(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 694 676**

(51) Int. CI.:

***H04L 29/06*** (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **27.06.2013 PCT/FR2013/051504**

(87) Fecha y número de publicación internacional: **03.01.2014 WO14001724**

(96) Fecha de presentación y número de la solicitud europea: **27.06.2013 E 13744647 (2)**

(97) Fecha y número de publicación de la concesión europea: **08.08.2018 EP 2868058**

(54) Título: **Procedimiento de emisión de un mensaje por un servidor de un núcleo de red IP multimedia IMS y servidor**

(30) Prioridad:

**29.06.2012 FR 1256258**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**26.12.2018**

(73) Titular/es:

**ORANGE (100.0%)**
**78, rue Olivier de Serres**
**75015 Paris, FR**

(72) Inventor/es:

**LE ROUZIC, JEAN-CLAUDE y**
**DOREE, JOSÉ**

(74) Agente/Representante:

**ISERN JARA, Jorge**

## DESCRIPCIÓN

Procedimiento de emisión de un mensaje por un servidor de un núcleo de red IP multimedia IMS y servidor

Antecedentes de la invención

La invención está relacionada con el campo general de las telecomunicaciones y, más particularmente, con el campo de las arquitecturas de red IP (Internet Protocol) multimedia, tales como, en concreto, unas arquitecturas de red que utilizan la tecnología designada por "voz sobre IP" (o VoIP para Voice over IP).

Tiene una aplicación prioritaria, pero no limitativa, en el contexto de núcleos de red IP multimedia que se apoyan en una arquitectura IMS (IP Multimedia Subsystem), tal como se propone por el estándar 3GPP (Third Generation Partnership Project) y que implementa el protocolo de inicio de sesiones multimedia SIP (Session Initiation Protocol). El protocolo SIP, definido por el estándar IETF (Internet Engineering Task Force), se describe en detalle en el documento RFC 3261 que lleva por título "SIP: Session Initiation Protocol", junio de 2002, editado por la IETF.

La invención puede utilizarse, no obstante, en asociación con otras arquitecturas de núcleos de red IP multimedia, tales como, por ejemplo, unas arquitecturas propietarias, que implementan o no el protocolo SIP para el establecimiento de sesiones multimedia (voz, texto, vídeo, datos, etc.).

La invención se refiere, más precisamente, a la seguridad de las comunicaciones entre un terminal y un núcleo de red IP multimedia.

Los operadores telefónicos han empezado, hoy en día, la migración de sus redes telefónicas de conmutación de circuitos hacia unas redes de voz sobre IP de conmutación de paquetes, tales como, por ejemplo, unas redes VoIP que se apoyan en una arquitectura IMS.

En estas redes VoIP, un terminal puede conectarse y registrarse respecto al núcleo de red IMS por mediación de varias redes de acceso, como, en concreto, por medio de una red de acceso 3GPP, xDSL (x Digital Subscriber Line), EPC (Evolved Packet Core), WLAN (Wireless Local Area Network), cable, WiMAX (Worldwide interoperability for Microwave Access) o CDMA2000 (Code Division Multiple Access 2000).

El estándar 3GPP, en su definición actual, prevé la posibilidad de establecer un vínculo seguro entre un terminal y su servidor de enlace al núcleo de red IMS, dicho de otra manera, entre el terminal y el servidor P-CSCF (Proxy-Call Session Control Function) que le está asociado. Este vínculo seguro, también conocido con el nombre de "túnel seguro" o "de asociación de seguridad" ("*security association*" en inglés), se traduce en el encriptado (esto es, el cifrado) de los datos vehiculados entre el terminal y el servidor P-CSCF y el control de la integridad de estos datos. Como se describe en las especificaciones RFC 3329 y TS 33.203 del 3GPP, los parámetros de este vínculo seguro (protocolo de seguridad utilizado, algoritmos de cifrado o de firma, números de puertos utilizados, etc.) se intercambian entre el terminal y el servidor P-CSCF durante el registro del terminal respecto al núcleo de red IMS. Una vez establecido este vínculo seguro, existe una asociación de seguridad entre el terminal y el servidor P-CSCF que ofrece una garantía contra el espionaje de los datos emitidos o recibidos por el terminal.

Más precisamente, cuando un terminal propone un método de autentificación que comprende el establecimiento de un túnel seguro, emite una petición de registro que comprende un "header" ("encabezamiento") (campo en la petición de registro) llamado "Authorization" ("Autorización"), así como un header (encabezamiento) "security-client" ("seguridad-cliente") que contiene:

- ya sea el valor "ipsec-3gpp", asociado al protocolo IPsec (Internet Protocol security) (cf. la Sección 5.1.1.2.2 de la especificación TS 24.229),
- ya sea el valor "tls", asociado al protocolo TLS (Transport Layer Security) (cf. la Sección 5.1.1.2.4 de la especificación TS 24.229),

que son los dos mecanismos de túnel seguro previstos por el 3GPP (cf. el Anexo H de la especificación TS 33.203). El protocolo IPsec está asociado al método de autentificación denominado "IMS AKA" y el protocolo TLS está asociado al método de autentificación denominado "SIP digest with TLS".

Ahora bien, el establecimiento y el mantenimiento de un túnel seguro de este tipo es relativamente costoso en cuanto a recursos, tanto al nivel de los terminales como al nivel de los servidores P-CSCF. Los algoritmos de cifrado consumen, en efecto, muchos recursos CPU (Central Processing Unit), lo que tiene un impacto sobre la vida útil de las baterías de los terminales móviles y necesita dimensionar en consecuencia los servidores P-CSCF.

El impacto sobre los recursos de los terminales móviles se acentúa, además, por el hecho de que el túnel seguro previsto por el estándar 3GPP llega a superponerse a los procesos de cifrado ya implementados por algunas redes de acceso móviles, tales como los procesos de cifrado previstos para proteger las informaciones transmitidas por los terminales móviles hacia los nodos SGSN (Serving GPRS Support Node) para el plan de control y BTS (Base

Transceiver Station) o Node B para el plan usuario de las redes GERAN (GSM EDGE Radio Access Network) y UTRAN (UMTS Terrestrial Radio Access Network) o hacia las entidades MME (Mobility Management Entity) para el plan de control y e-NodeB para el plan usuario de las redes LTE (Long Term Evolution).

En otras palabras, para estas redes de acceso, los datos intercambiados entre el terminal y el núcleo de red IP multimedia se cifran una primera vez por los procesos de cifrado aplicados por las redes de acceso, luego, los datos cifrados obtenidos se cifran una segunda vez en el túnel seguro establecido entre el terminal y el núcleo de red IP multimedia.

Por otra parte, es conveniente señalar, que un mismo terminal se verá obligado a establecer varios canales de comunicación sobre el plan usuario en función de los servicios utilizados (Internet, Voz sobre LTE,...) y para cada uno de ellos, podría instalarse entre el terminal y la red de acceso un túnel seguro.

Este cifrado múltiple de los datos, aunque garantiza una protección máxima de los datos emitidos o recibidos por los terminales, reduce, igualmente, de manera considerable la autonomía de los terminales.

Objeto y sumario de la invención

La invención permite paliar, en concreto, este inconveniente proponiendo un procedimiento de emisión de un mensaje por un servidor de un núcleo de red IP multimedia como continuación a la recepción por dicho servidor de una petición de registro de un terminal respecto al núcleo de red, proponiendo dicha petición de registro un método de autentificación que prevé (o de forma equivalente, que requiere) el establecimiento de un túnel seguro entre el terminal y una entidad de enlace de este terminal al núcleo de red, comprendiendo dicho procedimiento de emisión:

- una etapa de identificación de una red de acceso utilizada por el terminal para registrarse respecto al núcleo de red;
- una etapa de elaboración, en función de la red de acceso identificada, de una recomendación en cuanto al establecimiento o no del túnel seguro entre el terminal y la entidad de enlace para dicho método de autentificación; y
- una etapa de inserción de esta recomendación en el mensaje emitido por el servidor.

Correlativamente, la invención tiene como propósito, igualmente, un servidor de un núcleo de red IP multimedia, comprendiendo este servidor unos medios activados como continuación a la recepción por el servidor de una petición de registro de un terminal respecto al núcleo de red, proponiendo dicha petición de registro un método de autentificación que prevé el establecimiento de un túnel seguro entre el terminal y una entidad de enlace de este terminal al núcleo de red, comprendiendo estos medios:

- unos medios de identificación de una red de acceso utilizada por el terminal para registrarse respecto al núcleo de red;
- unos medios de elaboración, en función de la red de acceso identificada, de una recomendación en cuanto al establecimiento o no del túnel seguro entre el terminal y la entidad de enlace para dicho método de autentificación;
- unos medios de inserción de esta recomendación en un mensaje; y
- unos medios de emisión de este mensaje.

Se señalará que dicho método de autentificación propuesto por el terminal puede estar indicado de manera explícita, pero (como se explica más abajo) estará preferiblemente, en el estado actual de las normas 3GPP, indicado de manera implícita.

De este modo, la invención propone acondicionar el establecimiento del túnel seguro entre el terminal y el núcleo de red IP multimedia en función al menos de la red de acceso utilizada por el terminal para registrarse respecto al núcleo de red. En concreto, se puede tomar en cuenta para elaborar esta recomendación el tipo de la red de acceso utilizada por el terminal (ej. red UMTS, red WiFi, etc.), pero, igualmente, otros parámetros relacionados con esta red de acceso como, por ejemplo, la existencia de acuerdos de itinerancia seguros con esta red de acceso, el hecho de que la red de acceso utilizada por el terminal para registrarse respecto al núcleo de red es una red de acceso visitada (situación de *roaming* internacional) o también el hecho de que la red de acceso utilizada por el terminal se sitúa o no en la red nominal (red *home*) del servidor que establece la recomendación, etc.

Es conveniente señalar que, en el sentido de la invención, una red de acceso puede comprender una o varias (sub-) redes de acceso.

Este acondicionamiento se expresa, de conformidad con la invención, en forma de una recomendación de establecer o no el túnel seguro, emitida por un servidor del núcleo de red IP multimedia durante el registro del terminal (es decir, finalmente, cuando el establecimiento del túnel seguro es requerido por el terminal).

La recomendación está elaborada por el servidor, en función de la red de acceso identificada, tomando en cuenta preferentemente un nivel de seguridad de los datos asociado (o atribuido) por el núcleo de red IP multimedia a la red de acceso utilizada por el terminal.

Este nivel de seguridad puede depender de varios factores, como, por ejemplo, del tipo de la red de acceso (ej. acceso 3GPP, acceso WiFi (Wireless Fidelity), etc.), de la existencia de procesos de seguridad fuertes implementados sobre esta red, de la aplicación de acuerdos de itinerancia seguros por el núcleo de red con esta red de acceso, etc. Refleja la confianza que tiene el núcleo de red IP multimedia (esto es, el operador del núcleo de red IP multimedia) en la seguridad de los intercambios de datos asegurado por la red de acceso. De este modo, un núcleo de red IP multimedia puede asociar a una red de acceso un nivel de seguridad escaso a pesar de los algoritmos de cifrado implementados por esta red de acceso, por ejemplo, porque esta red de acceso está asociada a una zona geográfica sensible, etc.

Esta recomendación permite, de este modo, que el servidor indique un grado de necesidad (o de obligación) de establecer el túnel seguro normalmente previsto por el núcleo de red entre el terminal y la entidad de enlace, teniendo en cuenta el nivel de seguridad garantizado por la red de acceso según el núcleo de red IP multimedia.

Por supuesto, tiene como objetivo transmitirse al terminal y/o a la entidad de enlace para ejecutarse durante el registro del terminal.

La recomendación emitida por el servidor comprende preferentemente una de las siguientes indicaciones:

- una indicación de no establecer el túnel seguro entre el terminal y la entidad de enlace, por ejemplo, porque el núcleo de red IP considera que la red de acceso utilizada por el terminal comprende unos procesos de cifrado lo suficientemente fuertes y fiables como para garantizar la protección y la integridad de los datos transmitidos o recibidos por el terminal;
- una indicación de libre elección en cuanto al establecimiento del túnel seguro entre el terminal y la entidad de enlace;
- una indicación de establecer el túnel seguro entre el terminal y la entidad de enlace, por ejemplo, porque la red de acceso utilizada por el terminal no se considera como lo suficientemente segura a la vista de algunos criterios predeterminados (ej. ausencia de cifrado de los datos, ausencia de control de la integridad de los datos, etc.).

De este modo, por ejemplo, si la petición de registro del terminal se recibe mediante una red de acceso 3GPP (dicho de otra manera, mediante una red de acceso radio segura debido a la definición de la norma 3GPP), que, por otra parte, se identifica como que es la red de acceso nominal del terminal o una red de acceso con la cual se concluye un acuerdo de itinerancia fuerte, el servidor puede preconizar, en su recomendación, no establecer el túnel seguro entre el terminal y la entidad de enlace o, como variante, dejar libre elección en esta recomendación al terminal de establecer o no este túnel seguro.

Por el contrario, si el terminal intenta registrarse mediante una red de acceso fija desde un hot spot (punto caliente) WiFi público no seguro, entonces, el servidor puede preconizar en su recomendación establecer el túnel seguro entre el terminal y la entidad de enlace.

La recomendación del servidor puede estar elaborada por el servidor comparando unas características y/o el tipo de la red de acceso utilizada por el terminal con respecto a unos criterios de seguridad predeterminados, para determinar si el nivel de seguridad asegurado por la red de acceso es suficiente para relajar la restricción de establecimiento del túnel seguro entre el terminal y la entidad de enlace.

En una variante de realización prioritaria y relativamente sencilla, la recomendación del servidor está elaborada consultando una tabla o una base de datos preestablecida, en la cual se asocia a diferentes redes de acceso, una recomendación sobre la necesidad (o la obligación) o no de establecer el túnel de seguridad entre el terminal y la entidad de enlace.

Esta tabla puede estar notificada por el operador del núcleo de red IP multimedia en función del nivel de seguridad de los intercambios que asocia a las diferentes redes de acceso: este nivel de seguridad puede estar establecido por el operador del núcleo de red, como se ha mencionado anteriormente, teniendo en cuenta, en concreto, el conocimiento a *priori* de los procesos de seguridad (cifrado, control de la integridad, etc.) implementados sobres estas diferentes redes de acceso (ej. en función del tipo de red de acceso y/o del operador de estas redes, de la definición de los estándares respetados por estas redes de acceso), de la existencia o no de acuerdos de itinerancia "fuertes" (fiables) con las redes de acceso, incluso de la ausencia de informaciones suficientes sobre una red de acceso, etc.

La recomendación emitida por el servidor del núcleo de red IP multimedia ofrece, de este modo, la posibilidad de librarse del establecimiento de un vínculo (túnel) seguro entre el terminal y la entidad de enlace cuando ya está asegurada una protección fuerte de los datos y de su integridad por la red de acceso utilizada por el terminal.

Por este medio, se economizan unos recursos a la vez al nivel del terminal (se preserva la vida útil de la batería) y al nivel de la entidad de enlace.

Como variante, se pueden prever solo dos tipos de recomendación posibles emitidos por el servidor, esto es, una indicación de no establecer el túnel seguro o una indicación de establecer el túnel seguro, de modo que sea más directivo. Esta variante permite economizar más recursos al nivel del terminal y de la entidad de enlace.

Por lo tanto, la invención tiene una aplicación prioritaria, pero no limitativa, cuando el núcleo de red IP multimedia emplea una arquitectura IMS, en el cual está previsto el establecimiento de un túnel seguro durante el registro de un terminal de conformidad con el estándar 3GPP. De manera más general, se aplica a cualquier núcleo de red IP multimedia que prevea el establecimiento de un túnel seguro entre el terminal y el núcleo de red al acceso (durante el registro del terminal respecto al núcleo de red).

En un contexto IMS, el servidor del núcleo de red IP multimedia que emite la recomendación puede ser un servidor S-CSCF y el mensaje en el cual se inserta la recomendación se emite, entonces, por el servidor S-CSCF con destino al terminal mediante un servidor P-CSCF que enlaza el terminal al núcleo de red IP multimedia.

Es conveniente señalar que la recomendación elaborada por el servidor S-CSCF se inserta preferentemente en un mensaje de respuesta intermedia a la petición de registro del terminal, tal como un mensaje SIP 401 Unauthorized (No autorizado), emitido por el servidor S-CSCF con destino al terminal, de conformidad con el protocolo SIP.

Entonces, el servidor P-CSCF puede, propagar esta recomendación al terminal para inhibir o, por el contrario, disparar el establecimiento del túnel seguro entre el terminal y el servidor P-CSCF.

Pudiendo un mismo servidor S-CSCF estar en relación con varios servidores P-CSCF, esta variante presenta la ventaja de que limita la complejidad relacionada con la implementación de la invención y, por lo tanto, de que optimiza la explotación del núcleo de red (en concreto, tiene que memorizarse una sola tabla preestablecida al nivel del servidor S-CSCF para emitir unas recomendaciones relativas a varias entidades de enlace).

Por otra parte, esta variante ofrece la posibilidad de tomar en cuenta fácilmente, para elaborar la recomendación (o ponderarla), unas informaciones contenidas en el perfil del usuario del terminal. De este modo, por ejemplo, se puede considerar asociar en el perfil del usuario del terminal, una indicación según la cual, para este usuario, siempre debe establecerse un túnel de seguridad, independientemente del nivel de seguridad asociado a la red de acceso utilizada por el terminal para registrarse.

Como variante, el servidor del núcleo de red IP multimedia que emite la recomendación puede ser un servidor P-CSCF y el mensaje en el cual se inserta la recomendación se emite, entonces, hacia el terminal.

La recomendación elaborada por el servidor P-CSCF se inserta preferentemente en un mensaje de respuesta intermedia a la petición de registro del terminal, tal como un mensaje SIP 401 Unauthorized (No autorizado) emitido por el servidor S-CSCF con destino al terminal y que transita por el servidor P-CSCF, de conformidad con el protocolo SIP.

Dicho de otra manera, el servidor que emite la recomendación puede ser la propia entidad de enlace del terminal al núcleo de red IP multimedia. Esta variante permite tener una gestión más local del establecimiento del túnel seguro y tomar en cuenta más fácilmente unas especificidades locales del acceso al núcleo de red (ej. presencia de algunas redes de acceso (ej. WiFi) en una localización particular).

En otra variante también, se elabora una recomendación de conformidad con la invención a la vez por un servidor S-CSCF y por un servidor P-CSCF del núcleo de red IP multimedia. En esta variante de realización, si las recomendaciones elaboradas respectivamente por el servidor S-CSCF y por el servidor P-CSCF son diferentes, solo se toma en cuenta y transmite en definitiva al terminal la recomendación emitida por el servidor P-CSCF. Dicho de otra manera, la recomendación emitida por el servidor P-CSCF llega a machacar la recomendación emitida por el servidor S-CSCF en el mensaje de respuesta intermedia SIP 401 Unauthorized (No autorizado).

De manera más general, el servidor según la invención puede estar integrado en cualquier entidad del núcleo de red adecuada para recibir unas peticiones de registro de los terminales que contienen una solicitud de establecimiento de un túnel seguro entre el terminal y la entidad de enlace de este terminal al núcleo de red.

En un modo particular de realización de la invención, la recomendación se elabora en función, igualmente, de al menos un parámetro recibido con la petición de registro.

Este parámetro puede estar, en concreto, contenido en la petición de registro o vehiculado en la señalización asociada a esta petición de registro.

Este modo de realización permite, para una misma red de acceso o para un mismo tipo de red de acceso, ponderar el acondicionamiento en función de la red de acceso implementada por el servidor, por medio del parámetro contenido en la petición de registro.

Este parámetro puede ser, en concreto, una dirección IP de transporte de la petición de registro, es decir, la dirección fuente de la petición de registro del terminal tal como se recibe por el servidor. De forma conocida por el experto en la materia, esta dirección fuente puede, según las configuraciones de red consideradas, corresponder a la dirección de contacto o a la dirección IP del terminal que pretende registrarse (ej. para una red de acceso móvil) o a la dirección IP de una entidad intermedia entre el terminal y el servidor (ej. pasarela doméstica).

De este modo, a título de ejemplo, para una misma red de acceso, se podrá decidir ventajosamente emitir una recomendación firme de no establecer túnel seguro para un cierto intervalo de direcciones IP, mientras que se dejará una libre elección para otro intervalo de direcciones IP o una selección de direcciones IP.

Como variante, este parámetro puede ser un identificador asociado al usuario del terminal, tal como un identificador IMSI (International Mobile Subscriber Identity) o MSISDN (Mobile Station Integrated Services Digital Network).

De este modo, por ejemplo, para una misma red de acceso, se puede decidir emitir de forma general una recomendación de no establecer túnel seguro, salvo para algunos usuarios identificados de manera previa (por ejemplo, insertando en el perfil de estos usuarios un indicador apropiado), para los cuales siempre se emitirá, por el contrario, una recomendación de establecer un túnel seguro.

Más generalmente, la toma en cuenta de un parámetro tal como un identificador asociado al usuario del terminal permite ponderar la recomendación elaborada con respecto a la red de acceso utilizada por el terminal, en función de informaciones asociadas a este identificador y presentes, en concreto, en el perfil del usuario. Estas informaciones comprenden, por ejemplo, los servicios a los cuales se ha suscrito el usuario, sus preferencias, su pertenencia a una categoría de abonados sensibles para los cuales debe implementarse siempre un vínculo seguro, etc.

En un modo particular de realización de la invención, el mensaje emitido está conforme con el protocolo SIP y la recomendación del servidor se inserta en un campo "Security Server" ("Servidor de Seguridad") de este mensaje.

Este modo de realización permite establecer una interfaz fácilmente con el estándar SIP existente, mediando la añadidura de un parámetro idóneo en el campo "Security Server" ("Servidor de Seguridad") definido por el estándar 3GPP en el anexo H del documento de especificación TS 33.203, para informar al terminal o a la entidad de enlace de que debe (o puede) o no tener lugar la implementación de un túnel seguro.

En un modo particular de realización, el mensaje emitido por el servidor contiene, además, unas informaciones que permiten el establecimiento del túnel seguro entre el terminal y la entidad de enlace.

Este modo de realización es compatible con los terminales que no son capaces de interpretar y/o de ejecutar la recomendación emitida por el servidor. Un terminal de este tipo podrá, de este modo, sea el que sea el juicio emitido por el servidor y la seguridad asegurada por la red de acceso, establecer un vínculo seguro a partir de las informaciones contenidas en el mensaje, de modo que se garantice la protección y la integridad de los datos intercambiados con el núcleo de red.

Por otra parte, estas informaciones pueden utilizarse, igualmente, cuando la recomendación emitida por el servidor deja una libre elección en cuanto al establecimiento o no del túnel seguro.

Es conveniente señalar que la eficacia de la invención de reducir la complejidad y el sobrecoste en materia de recursos que resulta de la existencia de un doble cifrado de los datos se basa, por una parte, en el servidor que emite la recomendación en cuanto al establecimiento o no del túnel seguro en función de la red de acceso utilizada por el terminal y, por otra parte, en el propio terminal, en el momento en que este es adecuado para ejecutar la recomendación emitida por el servidor durante su registro respecto al núcleo de red.

De este modo, según otro aspecto, la invención tiene como propósito, igualmente, un procedimiento de registro de un terminal respecto a un núcleo de red IP, comprendiendo este procedimiento:

- una etapa de emisión, por el terminal, de una petición de registro respecto al núcleo de red, mediante una red de acceso, proponiendo dicha petición de registro un método de autentificación que prevé el establecimiento de un túnel seguro entre el terminal y una entidad de enlace de este terminal al núcleo de red;
- una etapa de recepción, por el terminal, con procedencia del núcleo de red, de una recomendación en cuanto al establecimiento o no del túnel seguro entre el terminal y la entidad de enlace para dicho método de autentificación, proviniendo esta recomendación de un mensaje emitido por un servidor del núcleo de red de conformidad con un procedimiento de emisión según la invención, ejecutado como continuación a la recepción de la petición de registro del terminal; y

- una etapa de interpretación de esta recomendación por el terminal.

Correlativamente, la invención también tiene como propósito un terminal que comprende:

- unos medios de emisión de una petición de registro respecto a un núcleo de red IP multimedia mediante una red de acceso, proponiendo dicha petición de registro un método de autentificación que prevé el establecimiento de un túnel seguro entre el terminal y una entidad de enlace de este terminal al núcleo de red;
- unos medios de recepción, con procedencia del núcleo de red, de una recomendación en cuanto al establecimiento o no del túnel seguro entre el terminal y la entidad de enlace para dicho método de autentificación, proviniendo esta recomendación de un mensaje emitido por un servidor del núcleo de red conforme con la invención, como continuación a la recepción de la petición de registro; y
- unos medios de interpretación de esta recomendación.

El procedimiento de registro y el terminal se benefician de las mismas ventajas que las citadas anteriormente para el procedimiento de emisión de un mensaje y el servidor.

La invención también tiene como propósito una entidad de enlace de un terminal a un núcleo de red IP multimedia, comprendiendo esta entidad de enlace:

- unos medios de recepción de una petición de registro del terminal respecto al núcleo de red, mediante una red de acceso, proponiendo dicha petición de registro un método de autentificación que prevé el establecimiento de un túnel seguro entre dicho terminal y dicha entidad de enlace;
- unos medios de transmisión de dicha petición de registro a un servidor conforme con la invención; unos medios de recepción, con procedencia del servidor, de un mensaje que contiene una recomendación en cuanto al establecimiento o no del túnel seguro entre el terminal y la entidad de enlace para dicho método de autentificación; y
- unos medios de transmisión de esta recomendación al terminal.

Correlativamente, la invención también tiene como propósito un procedimiento de transmisión destinado a implementarse por una entidad de enlace de un terminal a un núcleo de red IP multimedia, comprendiendo este procedimiento de transmisión:

- una etapa de recepción de una petición de registro del terminal respecto al núcleo de red, mediante una red de acceso, proponiendo dicha petición de registro un método de autentificación que prevé el establecimiento de un túnel seguro entre dicho terminal y dicha entidad de enlace;
- una etapa de transmisión de esta petición de registro a un servidor del núcleo de red;
- una etapa de recepción, con procedencia del servidor, de un mensaje que contiene una recomendación en cuanto al establecimiento o no del túnel seguro entre el terminal y la entidad de enlace para dicho método de autentificación, resultando el mensaje de la ejecución por el servidor de un procedimiento de emisión de un mensaje conforme con la invención; y
- una etapa de transmisión de esta recomendación al terminal.

La entidad de enlace transfiere, de este modo, la recomendación emitida por el servidor del núcleo de red IP multimedia hasta el terminal, con el fin de que este aplique esta recomendación. Es conveniente señalar que no se adscribe ninguna limitación a la forma en que se transmite la recomendación estrictamente hablando al terminal, esto es, la entidad de enlace puede justo incluir en el estado la recomendación en un mensaje enviado al terminal (ej. en un parámetro del campo Security Server (Servidor de Seguridad) de un mensaje SIP) o, por el contrario, modificar la forma estrictamente hablando de esta recomendación, por ejemplo, no enviando las informaciones necesarias para el establecimiento del túnel si la recomendación emitida por el servidor es de no establecer el túnel entre el terminal y la entidad de enlace.

En un modo particular de realización, las diferentes etapas del procedimiento de emisión de un mensaje y/o del procedimiento de registro y/o del procedimiento de trasmisión están determinadas por unas instrucciones de programas de ordenadores.

En consecuencia, la invención también tiene como propósito un programa de ordenador sobre un soporte de informaciones, siendo este programa susceptible de implementarse en un servidor o más generalmente en un ordenador, incluyendo este programa unas instrucciones adaptadas para la implementación de las etapas de un procedimiento de emisión de un mensaje tal como se ha descrito más arriba.

La invención tiene como propósito, igualmente, un programa de ordenador sobre un soporte de informaciones, siendo este programa susceptible de implementarse en un terminal o más generalmente en un ordenador, incluyendo este programa unas instrucciones adaptadas para la implementación de las etapas de un procedimiento de registro tal como se ha descrito más arriba.

La invención también tiene como propósito un programa de ordenador sobre un soporte de informaciones, siendo este programa susceptible de implementarse en una entidad de enlace o más generalmente en un ordenador, incluyendo este programa unas instrucciones adaptadas para la implementación de las etapas de un procedimiento de transmisión tal como se ha descrito más arriba.

Estos programas pueden utilizar cualquier lenguaje de programación y estar en forma de códigos fuente, código objeto o de códigos intermedios entre código fuente y código objeto, tal como en una forma parcialmente compilada o en cualquier otra forma deseable.

La invención también tiene como propósito un soporte de informaciones legible por un ordenador y que incluye unas instrucciones de un programa de ordenador tal como se ha mencionado más arriba.

El soporte de informaciones puede ser cualquier entidad o dispositivo capaz de almacenar el programa. Por ejemplo, el soporte puede incluir un medio de almacenamiento, tal como una ROM, por ejemplo, un CD ROM o una ROM de circuito microelectrónico o también un medio de registro magnético, por ejemplo, un disquete (floppy disc) o un disco duro.

Por otra parte, el soporte de informaciones puede ser un soporte transmisible tal como una señal eléctrica u óptica, que puede encaminarse mediante un cable eléctrico u óptico, por radio o por otros medios. El programa según la invención puede descargarse, en particular, desde una red de tipo Internet.

De manera alternativa, el soporte de informaciones puede ser un circuito integrado en el cual se incorpora el programa, estando el circuito adaptado para ejecutar o para ser utilizado en la ejecución del procedimiento en cuestión.

La invención tiene como propósito, igualmente, un sistema de comunicación que comprende:

- un servidor de un núcleo de red IP multimedia conforme con la invención;
- un terminal según la invención, adecuado para registrarse respecto al núcleo de red multimedia enviando una petición de registro al núcleo de red mediante una red de acceso,
- una entidad de enlace del terminal al núcleo de red IP multimedia;

siendo el terminal adecuado para ejecutar una recomendación elaborada por el servidor en cuanto al establecimiento o no de un túnel seguro entre el terminal y la entidad de enlace del terminal al núcleo de red.

De este modo, el sistema de comunicación según la invención permite relajar la restricción de establecimiento del túnel seguro entre el terminal y la entidad de enlace cuando se asocia un nivel de seguridad de los intercambios suficiente a la red de acceso por el núcleo de red IP multimedia. Por este medio, se economizan los recursos del terminal y de la entidad de enlace.

Se puede considerar, igualmente, en otros modos de realización, que el procedimiento de emisión de un mensaje, el procedimiento de registro, el procedimiento de transmisión, el servidor, el terminal, la entidad de enlace y el sistema de comunicación según la invención presenten en combinación todo o parte de las características anteriormente citadas.

Breve descripción de los dibujos

Otras características y ventajas de la presente invención se pondrán de manifiesto a partir de la descripción hecha más abajo, con referencia a los dibujos y anexos que ilustran unos ejemplos de realización de esta desprovistos de cualquier carácter limitativo:

- la figura 1 representa, de forma esquemática, un sistema de comunicación, un servidor, una entidad de enlace y un terminal conformes con la invención, en un primer modo de realización;
- las figuras 2A, 2B y 2C representan, de forma esquemática, las arquitecturas materiales respectivas del terminal, del servidor y de la entidad de enlace de la figura 1, en el primer modo de realización;
- la figura 3 representa, en forma de diagramas de flujo, las principales etapas de un procedimiento de registro, de un procedimiento de transmisión y de un procedimiento de emisión de un mensaje tales como se implementan respectivamente por el terminal, la entidad de enlace y el servidor de la figura 1 en el primer modo de realización;
- la figura 4 ilustra una tabla que asocia a diferentes redes de acceso, una recomendación en cuanto al establecimiento de un vínculo seguro y utilizada por el servidor de la figura 1 para elaborar su recomendación en el primer modo de realización;
- la figura 5 representa, de forma esquemática, un sistema de comunicación, un servidor y un terminal conformes con la invención, en un segundo modo de realización;
- la figura 6 representa esquemáticamente la arquitectura material del servidor de la figura 5;

- la figura 7 representa, en forma de diagramas de flujo, las principales etapas de un procedimiento de registro y de un procedimiento de emisión de un mensaje tales como se implementan respectivamente por el terminal y el servidor de la figura 5 en el segundo modo de realización;
- el anexo 1 da unos ejemplos de peticiones de registro del terminal de la figura 1 y de mensajes que contienen una recomendación emitida por el servidor de la figura 1, en el primer modo de realización; y
- el anexo 2 da unos ejemplos de una petición de registro del terminal de la figura 5 y de un mensaje que contiene una recomendación emitida por el servidor de la figura 5, en el segundo modo de realización.

Descripción detallada de la invención

La figura 1 representa, en su entorno, un sistema 1 de comunicación conforme con la invención, en un primer modo de realización.

El sistema 1 de comunicación comprende un terminal 2 conforme con la invención, adecuado para registrarse respecto a un núcleo CN de red IP multimedia mediante una red de acceso AN.

No se adscribe ninguna limitación en este documento a la naturaleza del terminal 2. Puede tratarse tanto de un terminal móvil, como un teléfono inteligente (o smartphone), un ordenador portátil o un asistente digital personal (o PDA para Personal Digital Assistant), como de un terminal fijo.

En el primer modo de realización descrito en este documento, el terminal 2 dispone de la arquitectura material de un ordenador, tal como se ilustra esquemáticamente en la figura 2A.

Incluye un procesador 2A, una memoria viva 2B, una memoria muerta 2C, una memoria flash no volátil 2D, así como unos medios de comunicación 2E que implementan, en concreto, el protocolo SIP y que le permiten comunicar mediante la red de acceso AN. Los medios de comunicación 2E permiten que el terminal 2 comunique, en concreto, con las entidades del núcleo de red CN.

La memoria muerta 2C del terminal 2 constituye un soporte de registro conforme con la invención, legible por el procesador 2A y sobre el cual está registrado un programa de ordenador conforme con la invención, que incluye unas instrucciones para la ejecución de las etapas de un procedimiento de registro respecto al núcleo de red CN conforme con la invención, descritas ulteriormente con referencia a la figura 3.

Es conveniente señalar que no se adscribe ninguna limitación a la red de acceso AN utilizada por el terminal 2 para conectarse y registrarse respecto al núcleo de red CN, desde el momento en que esta red de acceso la conoce el núcleo de red CN. Esta red de acceso puede ser, de este modo, por ejemplo, una red de acceso 3GPP, una red de acceso xDSL, una red de acceso EPC, etc. Puede estar gestionada por el mismo operador que el núcleo de red CN o por un operador distinto.

El núcleo de red CN se basa en este documento en una arquitectura IMS, que emplea el protocolo SIP, tal como se describe en el documento de especificación TS23.228 del estándar 3GPP, que lleva por título "IP Multimedia Subsystem; Stage 2", Edición 9, septiembre de 2010, disponible en el sitio web www. 3gpp. org.

De forma conocida, un núcleo de red que emplea una arquitectura IMS comprende varias entidades funcionales de las cuales, en concreto, una entidad CSCF (Call Session Control Function) compuesta por varios servidores, de entre los cuales:

- un servidor S-CSCF (Serving-Call Session Control Function), a cargo, en particular, del registro de los terminales sobre el núcleo de red; y
- un servidor P-CSCF (Proxy Call Session Control Function), que desempeña el papel de entidad de enlace de los terminales con el núcleo de red.

De este modo, en el ejemplo ilustrado en la figura 1, el núcleo de red CN comprende un servidor P-CSCF 3, punto de entrada del terminal 2 sobre el núcleo de red CN y un servidor S-CSCF 4, encargado del registro del terminal 2 respecto al núcleo de red CN. De conformidad con el funcionamiento del núcleo de red IMS CN, las peticiones de registro respecto al núcleo de red CN emitidas por el terminal 2 transitan por el servidor P-CSCF 3 antes de encaminarse para tratamiento hacia el servidor S-CSCF 4.

Como se ha mencionado anteriormente, el estándar 3GPP prevé (requiere), según el tipo de terminal y el tipo de tarjeta SIM (Subscriber Identity Module) que equipa el terminal (presencia de una tarjeta USIM (Universal Subscriber Identity Module) o ISIM (International Subscriber Identity Module)), durante el registro de un terminal respecto a un núcleo de red IMS (y, por lo tanto, respecto al núcleo de red CN), el establecimiento de un túnel seguro entre el terminal y la entidad de enlace de este terminal al núcleo de red, dicho de otra manera, entre el terminal y el servidor P-CSCF asociado a este terminal.

Por túnel seguro establecido entre dos entidades (ej. un terminal y un servidor P-CSCF), se entiende, de manera convencional, un vínculo seguro establecido entre las dos entidades que asegura, por medio de claves adecuadas, el cifrado y/o la integridad de los datos intercambiados entre estas dos entidades.

La invención propone ventajosamente, con el fin de preservar los recursos del terminal y del servidor P-CSCF, acondicionar el establecimiento de este túnel seguro en función al menos de la red de acceso tomada por el terminal.

Es conveniente señalar que la invención no se limita a una arquitectura de tipo IMS. En efecto, puede aplicarse a otras arquitecturas de núcleos de red IP Multimedia que prevean el establecimiento de un túnel seguro durante el registro de un terminal, tales como, en concreto, unas arquitecturas propietarias.

En el primer modo de realización descrito en este documento, el acondicionamiento del establecimiento del túnel seguro entre el terminal 2 y el servidor P-CSCF 3 se realiza mediante una recomendación elaborada por el servidor S-CSCF 4. El servidor S-CSCF 4 del núcleo de red CN integra, de este modo, por una parte, las funcionalidades de un servidor S-CSCF tal como se define por el estándar 3GPP y, por otra parte, las características de un servidor del sistema 1 de comunicación conforme con la invención.

El servidor S-CSCF 4 dispone en este documento de la arquitectura material de un ordenador, tal como se ilustra esquemáticamente en la figura 2B.

Incluye, en concreto, un procesador 4A, una memoria viva 4B, una memoria muerta 4C, una memoria flash no volátil 4D, así como unos medios de comunicación 4E que implementan, en concreto, el protocolo SIP. Estos medios de comunicación le permiten comunicar con las entidades del núcleo de red CN y con el terminal 2.

La memoria muerta 4C el servidor S-CSCF 4 constituye un soporte de registro conforme con la invención, legible por el procesador 4A y sobre el cual está registrado un programa de ordenador conforme con la invención, que incluye unas instrucciones para la ejecución de las etapas de un procedimiento de emisión de un mensaje conforme con la invención descritas ulteriormente con referencia a la figura 3.

Por otra parte, en el primer modo de realización, la recomendación elaborada por el servidor S-CSCF 4 en cuanto al establecimiento o no del túnel seguro entre el terminal 2 y el servidor P-CSCF 3 se transfiere por el servidor P-CSCF 3 hasta el terminal 2. De este modo, el servidor P-CSCF 3 integra no solamente las funcionalidades de un servidor P-CSCF tal como se define por el estándar 3GPP, sino, igualmente, las características de una entidad de enlace conforme con la invención.

El servidor P-CSCF 3 dispone en este documento de la arquitectura material de un ordenador, tal como se ilustra esquemáticamente en la figura 2C.

Incluye un procesador 3A, una memoria viva 3B, una memoria muerta 3C, una memoria flash no volátil 3D, así como unos medios de comunicación 3E que implementan, en concreto, el protocolo SIP. Estos medios de comunicación 3E le permiten comunicar, en concreto, con el terminal 2, así como con las otras entidades del núcleo de red CN tales como el servidor S-CSCF 4.

La memoria muerta 3C el servidor P-CSCF 3 constituye un soporte de registro conforme con la invención, legible por el procesador 3A y sobre el cual está registrado un programa de ordenador conforme con la invención, que incluye unas instrucciones para la ejecución de las etapas de un procedimiento de transmisión conforme con la invención, descritas en este momento con referencia a la figura 3.

En este momento, vamos a describir, con referencia a la figura 3, las principales etapas de un procedimiento de registro, de un procedimiento de transmisión y de un procedimiento de emisión de un mensaje implementadas respectivamente por el terminal 2, por el servidor P-CSCF 3 y por el servidor S-CSCF 4, en el primer modo de realización.

Por razones de simplificación, en este primer modo de realización se limita uno, a una recomendación elaborada por el servidor S-CSCF 4 únicamente en función de la red de acceso utilizada por el terminal 2 para registrarse respecto al núcleo de red CN.

No obstante, esta hipótesis no es limitativa y pueden tomarse en cuenta otros parámetros, además de la red de acceso utilizada por el terminal 2, para elaborar una recomendación. Estos parámetros permiten ventajosamente ponderar la recomendación establecida en función de la red de acceso del terminal 2, como se menciona ulteriormente en la descripción.

Se supone que el terminal 2 desea registrarse respecto al núcleo de red CN, mediante la red de acceso AN, para acceder, por ejemplo, a unos servicios multimedia gestionados por el núcleo de red CN.

Con este fin, el terminal 2 emite, mediante sus medios de comunicaciones 2E, una petición de registro REG1 con destino al núcleo de red CN (etapa E10). En el primer modo de realización descrito en este documento, esta petición de registro REG1 es una petición SIP REGISTER (REGISTRO).

Un ejemplo de una petición de este tipo se da en anexo 1 (cf. ejemplo Ej. 1). Comprende, en concreto, de forma conocida, un identificador del usuario del terminal 2 en los campos "From" ("De") y "To" ("A"), así como una información relativa a la red de acceso AN utilizada por el terminal 2 para registrarse respecto al núcleo de red CN. Esta información se encuentra en el campo "P-Access-Network-Info" ("Info-Red-Acceso-P") de la petición REG. De este modo, en el ejemplo del anexo 1, AN es una red de acceso de tipo 3GPP-UTRAN-TDD.

La petición REG1 emitida por el terminal 2 contiene, igualmente, unas informaciones relativas al establecimiento de un túnel seguro con el servidor P-CSCF 3 del núcleo de red CN, de conformidad con el estándar 3GPP. Estas informaciones están contenidas en el campo "Security-Client" ("Seguridad-Cliente") de la petición de registro. De este modo, el túnel seguro propuesto por el terminal será de tipo IPsec para una autentificación IMS AKA y de tipo TLS para una autentificación SIP digest con TLS. Por ejemplo, en el ejemplo Ej. 1 del anexo 1, la información "ipsec-3gpp" indica que se trata del protocolo IPsec. Dichas informaciones pueden comprender, igualmente, los algoritmos de cifrado y de control de integridad considerados (en el ejemplo Ej. 1, se trata de los algoritmos conocidos "hmac-sha1-96" y "des-ede3-cbc"), los puertos sobre los cuales el túnel debe montarse, etc.

La petición de registro REG1 se recibe por el servidor P-CSCF 3 que enlaza el terminal 2 al núcleo de red CN (etapa F10).

Tras recepción de esta petición, el servidor P-CSCF 3 identifica qué red de acceso AN está utilizada por el terminal 2 para registrarse respecto al núcleo de red CN (etapa F20).

Es conveniente señalar que la información de red de acceso, incluida por el terminal 2 en su petición de registro REG1, no es necesariamente fiable, de modo que el servidor P-CSCF 3 determina, en este documento, por sus propios medios qué red de acceso AN toma el terminal 2.

Con este fin, utiliza unas técnicas conocidas por el experto en la materia.

Una de estas técnicas consiste en establecer durante una fase preliminar y en mantener actualizada, al nivel del servidor P-CSCF 3, una tabla de correspondencia en la cual se asocia a un rango de direcciones IP, una red de acceso. Estas direcciones IP corresponden a unas direcciones IP de transporte susceptibles de utilizarse para transportar las peticiones de los terminales que pretenden conectarse al núcleo de red CN (y, por lo tanto, registrarse respecto al núcleo de red CN). Puede tratarse, según las configuraciones de red consideradas, de las direcciones IP o direcciones de contacto de los terminales que pretenden conectarse o de las direcciones IP de entidades intermedias entre estos terminales y el servidor P-CSCF 3.

Una tabla de este tipo puede establecerse fácilmente por el operador del núcleo de red CN, para cada red de acceso conocida por el operador (en cada nueva instalación de una red de acceso, por ejemplo).

De este modo, en el primer modo de realización descrito en este documento, el servidor P-CSCF 3 determina en un primer momento, según unos medios conocidos por el experto en la materia, la dirección IP de transporte de la petición de registro REG1 que ha recibido (es decir, la dirección IP fuente de la petición REG1 tal como se recibe por el servidor P-CSCF 3).

Luego, compara esta dirección IP de transporte con los rangos de direcciones IP notificadas en la tabla de correspondencia. De este modo, de ello deduce la red de acceso AN utilizada por el terminal 2 para registrarse (etapa F20).

El servidor P-CSCF 3 sustituye, en caso necesario, la información contenida en el campo "P-Access-Network-Info" ("Info-Red-Acceso-P") de la petición de registro REG1, por la red AN obtenida con la ayuda de la dirección IP de transporte de la petición REG1 (etapa F30). La información contenida en el campo P-Access-Network-Info (Info-Red-Acceso-P), como continuación a esta modificación, es una información de red certificada por el servidor P-CSCF 3.

El servidor P-CSCF 3 modifica, igualmente, algunos campos de la petición, de forma conocida de por sí, de conformidad con el estándar 3GPP. De este modo, por ejemplo, suprime de la petición el campo "Security-Client" ("Seguridad-Cliente").

La petición de registro del terminal modificada por el servidor P-CSCF 3 se transmite, entonces, con la ayuda de sus medios de comunicaciones 3E al servidor S-CSCF 4, en forma de una petición REG2 (etapa F40). La petición REG2 es, a pesar de las modificaciones aportadas a la petición REG1 recibida del terminal 2, una petición de registro del terminal 2 en el sentido de la invención.

En Anexo 1, se proporciona en el ejemplo Ej. 2 un ejemplo de petición REG2 derivada de la petición REG1 dada en el ejemplo Ej. 1.

Tras recepción de la petición REG2 de registro del terminal 2 (etapa G10), el servidor S-CSCF 4 identifica la red de acceso AN utilizada por el terminal 2 para registrarse, consultando el campo "P-Access-Network-Info" ("Info-Red-Acceso-P") de la petición, posicionado por el servidor P-CSCF 3 (etapa G20).

Luego elabora, en función de la red de acceso identificada de este modo, una recomendación RECO en cuanto al establecimiento o no del túnel seguro entre el terminal 2 y el servidor P-CSCF 3 (etapa G30). Esta recomendación traduce el carácter oportuno (es decir, útil u obligatorio) del establecimiento del túnel seguro entre el terminal 2 y el servidor P-CSCF 3, de modo que se garantice la protección y la integridad de los datos intercambiados entre el terminal 2 y el núcleo de red CN.

Esta recomendación se elabora en este documento tomando en cuenta un nivel de seguridad de los datos asociado por el núcleo de red IP multimedia a la red de acceso utilizada por el terminal.

Con este fin, en el primer modo de realización descrito en este documento, el servidor S-CSCF 4 utiliza una tabla (o base de datos) T preestablecida, en la cual se asocia a diferentes redes de acceso, una recomendación sobre la necesidad o no de establecer el túnel de seguridad entre el terminal y la entidad de enlace. La tabla T se almacena, por ejemplo, en la memoria no volátil 4D del servidor S-CSCF 4.

Esta tabla T está notificada en este documento por el operador del núcleo de red CN, en función del nivel de seguridad de los intercambios (ej. insuficiente o escaso *versus* suficiente o fuerte) que asocia a las diferentes redes de acceso. De este modo, si el nivel de seguridad de una red de acceso se considera como fuerte, está asociada en la tabla T a esta red de acceso una recomendación de no establecer túnel seguro. De manera inversa, si el nivel de seguridad de una red de acceso se considera como escaso, está asociada en la tabla T a esta red de acceso una recomendación de establecer el túnel seguro.

El nivel de seguridad de una red de acceso puede estar establecido por el operador teniendo en cuenta, en concreto, el conocimiento a *priori* de los procesos de seguridad (cifrado, control de la integridad, etc.) implementados sobres estas diferentes redes de acceso (ej. en función del tipo de red de acceso y/o del operador de estas redes, de la definición de los estándares respetados por estas redes de acceso), de la existencia o no de acuerdos de itinerancia "fuertes" (fiables) con las redes de acceso, incluso de la ausencia de informaciones suficientes sobre los procesos de seguridad implementados por una red de acceso, etc.

Un ejemplo de una tabla T de este tipo se ilustra en la figura 4. En este ejemplo, se asocia a una red de acceso 3GPP-UTRAN-TDD y a una red de acceso 3GPP-UTRAN-FDD, una recomendación de no establecer túnel seguro entre el terminal 2 y el servidor P-CSCF 3 (recomendación "Not required") ("No requerido"), mientras que se asocia a una red de acceso WiFi Pública, una recomendación de establecer el túnel seguro (recomendación "Required") ("Requerido"). Dicho de otra manera, se asocia implícitamente en esta tabla un nivel de seguridad fuerte a las redes de acceso 3GPP-UTRAN-TDD y 3GPP-UTRAN-FDD y un nivel de seguridad escaso a la red de acceso WiFi Pública.

Como variante, se puede considerar otro tipo de recomendación, dejando libre elección al terminal 2 y/o al servidor P-CSCF 3 de establecer o no el túnel seguro preconizado por el estándar 3GPP.

En el ejemplo ilustrado en Anexo 1, la red de acceso AN utilizada por el terminal 2 es una red de acceso de tipo 3GPP-UTRAN-TDD. Está asociada a una recomendación RECO de no establecer el túnel seguro entre el terminal 2 y el servidor P-CSCF 3.

El servidor S-CSCF 4 inserta la recomendación RECO obtenida consultando la tabla T a partir de la red de acceso AN en un mensaje M1 con destino al terminal 2 (etapa G40). En el ejemplo descrito en este documento, el mensaje M1 es un mensaje SIP 401 Unauthorized (No autorizado) de respuesta intermedia a la petición de registro del terminal 2, que transita por el servidor P-CSCF 3, de conformidad con el protocolo SIP.

Un ejemplo de un mensaje M1 de este tipo que contiene la recomendación RECO del servidor S-CSCF 4 se da en Anexo 1 (cf. ejemplo Ej. 3). La recomendación se inserta en este ejemplo en el header (encabezado) (campo) "Security-Server" ("Seguridad-Servidor") (cf. el Anexo H de la especificación TS 33.203) del mensaje SIP M1, con la ayuda de un parámetro "tunnel" ("túnel") posicionado en el valor "not_required" ("no_requerido").

Por supuesto, pueden considerarse como variante otras formas de insertar esta recomendación en el mensaje SIP M1, como, por ejemplo, en otro campo del mensaje SIP M1 (tal como un campo recientemente creado para las necesidades de la invención) o en otro parámetro.

El servidor P-CSCF 3 recibe el mensaje M1 que contiene la recomendación RECO del servidor S-CSCF 4 en cuanto al establecimiento del túnel seguro con el terminal 2 (etapa F50).

Transmite (esto es, propaga) esta recomendación RECO al terminal 2 en un mensaje M2 derivado del mensaje M1 recibido del servidor S-CSCF 4 (etapa F60). El mensaje M2 es, por lo tanto, igualmente, un mensaje SIP 401 Unauthorized (No autorizado).

En el primer modo de realización descrito en este documento, el mensaje M2 contiene, además, unas informaciones que permiten el establecimiento del túnel seguro entre el terminal 2 y el servidor P-CSCF 3, independientemente del contenido de la recomendación RECO. De este modo, el servidor P-CSCF 3 asegura que, si el terminal 2 no es capaz de ejecutar la recomendación RECO, el túnel se establecerá de acuerdo con estas informaciones y la protección de los datos intercambiados entre el terminal 2 y el núcleo de red CN está, de este modo, asegurada.

Un ejemplo de un mensaje M2 que contiene la recomendación RECO del servidor S-CSCF 4 se da en Anexo 1 (cf. ejemplo Ej. 4). La recomendación se inserta en este ejemplo, en el campo "Security-Server"("Seguridad-Servidor") del mensaje SIP M2, en forma de "tunnel=not_required" ("túnel= no_requerido"), con las informaciones que permiten el establecimiento del túnel de seguridad ("ipsec-3gpp", "alg=hmac-sha1-96", etc.).

Tras recepción del mensaje M2 (etapa E20), el terminal 2 interpreta y ejecuta la recomendación RECO contenida en el mensaje M2 (etapa E30): dicho de otra manera, en este documento, no establece túnel con el servidor P-CSCF 3.

La recomendación elaborada por el servidor S-CSCF 4 permite, por lo tanto, bloquear el establecimiento del túnel inicialmente previsto por el núcleo de red CN y, de este modo, preservar los recursos del terminal 2 y del servidor P-CSCF 3.

El registro del terminal 2 respecto al núcleo de red CN se continúa, a continuación, de forma conocida de por sí.

En el primer modo de realización, la recomendación de establecer o no el túnel seguro entre el terminal 2 y su entidad de enlace al núcleo de red CN (esto es, el servidor P-CSCF 3), se elabora por el servidor S-CSCF 4.

En este momento, vamos a describir, con referencia a las figuras 5 a 7 y al anexo 2, un segundo modo de realización, en el cual esta recomendación se elabora por la propia entidad de enlace del terminal al núcleo de red, dicho de otra manera, en una arquitectura de tipo IMS, por el servidor P-CSCF asociado al terminal.

La figura 5 representa, en su entorno, un sistema 1' de comunicación conforme con la invención, en este segundo modo de realización.

El sistema 1' de comunicación comprende un terminal 2' conforme con la invención, adecuado para registrarse respecto a un núcleo CN' de red IP multimedia mediante una red de acceso AN'.

Como anteriormente para el primer modo de realización, no se adscribe ninguna limitación a la naturaleza del terminal 2' ni a la red de acceso AN' utilizada por el terminal 2' para registrarse y conectarse al núcleo de red CN'.

El terminal 2' dispone de una arquitectura material idéntica a la del terminal 2, ilustrada en la figura 2A descrita anteriormente. Su memoria muerta constituye un soporte de registro conforme con la invención, legible por el procesador del terminal 2' y sobre el cual está registrado un programa de ordenador conforme con la invención, que incluye unas instrucciones para la ejecución de las etapas de un procedimiento de registro respecto al núcleo de red CN' conforme con la invención, descritas ulteriormente con referencia a la figura 7.

El núcleo de red CN' se basa en este documento en una arquitectura IMS y comprende un servidor P-CSCF 3', punto de entrada del terminal 2' sobre el núcleo de red CN' y un servidor S-CSCF 4', encargado del registro del terminal 2' respecto al núcleo de red CN'. Como se ha descrito anteriormente para el núcleo de red CN y de conformidad con el estándar 3GPP, el núcleo de red CN' requiere el establecimiento de un túnel seguro entre el terminal 2' y la entidad de enlace de este terminal al núcleo de red, dicho de otra manera, entre el terminal 2' y el servidor P-CSCF 3' asociado a este terminal.

El servidor P-CSCF 3' dispone en este documento de la arquitectura material de un ordenador, tal como se ilustra esquemáticamente en la figura 6.

Incluye, en concreto, un procesador 3A', una memoria viva 3B', una memoria muerta 3C', una memoria flash no volátil 3D', así como unos medios de comunicación 3E' que implementan, en concreto, el protocolo SIP. Estos medios de comunicación le permiten comunicar con las entidades del núcleo de red CN' y con el terminal 2'.

La memoria muerta 3C' del servidor P-CSCF 3' constituye un soporte de registro conforme con la invención, legible por el procesador 3A' y sobre el cual está registrado un programa de ordenador conforme con la invención, que incluye unas instrucciones para la ejecución de las etapas de un procedimiento de emisión de un mensaje conforme con la invención descritas en este momento con referencia a la figura 7.

La figura 7 ilustra las principales etapas de un procedimiento de registro y de un procedimiento de emisión de un mensaje implementadas respectivamente por el terminal 2' y por el servidor P-CSCF 3' en el segundo modo de realización.

Es conveniente señalar que las etapas implementadas por el terminal 2' y representadas en la figura 7 son idénticas a las etapas implementadas por el terminal 2 y representadas en la figura 3 para el primer modo de realización. Por lo tanto, no se describirán en detalle en este documento.
Por otra parte, por razones de simplificación, en este segundo modo de realización se limita uno, a una recomendación elaborada por el servidor P-CSCF 3' únicamente en función de la red de acceso utilizada por el terminal 2' para registrarse respecto al núcleo de red CN'. No obstante, esta hipótesis no es limitativa y pueden tomarse en cuenta otros parámetros, además de la red de acceso utilizada por el terminal 2', para elaborar una recomendación, como se menciona ulteriormente en la descripción.

Se supone que el terminal 2' desea registrarse respecto al núcleo de red CN', mediante la red de acceso AN', para acceder, por ejemplo, a unos servicios multimedia gestionados por el núcleo de red CN'.

Con este fin, el terminal 2' emite, mediante sus medios de comunicaciones 2E', una petición de registro REG1' con destino al núcleo de red CN' (etapa E10'). Esta petición de registro REG1' es una petición SIP REGISTER (REGISTRO).

Un ejemplo de una petición de este tipo se da en Anexo 2 (cf. ejemplo Ej. 1). Comprende, en concreto un identificador del usuario del terminal 2' en los campos "From" ("De") y "To" ("A"), así como una información relativa a la red de acceso AN' utilizada por el terminal 2' para registrarse respecto al núcleo de red CN'. Esta información se encuentra en el campo "P-Access-Network-Info" ("Info-Red-Acceso-P") de la petición REG1'. De este modo, en el ejemplo Ej. 1 del Anexo 2, AN' es una red de acceso de tipo 3GPP-UTRAN-TDD.

La petición REG1' emitida por el terminal 2' contiene, igualmente, unas informaciones relativas al establecimiento de un túnel seguro con el servidor P-CSCF 3' del núcleo de red CN', de conformidad con el estándar 3GPP, en el campo "Security-Client" ("Seguridad-Cliente") de la petición de registro. De este modo, el túnel seguro propuesto por el terminal será de tipo IPsec para una autentificación IMS AKA y de tipo TLS para una autentificación SIP digest con TLS. Por ejemplo, en el ejemplo Ej. 1 del anexo 2, la información "ipsec-3gpp" indica que se trata del protocolo IPsec. Dichas informaciones pueden comprender, igualmente, los algoritmos de cifrado y de control de integridad considerados (en el ejemplo Ej. 1, se trata de los algoritmos conocidos "hmac-sha1-96" y "des-ede3-cbc"), los puertos sobre los cuales el túnel debe montarse, etc.

La petición de registro REG1' se recibe por el servidor P-CSCF 3' que enlaza el terminal 2' al núcleo de red CN' (etapa F10').

Tras recepción de esta petición, el servidor P-CSCF 3' identifica qué red de acceso AN' está utilizada por el terminal 2' para registrarse respecto al núcleo de red CN' (etapa F20'). Procede, con este fin, de forma idéntica al servidor P-CSCF 3 durante la etapa F20 del primer modo de realización, utilizando la dirección IP de transporte de la petición REG1' que ha recibido.

En caso necesario, sustituye, la información contenida en el campo "P-Access-Network-Info" ("Info-Red-Acceso-P") de la petición de registro REG1' recibida, por una información certificada obtenida a partir de la identificación de la red AN' deducida de la dirección IP de transporte de la petición REG1', luego, transmite la petición de registro modificada de este modo, en forma de una petición REG2', al servidor S-CSCF 4' para tratamiento.

Luego, el servidor P-CSCF3' elabora, en función de la red de acceso AN' identificada, una recomendación RECO' en cuanto al establecimiento o no del túnel seguro entre el terminal 2' (etapa F30'). Como se ha descrito anteriormente, esta recomendación traduce el carácter oportuno (es decir, útil u obligatorio) del establecimiento del túnel seguro entre el terminal 2' y el servidor P-CSCF 3', de modo que se garantice la protección y la integridad de los datos intercambiados entre el terminal 2' y el núcleo de red CN'.

Esta recomendación se elabora de forma idéntica a la recomendación RECO elaborada por el servidor S-CSCF 4 en el primer modo de realización (cf. etapa G30 descrita anteriormente), utilizando la tabla T, que está, en el segundo modo de realización, almacenada en la memoria no volátil 3D' del servidor P-CSCF 3'.

En el ejemplo ilustrado en Anexo 2, la red de acceso AN' utilizada por el terminal 2' es una red de acceso 3GPP-UTRAN-TDD. Está asociada, en la tabla T, a una recomendación de no establecer el túnel seguro entre el terminal 2' y el servidor P-CSCF 3'.

El servidor P-CSCF 3' inserta la recomendación RECO' obtenida consultando la tabla T a partir de la red de acceso AN', en un mensaje M2' que envía, entonces, al terminal 2' (etapa F40'). Este mensaje M2', en el cual el servidor P-CSCF 3' inserta la recomendación RECO', se deriva del mensaje M1' SIP 401 Unauthorized (No autorizado) de

respuesta intermedia enviado por el servidor S-CSCF 4' con destino al terminal 2' como respuesta a la petición REG2' de registro del terminal 2' y que transita, de conformidad con el protocolo SIP, por el servidor P-CSCF 3'.

Un ejemplo de un mensaje M2' de este tipo que contiene la recomendación RECO' del servidor P-CSCF 3' se da en Anexo 2 (cf. ejemplo Ej. 2). La recomendación se inserta en este ejemplo en un campo "Security-Server" ("Seguridad-Servidor") del mensaje SIP M2', en un parámetro "tunnel" ("túnel") posicionado en el valor "not_required" ("no_requerido").

En el segundo modo de realización descrito en este documento, el mensaje M2' contiene, además, unas informaciones que permiten el establecimiento del túnel seguro entre el terminal 2' y el servidor P-CSCF 3', independientemente del contenido de la recomendación RECO'. De este modo, el servidor P-CSCF 3' asegura que, si el terminal 2' no es capaz de ejecutar la recomendación RECO', el túnel se establecerá de acuerdo con estas informaciones y la protección de los datos intercambiados entre el terminal 2' y el núcleo de red CN' está, de este modo, asegurada.

Tras recepción del mensaje M2' (etapa E20'), el terminal 2' interpreta y ejecuta la recomendación RECO' contenida en el mensaje M2' (etapa E30'): dicho de otra manera, en el ejemplo considerado, no establece túnel con el servidor P-CSCF 3'. El registro del terminal 2' respecto al núcleo de red CN' se continúa, a continuación, de forma conocida de por sí.

En los dos modos de realización descritos en este documento, los servidores S-CSCF 4 y P-CSCF 3' utilizan para elaborar su recomendación, una tabla T preestablecida que asocia a diversas redes de acceso, una recomendación en cuanto al establecimiento o no de un túnel seguro entre el terminal y el servidor P-CSCF que enlaza el terminal al núcleo de red. Como se ha mencionado anteriormente, esta tabla T toma en cuentea implícitamente los niveles de seguridad asociados por el núcleo de red a las diferentes redes de acceso.

Como variante, se pueden considerar otras maneras de tomar en cuenta las redes de acceso y sus niveles de seguridad para elaborar la recomendación.

De este modo, por ejemplo, la recomendación puede elaborarse tras recepción de la petición de registro del terminal comparando dinámicamente unas características y/o el tipo de la red de acceso utilizada por el terminal con respecto a unos criterios de seguridad predeterminados, de modo que se asocie en un primer momento a la red de acceso un nivel de seguridad de los datos, luego que se determine si el nivel de seguridad asegurado por la red de acceso es suficiente para relajar la restricción de establecimiento del túnel seguro entre el terminal y la entidad de enlace.

Por otra parte, en los dos modos de realización descritos en este documento, en la tabla T, solo se toma en cuenta en definitiva el tipo estrictamente hablando de la red de acceso utilizada por el terminal para registrarse respecto al núcleo de red. Como variante, se puede considerar tomar en cuenta otras características de la red de acceso, como, por ejemplo, el operador de la red de acceso utilizada por el terminal (en concreto, para determinar si se trata del mismo operador que el del núcleo de red o de un operador de confianza) u otras informaciones relativas a la red de acceso como, por ejemplo, si la red utilizada por el terminal es su red nominal o una red visitada o si la red visitada y utilizada por el terminal es la red del servidor que elabora la recomendación u otra red, etc.

De este modo, a título de ejemplo, se puede decidir elaborar una recomendación de establecer un túnel seguro si la red visitada utilizada por el terminal está asociada por el núcleo de red a un nivel de seguridad escaso y, de manera inversa, una recomendación de no establecer túnel seguro si la red visitada está asociada por el núcleo de red a un nivel de seguridad fuerte.

Estas características o informaciones pueden deducirse por el servidor de la petición de registro del terminal o de la señalización asociada a esta petición, por ejemplo, a partir del campo P-Visited-Network-Id (Id-Red-Visitada-P) descrito en el documento RFC 3455 editado por la IETF.

Además, en otro modo de realización, se puede considerar, igualmente, tomar en cuenta para elaborar la recomendación, además de la red de acceso utilizada por el terminal, otros factores "discriminatorios" que tienen una influencia sobre el nivel de seguridad asegurado por la red de acceso, tales como, por ejemplo, la localización del terminal, su usuario, etc. Con este fin, se pueden utilizar algunos parámetros contenidos en unos campos de la petición de registro del terminal o recibidos con la petición de registro, en concreto, en la señalización asociada a esta petición, como, por ejemplo, la dirección IP del terminal, la dirección IP de transporte de la petición de registro, el identificador del usuario del terminal o también los algoritmos de cifrado solicitados en la petición de registro por el terminal (en el campo Security Client) (Seguridad Cliente) y notificar a la tabla T, de modo que traduzca diferentes recomendaciones que se refieren al establecimiento del túnel seguro en función de estos parámetros igualmente.

De este modo, por ejemplo, para una red de acceso WIFI pública, se puede considerar tener una recomendación "Not required" ("No requerido") para un primer rango de direcciones IP de transporte de la petición y una recomendación "Required" ("Requerido") para un segundo rango de direcciones IP.

De forma similar, para una red de acceso de tipo 3GPP, se puede considerar tener una recomendación "Not required" ("No requerido) para el conjunto de los usuarios de los terminales que pretenden registrarse respecto al núcleo de red, con la excepción de algunos usuarios para los cuales se elaborará una recomendación "Required" ("Requerido"). Estos usuarios pueden estar identificados por el servidor según la invención, por ejemplo, consultando su perfil de usuario almacenado al nivel del servidor HSS (Home Subscriber Server) del núcleo de red y en el cual se habrá inscrito una indicación apropiada. En paralelo, podrá integrarse una indicación en la tabla T que especifique la existencia de unos usuarios de este tipo para la cual debe ponderarse la recomendación establecida en función del tipo de red de acceso en función del identificador del usuario del terminal.

Se señalará que en, la descripción de más arriba, se ha priorizado la red de acceso utilizada por el terminal como criterio principal para elaborar la recomendación de establecer o no el túnel seguro y considerar eventualmente a título complementario otros parámetros tales como la identidad del usuario del terminal que pretende registrarse. No obstante, es posible invertir este orden de prelación, incluso considerar solo uno de estos parámetros como único criterio para elaborar la recomendación de establecer o no el túnel seguro.

ANEXO 1

| Ej. 1: petición de registro REG1 del terminal 2 recibida por el servidor P-CSCF 3 |
|---|
| REGISTRO sip: home.com SIP/2.0<br>Mediante: SIP/2.0/UDP....<br>Info-Red-Acceso-P: 3gpp-utran-TDD; utran-cell-id-3gpp=<br>De: <sip: bob@home.com>; etiqueta=1234<br>A: <sip: bob@home.com><br>Contacto: <sip: AoC_bob>; Expira=3600<br>Llamada-ID: 5678<br>Autorización: Digest nombre de usuario="bob private@home.com", realm="home.com", hápax="", uri="sip:home.com", respuesta=""<br>Seguridad-Cliente: ipsec-3gpp; alg=hmac-sha1-96; ealg=des-ede3-cbc; spi-c=2482; spi-s=2483; puerto-c=32045; puerto-s=40375<br>Requerir: seg-acuerdo<br>Proxy-Requerir: seg-acuerdo<br>Csec: 1 REGISTRO<br>Contenido-Longitud: 0 |

| Ej. 2: petición de registro REG2 del terminal 2 transmitida por el servidor P-CSCF 3 y recibida por el servidor S-CSCF 4 |
|---|
| REGISTRO sip: home.com SIP/2.0<br>Mediante: SIP/2.0/UDP P-CSCF....<br>Mediante: SIP/2.0/UDP....<br>Info-Red-Acceso-P: 3gpp-utran-TDD; utran-cell-id-3gpp=<br>De: <sip: bob@home.com>; etiqueta=1234<br>A: <sip: bob@home.com><br>Contacto: <sip: AoC_bob>; expira=3600 Llamada-ID: 5678<br>Autorización: Digest nombre de usuario="bob private@home.com", realm="home.com", hápax="", uri="sip:home.com", respuesta=""<br>Requerir: seg-acuerdo<br>Proxy-Requerir: seg-acuerdo<br>Csec: 1 REGISTRO<br><br>…<br>Contenido-Longitud: 0 |

| Ej. 3: mensaje M1 emitido por el servidor S-CSCF 4 que contiene una recomendación |
|---|
| SIP/2.0 401 No autorizado<br>Mediante: SIP/2.0/UDP P-CSCF....<br><br>Mediante: SIP/2.0/UDP....<br>De: <sip: bob@home.com>; etiqueta=1234<br>A: <sip: bob@home.com>; etiqueta=rem_9876<br>Llamada-ID: 5678<br>WWW-Autentificar: Digest realm="home.com", hápax="V4pj+BE4T3J/ CmetlDNW9p6hNnAQR0IDQeVyt5NQvhE=", algoritmo=AKAv1-MD5<br>Seguridad-Servidor: túnel=no_requerido<br>Csec: 1 REGISTRO<br>Contenido-Longitud: 0 |

Ej. 4: mensaje M2 transmitido al terminal 2 por el servidor P-CSCF 3 que contiene la recomendación del servidor S-CSCF 4
SIP/2.0 401 No autorizado
Mediante: SIP/2.0/UDP....
De: <sip: bob@home.com>; etiqueta=1234
A: <sip: bob@home.com>; etiqueta=rem_9876
Llamada-ID: 5678
WWW-Autentificar: Digest realm="home.com", hápax="V4pj+BE4T3J/CmetlDNW9p6hNnAQR0IDQeVyt5NQvhE=", algoritmo=AKAv1-MD5
Seguridad-Servidor: ipsec-3gpp; q=0,5; alg=hmac-sha1-96; ealg=des-ede3-cbc; spi-c=5142; spi-s=5143; puerto-c=6045; puerto-s=6044; túnel=no_requerido
Csec: 1 REGISTRO
Contenido-Longitud: 0

ANEXO 2

Ej. 1: petición de registro REG1' del terminal 2' recibida por el servidor P-CSCF 3'
REGISTRO sip:home.com SIP/2.0
Mediante: SIP/2.0/UDP....
Info-Red-Acceso-P: 3gpp-utran-TDD; utran-cell-id-3gpp=…..
De: <sip: bob@home.com>; etiqueta=1234
A: <sip: bob@home.com>
Contacto: <sip: AoC_bob>; Expira=3600
Llamada-ID: 5678
Autorización: Digest nombre de usuario="bob private@home.com", realm="home.com", hápax="",uri="sip:home.com", respuesta=""
Seguridad-Cliente: ipsec-3gpp; alg=hmac-sha1-96; ealg=des-ede3-cbc; spi-c=2482; spi-s=2483; puerto-c=32045; puerto-s=40375
Requerir: seg-acuerdo
Proxy-Requerir: seg-acuerdo
Csec: 1 REGISTRO
Contenido-Longitud: 0

Ej. 2: mensaje M2' emitido por el servidor P-CSCF 3' hacia el terminal 2' que contiene una recomendación
SIP/2.0 401 No autorizado
Mediante: SIP/2.0/UDP....
De: <sip: bob@home.com>; etiqueta=1234
A: <sip: bob@home.com>; etiqueta=rem_9876
Llamada-ID: 5678
WWW-Autentificar: Digest realm="home.com", hápax="V4pj+BE4T3J/CmetlDNW9p6hNnAQR0IDQeVyt5NQvhE=", algoritmo=AKAv1-MD5
Seguridad-Servidor: ipsec-3gpp; q=0,5; alg=hmac-sha1-96; ealg=des-ede3-cbc; spi-c=5142; spi-s=5143; puerto-c=6045; puerto-s=6044; túnel=no_requerido
Csec: 1 REGISTRO
Contenido-Longitud: 0

**REIVINDICACIONES**

1. Procedimiento de emisión de un mensaje (M1, M1') por un servidor (4, 3') de un núcleo de red IP multimedia (CN, CN') como continuación a la recepción (G10, F10') por dicho servidor de una petición de registro (REG2, REG1') de un terminal (2, 2') respecto al núcleo de red, proponiendo dicha petición de registro un método de autentificación que prevé el establecimiento de un túnel seguro entre el terminal y una entidad de enlace (3, 3') de este terminal al núcleo de red, comprendiendo dicho procedimiento de emisión:
- una etapa de identificación (G20, F20') de una red de acceso (AN, AN') utilizada por el terminal para registrarse respecto al núcleo de red IP multimedia;
- una etapa de elaboración (G30, F30'), en función de la red de acceso identificada, de una recomendación (RECO, RECO') en cuanto al establecimiento o no del túnel seguro entre el terminal y la entidad de enlace para dicho método de autentificación; y
- una etapa de inserción (G40, F40') de esta recomendación en el mensaje emitido por el servidor.

2. Procedimiento según la reivindicación 1 en el que la recomendación (RECO, RECO') se elabora por el servidor tomando en cuenta un nivel de seguridad de los datos asociado por el núcleo de red a la red de acceso.

3. Procedimiento según la reivindicación 1 en el que:
- el núcleo de red IP (CN) multimedia emplea una arquitectura IMS;
- el servidor del núcleo de red IP multimedia es un servidor S-CSCF (4); y
- el mensaje (M1) en el que se inserta la recomendación (RECO) se emite por el servidor S-CSCF con destino al terminal mediante un servidor P-CSCF (3) que enlaza el terminal (2) al núcleo de red IP multimedia.

4. Procedimiento según la reivindicación 1 en el que:
- el núcleo de red IP (CN') multimedia emplea una arquitectura IMS;
- el servidor del núcleo de red IP multimedia es un servidor P-CSCF (3'); y
- el mensaje (M1') en el que se inserta la recomendación (RECO') se emite hacia el terminal (2).

5. Procedimiento según la reivindicación 1 en el que el mensaje emitido (M1, M1') está conforme con el protocolo SIP y la recomendación se inserta en un campo "Security Server" ("Servidor de Seguridad") de este mensaje.

6. Procedimiento según la reivindicación 1 en el que la recomendación se elabora en función, igualmente, de al menos un parámetro recibido con la petición de registro.

7. Procedimiento según la reivindicación 6 en el que dicho al menos un parámetro comprende una dirección IP de transporte de la petición de registro o un identificador asociado a un usuario del terminal.

8. Procedimiento según la reivindicación 1 en el que el mensaje (M1') emitido por el servidor contiene, además, unas informaciones que permiten el establecimiento del túnel seguro entre el terminal y la entidad de enlace de este terminal al núcleo de red IP multimedia.

9. Procedimiento según la reivindicación 1 en el que la recomendación insertada en el mensaje comprende una de las siguientes indicaciones:
- una indicación de no establecer el túnel seguro entre el terminal y la entidad de enlace;
- una indicación de libre elección en cuanto al establecimiento del túnel seguro entre el terminal y la entidad de enlace;
- una indicación de establecer el túnel seguro entre el terminal y la entidad de enlace.

10. Procedimiento de registro de un terminal (2, 2') respecto a un núcleo de red IP (CN, CN'), comprendiendo dicho procedimiento:
- una etapa de emisión (E10, E10), por el terminal, de una petición de registro (REG1, REG1') respecto al núcleo de red, mediante una red de acceso, proponiendo dicha petición de registro un método de autentificación que prevé el establecimiento de un túnel seguro entre el terminal y una entidad de enlace (3, 3') de este terminal al núcleo de red;
- una etapa de recepción (E20, E20'), por el terminal, con procedencia del núcleo de red, de una recomendación (RECO, RECO') en cuanto al establecimiento o no del túnel seguro entre el terminal y la entidad de enlace para dicho método de autentificación, proviniendo esta recomendación de un mensaje (M1, M1') emitido por un servidor (4, 3') del núcleo de red de conformidad con un procedimiento de emisión según la reivindicación 1, ejecutado como continuación a la recepción de la petición de registro del terminal; y
- una etapa de interpretación (E30, E30') de esta recomendación por el terminal.

11. Procedimiento de transmisión destinado a implementarse por una entidad de enlace (3, 3') de un terminal (2, 2') a un núcleo de red IP multimedia (CN, CN'), comprendiendo dicho procedimiento de transmisión:
- una etapa de recepción (F10) de una petición de registro del terminal respecto al núcleo de red, mediante una red de acceso, proponiendo dicha petición de registro un método de autentificación que prevé el establecimiento de un túnel seguro entre dicho terminal y dicha entidad de enlace;

- una etapa de transmisión (F40) de esta petición de registro a un servidor (4, 3') del núcleo de red;
- una etapa de recepción (F50), con procedencia del servidor, de un mensaje que contiene una recomendación en cuanto al establecimiento o no del túnel seguro entre el terminal y la entidad de enlace para dicho método de autentificación, resultando el mensaje de la ejecución por el servidor de un procedimiento de emisión de un mensaje según la reivindicación 1; y
- una etapa de transmisión (F60) de esta recomendación al terminal.

12. Programa de ordenador que incluye unas instrucciones para la ejecución de las etapas del procedimiento de emisión según la reivindicación 1 o del procedimiento de registro según la reivindicación 10 o del procedimiento de transmisión según la reivindicación 11, cuando dicho programa se ejecuta por un ordenador.

13. Soporte de informaciones legible por un ordenador y que incluye unas instrucciones de un programa de ordenador según la reivindicación 12.

14. Servidor (4, 3') de un núcleo de red IP multimedia (CN, CN'), comprendiendo dicho servidor unos medios activados como continuación a la recepción por el servidor de una petición de registro (REG2, REG1') de un terminal (2, 2') respecto al núcleo de red, proponiendo dicha petición de registro un método de autentificación que prevé el establecimiento de un túnel seguro entre el terminal y una entidad de enlace (3, 3') de este terminal al núcleo de red, comprendiendo dichos medios:
- unos medios de identificación de una red de acceso (AN, AN') utilizada por el terminal para registrarse respecto al núcleo de red;
- unos medios de elaboración (T), en función de la red de acceso identificada, de una recomendación en cuanto al establecimiento o no del túnel seguro entre el terminal y la entidad de enlace para dicho método de autentificación;
- unos medios de inserción de esta recomendación en un mensaje (M1, M1'); y
- unos medios de emisión (4E, 3E') del mensaje.

15. Terminal (2, 2') que comprende:
- unos medios de emisión (2E, 2E') de una petición de registro (REG1, REG1') respecto a un núcleo de red IP multimedia (CN, CN') mediante una red de acceso (AN, AN'), proponiendo dicha petición de registro un método de autentificación que prevé el establecimiento de un túnel seguro entre el terminal y una entidad de enlace (3, 3') de este terminal al núcleo de red;
- unos medios de recepción (2E, 2E'), con procedencia del núcleo de red, de una recomendación (RECO, RECO') en cuanto al establecimiento o no del túnel seguro entre el terminal y la entidad de enlace para dicho método de autentificación, proviniendo esta recomendación de un mensaje (M1, M1) emitido por un servidor (4, 3') del núcleo de red conforme con la reivindicación 14, como continuación a la recepción de la petición de registro; y
- unos medios de interpretación (2A, 2A') de esta recomendación.

16. Entidad de enlace (3) de un terminal (2) a un núcleo de red IP multimedia (CN), comprendiendo dicha entidad de enlace:
- unos medios de recepción (3E) de una petición de registro (REG1) respecto al núcleo de red, mediante una red de acceso (AN), proponiendo dicha petición de registro un método de autentificación que prevé el establecimiento de un túnel seguro entre dicho terminal y dicha entidad de enlace;
- unos medios de transmisión (3E) de dicha petición de registro (REG2) a un servidor (4) conforme con la reivindicación 14;
- unos medios de recepción (3E), con procedencia del servidor, de un mensaje que contiene una recomendación (RECO) en cuanto al establecimiento o no del túnel seguro entre el terminal y la entidad de enlace para dicho método de autentificación; y
- unos medios de transmisión (3E) de esta recomendación a dicho terminal.

17. Sistema de comunicación (1, 1') que comprende:
- un servidor (4, 3') de un núcleo de red IP multimedia (CN, CN') conforme con la reivindicación 14;
- un terminal (2, 2') según la reivindicación 15 adecuado para registrarse respecto al núcleo de red multimedia enviando una petición de registro (REG1, REG1') a dicho núcleo de red mediante una red de acceso (AN, AN'); y
- una entidad de enlace (3) del terminal al núcleo de red IP multimedia;

siendo dicho terminal adecuado para ejecutar una recomendación elaborada por el servidor en cuanto al establecimiento o no de un túnel seguro entre el terminal y la entidad de enlace del terminal al núcleo de red.

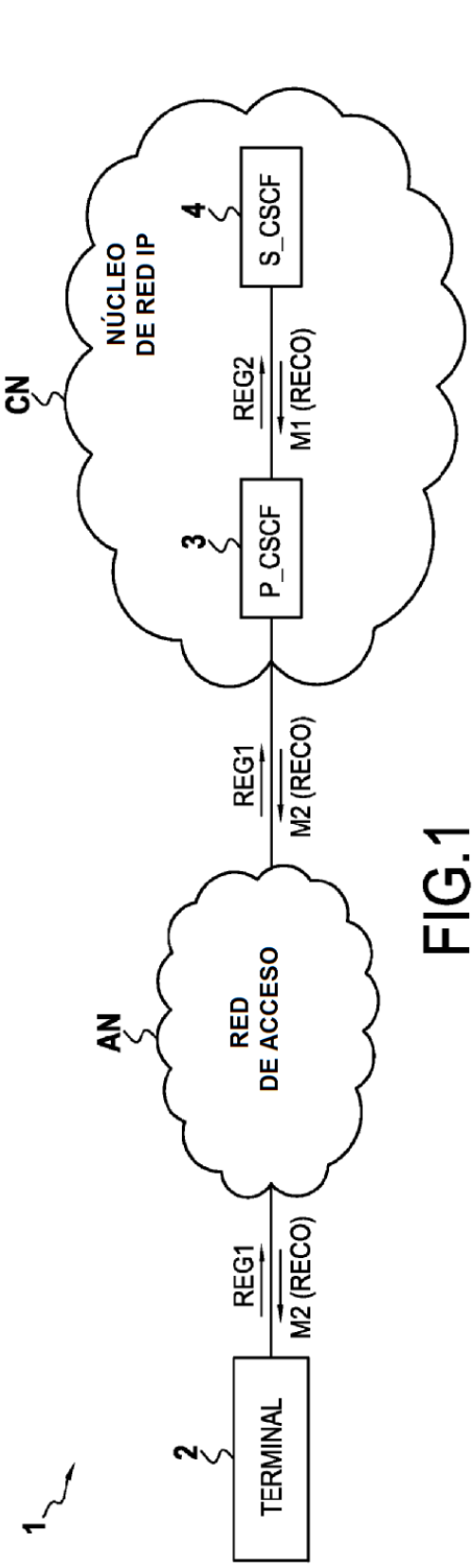


FIG.1

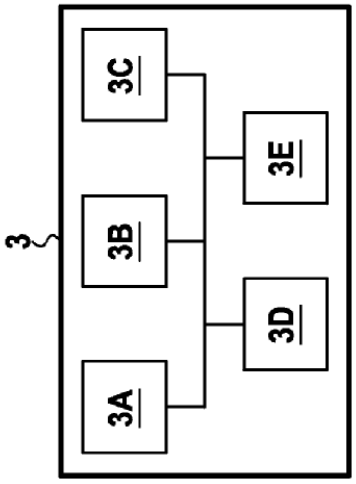


FIG.2C

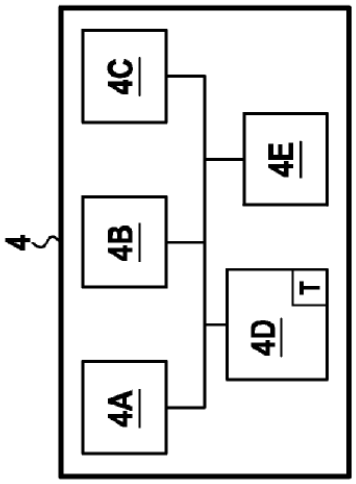


FIG.2B

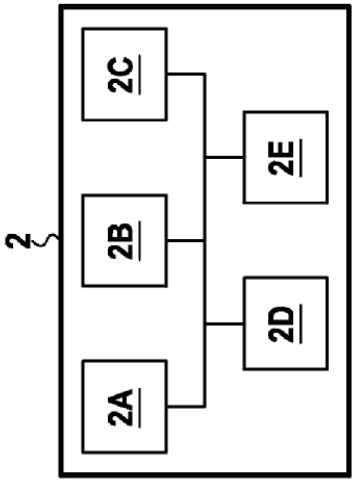


FIG.2A

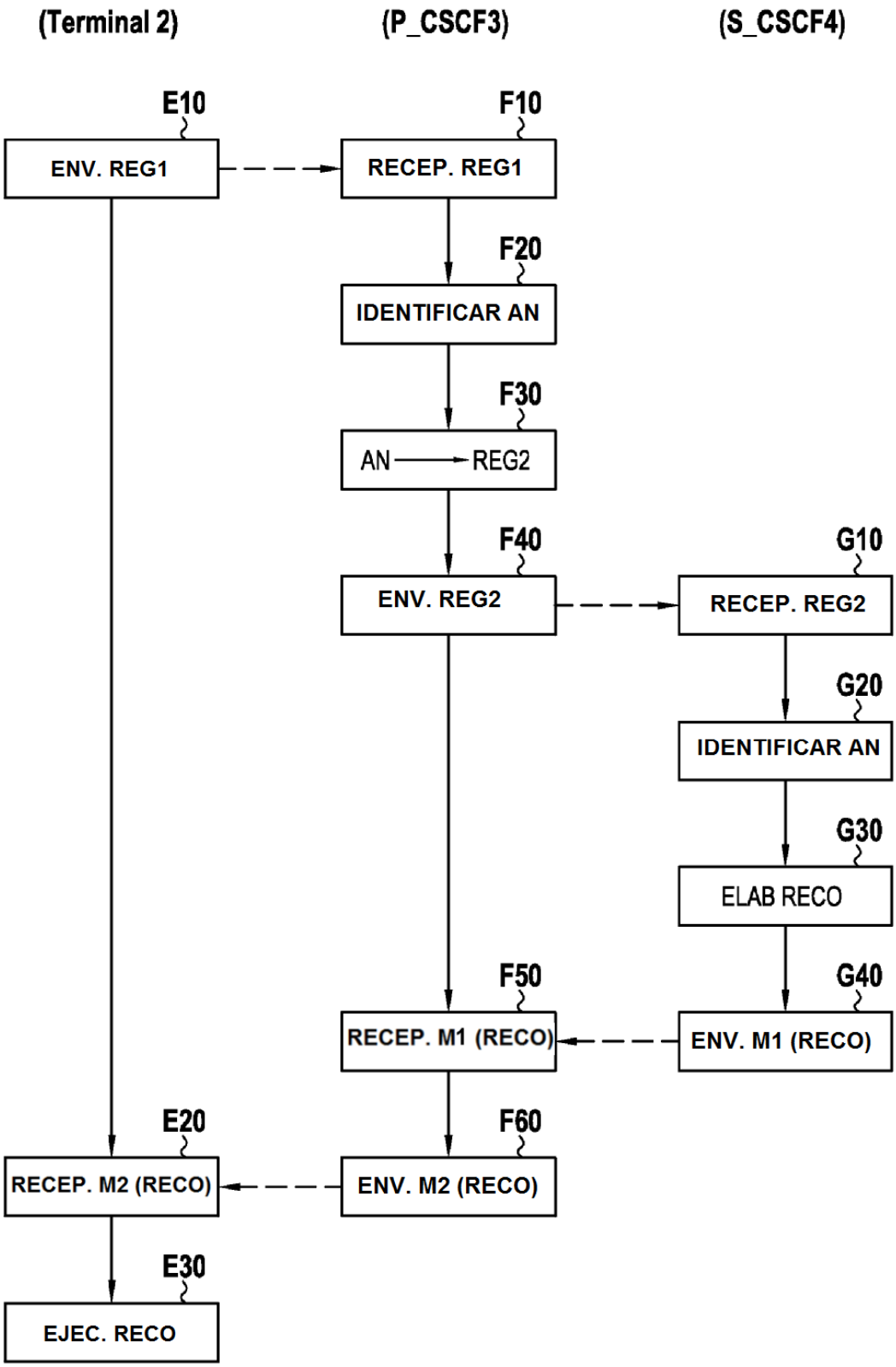
(Terminal 2)
(P_CSCF3)
(S_CSCF4)
E10
ENV. REG1
F10
RECEP. REG1
F20
IDENTIFICAR AN
F30
AN
REG2
F40
ENV. REG2
G10
RECEP. REG2
G20
IDENTIFICAR AN
G30
ELAB RECO
G40
ENV. M1 (RECO)
F50
RECEP. M1 (RECO)
F60
ENV. M2 (RECO)
E20
RECEP. M2 (RECO)
E30
EJEC. RECO

FIG.3

| RED DE ACCESO | RECO / TÚNEL |
|---|---|
| 3GPP_UTRAN_TDD | NO REQUERIDO |
| 3GPP_UTRAN_FDD | NO REQUERIDO |
| WIFI PÚBLICO | REQUERIDO |
| ⋮ | ⋮ |

T

FIG.4

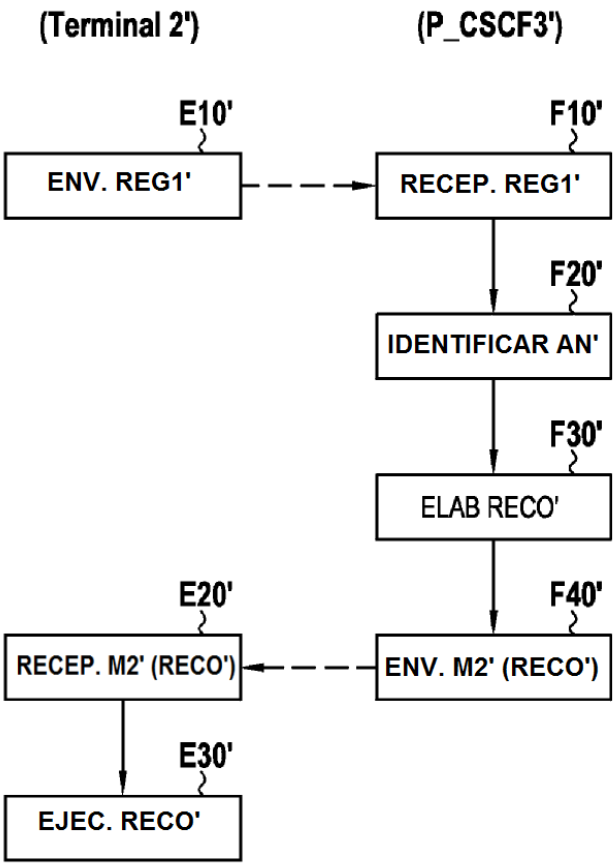


FIG.7

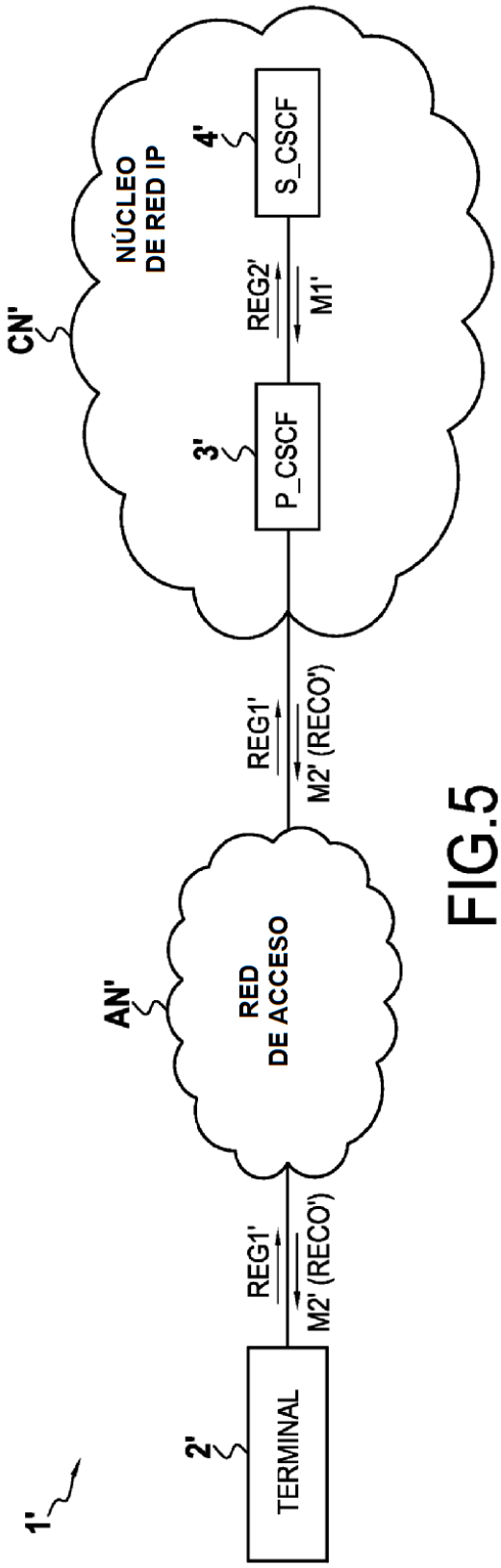
1'
2'
TERMINAL
REG1'
M2' (RECO')
AN'
RED
DE ACCESO
REG1'
M2' (RECO')
CN'
NÚCLEO
DE RED IP
3'
P_CSCF
REG2'
M1'
4'
S_CSCF

FIG.5

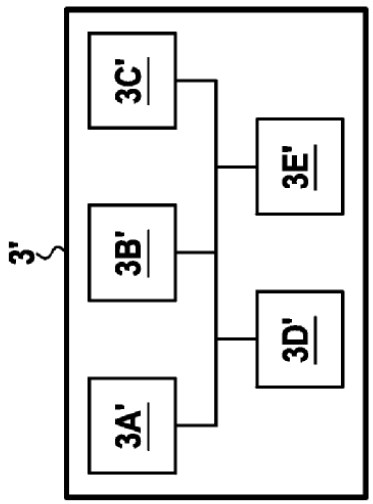
3'
3A'
3B'
3C'
3D'
3E'

FIG.6