(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 402 862**

(51) Int. CI.:

H04L 9/08 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA MODIFICADA TRAS OPOSICIÓN T5

(86) Fecha de presentación y número de la solicitud internacional: **26.01.2006 PCT/CN2006/000168**

(87) Fecha y número de publicación internacional: **10.08.2006 WO06081765**

(96) Fecha de presentación y número de la solicitud europea: **26.01.2006 E 06705589 (7)**

(97) Fecha y número de publicación de la concesión europea modificada tras oposición: **15.11.2017 EP 1808978**

(54) Título: **Un método y sistema para distribuir la clave de sesión a través de las zonas con múltiples controladores de acceso, Gatekeeper, según el modo de encaminamiento directo**

(30) Prioridad:

04.02.2005 CN 200510005397

(45) Fecha de publicación y mención en BOPI de la traducción de la patente modificada:
08.03.2018

(73) Titular/es:

HUAWEI TECHNOLOGIES CO., LTD. (100.0%)
Huawei Administration Building Bantian Longgang District
Shenzhen, Guangdong Province 518129, CN

(72) Inventor/es:

LI, KUN

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

ES 2 402 862 T5

DESCRIPCIÓN

Un método y sistema para distribuir la clave de sesión a través de las zonas con múltiples controladores de acceso, Gatekeeper, según el modo de encaminamiento directo

Campo de la invención

La presente invención se refiere a tecnologías de autenticación entre una parte llamante y una parte llamada en un modo de encaminamiento directo en un sistema de comunicación, en particular a un método y un sistema para distribuir una clave de sesión a través de zonas de Gatekeeper (GK) en un modo de encaminamiento directo.

Antecedentes de la invención

Un sistema H.323 se pone en práctica por una Red Basada en Paquetes (PBN) sin garantía de Calidad de Servicio (QoS). Debido a su propia limitación técnica, la red PBN es incapaz de ofrecer calidad de servicio QoS o servicios seguros. Por lo tanto, en el sistema H.323, la forma de proporcionar servicios en tiempo real y seguros constituye un problema a resolver.

Las versiones anteriores al protocolo H.235 V.3 describen algunas soluciones técnicas sobre autenticación y encriptación para el sistema H.323, pero la totalidad de las soluciones técnicas están basadas en un modo de encaminamiento de GK. El ANEXO I del protocolo H.235 V.3 proporciona una solución de seguridad basada en el modo de encaminamiento directo, que utiliza principalmente las características básicas del ANEXO D y del ANEXO F del protocolo H.235 V.3 para ofrecer un servicio seguro para la comunicación en el sistema H.323, pero la puesta en práctica de la solución está limitada en una sola zona de GK.

En un ambiente operativo de red práctica, un sistema de H.323 suele incluir dos o más GKs. La Figura 1 es un diagrama de bloques que ilustra una estructura de redes lógicas de un sistema H.323 con dos GKs.

Según se ilustra en la Figura 1, las líneas de trazos indican las rutas de transmisión de mensajes de registro, admisión y estado (RAS) descritos en H.225 en el modo de encaminamiento de GK; las líneas continuas indican rutas de transmisión de los mensajes de Q.931 en el H.225 en el modo de encaminamiento directo. El punto extremo a (EPa) y e EPb son dos H.323 EPs, GKg y GKh son dos GKs. En donde el Kgh es el GK del EPa llamante y el GKh es el GK del EPb llamado.

Cuando el sistema H.323 incluye dos o más GKs, un mecanismo de asignación de prellamada se suele utilizar para hacer que el EPa llamante y el GKg tengan una clave compartida Kag, el EPb llamado y el GKh tengan otra clave compartida Kbh y el GKg y el GKh tengan también otra clave compartida GKg, con el fin de garantizar la transmisión fiable de los mensajes de RAS.

Si el EPa llamante efectúa una llamada al EPb llamado en el modo de encaminamiento directo, una transmisión fiable de los mensajes de RAS es requerida por ambos EPs para adquirir una clave de sesión Kab, que garantice la transmisión directa fiable de los mensajes de Q.931 en el H.225 entre el EPa llamante y el EPb llamado.

En la técnica anterior, existen dos métodos para que el EPa llamante y el EPb llamado realicen una autenticación con la clave de sesión Kab cuando se realice una transmisión directa de los mensajes Q.931 en el H.225.

Método 1: El GKh genera la clave de sesión Kab, el EPa llamante y el EPb llamado realizan una autenticación con la clave de sesión Kab generada por el GKh cuando transmite los mensajes Q.931 en el H.225.

Una descripción detallada de este método se proporciona a continuación:

Según se ilustra en la Figura 1, el EPa llamante envía una demanda de admisión (ARQ) al GKg, cuya demanda contiene un denominado ClearToken con un campo TokenOID establecido en “I0”, lo que indica que el EPa llamante es capaz de soportar el ANEXO I del H.235 V.3; dicho de otro modo, el EPa llamante soporta la transmisión de mensajes RAS en el modo de encaminamiento de GK.

Después de recibir el mensaje ARQ desde el EPa llamante, el GKg determina la información del EPb llamado en función del valor de un campo *destinationInfo* o un campo *destCallSignalAddress* en el mensaje ARQ y determina que el EPb llamado no está en la zona del GKg en función de la información del EPb llamado, por ello, el GKg envía una demanda de localización (LRQ) al GKh, para localizar el EPb llamado. Un campo de identificador de punto final, en el mensaje LRQ, puede transmitir un identificador (ID) del EPa llamante, indicando que es el EPa llamante el que localiza al EPb llamado.

Cuando el GKg recibe el mensaje ARQ y encuentra que el valor de campo TokenOID del ClearToken en el mensaje ARQ es “I0”, determina que el EPa llamante es capaz de soportar el ANEXO I de H.235 V.3 y luego, genera un ClearToken con el indicador TokenOID establecido a "I0" en el mensaje LRQ. Si el GKg no soporta el ANEXO I del H.235

V.3, el GKg no necesita crear el ClearToken con el indicador TokenOID establecido a "I0" en el mensaje LRQ y el proceso de intercambio de información subsiguiente del mensaje LRQ se realiza en un modo normal como el de cuando el ANEXO I del H.235 V.3 no es soportado; dicho de otro modo, los mensajes no serán encriptados ni desencriptados en GKs durante la transmisión.

Después de recibir el mensaje LRQ, el GKh comprueba si el valor del indicador TokenOID del ClearToken en el mensaje LRQ es "I0"; si el valor es "I0", ello indica que el EPa llamante es capaz de soportar el ANEXO I de H.235 V.3. Si el GKh soporta también el ANEXO I de H.235 V.3, el GKh consulta sobre si el EPb llamado sea capaz, o no, de soportar el ANEXO I de H.235 V.3 y obtiene la dirección del EPb llamado en función de la información del EPb llamado en el mensaje LRQ.

A continuación, el GKh genera un número aleatorio "*challenge*" así como una clave de sesión Kab para la transmisión entre el EPa y el EPb. El GKh genera un Ekgh a partir de una clave compartida Kgh entre el GKh y el GKg y el número aleatorio "*challenge*" utilizando un algoritmo de derivación de claves designado y realiza la encriptación de la clave de sesión Kab con el Ekgb para generar un EKab1. A continuación el GKh establece el EKab1 y los parámetros utilizados en la encriptación, tal como el número aleatorio "*challenge*", para un subcampo correspondiente de un campo independiente *ClearToken.h235Key.secureSharedSecret.*

Cuando existe un campo de identificador de punto extremo en el mensaje LRQ, el GKh necesita también establecer el EKab1 para un campo ClearToken.h235Key.secureSharedSecret.generalID y establece el algoritmo de derivación de claves designado para la generación de las claves correspondientes para un campo denominado ClearToken.h235Key.secureSharedSecret.KeyDerivationOID, establece el número aleatorio "*challenge*" utilizado para la generación de claves para un campo ClearToken.challenge. Al mismo tiempo, el GKh establece un ClearToken.generalID para que sea el identificador ID del GKg y establece un ClearToken.senderID para que sea un identificador ID del GKh y por último, establece el valor del campo TokenOID en el ClearToken para que sea "I3". El ClearToken será referido, en adelante, como CTg.

El GKh genera la clave EKbh a partir de otro número aleatorio "*challenge*" y la clave compartida Kgh entre el GKh y el GKg utilizando el algoritmo de derivación de claves designado y luego, realiza la encriptación de la clave de sesión Kab con el EKbh para obtener un EKab2. Después de que el GKh establezca EKab2 y los parámetros utilizados en la encriptación, tales como el algoritmo de derivación de claves designado y el segundo número aleatorio "*challenge*" para que sea el campo de h235Key.secureSharedSecret de otro ClearToken.

Cuando existe un campo de identificador de punto extremo en el mensaje LRQ, el GKh necesita también establecer el EKab2 para el campo ClearToken.h235Key.secureSharedSecret.generalID y establecer el segundo número aleatorio "*Challenge*" utilizado para la generación de claves para el campo ClearToken.challenge. Y el GKh establece, además, el campo ClearToken.generalID para ser el identificador ID del EPb llamado, establece el campo ClearToken.senderID para ser el ID del GKh y por último, establece el valor del campo TokenOID en el ClearToken para "I2". Este ClearToken se referirá en adelante como CTb.

Después de las configuraciones anteriores, el GKh envía un mensaje de Confirmación de Localización (LCF) que transmite el CTb y el CTg al GKg.

Después de recibir el mensaje de LCF desde el GKh, el GKg extrae la información de ClearToken separada, esto es, los dos ClearTokens, a partir del mensaje de LCF. El valor del TokenOID de uno de los ClearToken es "I3", lo que indica que el ClearToken es CTg y el valor de TokenOID de los otros ClearToken es "I2", lo que indica que el ClearToken es el CTb. Se indica así que ambos EPb llamado y GKh son capaces de soportar el ANEXO I del H.235 V.3 y adoptar el H.235 V.3 en el plan de seguridad.

El GKg genera un mensaje de Confirmación de Admisión (ACF) y crea un ClearToken en el mensaje de ACF. El valor de TokenOID del ClearToken se establece en "I1". A continuación, el GKg selecciona un tercer número aleatorio "*challenge*" y lo establece para que sea el campo de CTa.challenge y obtiene los parámetros que el CTg utilizó en la encriptación, tal como el número aleatorio "*challenge*" y el algoritmo de derivación de claves designado, con el fin de derivar una clave Ekgh a partir de la clave compartida Kgh entre el GKg y el EPb llamado utilizando el algoritmo de derivación de claves designado por el número aleatorio "*challenge*". A continuación, se efectúa la desencriptación del EKab1 en el campo CTg.h235Key.secureSharedSecret del mensaje LCF con la clave Ekgh y de este modo, se obtiene la clave de sesión Kab. El GKg genera, entonces una clave EKag con el tercer número aleatorio "*challenge*" en el campo CTa.*challenge* y una clave compartida Kag entre el EPa llamante y el GKg utilizando un algoritmo de derivación de claves designado. Después de que el GKg realice la encriptación de la clave de sesión Kab con la clave EKag y establezca los datos encriptados y los parámetros utilizados en la encriptación, tal como el tercer número aleatorio "*challenge*" y el algoritmo de derivación de encriptación designado a los correspondientes subcampos del CTa.h235Key.secureSharedSecret. El resultado encriptado de la operación de encriptación de Kab con el EKag y los parámetros utilizados en la encriptación se referirán como CTa en adelante. Por último, el GKg copia el campo CTb.generalID en el campo CTa.h235Key.secureSharedSecret.generalID, copia el CTb en el mensaje de ACF y envía el mensaje de ACF que transmite el CTb y al CTa al EPa llamante.

Después de recibir el mensaje de ACF, el EPa llamante extrae el CTa y el CTb y desencripta los datos encriptados en el CTa con la clave Kag derivada de la clave compartida Kag entre el EPa llamante y el GKg y mediante el algoritmo de derivación de encriptación designado y el tercer número aleatorio "*challenge*" en el CTa, con el fin de obtener la clave de sesión Kab.

Después de obtener la clave de sesión Kab, el EPa llamante establece una demanda de establecimiento de Setup con la clave de sesión y copia el CTb en el mensaje de ACF en la demanda Setup, a continuación, el EPa llamante establece la información de autenticación que se describe en el ANEXO D de H.235 V.3 en la demanda de Setup con la clave de sesión Kab y envía la demanda de Setup a través de la ruta directa al EPb llamado.

Después de la recepción de la demanda de Setup, el EPb llamado extrae el CTb y deduce la clave EKbh basada en el identificador CTb.generalID, el CTb.senderID y el CTb.challenge en el CTb y la clave compartida Kbh entre el EPb llamado y el GKh. A continuación, el EPb llamado desencripta EKab2 en el campo CTb.h235Key.SecureSharedSecret del CTb para obtener la clave de sesión Kab.

Después de obtener la clave de sesión Kab, el EPb llamado realiza la autenticación de la información de autenticación en la demanda de Setup; si la autenticación es satisfactoria, se procesa la transmisión de mensaje Q.931.

En el método anteriormente descrito, la clave de sesión Kab entre el EPa llamante y el EPb llamado se encripta y desencripta en el GK de cada salto operativo; por lo tanto, cuando existe un gran número de GKs entre el EPa llamante y el EPb llamado, el retardo en la transmisión de mensajes de RAS aumentará y puesto que la clave de sesión Kab está expuesta en el GK de cada salto operativo, se mantiene deficientemente la seguridad de la información.

Método 2: el GKg y el GKh realizan un intercambio de claves de Diffie-Hellman (DH) para generar una clave de sesión Kab, que se utiliza para la autenticación en la transmisión directa de los mensajes de Q.931 en el H.225 entre el EPa llamante y el EPb llamado.

Una descripción detallada de este método se proporciona a continuación: Según se ilustra en la Figura 1, el EPa llamante envía un mensaje ARQ al GKg, en el que existe un ClearToken separado con un TokenOID establecido a "I0". El EPa llamante genera una clave pública para una negociación de DH y establece la clave pública para el campo ClearToken.dhkey antes de enviar el mensaje ARQ.

El GKg, que es capaz de soportar el ANEXO I del H.235 V.3 recibe el mensaje ARQ y determina que el EPb llamado no está en la zona del GKg en función de la información del EPb llamado en el mensaje ARQ. A continuación, el GKg envía un mensaje LRQ al GKh, en el que existe un ClearToken separado con un TokenOID establecido a "I0" y un campo de ClearToken.dhkey que es idéntico al campo ClearToken.dhkey en el mensaje de ARQ. El campo ClearToken.dhkey incluye la clave pública DH generada por el EPa llamante para la negociación de DH.

Cuando existen otros GKs entre el GKg y el GKh, estos GKs intermedios duplican el mensaje de LRQ después de recibir el mensaje de LRQ y envían el mensaje LRQ duplicado a un GK de capa superior hasta que el mensaje LRQ duplicado alcance el GKh.

Después de recibir el mensaje de LRQ, el GKh determina que el EPa llamante y el EPb llamado soportan el ANEXO I del H.235 V.3 basado en el campo ClearToken.TokenOID y en la información del EPb llamado en el mensaje LRQ. A continuación, el GKh crea un ClearToken con un TokenOID establecido a "I2". El ClearToken se refiere como CTb en adelante.

El GKh genera una clave pública para la negociación de DH y calcula, además, una clave de sesión Kab a partir de la clave pública que acaba de generarse y la clave pública en el mensaje LRQ recibido, que utiliza el algoritmo DH para la transmisión directa de mensajes de Q.931 entre el EPa llamante y el EPb llamado.

El GKh genera luego un número aleatorio "*challenge*" y lo establece para el campo CTb.challenge. Después de dicha operación, el GKh deduce una clave EKbh y una clave KSbh mediante el algoritmo de derivación de claves designado sobre la base del número aleatorio "*challenge*" y la clave compartida Kbh entre el EPb llamado y el GKh. El GKh genera un vector de inicialización aleatorio IV y lo establece para el campo CTb.h235Key.securitySharedSecret.paramS.IV. El GKh realiza la encriptación de la clave de sesión Kab con la clave EKbh, la clave KSbh y el vector de inicialización IV para obtener un $ENC_{EKbh,\ KSbh,\ IV}(Kab)$ y establece el $ENC_{EKbh,\ KSbh,\ IV}(Kab)$ al campo CTb.h235Key.securitySharedSecret.encryptedSessionKeyfield. Dicho método para la encriptación de la clave de sesión Kab se describe en el ANEXO I de H.235 V.3.

El GKh envía un mensaje de LCF incluyendo la clave pública y el CTb generado por el GKh al GKg.

El GKg recibe el mensaje de LCF desde el GKh, obtiene el CTb y la clave pública generada por el GKh, copia el CTb y la clave pública en un mensaje de ACF y envía el mensaje de ACF al EPa llamante.

Después de recibir el mensaje de ACF, el EPa llamante deduce la clave de sesión Kab a partir de la clave pública generada por el GKh en el mensaje de ACF y la clave pública del EPa llamante utilizando el algoritmo de DH.

Después de obtener la clave de sesión Kab, el EPa llamante crea una demanda de Setup que contiene la clave de sesión Kab y copia el CTb en el mensaje de ACF en la demanda de Setup y a continuación, el EPa llamante configura la información de autenticación que se describe en el ANEXO D del H.235 V.3 en la demanda de Setup con la clave de sesión Kab y envía la demanda de Setup al EPb llamado.

El EPb llamado recibe la demanda de Setup y extrae el CTb. En función de la información en el CTb, que es el número aleatorio "*challenge*", el algoritmo de derivación de clave designado y la clave compartida Kbh entre el EPb llamado y el GKh, el EPb llamado deduce la clave EKbh y la clave KSbh y luego, desencripta la $ENC_{EKbh,\ KSbh,\ IV}(Kab)$ en el campo CTb.h235Key.secureSharedSecret.encryptedSessionKey con el EKbh, el KSbh y el vector de inicialización IV en el CTb para obtener la clave de sesión Kab. Por último, el EPb realiza la autenticación de la demanda de Setup con la clave de sesión Kab.

El segundo método anteriormente descrito resuelve el problema del retardo en la transmisión de mensajes de RAS y el problema de seguridad generado por la exposición de la clave de sesión Kab en GK de cada salto operativo, pero el método requiere que el EPa llamante y todos los GKs entre el EPa llamante y el EPb llamado soporten la negociación de DH, lo que limita su aplicación.

Aunque este método ha resuelto el problema del aumento del retardo en la transmisión del mensaje de RAS y el rendimiento de seguridad deficiente de la clave de sesión Kab incurrido por la exposición cuando se pasa a través de GK de cada salto operativo. Sin embargo, el método necesita que el EPa llamante y el GKs entre el EPa llamante y el EPb llamado soporten el proceso de negociación de DH, lo que limita la aplicación del método.

El documento temporal TD32 (WP 2/16) “Borrador de la nueva recomendación H.235.4”, periodo de estudio de borrador de ITU-T 2005-2008, Grupo de Estudio 16, Unión Internacional de Telecomunicaciones (2004-11-16) y la contribución “Método propuesto de generación de una clave secreta compartida entre el llamante y el llamado en múltiples dominios de administración”, periodo de estudio de borrador de ITU-T 2005-2008, Grupo de Estudio 16, Unión Internacional de Telecomunicaciones (2004-11-16), examinan, además, los modos de distribución de claves de sesión para llamadas de encaminamiento directo.

En resumen, el GK del llamante y el GK del llamado no pueden seleccionar el método para distribuir la clave de sesión para el llamante y los llamados, lo que hace que los métodos de distribución de clave de sesión carezcan de flexibilidad.

SUMARIO DE LA INVENCIÓN

Formas de realización de la presente invención dan a conocer un método y un sistema para distribuir una clave de sesión a través de zonas de GateKeeper (GK) en un modo de encaminamiento directo, que posibilita a un GK de un punto extremo (EP) seleccionar un modo de distribución de clave de sesión, con el fin de mejorar la flexibilidad del GK cuando se distribuya la clave de sesión.

Según un aspecto de la idea inventiva, el método para distribuir una clave de sesión a través de zonas de GK en el modo de encaminamiento directo se da a conocer según se establece en la reivindicación 1. Características preferidas de este aspecto se establecen en las reivindicaciones 2 a 16.

Según otro aspecto de la presente invención, un sistema para distribuir una clave de sesión a través de zonas de GateKeeper (GK) en un modo de encaminamiento directo, se da a conocer según se establece en la reivindicación 17.

A partir del sistema anterior, resulta evidente que, a través del establecimiento de modos de distribución de claves de sesión abiertos a la selección en el GK llamante y en el GK llamado, algunas formas de realización de la presente invención lo hacen flexible para el GK del llamante y el GK del llamado para seleccionar una clave de sesión entre el llamante y el llamado en función de las situaciones de redes prácticas. Cuando el llamante y el llamado no soportan una negociación de DH, algunas formas de realización de la presente invención pueden poner en práctica la distribución de la clave de sesión entre el GK del llamante y el GK del llamado, que proporciona un nuevo servicio de seguridad extremo a extremo para el llamante y el llamado y mejora la seguridad de la clave de sesión. Por lo tanto, la solución técnica de las formas de realización de la presente invención puede mejorar la flexibilidad del GK del llamante y del GK del llamado en la distribución de claves de sesión y el nivel de seguridad de equilibrio con retardo de transmisión de mensaje.

Breve descripción de los dibujos

La Figura 1 es un diagrama de bloques que ilustra una estructura de red lógica de un sistema H.323 con dos GKs.

Descripción detallada de la invención

La presente invención se describirá, en detalle, a continuación, haciendo referencia al dibujo adjunto y a las formas de realización.

Con el fin de permitir a un GK de llamante y un GK de llamado seleccionar un modo de distribución de claves de sesión, el GK del llamante y el GK del llamado, en la forma de realización de la presente invención, determinan el modo de distribución de claves de sesión en función de la información transmitida en el mensaje recibido y las reglas preconfiguradas para seleccionar el modo de distribución de claves de sesión y luego, distribuir las claves de sesión para el llamante y el llamado.

El método se describirá, en detalle, a continuación.

El método es aplicable al modo de encaminamiento directo a través de zonas de GK en un sistema H.323; dicho de otro modo, es aplicable a una situación en la que la parte llamante y la parte llamada pertenecen a diferentes GKs y el intercambio de información directo entre la parte llamante y la parte llamada se realiza en una red no segura, tal como una Red de Protocolo Internet (IP).

El principio básico de la realización práctica es que un GK realiza la autenticación de la totalidad de los mensajes de RAS de los EPs, en su zona, durante la distribución de la clave de sesión; los EPs realizan la autenticación de los mensajes de RAS del GK de la parte llamante y el GK de la parte llamada con el fin de mantener una confianza mutua entre EPs y el GK de la parte llamante y el GK de la parte llamada y los GKs interenlazados realizan una autenticación mutua para evitar ataques hostiles y mantener una confianza mutua entre ellos. Los procesos de autenticación anteriores pueden garantizar la seguridad de los mensajes de RAS entre las entidades de la red en el sistema H.323.

En primer lugar, necesitan configurarse las reglas para que el GK seleccione el modo de distribución de claves de sesión. En donde, las reglas se pueden configurar de forma estática, dinámica o mediante otros modos en el GK.

Las reglas preconfiguradas se pueden dividir en reglas preconfiguradas de la parte de la llamante y reglas preconfiguradas de la parte llamada en función de la localización del GK. Los contenidos de las reglas preconfiguradas se pueden establecer en función de los requisitos de las redes prácticas. Por ejemplo, las reglas preconfiguradas de la parte llamante pueden incluir cualquiera o alguna combinación de los siguientes elementos: recursos informáticos disponibles en el GK, modos de distribución de claves de sesión soportados por la parte llamante y nivel de seguridad de la parte llamante, etc. Las reglas preconfiguradas de la parte llamada pueden incluir cualquiera o una combinación de los elementos siguientes: recursos informáticos disponibles en el GK, modos de distribución de claves de sesión de la parte llamante y nivel de seguridad de la parte llamada, etc.

Después de las configuraciones anteriores, el GK de la parte llamante y el GK de la parte llamada pueden seleccionar, de forma flexible, los modos de distribución de claves de sesión en función de factores diversificados.

El proceso del GK de la parte llamante y del GK de la parte llamada seleccionando los modos de distribución de claves de sesión se describirán, en detalle, haciendo referencia a las tres clases de procesos siguientes.

Las tres clases de procesos de distribución de claves de sesión son:

Llamada de encaminamiento directo (DRC) I: los modos de distribución de claves de sesión de ambas partes llamante y llamada son el GK de la parte llamada que genera la clave de sesión.

DRC II: el modo de distribución de claves de sesión de la parte llamante es una negociación de DH entre el GK de la parte llamante y el GK de la parte llamada y el modo de distribución de claves de sesión de la parte llamada es una negociación de DH.

DRC III: el modo de distribución de claves de sesión de la parte llamante es una negociación de DH entre la parte llamante y el GK de la parte llamada y el modo de distribución de claves de sesión de la parte llamada es una negociación de DH.

El EP puede indicar si soporta el ANEXO I del H.235 V.3 para su GK base durante los procesos de descubrimiento de GK o de registro de EP, esto es, indicar si soporta el método de la presente forma de realización. Por ejemplo, el EP puede contener un ClearToken separado en un mensaje de demanda de Gatekeeper (GRQ) o un mensaje de Demanda de Registro (RRQ) y establecer un campo TokenOID en el ClearToken para que sea "I0". Cuando el GK base del EP recibe el mensaje GRQ o el mensaje RRQ, reconoce el valor del campo TokenOID en ClearToken como siendo "I0" y reenvía un mensaje de Confirmación de Gatekeeper (GCF) o un mensaje de Confirmación de Registro (RCF) para aceptar el EP. En donde, el mensaje de GCF o el mensaje de RCF transmite un ClearToken que es idéntico con el del mensaje GRQ o el mensaje RRQ.

Cuando la parte llamante no soporta la negociación de DH, el GK de la parte llamante puede seleccionar, respectivamente, los procesos DRC I y DRC II para distribuir la clave de sesión entre la parte llamante y la parte llamada

en función de las reglas preconfiguradas de la parte llamante. De modo similar, el GK de la parte llamada puede seleccionar los procesos DRC I y DRC II para distribuir la clave de sesión entre la parte llamante y la parte llamada.

Cuando la parte llamante soporta la negociación de DH, el GK de la parte llamante puede seleccionar, respectivamente, los procesos DRC I y DRC III para distribuir la clave de sesión entre la parte llamante y la parte llamada. De modo similar, el GK de la parte llamada puede seleccionar los procesos de DRC I y de DRC III para distribuir la clave de sesión entre la parte llamante y la parte llamada.

El proceso del GK de la parte llamante y el GK de la parte llamada en la distribución de la clave de sesión entre la parte llamante y la parte llamada a través de los procesos DRC I, DRC II y DRC III se describirá, en detalle, a continuación, haciendo referencia a la Figura 1.

La etapa 1 del proceso DRC I, antes de llamar a la EPb llamada en el modo de encaminamiento directo, la EPa llamante envía un mensaje ARQ al GKg. En donde el mensaje contiene un ClearToken separado y el campo TokenOID del ClearToken se establece como "I0", lo que significa que el EPa llamante no soporta la negociación de DH y los demás campos del ClearToken permanecen sin utilizar.

En la etapa 2 del proceso DRC I, el GKg recibe el mensaje ARQ y determina que el EPb llamado no pertenece por sí mismo según la información del EPb llamado transmitido en el mensaje ARQ. El GKg inicia un mensaje LRQ para consultar sobre la dirección del GKh.

El GKg genera un mensaje LRQ. Cuando el valor del TokenOID del ClearToken transmitido en el mensaje ARQ es "I0", y el modo de distribución de claves de sesión de la parte llamante es el GK de la parte llamada que genera la clave de sesión, un ClearToken está contenido en el mensaje LRQ y el TokenOID del ClearToken se establece a "I0", lo que indica que el modo de distribución de la clave de sesión de la parte llamante es el GK de la parte llamada que genera la clave de sesión y los demás campos del ClearToken permanecen sin utilizar. Después de las configuraciones, el GKg envía el mensaje LRQ al GKh.

En la etapa 3 del proceso DRC I, después de recibir el mensaje LRQ, el GKh obtiene el campo de TokenOID del ClearToken en el mensaje y confirma que el valor es "I0" y selecciona el modo de distribución de claves de sesión del GK de la parte llamada que genera la clave de sesión en función de las reglas preconfiguradas de la parte llamada y luego, el GKh genera una clave de sesión Kab utilizando un número aleatorio. Con el fin de realizar la encriptación de la clave de sesión Kab, en primer lugar, el GKh genera un número aleatorio "*challenge*" y deriva una clave Ekgh utilizando una clave compartida Kgh entre el GKh y el GKg junto con el número aleatorio "*challenge*" mediante un algoritmo de derivación de claves designado. Y luego, el GKh realiza la encriptación de la clave Kab por el EKgh para generar una EKab1 y establece la EKab1 junto con un parámetro de encriptación, tal como un algoritmo de encriptación y un vector de inicialización utilizado para la encriptación, en un campo ClearToken.h235Key.secureSharedSecret. En donde el valor del TokenOID del ClearToken es “I3”, referido como CTg. Al mismo tiempo, el GKh genera otro ClearToken mediante un proceso similar y el valor del TokenOID de este ClearToken es “I2”, referido como CTb. Por último, el GKh genera un mensaje LCF que transmite el CTg y el CTb. El GKh transmite directamente el mensaje de LCF al GKg o transmite el mensaje de LCF a un GK superior del GKh, hasta que el mensaje alcance el GKg.

En la etapa 4 del proceso de DRC I, después de recibir el mensaje de LCF, cuando se obtiene el valor “I3” del campo TokenOID del ClearToken en el mensaje, el GKh realiza la desencriptación del CTg y genera un CTa. El proceso detallado incluye las etapas siguientes: en primer lugar, el GKg calcula la clave Ekgh utilizando el número aleatorio "*challenge*" y un parámetro IV en el CTg mediante el algoritmo de derivación de claves designado. Y luego, el GKg obtiene la clave de sesión Kab efectuando la desencriptación de EKab1 con la clave Ekgh. Con el fin de generar el CTa, en primer lugar, el GKg deriva una clave EKag utilizando la clave compartida Kag entre sí mismo y el EPa de la parte llamante, el número aleatorio "*challenge*" y el algoritmo de derivación de claves designado. Y luego, el GKg realiza la encriptación de la clave de sesión Kab con la clave Ekag para obtener la EKab1 y establece la EKab1 junto con un parámetro de encriptación, tal como el algoritmo de encriptación y el vector de inicialización utilizado durante la encriptación, en un campo ClearToken.h235Key.secureSharedSecret separado. En donde, el valor del campo TokenOID del ClearToken es “I1” y el ClearToken se refiere como CTa. Por último, el GKg genera un mensaje de ACF, que transmite el CTa y el CTb que se duplica desde que se reciba el mensaje de LCF.

Si existe un GK de nivel más bajo en la zona de gestión del GKg, el mensaje de ACF debe contener el CTa y un CTg que se genera por el GK de capa más baja a través de la encriptación de la clave Kab utilizando una clave derivada entre el GKg y dicho GK.

Después de las configuraciones, el GKg transmite el mensaje de ACF al EPa de la parte llamante.

En la etapa 5 del proceso DRC I, después de recibir el mensaje de ACF, el EPa llamante extrae el CTa desde el mensaje y deriva la clave EKag en función de la información en el CTa y la clave compartida Kag entre la de GKg y la suya propia. Y luego, el EPa de la parte llamante obtiene la clave de sesión Kab efectuando la desencriptación del campo CTa.h235key.secureSharedSecret.encryptedSessionKey utilizando el Ekag.

El EPa llamante crea un mensaje de Setup, duplica el CTb en el mensaje de ACF en el mensaje de Setup y luego, configura la información de autenticación del ANEXO D y ANEXO F del H.235 V.3 utilizando la clave Kab. A continuación, el EPa llamante transmite directamente el mensaje de Setup al EPb llamado.

Después de recibir el mensaje de Setup, el EPb llamado extrae el CTb desde el mensaje, deriva la calve EKbh en función de la información de autenticación en el CTb y la clave compartida Kbh entre él mismo y el GKh y luego, efectúa la desencriptación de la CTb.h235Key.secureSharedSecret.encryptedSessionKey utilizando la EKbh para obtener la clave de sesión Kab. En este momento, el EPb llamado puede realizar la autenticación del mensaje de Setup utilizando la clave de sesión Kab, si la autenticación fue satisfactoria, y la clave de sesión Kab se determina como siendo la clave de sesión para la transmisión de mensajes Q.931 entre el EPb llamado y el EPa llamante.

Los procesos de llamadas posteriores pueden ser objeto de autenticación por el ANEXO D y el ANEXO F del H.235 V.3.

En la etapa 1 del proceso DRC II, antes de llamar al EPb llamado en el modo de encaminamiento directo, el EPa llamante transmite un mensaje ARQ al GKg, en donde el mensaje contiene un ClearToken separado y el campo de TokenOID del ClearToken se establece como "I0", lo que significa que el EPa llamante no soporta la negociación de DH y los demás campos del ClearToken permanecen sin utilizar.

En la etapa 2 del proceso de DRC II, el GKg recibe el mensaje ARQ y determina que el EPb llamado no pertenece al GKg en función de la información del EPb llamado transmitida en el mensaje ARQ. El GKg inicia un mensaje LRQ para localizar el GKh.

El GKg genera el mensaje de LRQ, cuando determina que el valor del TokenOID del ClearToken transmitido en el mensaje de ARQ es "I0" y el modo de distribución de clave de sesión del EPa llamante es el GK de la parte llamante y el GK de la parte llamada que genera la clave de sesión a través de la negociación de DH, establece un ClearToken en el mensaje LRQ, con el campo TokenOID del ClearToken establecido en “I4”, lo que indica que el modo de distribución de las claves de sesión del EPa llamante es el GK de la parte llamante y el GK de la parte llamada que genera la clave de sesión a través de la negociación de DK. El GKg genera una clave pública DH de sí mismo y establece la clave pública de DH en el campo dhkey del ClearToken.

Después de las configuraciones, el GKg transmite el mensaje de LRQ al GKh.

En la etapa 3 del proceso de DRC II, después de recibir el mensaje de LRQ, el GKh confirma que el valor del campo TokenOID del ClearToken en el mensaje es “I4” y confirma que el modo de distribución de las claves de sesión del EPb llamado es la negociación de DH según las reglas preconfiguradas de la parte llamada y luego, comienza a generar la clave de sesión entre la EPa llamante y la EPb llamada a través de la negociación de DH con el GKg. El proceso detallado incluye las etapas siguientes: en primer lugar, el GKh genera una clave pública DH propia y calcula la clave de sesión Kab utilizando su clave pública DH y la clave pública DH obtenida a partir del mensaje LRQ por el algoritmo de DH. Y luego, el GKh genera un CTb con un TokenOID establecido a “I2” siguiendo el paso 3 del proceso DRC I. Por último, el GKh genera un mensaje de LCF que transmite el CTb, un ClearToken separado cuyo TokenOID se establece a “I5” y la clave pública de DH generada por sí mismo. En donde el valor “I5” indica que el ClearToken contiene la clave pública de DH del GK de la parte llamada.

Si el modo de distribución de claves de sesión del EPb llamado se determina como siendo el GK de la parte llamada que genera la clave de sesión debido a factores tales como el GKh que no soporta el algoritmo de DH o políticas de seguridad, etc., el GKh genera el mensaje de LCF siguiendo la etapa 3 del proceso DRC I.

Después de las configuraciones, el GKh transmite el mensaje de LCF al GKg.

En la etapa 4 del proceso DRC II, después de recibir el mensaje de LCF, el GKg confirma que el valor del campo TokenOID del ClearToken en el mensaje es “I5” y confirma que el EPa llamante no soporta la negociación de DH, el GKg calcula la clave de sesión y genera un CTa. El proceso detallado incluye las etapas siguientes: el GKg obtiene la clave pública DH a partir del ClearToken separado en el mensaje de LCF y calcula la clave de sesión Kab utilizando la clave pública DH obtenida y la clave pública DH generada por el propio algoritmo DH. Y luego, el GKg genera el CTa siguiendo un proceso similar a la etapa 4 del proceso DRC I. Por último, el GKg genera un mensaje de ACF que transmite el CTa y el CTb que es duplicado desde el mensaje de LCF.

Si el GKg detecta que el valor del TokenOID del ClearToken en el mensaje de LCF es “I5” y confirma que el EPa llamante soporta la negociación de DH, el GKg debe generar el mensaje de ACF siguiendo la etapa 4 del proceso DRC III.

Si el GKg detecta que el valor del TokenOID del ClearToken, en el mensaje de LCF, es “I3”, debe generar el mensaje de ACF siguiendo la etapa 4 del proceso DRC I.

Después de las configuraciones, el GKg transmite el mensaje de ACF al EPa llamante.

En la etapa 5 del proceso de DRC II, después de recibir el mensaje de ACF, si el EPa llamante detecta que no existe ningún ClearToken con un TokenOID establecido a “I5”, el EPa llamante extrae el CTa desde el mensaje y deriva la clave EKag en función de la información en el CTa y la clave compartida Kag entre el GKg y él mismo. Y luego, el EPa llamante obtiene la clave de sesión Kab efectuando la desencriptación del campo CTa.h235Key.secureSharedSecret. encryptedSessionKey utilizando la clave EKag.

Si el EPa llamante detecta que el mensaje de ACF contiene un ClearToken cuyo TokenOID es del valor “I5”, calcula la clave de sesión Kab siguiendo la etapa 5 del proceso DRCIII.

El EPa llamante crea un mensaje de Setup, duplica el CTb en el mensaje de ACF en el mensaje de Setup y luego, configura la información de autenticación del ANEXO D y del ANEXO F del H.235 V.3 utilizando la clave Kab. A continuación, el EPa llamante transmite directamente el mensaje de Setup al EPb llamado.

Después de recibir el mensaje de Setup, el EPb llamado extrae el CTb desde el mensaje, deriva la clave EKbh en función de la información de autenticación en CTb y la clave compartida Kbh que comparte con el GKh y luego, efectúa la desencriptación de CTb.h235Key.secureSharedSecret.encryptedSessionKey utilizando EKbh para obtener la clave de sesión Kab. En este momento, el EPb llamado puede realizar la autenticación del mensaje de Setup utilizando la clave de sesión Kab, si la autenticación fue operativamente satisfactoria, siendo la clave de sesión Kab determinada como la clave de sesión para la transmisión de mensajes de Q.931 entre el EPb llamado y el EPa llamante.

Los procesos de llamadas posteriores pueden ser objeto de autenticación por el ANEXO D y el ANEXO F del H.235 V.3.

En la etapa 1 del proceso DRC III, el EPa llamante soporta el proceso de negociación de DH. El EPa llamante genera una clave pública DH antes de llamar al EPb llamado en el modo de encaminamiento directo. Y el EPa llamante establece la clave pública DH generada en un campo dhkey de un ClearToken separado en un mensaje ARQ, en donde el valor del campo TokenOID del ClearToken se establece en “I4” y los demás campos permanecen sin utilizar.

En la etapa 2 del proceso DRC III, el GKg recibe el mensaje ARQ y determina que el EPb llamado no pertenece a él mismo en función de la información del EPb llamado transportada en el mensaje ARQ. El GKg inicia un mensaje de LRQ para consultar sobre la dirección del GKh.

El GKg genera un mensaje de LRQ, cuando determina que el valor del TokenOID del ClearToken transmitido en el mensaje ARQ es “I4” y el modo de distribución de claves de sesión del EPa llamante es el GK de la parte llamante y el GK de la parte llamada que genera la clave de sesión a través de la negociación de DH, el GKg copia el ClearToken en el mensaje ARQ al mensaje LRQ y transmite el mensaje LRQ al GKh.

En la etapa 3 del proceso DRC III, después de recibir el mensaje de LRQ, el GKh confirma que el mensaje contiene un ClearToken separado con TokenOID establecido a “I4” y confirma que el modo de distribución de claves de sesión del EPb llamado es la negociación DH en función de las reglas preconfiguradas de la parte llamada y luego, comienza a negociar una clave de sesión entre el EPa llamante y el EPb llamado a través de la negociación de DH con el GKg. El proceso detallado incluye las etapas siguientes: en primer lugar, el GKh genera una clave pública DH propia y calcula la clave de sesión Kab utilizando la clave pública DH propia y la clave pública DH obtenida a partir del mensaje de LRQ mediante el algoritmo DH. Y luego, el GKh genera un CTb con TokenOID establecido en “I2” siguiendo la etapa 3 del proceso DRC I. Por último, el GKh genera un mensaje de LCF que transmite el CTb, un ClearToken separado con TokenOID establecido a “I5” y la clave pública DH generada por sí mismo. En donde el valor “I5” indica que el ClearToken contiene la clave pública DH del GK de la parte llamada.

Si el modo de distribución de claves de sesión del EPb llamado se determina como siendo el GK de la parte llamada que genera la clave de sesión debido a factores tales como que el GKh no soporta el algoritmo DH o políticas de seguridad, etc., el GKh genera el mensaje LCF siguiendo la etapa 3 del proceso DRCI.

Después de las configuraciones, el GKh transmite el mensaje de LCF al GKg.

En la etapa 4 del proceso de DRC III, después del recibir el mensaje de LCF, si el GKg confirma que el mensaje de LCF contiene el ClearToken con TokenOID establecido a “I5” y confirma que la negociación de DH es soportada por sí misma, el GKg genera un mensaje ACF. En donde, el mensaje contiene todos los ClearTokens duplicados desde el mensaje LCF. A continuación, el GKg transmite el mensaje de ACF al EPa llamante.

Si el GKg detecta que el valor del TokenOID del ClearToken, en el mensaje LCF, es “I3” y confirma que el EPa llamante no soporta la negociación DH, el GKg debe generar el mensaje de ACF siguiendo la etapa 4 del proceso DRCI.

En la etapa 5 del proceso DRC III, después de recibir el mensaje de ACF, si el EPa llamante confirma que el mensaje contiene un ClearToken separado con un TokenOID establecido a “I5”, calcula la clave de sesión. El proceso detallado incluye las etapas siguientes: el EPa llamante obtiene la clave pública DH de GKh desde el ClearToken y calcula la clave de sesión Kab mediante el algoritmo DH utilizando la clave pública DH obtenida y la clave pública DH generada por sí misma.

Si el EPa llamante detecta que el mensaje de ACF contiene un ClearToken con TokenOID establecido a “I3”, calcula la clave de sesión Kab siguiendo la etapa 5 del proceso DRCI.

El EPa llamante crea un mensaje de Setup, duplica el CTb en el mensaje ACF en el mensaje de Setup y luego, configura la información de autenticación del ANEXO D y del ANEXO F del H.235 V.3 utilizando la clave Kab en el mensaje de Setup. A continuación, el EPa llamante transmite el mensaje de Setup al EPb llamado directamente.

Después de recibir el mensaje de Setup, el EPb llamado extrae el CTb desde el mensaje, deriva la clave EKbh en función de la información de autenticación en CTb y la clave compartida kbh entre sí mismo y el GKh y luego, efectúa la desencriptación de CTb.h235Key.secureSharedSecret. encryptedSessionKey utilizando la EKbh para obtener la clave de sesión Kab. En este momento, el EPb llamado puede realizar la autenticación del mensaje de Setup utilizando la cal Kab, si la autenticación fue operativamente satisfactoria y se determina que la clave de sesión Kab es la clave de sesión para la transmisión de mensajes Q.931 entre el EPb llamado y el EPa llamante.

Los procesos de llamada posteriores pueden ser objeto de autenticación por el ANEXO D y el ANEXO F de H.235 V.3.

Los significados detallados de TokenOID se indican en la tabla 1:

Referencia de identificador de objeto	Valor de identificador de objeto	Descripción
"I0"	{itu-t (0) recomendación (0) h (8) 235 versión (0) 3 48}	Se utiliza en ClearTokens separados de GRQ/RRQ, GCF/RCF y ARQ, indicando que un EP no soporta la negociación DH. Se utiliza en un ClearToken separado del LRQ indicando que el ClearToken contiene una clave pública DH de una parte llamante
“I1”	{itu-t (0) recomendación (0) h (8) 235 versión (0) 3 49}	Se utiliza en ClearTokens separados presentados a la parte llamante, indicando que el ClearToken contiene una clave de sesión.
“I2”	{itu-t (0) recomendación (0) h (8) 235 versión (0) 3 50}	Se utiliza en ClearTokens separados presentados a la parte llamada, indicando que el ClearToken contiene una clave de sesión.
“I3”	{itu-t (0) recomendación (0) h (8) 235 versión (0) 3 51}	Se utiliza en un ClearToken separado del LCF, indicando que el ClearToken contiene una clave de sesión.
“I4”	{itu-t (0) recomendación (0) h (8) 235 versión (0) 3 52}	Se utiliza en ClearTokens separados de GRQ/RRQ, GCF/RCF y ARQ, indicando que un EP soporta el proceso DH. Se utiliza en un ClearToken separado del LRQ indicando que el ClearToken contiene una clave pública DH de una parte llamante
“I5”	{itu-t (0) recomendación (0) h (8) 235 versión (0) 3 53}	Se utiliza en ClearTokens separados presentados a una parte llamante, indicando que el ClearToken contiene una clave pública DH de una parte llamada.

Tabla 1

Aunque la presente invención se describe con referencia a las formas de realización antes citadas, los expertos en esta técnica pueden conocer que se pueden realizar varios cambios, modificaciones y variaciones sin desviarse por ello del alcance de protección de la invención y por lo tanto, deben protegerse por el alcance de protección según se establece por las reivindicaciones adjuntas de la presente invención.

REIVINDICACIONES

1. Un método para distribuir una clave de sesión a través de zonas de GateKeeper, GK, en modo de encaminamiento directo, caracterizado porque comprende:

una parte llamante que transmite modos de distribución de claves de sesión soportados por la parte llamante en un mensaje de demanda de admisión, ARQ, y el envío del mensaje ARQ a un GK de la parte llamante;

la determinación, por el GK de la parte llamante, de un modo de distribución de claves de sesión de la parte llamante en función de los modos de distribución de claves de sesión soportados por la parte llamante que se transmite en el mensaje ARQ y las reglas preconfiguradas de la parte llamante, la transmisión del modo de distribución de claves de sesión determinado de la parte llamante en un mensaje de demanda de localización, LRQ, y el envío del mensaje LRQ a un GK de una parte llamada;

la determinación por el GK de la parte llamada de un modo de distribución de claves de sesión de la parte llamada en función de la información transmitida en el mensaje LRQ y las reglas preconfiguradas de la parte llamada, la generación de una clave de sesión entre la parte llamante y la parte llamada y el envío de un mensaje de confirmación de localización, LCF, que contiene el modo de distribución de claves de sesión de la parte llamada y la clave de sesión generada al GK de la parte llamante;

el envío por el GK de la parte llamante de un mensaje de confirmación de admisión de llamada, ACF, que contiene la clave de sesión determinada a la parte llamante;

el envío, por la parte llamante, de un mensaje de establecimiento Setup que contiene la clave de sesión a la parte llamada.

2. El método según la reivindicación 1, en donde la etapa de la determinación por el GK de la parte llamante de un modo de distribución de claves de sesión de la parte llamante, según los modos de distribución de claves de sesión soportados por la parte llamante, que se soportan en el mensaje ARQ, comprende: la determinación por el GK de la parte llamante del modo de distribución de claves de sesión de la parte llamante según los modos de distribución de claves de sesión soportados por la parte llamante en el mensaje ARQ y dichas reglas preconfiguradas de la parte llamante que comprenden al menos uno de los recursos informáticos disponibles del GK, modos de distribución de claves de sesión soportados por la parte llamante y el nivel de seguridad de la parte llamante.

3. El método según la reivindicación 1, en donde la etapa de la determinación por el GK de la parte llamada de un modo de distribución de claves de sesión de la parte llamada en función de la información transmitida en el mensaje LRQ comprende: la determinación por el GK de la parte llamada de modos de distribución de claves de sesión de la parte llamada, en función de la información transmitida en el mensaje LRQ y dichas reglas preconfiguradas de la parte llamada, que comprenden al menos uno de los recursos informáticos disponibles del GK, modos de distribución de claves de sesión soportados por la parte llamante y el nivel de seguridad de la parte llamada.

4. El método según la reivindicación 1, en donde la etapa de una parte llamante que transmite modos de distribución de claves de sesión, soportados por la parte llamante en un mensaje ARQ, y el envío del mensaje ARQ a un GK de la parte llamante comprende:

cuando la parte llamante soporta una negociación de Diffie-Hellman, DH, el establecimiento de un valor “I4” en un identificador TokenOID de un ClearToken en el mensaje ARQ y el envío del mensaje ARQ al GK de la parte llamante y de no ser así,

el establecimiento de un valor "I0" en el identificador TokenOID del ClearToken en el mensaje ARQ y el envío del mensaje ARQ al GK de la parte llamante.

5. El método según la reivindicación 1 o 4, en donde el modo de distribución de claves de sesión de la parte llamante, determinado por el GK de la parte llamante, es el GK de la parte llamada que genera la clave de sesión y

la etapa de realización del modo de distribución de claves de sesión determinado de la parte llamante en un mensaje LRQ y el envío del mensaje LRQ a un GK de la parte llamada por el GK de la parte llamante comprende: el establecimiento por el GK de la parte llamante de un valor "I0" en un TokenOID de un ClearToken en el mensaje LRQ y el envío del mensaje LRQ al GK de la parte llamada.

6. El método según la reivindicación 1 o 4, en donde el modo de distribución de claves de sesión de la parte llamante determinado por el GK de la parte llamante es el GK de la parte llamante y el GK de la parte llamada que realiza la negociación DH y

la etapa de realizar el modo de distribución de claves de sesión determinado en un mensaje LRQ y el envío del mensaje LRQ a un GK de la parte llamada por el GK de la parte llamante comprende: el GK de la parte llamante genera una clave

pública DH, el soporte de la clave pública DH en un campo dhkey de un ClearToken en el mensaje LRQ, el establecimiento de un valor “I4” en el TokenOID del ClearToken y el envío del mensaje LRQ al GK de la parte llamada.

7. El método según la reivindicación 6, en donde el modo de distribución de claves de sesión de la parte llamante, determinado por el GK de la parte llamante, es la parte llamante y el GK de la parte llamada que realiza la negociación DH y

la etapa de transmitir el modo de distribución de claves de sesión determinado en un mensaje LRQ y el envío del mensaje LRQ a un GK de la parte llamada por el GK de la parte llamante comprende: el GK de la parte llamante transmite el ClearToken del mensaje ARQ en el mensaje LRQ y envía el mensaje LRQ al GK de la parte llamada.

8. El método según la reivindicación 5, en donde la etapa de la determinación por el GK de la parte llamada del modo de distribución de claves de sesión de la parte llamada, en función de la información transmitida en el mensaje LRQ, comprende: la determinación por el GK de la parte llamada de que el modo de distribución de claves de sesión de la parte llamada es el GK de la parte llamada que genera la clave de sesión en función del valor "I0" en el TokenOID del ClearToken en el mensaje LRQ y

la etapa de enviar un mensaje de LCF que contiene el modo de distribución de claves de sesión de la parte llamada y la clave de sesión al GK de la parte llamante comprende: la encriptación por el GK de la parte llamada de la clave de sesión para obtener una primera clave de sesión encriptada y una segunda clave de sesión encriptada; el GK de la parte llamada genera un CTb de ClearToken que contiene la primera clave de sesión encriptada y que tiene un TokenOID establecido a “I2” y un CTg de ClearToken que contiene la clave de sesión encriptada y que tiene un TokenOID establecido a “I3”, el envío del mensaje LCF que contiene el CTb y el CTg al GK de la parte llamante.

9. El método según la reivindicación 6 o 7, en donde la etapa de determinación por el GK de la parte llamada de los modos de distribución de claves de sesión de la parte llamada, en función de la información transmitida en el mensaje LRQ, comprende: la determinación por el GK de la parte llamada de que el modo de distribución de claves de sesión de la parte llamada es la negociación DH en función del valor “I4” en el TokenOID del ClearToken en el mensaje LRQ y

la etapa de generar una clave de sesión entre la parte llamante y la parte llamada comprende: el GK de la parte llamada genera una clave privada DH y calcula la clave de sesión entre la parte llamante y la parte llamada a partir de la clave privada DH generada, junto con la clave pública DH obtenida a partir del mensaje LRQ utilizando un algoritmo DH y

la etapa de enviar un mensaje LCF que contiene el modo de distribución de claves de sesión de la parte llamada y la clave de sesión para el GK de la parte llamante comprende: el GK de la parte llamada realiza la encriptación de la clave de sesión para obtener una primera clave de sesión encriptada, generando un CTb de ClearToken que contiene la primera clave de sesión encriptada y que tiene un TokenOID establecido a “I2” y un ClearToken con TokenOID establecido a “I5” y el campo dhkey del ClearToken contiene una clave privada DH generada por el GK de la parte llamada y el envío del mensaje de LCF que contiene el CTb y el ClearToken al GK de la parte llamante.

10. El método según la reivindicación 8 que comprende, además:

antes de que el GK de la parte llamante envíe el mensaje ACF que contiene la clave de sesión a la parte llamante, el GK de la parte llamante obtiene y determina el modo de distribución de claves de sesión de la parte llamada transmitida en el mensaje LCF y la determinación de que el modo de distribución de claves de sesión de la parte llamada es el GK de la parte llamada que genera la clave de sesión, obteniendo el GK de la parte llamante la clave de sesión en función del CTg transmitido en el mensaje LCF y realizando la encriptación de la clave de sesión para obtener una tercera clave de sesión encriptada, generando un CTa de ClearToken que contiene la tercera clave de sesión encriptada y que tiene un TokenOID establecido en “I1” y la etapa en la que el GK de la parte llamante envía el mensaje ACF que contiene la clave de sesión a la parte llamante comprende: el envío del mensaje ACF que contiene el CTa y el CTb en el mensaje LCF a la parte llamante.

11. El método según la reivindicación 9 que comprende, además:

antes de que el GK de la parte llamante envíe el mensaje ACF que contiene la clave de sesión a la parte llamante,

el GK de la parte llamante obtiene y determina el modo de distribución de claves de sesión de la parte llamada transmitida en el mensaje LCF y la determinación de que el modo de distribución de claves de sesión de la parte llamada es la negociación DH y la parte llamante no soporta la negociación DH, el cálculo de la clave de sesión a partir de la clave pública DH del GK de la parte llamante y la clave privada DH del GK de la parte llamada que se transmite en el mensaje LCF utilizando el algoritmo DH, la encriptación de la clave de sesión para obtener una segunda clave de sesión encriptada, la generación de un ClearToken Cta que contiene la segunda clave de sesión encriptada y que tiene un TokenOID establecido a “I1” y la etapa en la que el GK de la parte llamante envía el mensaje ACF que contiene la clave de sesión a la parte llamante comprende: el envío del mensaje ACF que contiene el CTa, junto con el CTb, en el mensaje LCF a la parte llamante.

12. El método según la reivindicación 9, en donde la etapa en la que el GK de la parte llamante envía un mensaje ACF que contiene la clave de sesión a la parte llamante comprende:

la obtención y determinación, por el GK de la parte llamante, del modo de distribución de claves de sesión de la parte llamada transmitido en el mensaje LCF y la determinación de que el modo de distribución de claves de sesión de la parte llamada es la negociación DH y la parte llamante soporta la negociación DH, la obtención del ClearToken con un TokenOID establecido a "I5" y el CTb en el mensaje LCF y el envío del mensaje ACF que transmite el ClearToken con el TokenOID establecido a "I5" y el CTb a la parte llamante.

13. El método según la reivindicación 10 que comprende, además:

después de que el GK de la parte llamante envíe un mensaje ACF que contiene la clave de sesión a la parte llamante a través del mensaje ACF, la parte llamante determina que el mensaje ACF no contiene un ClearToken con TokenOID establecido a "I5", el cálculo de la clave de sesión entre la parte llamante y la parte llamada en función de una clave compartida entre el GK de la parte llamante y la parte llamante.

14. El método según la reivindicación 11 o 12 que comprende, además:

después de que el GK de la parte llamante envíe el mensaje ACF que contiene la clave de sesión a la parte llamante a través del mensaje ACF, la parte llamante determina que el mensaje ACF contiene un ClearToken con un TokenOID establecido a "I5", el cálculo de la clave de sesión entre la parte llamante y la parte llamada en función de la clave pública DH de la parte llamante y la clave privada DH del GK de la parte llamada que se transmite en el mensaje ACF.

15. El método según la reivindicación 13 o 14, en donde la etapa de enviar un mensaje de Setup, que contiene la clave de sesión a la parte llamada, comprende:

la configuración, por la parte llamante, de la información de autenticación del mensaje de Setup en función de la clave de sesión y la transmisión del mensaje de Setup que transmite el CTb a la parte llamada;

el método comprende, además:

la obtención por la parte llamada de la clave de sesión en función de CTb en el mensaje de Setup y la autenticación del mensaje de Setup en función de la clave de sesión;

la determinación, por la parte llamada, de la clave de sesión como la clave de sesión utilizada para enviar mensajes con la parte llamante en el modo de encaminamiento directo.

16. El método según la reivindicación 1 que comprende, además:

antes de que la parte llamante envíe el mensaje ARQ al GK de la parte llamante, la parte llamante y la parte llamada transmiten información de si soportan la negociación de DH en el ClearToken de un mensaje de Demanda de Gatekeeper, GRQ, o un mensaje de Demanda de Registro, RRQ, y el envío del mensaje al GK de la parte llamante y al GK de la parte llamada, respectivamente.

17. Un sistema para distribuir una clave de sesión a través de las zonas de GateKeeper, GK, en un modo de encaminamiento directo, caracterizado porque comprende:

una parte llamante, configurada para transmitir los modos de distribución de claves de sesión soportados por la parte llamante en un mensaje de demanda de admisión, ARQ, y el envío del mensaje ARQ a un GK de la parte llamante;

el GK de la parte llamante, configurado para determinar un modo de distribución de claves de sesión para la parte llamante en función de los modos de distribución de claves de sesión soportados por la parte llamante que se transmiten en el mensaje ARQ y las reglas preconfiguradas de la parte llamante, para transmitir el modo de distribución de claves de sesión determinado en un mensaje de Demanda de Localización, LRQ, y para enviar el mensaje LRQ a un GK de la parte llamada;

el GK de la parte llamada, configurado para determinar el modo de distribución de claves de sesión de una parte llamada en función de la información transmitida en el mensaje LRQ y las reglas preconfiguradas de la parte llamada, para generar una clave de sesión entre la parte llamante y la parte llamada y para enviar un mensaje de confirmación de localización, LCF, que contiene el modo de distribución de claves de sesión de la parte llamada y la clave de sesión generada al GK de la parte llamante;

el GK de la parte llamante está configurado, además, para enviar un mensaje de Confirmación de Admisión de Llamada, ACF, que contiene la clave de sesión determinada a la parte llamante;

la parte llamante está configurada, además, para enviar un mensaje de Setup que contiene la clave de sesión a la parte llamada.

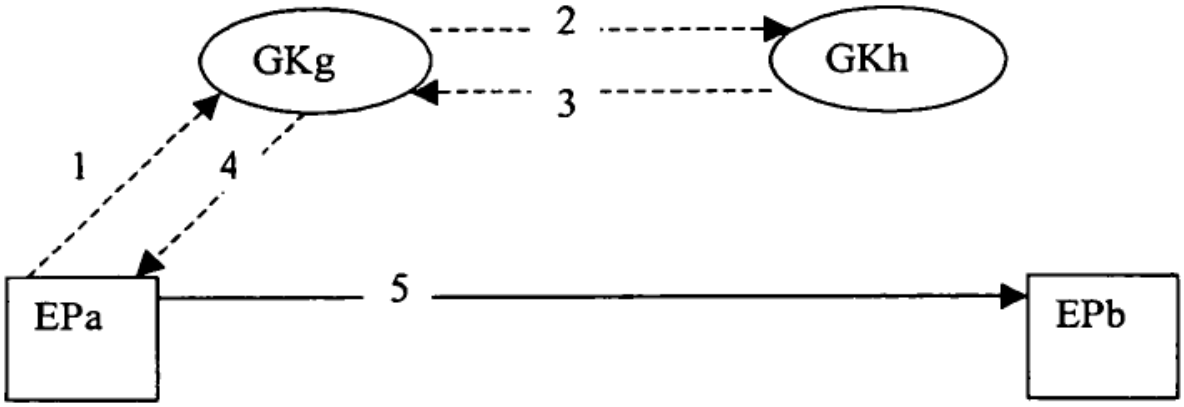

Fig. 1