se colocará dentro de $CT_{HG} \rightarrow \mathbf{h235Key} \rightarrow \mathbf{V3KeySyncMaterial} \rightarrow \mathbf{secureSharedSecret} \rightarrow \mathbf{clearSaltingKey}$. $CT_{HG} \rightarrow \mathbf{generalID}$ se fijará conforme al identificador G del controlador de acceso mientras que $CT_{HG} \rightarrow \mathbf{sendersID}$ se fijará según el identificador H del controlador de acceso. La respuesta **LCF** mantendrá el ClearToken CT_{HG} .

El controlador de acceso G al reconocer que los puntos extremos A y B soportan este anexo, generará material de clave y los ClearTokens como se indica a continuación.

El controlador de acceso puede evaluar un secreto compartido K_{AB} basado en llamada, además de las operaciones normales **ARQ**. Este secreto compartido basado en llamada se propaga entonces a ambos puntos extremos utilizando ClearTokens. Estos ClearTokens se transportan dentro del mensaje **ACF** y se envían de nuevo al llamante.

Se incluirán dos ClearTokens, un CT_A para el llamante A y otro CT_B para el destinatario B. Cada **ClearToken** contendrá un OID ("I1" o "I2") dentro del **tokenOID** que indique si está destinado al llamante (OID "I1" para CT_A) o al destinatario (OID "I2" para CT_B).

El **ClearToken**, como se define en este anexo, puede ser utilizado junto con otros perfiles de seguridad, como aquellos del anexo D o anexo F, que utilicen también los **ClearTokens**. En dicho caso, el ClearToken del anexo I también utilizará aquellos otros campos **ClearToken**. Por ejemplo, si se quiere utilizar el anexo I junto con el anexo D, los campos **timeStamp**, **random**, **generalID**, **sendersID** y **dhkey** estarán presentes, y se utilizarán como se describe en los perfiles de seguridad del anexo D.

El identificador de controlador de acceso (GKID) se pondrá dentro del **sendersID**, mientras que el **generalID** mantendrá el identificador de punto extremo del punto extremo A (CT_A) o el de punto extremo B (CT_B). El ID del controlador de acceso (GKID) G se colocará en $CT_A \rightarrow \mathbf{sendersID}$ y en $CT_B \rightarrow \mathbf{sendersID}$ mientras que $CT_A \rightarrow \mathbf{generalID}$ mantendrá el identificador del punto extremo A y $CT_B \rightarrow \mathbf{generalID}$ el identificador del punto extremo B.

EK indica la clave de criptación compartida entre un punto extremo y su controlador de acceso. El controlador de acceso G generará material de clave adicional K_{SGH} y material de clave de criptación

EK_{HG} a partir de K_{HG} utilizando el procedimiento de cálculo de clave basado en PRF como se define en la cláusula 11 con **challenge** sustituido por $CT_{HG} \rightarrow \text{challenge}$.

Las claves de criptación EK_{AG} y EK_{BH} para la clave extremo a extremo criptada K_{AB} serán calculadas a partir del secreto compartido entre el controlador de acceso y los puntos extremo (EK_{AG} o EK_{BH}) utilizando el procedimiento de cálculo de clave **basada** en PRF como se define en I.10 donde ~~keyDerivationOID en V3KeySyncMaterial mantendrá "Annex I-HMAC-SHA1-PRF", véase la cláusula I.12 ambos~~
 $CT_A \rightarrow h235Key \rightarrow V3KeySyncMaterial \rightarrow secureSharedSecret \rightarrow keyDerivationOID$ y
 $CT_B \rightarrow h235Key \rightarrow V3KeySyncMaterial \rightarrow secureSharedSecret \rightarrow keyDerivationOID$ mantendrán
"Annex I-HMAC-SHA1-PRF", véase I.12, y $CT_A \rightarrow \text{challenge}$ mantendrá Challenge-A.

~~El controlador de acceso G generará un secreto de sesión compartida común K_{AB} , que será compartido entre los puntos extremos A y B. El controlador de acceso G copiará Challenge-B de $CT_{HG} \rightarrow h235Key \rightarrow V3KeySyncMaterial \rightarrow secureSharedSecret \rightarrow clearSaltingKey$ a $CT_B \rightarrow \text{challenge}$.~~

Este secreto de sesión K_{AB} será criptado por EK_{AG} (para el CT destinado al punto extremo A) o por EK_{BH} (para el CT destinado al punto B) utilizando un algoritmo de criptación.

El modo de criptación OFB ampliado (EOFB) (véase B.2.5) será utilizado con la clave adicional secreta específica del punto extremo KS_{AG} ~~respuesta a o~~ KS_{BH} . Los algoritmos de criptación que se pueden aplicar son (véase la cláusula D.11):

- DES (56 bits) en modo EOFB que utiliza el OID "Y1": facultativo;
- 3DES (168 bits) en modo EOFB externo que utiliza el OID "Z1": facultativo;
- AES (128 bits) en modo EOFB que utiliza el OID "Z2": por defecto y es recomendado;
- RC2 compatible (56 bits) en modo EOFB que utiliza el OID "X1": facultativo.

Para el modo de criptación EOFB, el ~~controlador de acceso G~~ generará un valor aleatorio inicial IV. Para OID "X1", OID "Y1" y OID "Z1" el IV tiene 64 bits y será transportado en
 $CT_A \rightarrow h235Key \rightarrow V3KeySyncMaterial \rightarrow secureSharedSecret \rightarrow params \rightarrow iv8$ y en
 $CT_B \rightarrow h235Key \rightarrow V3KeySyncMaterial \rightarrow secureSharedSecret \rightarrow params \rightarrow iv8$; mientras que para
el OID "Z2" el IV tiene 128 bits y será transportado en
 $CT_A \rightarrow h235Key \rightarrow V3KeySyncMaterial \rightarrow secureSharedSecret \rightarrow params \rightarrow iv16$ y en
 $CT_B \rightarrow h235Key \rightarrow V3KeySyncMaterial \rightarrow secureSharedSecret \rightarrow params \rightarrow iv16$.

El texto cifrado obtenido $ENC_{EK_{AG}, KS_{AG}, IV}(K_{AB})$ será transportado en
 $CT_A \rightarrow h235Key \rightarrow V3KeySyncMaterial \rightarrow secureSharedSecret \rightarrow encryptedSessionKey$ y
 $ENC_{EK_{BH}, KS_{BH}, IV}(K_{AB})$ será transportado en
 $CT_B \rightarrow h235Key \rightarrow V3KeySyncMaterial \rightarrow secureSharedSecret \rightarrow encryptedSessionKey$. El
algoritmo de criptación será indicado en
 $CT_A \rightarrow h235Key \rightarrow V3KeySyncMaterial \rightarrow secureSharedSecret \rightarrow algorithmOID$ y en
 $CT_B \rightarrow h235Key \rightarrow V3KeySyncMaterial \rightarrow secureSharedSecret \rightarrow algorithmOID$ ("X1", "Y1",
"Z1" o "Z2"). dentro del **iv8 de params en V3KeySyncMaterial**; mientras que para el OID "Z2",
el IV tiene 128 bits y ha de ser transportado dentro del **iv16 de params en V3KeySyncMaterial**.

~~El texto cifrado obtenido $ENC_{EK_{AG}, KS_{AG}, IV}(K_{AB})$ resp. $ENC_{EK_{BH}, KS_{BH}, IV}(K_{AB})$ será entonces transportado en la estructura de datos **h235key** como parte de **secureSharedSecret**, donde estará en el **encryptedSessionKey** de la estructura de datos **secureSharedSecret**. Se indicará cuál es el algoritmo de criptación en **algorithmOID** ("X1", "Y1", "Z1" o "Z2") en **V3KeySyncMaterial**.~~

Para el ClearToken destinado al punto extremo A, el identificador del punto extremo B ($EPID_B$) se colocará en
 $CT_A \rightarrow h235Key \rightarrow V3KeySyncMaterial \rightarrow secureSharedSecret \rightarrow generalID$ de
V3KeySyncMaterial. De igual manera que para el ClearToken destinado al punto extremo B, el
identificador del punto extremo A ($EPID_A$) se colocará en

~~CT_B→h235Key→V3KeySyncMaterial→secureSharedSecret→generalID~~ de ~~V3KeySyncMaterial~~.

En el caso de los algoritmos de criptación EOFB, no se utilizará **encryptedSaltingKey**.

El controlador de acceso G incluirá tanto los ClearToken CT_A como CT_B en la ACF hacia el punto extremo A.

El punto extremo A identificará CT_A inspeccionando el **tokenOID** "I1" dentro de ClearToken.

El punto extremo A verificará que el CT_A obtenido es nuevo comprobando el **timestamp**. Algunas pruebas adicionales de seguridad permitirán verificar el **generalID** y **sendersID** del ClearToken y el **generalID** dentro de **V3KeySyncMaterial**. Si se verificó el CT_A recibido y se concluyó que era nuevo, el punto extremo A recuperará el IV y calculará EK_{AG} y KS_{AG} como se describe antes para el controlador de acceso G. El punto extremo A describirá la información **encryptedSessionKey** encontrada dentro de **V3KeySyncMaterial** de CT_A para obtener el EK_{AB}.

Si se verificó el CT_A recibido y se concluyó que era nuevo, el punto extremo A puede enviar un mensaje SETUP al punto extremo B. Este mensaje SETUP incluye CT_B. El mensaje SETUP se asegurará (autenticándolo y/o protegiendo su integridad) conforme al anexo D o F, utilizando K_{AB} como el secreto compartido aplicado. Para ello, el **generalID** del ClearToken generado numéricamente del anexo D (¡no CT_B!) no se utilizará, a menos que el punto extremo A ya tenga un EPID_B disponible (por ejemplo, mediante configuración o memorizado de una comunicación anterior). Si el punto extremo A utiliza un valor EPID_B para **generalID** en SETUP, el punto extremo A aceptará el valor del **sendersID** en el mensaje de señalización de llamada devuelto, como el verdadero EPID_B.

El punto extremo B identificará CT_B inspeccionando el **tokenOID** "I2" dentro de ClearToken.

El punto extremo B verificará que el CT_B obtenido es nuevo revisando el **timestamp**. Otras pruebas de seguridad adicionales permitirán verificar el **sendersID** del ClearToken y el **generalID** dentro de **V3KeySyncMaterial**. Si se verificó el CT_B recibido y se encontró que era nuevo, el punto extremo B podrá recuperar el IV y calcular EK_{BHG} y KS_{BHG} como en el caso descrito para el controlador de acceso. El punto extremo B describirá la información **encryptedSessionKey** encontrada dentro del **V3KeySyncMaterial** del CT_B para obtener EK_{AB}.

Cuando se haya verificado CT_B y se haya encontrado que es nuevo, el punto extremo B puede proseguir con la señalización de llamada respondiendo con CALL-PROCEEDING, ALERTING o CONNECT, etc. cuando sea necesario. Cuando se haya encontrado que CT_B no es nuevo o que la verificación de seguridad del mensaje SETUP ha fallado, el punto extremo B responderá con RELEASE-COMplete y con la **ReleaseCompleteReason** puesta a error de seguridad, como se define en B.2.2.

Cuando se deba utilizar seguridad de medios (véase D.7), los puntos extremos A y B intercambiarán medias claves Diffie-Hellman conforme a D.7.1 y establecerán una clave maestra dinámica basada en la sesión a partir de la cual se puedan calcular las claves de sesión específica de medios.

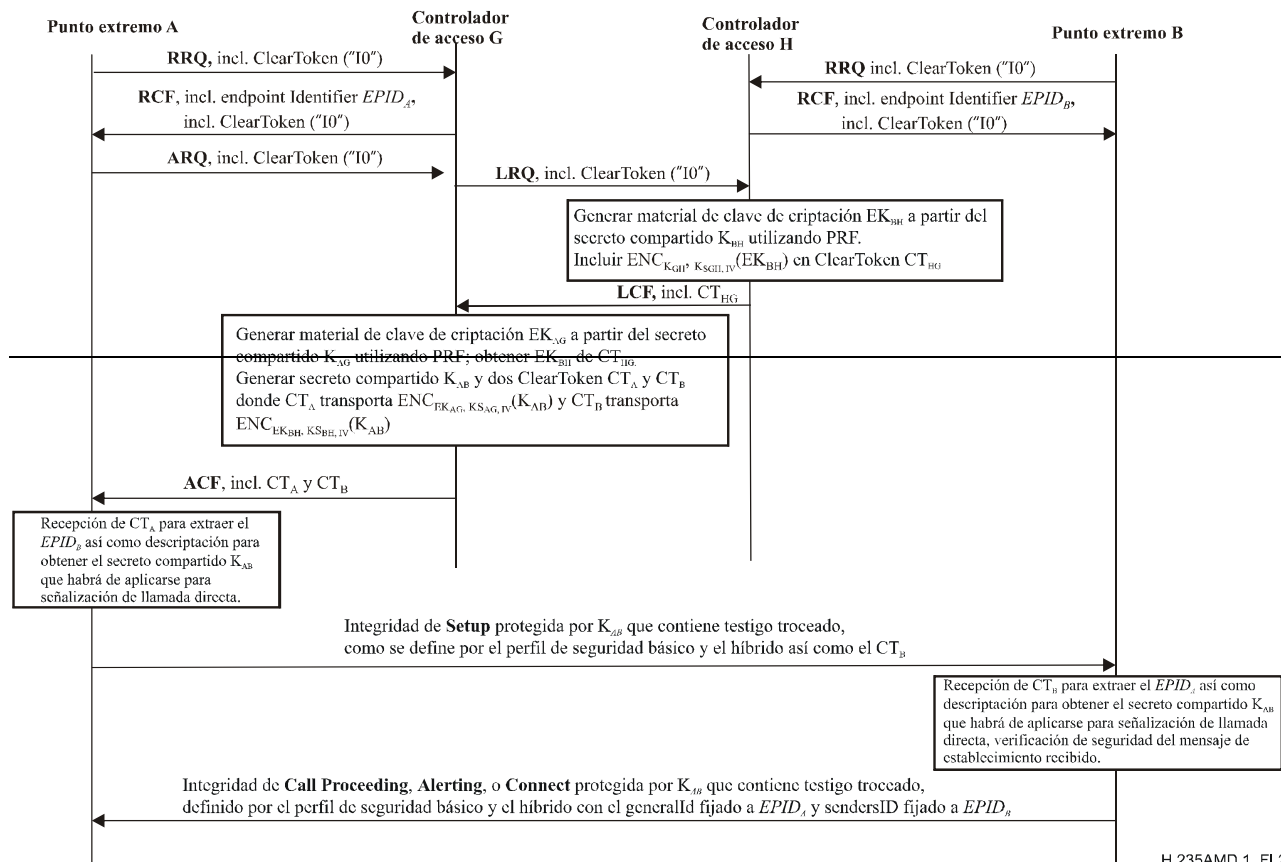
El punto extremo B incluirá generalID fijado a EPID_A y sendersID fijado a EPID_B para la protección de cualquier mensaje de señalización de llamada H.225.0 destinado a EP A (por ejemplo, Call Proceeding, Alerting o Connect).

En la figura I.2 se muestra el flujo básico de comunicación.

Perfil de seguridad básico del anexo D/H.235 o perfil de seguridad híbrido del anexo F/H.235 desplegados mediante la aplicación de un secreto compartido K_{AG} a la comunicación entre el punto extremo A y el controlador de acceso G.

Perfil de seguridad básico del anexo D/H.235 o perfil de seguridad híbrido del anexo F/H.235 desplegados mediante la aplicación de un secreto compartido K_{GH} a la comunicación entre el controlador de acceso G y el controlador de acceso H.

Perfil de seguridad básico del anexo D/H.235 o perfil de seguridad híbrido del anexo F/H.235 desplegados mediante la aplicación de un secreto compartido K_{BH} a la comunicación entre el punto extremo B y el controlador de acceso H.



H.235AMD.1_FI.2

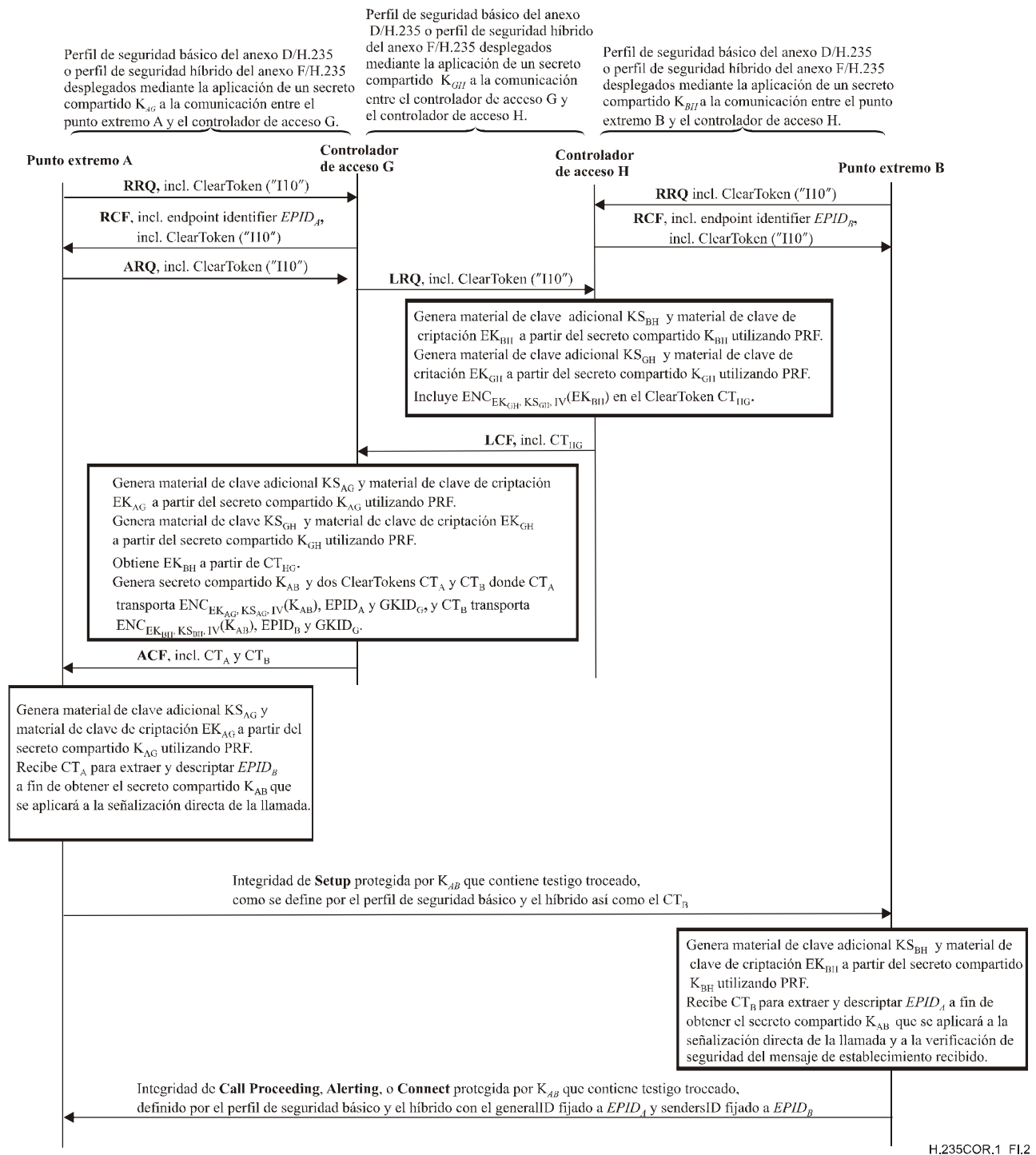


Figura I.2/H.235 – Flujo básico de comunicación

I.10 Procedimiento de cálculo de clave basado en PRF

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

La clave de criptación EK'_{AG} se calculará utilizando la PRF (véase la cláusula B.7) con el parámetro *inkey* puesto a K_{AG} y *label* se fijará a la constante $0x2AD01C64 \parallel \text{challenge}$.

De igual manera, la clave de criptación EK'_{BG} se calculará utilizando la PRF con el parámetro *inkey* puesto a K_{BH} y *label* se pondrá al valor constante $0x1B5C7973 \parallel \text{challenge}$. En ambos casos, se

asignará a *outkey_len* la longitud requerida de la clave de criptación para el algoritmo de criptación seleccionado.

Utilizando la misma PRF, el controlador de acceso y cada punto extremo generarán la clave adicional compartida y secreta. La clave adicional, siempre que se utilice junto con el modo de criptación EOFB, protege contra ataques de la CT_B del tipo texto claro conocido por un punto extremo A, siempre que dicho punto pueda de lo contrario intentar descubrir la K_{BH} .

KS_{AG} es la clave adicional compartida y secreta entre el punto extremo A y el controlador de acceso G. KS_{AG} se calculará utilizando la PRF con el parámetro *inkey* puesto a K_{AG} y *label* se pondrá a $0x150533E1 \parallel \text{challenge}$. KS_{BH} se calculará utilizando la PRF con el parámetro *inkey* puesto a K_{BH} y *label* se pondrá a $0x39A2C14B \parallel \text{challenge}$. El procedimiento de esta cláusula permite calcular una clave de criptación y una clave adicional a partir de una clave compartida. El procedimiento es uniforme independientemente del secreto compartido (K_{AG} , K_{BH} o K_{GH}).

Para obtener el material de clave objetivo (por ejemplo, EK_{AG}), se utilizará la PRF (véase B.7) con los parámetros del cuadro I.0, con el parámetro *inkey* fijado a la clave compartida correspondiente (por ejemplo, K_{AG}), y *label* se fijará a la constante correspondiente (por ejemplo, $0x2AD01C64 \parallel \text{challenge-A}$) donde \parallel significa concatenación. El *outkey_len* se fijará a la longitud requerida por el material de clave objetivo que depende del algoritmo de criptación seleccionado.

NOTA — Los enteros constantes de 32 bits (por ejemplo $0x2AD01C64$, etc.) se toman de las cifras decimales de e (es decir, 2,7182 ...), y cada constante consta de nueve cifras decimales (por ejemplo, las primeras nueve cifras decimales $718281828 = 0x2AD01C64$). Las cadenas de nueve cifras decimales no se escogen al azar, sino como "pedazos" de las cifras decimales de e .

NOTA — Para EK_{AG} , KS_{AG} , EK_{BH} y KS_{BH} los enteros constantes de 32 bits (es decir, $0x2AD01C64$, etc.) se toman de las cifras decimales de e (es decir, 2,7182 ...), y para EK_{GH} y KS_{GH} los enteros constantes de 32 bits se toman de las cifras decimales de π (es decir, 3,1415 ...). Para EK_{AG} , EK_{BH} , KS_{AG} y KS_{BH} los enteros de 32 bits se toman de los bloques de nueve cifras decimales respectivamente de los bloques primero, segundo, cuarto y séptimo. El valor para EK_{GH} se toma de los diez primeros decimales de π , mientras que para KS_{GH} se toma de los ocho decimales siguientes de π .

**Cuadro I.0/H.235 – Cálculo de las claves adicionales y de criptación
a partir de un secreto compartido**

<u>Clave objetivo</u>	<u>PRF inkey</u>	<u>Constante \parallel challenge</u>
EK_{AG}	K_{AG}	$0x2AD01C64 \parallel \text{Challenge-A}$
KS_{AG}	K_{AG}	$0x150533E1 \parallel \text{Challenge-A}$
EK_{BH}	K_{BH}	$0x1B5C7973 \parallel \text{Challenge-B}$
KS_{BH}	K_{BH}	$0x39A2C14B \parallel \text{Challenge-B}$
EK_{GH}	K_{GH}	$0x54655307 \parallel \text{Challenge-G}$
KS_{GH}	K_{GH}	$0x35855C60 \parallel \text{Challenge-G}$

I.11 Procedimiento de cálculo de clave basado en FIPS-140

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

I.12 Lista de identificadores de objeto

Cuadro I.1/H.235 – Identificadores de objeto utilizados por el anexo I

Referencia de identificador de objeto	Valor de identificador de objeto	Descripción
"I0"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 48}	Utilizado en el procedimiento DRC durante GRQ/RRQ y GCF/RCF y ARQ para dejar que los puntos extremos/controlador de acceso indiquen soporte del anexo I.
"I1"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 49}	Utilizado en el procedimiento DRC por el tokenOID del ClearToken que indica que el ClearToken <u>CT_A</u> mantiene una clave extremo a extremo para el llamante.
"I2"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 50}	Utilizado en el procedimiento DRC por el tokenOID del ClearToken que indica que el ClearToken <u>CT_B</u> mantiene una clave extremo a extremo para el llamado.
"I3"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 52}	Utilizado en el procedimiento DRC para el tokenOID de ClearToken entre controladores de acceso, que indica que el ClearToken <u>CT_{HG}</u> mantiene una clave de criptación para el controlador de acceso iniciador.
"Annex I-HMAC-SHA1-PRF"	{itu-t (0) recommendation (0) h (8) 235 version (0) 3 51}	Usado en el procedimiento DRC para el keyDerivationOID dentro del V3KeySyncMaterial para indicar el método de derivación de cálculo de clave aplicado en I.10 utilizando la función pseudoaleatoria 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 multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
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