(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 445 647**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04M 1/725 (2006.01)
H04W 12/06 (2009.01)
H04W 76/00 (2009.01)
H04W 76/02 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **05.02.2008 E 08708686 (4)**

(97) Fecha y número de publicación de la concesión europea: **11.12.2013 EP 2122983**

(54) Título: **Soporte de llamadas sin UICC**

(30) Prioridad:

06.02.2007 US 899643 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
04.03.2014

(73) Titular/es:

NOKIA CORPORATION (100.0%)
KEILALAHDENTIE 4
02150 ESPOO, FI

(72) Inventor/es:

ZHANG, DAJIANG;
LI, CHANGHONG y
ERONEN, PASI

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Soporte de llamadas sin UICC

Antecedentes de la invención

Campo de la invención

La invención se refiere a un método y dispositivo para soportar llamadas tales como llamadas de emergencia de IMS) a partir de un terminal de abonado que no tiene módulo de identidad de abonado (sin UICC) en la red de acceso I-WLAN.

Descripción de la técnica relacionada

El crecimiento de las WLAN públicas proporciona una oportunidad para que los dispositivos terminales (o equipos de usuario (UE) en la terminología de tercera generación) equipados de forma apropiada accedan a las redes domésticas celulares y redes visitadas a través de tales WLAN. Por lo tanto, se hace referencia a las WLAN que proporcionan tal funcionalidad de interfuncionamiento como I-WLAN. Las I-WLAN están conectadas a redes móviles terrestres públicas (PLMN, *public land mobile network*) que permiten a las UE el acceso a servicios de red en redes domésticas (HPLMN) y redes visitadas (VPLMN).

Los dispositivos inalámbricos estarán obligados por ley a soportar las llamadas de emergencia. La notificación de una emergencia debería ser posible incluso cuando no esté actualmente activa sesión alguna sobre un canal radioeléctrico particular de un dispositivo de acceso múltiple, es decir el usuario actualmente no está conectado a radio alguna, o un módulo de identidad de abonado (SIM, *subscriber identity module*) o SIM de sistema de telecomunicaciones móviles universales (USIM) no está insertado actualmente en el dispositivo.

Habitualmente, las notificaciones de emergencia iniciadas al tirar de un interruptor o al llamar a un número de emergencia generalmente se tratan de una manera priorizada, de tal modo que el acceso está fácilmente disponible para invocar la alarma de emergencia. No obstante, los dispositivos inalámbricos pueden no tener funciones fiables o no usarse de manera fiable durante una emergencia, de tal modo que la introducción de contraseñas u otros procesos de autenticación no se pueden hacer correctamente. Además, un dispositivo inalámbrico puede estar cerca de una red o red de acceso pero no asociado a esa red. Por lo tanto, no se necesita autorización antes de que suene la alarma o de que se realice el contacto con el centro de emergencia con el fin de agilizar la llamada de Emergencia.

El acceso a I-WLAN (*interactive wireless local area network*, red de área local inalámbrica interactiva) se define en las especificaciones TS 23.234, 33.234, 24.234 y 29.234 del proyecto de asociación de tercera generación (3GPP, *3rd generation partnership project*). Para el acceso a IP directo (así denominado escenario 2) y el acceso a IP de 3GPP (así denominado escenario 3), se usa un procedimiento de SIM / AKA (*Authentication and Key Agreement*, Autenticación y Acuerdo de Clave) de Protocolo de Autenticación Extensible (EAP, *Extensible Authentication Protocol*) para la autenticación, en el que la autorización se efectúa basándose en una comprobación de abonado contra la información contenida en una base de datos de abonado, por ejemplo, un servidor de abonado doméstico (HSS, *Home Subscriber Server*).

El Identificador de red de W-APN para el soporte de las llamadas de Emergencia de IMS adoptará la forma de un Identificador de red reservada, común de la forma “sos”, por ejemplo “sos.wap-n. mnc012.mcc345.pub.3gppnetwork.org”, tal como se define en la norma TS23.003.

Este tipo de W-APN indica a una red de acceso de WLAN o a un Servidor de AAA de 3GPP que se necesita el acceso para una llamada de emergencia u otra llamada priorizada.

En la actualidad, aún no hay solución aceptada en 3GPP para qué tipo de método de autenticación e ID de usuario se usará para que los usuarios sin UICC (usuarios sin una tarjeta de circuito integrado universal) accedan a I-WLAN para la emergencia de IMS.

Es posible usar un nombre de usuario común y contraseña común para todos los usuarios en I-WLAN para llamada de emergencia de IMS sin UICC.

En el documento temporal S2-051950 de la Arquitectura de WG2 de SA de TSG de 3GPP, 5-9 septiembre de 2005, se describe un soporte de llamada de emergencia de Protocolo de Voz sobre Internet (VoIP, *Voice over Internet Protocol*), en el que las llamadas de emergencia de VoIP están soportadas a través de una WLAN mediante el uso de una pseudo-IMSI (Identidad de Abonado Móvil Internacional, *International Mobile Subscriber Identity*) para facilitar el acceso de WLAN. La pseudo-IMSI se puede usar entonces para crear un pseudo-identificador de acceso a la red (NAI, *Network Access Identifier*) específico de usuario para usarse para el acceso inicial y el procedimiento de autenticación. La pseudo-IMSI está constituida por una combinación única de código de país móvil (MCC, *Mobile*

Country Code) y código de red móvil (MNC, *Mobile Network Code*) y dígitos a partir de la identidad de equipo móvil internacional (IMEI, *International Mobile Equipment Identity*). Las VPLMN anunciadas por la WLAN o bien podrían ser todas capaces de soportar la autenticación usando la pseudo-NAI para los servicios de emergencia o bien podrían ser presentadas a una UE en un orden priorizado que indica capacidad y buena disposición para soportar esto. La VPLMN trataría entonces al UE como un abonado doméstico temporal y o bien pasaría por alto la autenticación y la autorización (AAA, *Authentication and Authorization*) o bien aseguraría que esta tuviera éxito.

No obstante, también en este caso, no puede continuarse la sesión.

En la norma TS 23.234 actual, el requisito para soportar llamadas de emergencia de IMS ha de proporcionar a las UE de WLAN una capacidad de portador de IP para acceder a las llamadas de Emergencia de IMS para los casos tanto de UICC como sin UICC. Además, la autenticación puede (i) pasarse por alto en su totalidad o (ii) usar un método de autenticación nulo o ficticio.

Por lo tanto, en la actualidad, no se especifica mecanismo fiable alguno para las llamadas de Emergencia de IMS del usuario sin UICC a través de I-WLAN, y no hay definición alguna de la ID del usuario que ha de usarse para el usuario sin UICC, lo que es necesario para formar el NAI (junto con la W-APN).

El documento WO 2005/112488A2 divulga un método para soportar llamadas de emergencia sobre una red de área local inalámbrica. Este documento D1 describe, en particular, un identificador para identificar una llamada como una llamada de emergencia, en el que también se incluye información adicional tal como la ubicación.

Sumario de la invención

Por lo tanto, es un objetivo de la presente invención solucionar el problema que se ha mencionado en lo que antecede y proporcionar un mecanismo fiable para la gestión de llamadas tales como llamadas de emergencia de IMS provenientes de un usuario sin UICC en un sistema de I-WLAN.

Este objetivo se consigue por un método tal como se expone en la reivindicación 1 o por un método tal como se expone en la reivindicación 4 o, como alternativa, por un aparato tal como se expone en la reivindicación 9 o por un aparato tal como se expone en la reivindicación 13.

Por lo tanto, de acuerdo con las reivindicaciones, la autenticación de EAP / TPS se realiza por un procedimiento (método o protocolo de autenticación) que no realiza una autenticación de cliente, sino que realiza una autenticación de servidor.

De este modo, las llamadas de emergencia provenientes de terminales de abonado sin UICC se pueden gestionar de manera fiable.

Breve descripción de los dibujos

La invención se describe haciendo referencia a los dibujos adjuntos, en los que:

la figura 1 muestra un diagrama de señalización de mensajes de acuerdo con una primera realización de la invención, y

las figuras 2A a 2D son configuraciones básicas de elementos de red implicados en las realizaciones de la presente invención.

Descripción detallada de la realización preferida

En lo siguiente, se describen realizaciones preferidas de la presente invención haciendo referencia a los dibujos adjuntos.

De acuerdo con la presente realización, se propone usar un protocolo de autenticación extensible - seguridad de capa de transporte (EAP-TLS) como un método de autenticación en I-WLAN para usuarios sin UICC en el caso de una emergencia de IMS. En concreto, EAP-TLS puede pasar por alto la autenticación de cliente. No obstante, todavía se proporciona la autenticación de servidor. Esto quiere decir que aún es posible conseguir claves para continuar y cifrar al usuario si se necesita. De esta manera, no se requiere cambio alguno en la AN de WLAN.

En la figura 1 se muestra una secuencia de señalización detallada para una llamada de emergencia de un usuario sin UICC. Se observa que solo se muestran los elementos de red principales en esta secuencia, en concreto una entidad de usuario (UE, *user entity*), una red de acceso (AN, *Access Network*) de WLAN, que puede ser un solo elemento de red o elementos distribuidos, una pasarela de acceso de datos por paquetes (PDG, *packet data gateway*) y un servidor de autorización y contabilidad (AAA, *authorization and accounting*).

En la etapa 1, se establece una conexión entre la entidad de usuario (UE) de WLAN y la red de acceso (AN) de WLAN, usando un procedimiento específico de la tecnología de LAN Inalámbrica.

En la etapa 2, la AN de WLAN envía una Solicitud de EAP / Identidad para el UE de WLAN. Se observa que los paquetes de EAP se transportan a través de la interfaz de LAN Inalámbrica con encapsulado dentro de un protocolo específico de la tecnología de LAN Inalámbrica.

En la etapa 3, la UE de WLAN envía un mensaje de Respuesta de EAP / Identidad. La UE de WLAN envía una identidad de usuario, cumpliendo con el formato del identificador de acceso a la red (NAI) especificado en la norma 23.003 de 3GPP. La parte de dominio del NAI en la identidad de usuario está poblada con el dominio específico de emergencia. Es decir, tal como se ha mencionado en lo que antecede, el dominio puede comprender “sos”, por ejemplo. La identidad de la UE de WLAN sin UICC puede ser IMEI, dirección de MAC o dirección de IP local asignada por AN de WLAN (como un ejemplo, para un elemento de red de acceso) junto con una información de AN de WLAN, tal como se describirá en lo siguiente con más detalle.

En la etapa 4, el mensaje se encamina hacia el servidor de autenticación, autorización y contabilidad (AAA, *authentication, authorization and accounting*) de 3GPP correcto basándose en la parte de dominio del NAI. La trayectoria de encaminamiento puede incluir uno o varios apoderados de AAA (que no se muestran en la figura).

Se observa que también se puede aplicar una referencia de diámetro para encontrar el servidor de AAA.

En la etapa 5, el Servidor de AAA de 3GPP recibe el paquete de Respuesta de EAP / Identidad que contiene la identidad del terminal. Con la parte de dominio del NAI en la identidad de usuario poblada con el dominio específico de emergencia tal como se define en la norma TS 23.003 de 3GPP, el Servidor de AAA de 3GPP identifica que el usuario está solicitando una llamada de emergencia, basándose en la identidad recibida. El Servidor de AAA de 3GPP establecerá un indicador de Acceso de Emergencia (*Emergency_Access*).

El identificador de la red radioeléctrica de WLAN y la dirección de MAC de la UE de WLAN también se recibirán por el Servidor de AAA de 3GPP en el mismo mensaje.

En la etapa 6, el Servidor de AAA de 3GPP inicia la autenticación usando EAP-TLS, en la que se omite la autenticación de cliente. Es decir, no se comprueba la identidad de abonado como tal (es decir, como sería en el caso de un abonado con una UICC).

En la etapa 7, la AN de WLAN reenvía la Solicitud de EAP / TLS al UE de WLAN.

En la etapa 8, la UE de WLAN responde con la Respuesta de EAP / TLS.

En la etapa 9, la AN de WLAN reenvía la Respuesta de EAP / TLS al Servidor de AAA de 3GPP.

En la etapa 10, se obtiene una clave de sesión maestra (MSK, *Master Session Key*) a partir del secreto maestro de TLS, véase el documento RFC 4346.

En la etapa 11, el Servidor de AAA de 3GPP envía el mensaje de éxito de EAP a la AN de WLAN. La AN de WLAN puede almacenar el material de claves (MSK) que se puede usar en comunicación con la UE de WLAN autenticado.

En la etapa 12, el mensaje de éxito de EAP se reenvía al UE de WLAN.

En la etapa 13, la UE de WLAN y la PDG intercambian el primer par de mensajes, conocido como IKE_SA_INIT (véase la norma TS 33.324, por ejemplo), en el que la PDG y los algoritmos criptográficos de negociación de UE de WLAN, intercambian nonces y realizan un intercambio de Diffie_Hellman.

En la etapa 14, la UE de WLAN sin UICC envía la identidad de usuario (en la carga útil de Idi) y la información de W-APN de emergencia (en la carga útil de Idr) en este primer mensaje de la fase IKE_AUTH, y empieza la negociación de asociaciones de seguridad secundarias. La UE de WLAN indica mediante la parte de dominio en su NAI a la PDG que la solicitud de conexión es para llamada de emergencia y que quiere usar EAP sobre IKEv2.

La identidad de usuario será conforme al formato del Identificador de Acceso a la Red (NAI) especificado en el documento RFC 4282 de IETF (diciembre de 2005: “The Network Access Identifier”). De acuerdo con el documento RFC 4306 de IETF: (diciembre de 2005: “Internet Key Exchange (IKEv2) Protocol”), el secreto compartido generado en un intercambio de EAP (la MSK), cuando se usa sobre IKEv2, se usará para generar el parámetro de AUTH.

Si la dirección del IP Remoto de la UE de WLAN necesita configurarse de manera dinámica, entonces la UE de WLAN enviará la carga útil de configuración (CFG_REQUEST) dentro del mensaje de solicitud de IKE_AUTH para obtener una dirección de IP remoto.

En la etapa 15, la PDG envía el mensaje de solicitud de autenticación con un par de atributo-valor (AVP, *attribute - value pair*) de EAP vacío al Servidor de AAA de 3GPP, que contiene la identidad de usuario. La PDG ha de incluir un parámetro que indique que la autenticación se está realizando para el establecimiento de túnel. Esto ayudará a que el Servidor de AAA de 3GPP distinga entre las autenticaciones para el acceso de WLAN y las autenticaciones para el establecimiento de túnel.

En la etapa 16, el Servidor de AAA de 3GPP verificará si el indicador de Emergency_Access está establecido para el usuario. Si el indicador de Emergency_Access está establecido y la W-APN no es aquella para emergencia tal como se define en la norma TS 23.003 de 3GPP, se establecerá el Código de Resultado a DIAMETER_AUTHORIZATION_REJECTED (autorización de diámetro rechazada).

Cuando todas las comprobaciones tienen éxito, el Servidor de AAA de 3GPP envía la Respuesta de Autenticación incluyendo un éxito de EAP y el material de claves a la PDG. Este material de claves ha de consistir en la clave de sesión maestra (MSK) generada durante el proceso de autenticación. Cuando la interfaz de Wm (Servidor de AAA de PDG-3GPP) se implementa usando Diámetro, la MSK ha de encapsularse en el parámetro de clave de sesión maestra de EAP, tal como se define en la referencia RFC 4072 (agosto de 2005: “Diameter Extensible Authentication Protocol (EAP) Application”).

En la etapa 17, la MSK se usará por la PDG para comprobar los parámetros de AUTH con el fin de autenticar los mensajes de fase de IKE_SA_INIT, tal como se especifica en la referencia RFC 4306 de IETF (diciembre de 2005: “Internet Key Exchange (IKEv2) Protocol)”.

En la etapa 18, la PDG responde con su identidad y un certificado. Esto también completa la negociación de las asociaciones de seguridad secundarias. El mensaje de éxito de EAP también se reenvía al UE de WLAN.

A continuación, se describe cómo se puede formar la identidad de usuario (tal como se usa en las etapas 3 y 13, por ejemplo).

En concreto, si se proporciona un nombre / contraseña de usuario común a todos los usuarios para la llamada de emergencia de IMS sin UICC, el problema es cómo definir tal nombre / contraseña y si alguien hace una llamada de emergencia falsa de manera deliberada, no hay manera alguna de rastrear este basándose en el nombre / la contraseña común.

De acuerdo con la presente realización, se proponen tres tipos de identidades para una UE sin UICS: identidad de equipo móvil internacional (IMEI), dirección de control de acceso a medios (MAC, *medium access control*) y dirección de IP.

En particular, en el caso de que 3GPP restrinja la conexión de tal forma que deba ser a partir de un terminal móvil (es decir, a partir de un terminal móvil en el que se puede insertar una tarjeta SIM), entonces se usará IMEI o IMEI a la que se ha aplicado función de troceo. La IMEI se puede usar en una forma a la que se ha aplicado función de troceo debido a que la longitud de la IMEI es de 15 bytes, lo que podría no ser apropiado para todos los casos. La IMEI o la IMEI a la que se ha aplicado función de troceo se usa entonces como la identidad de usuario en las etapas 3 y 14 en la figura 1.

El beneficio de usar IMEI a la que se ha aplicado función de troceo en esta etapa es que puede prevenir la suplantación de identidad. La UE puede usar IMEI a la que se ha aplicado función de troceo en esta etapa 3 y usar la IMEI completa original en la etapa 14. De este modo, incluso un atacante puede interceptar la IMEI a la que se ha aplicado función de troceo y usar esta para iniciar otra llamada de emergencia, este puede obtener la IMEI apropiada que ha de usarse en la etapa 14. La IMEI a la que se ha aplicado función de troceo apropiada no se generará en la PDG si la PDG recibe de un atacante una IMEI equivocada en la etapa 14. Es decir, cuando una IMEI a la que se ha aplicado función de troceo está incluida en la respuesta de EAP / Identidad en la etapa 3, un atacante posiblemente podría conseguir esta IMEI a la que se ha aplicado función de troceo escuchando en el enlace inalámbrico y podría usar esta para atacar la PDG en la etapa 14. Por tanto, en el caso de que se use una IMEI completa a la que no se ha aplicado función de troceo en la AUTH_request en la etapa 14, entonces, incluso si el atacante hubiera sido capaz de conseguir la IMEI a la que se ha aplicado función de troceo (en la etapa 3), este no podría usar la misma para atacar la PDG, debido a que no conoce la IMEI completa.

Como alternativa, en el caso de que 3GPP permita que otra UE de WLAN, tal como un PDA o bloc de notas, realice una llamada de emergencia de IMS, la dirección de MAC se puede usar de las siguientes maneras, en las etapas 3 y 14:

1) Dirección de MAC. Cada UE de WLAN debería tener una dirección de MAC única.
Cada UE de WLAN debería tener una dirección de MAC única.
La longitud de la ID es la más corta.
2) Dirección de WLAN + ID de AN de WLAN (SSID).
Esto puede proporcionar la ubicación de la llamada de emergencia para lograr saber la ubicación de la

emergencia, o para rastrear las llamadas falsas. Si un atacante usa otra dirección de MAC en la misma AN de WLAN, esto se detectará. Como alternativa, es posible usar una (dirección de MAC + ID de AN de WLAN (SSID)) a la que se ha aplicado función de troceo.

3) Dirección de IP local (asignada por AN de WLAN) + ID de AN de WLAN (SS ID).

Esto puede proporcionar la ubicación de la llamada de emergencia, de tal modo que es posible rastrear las llamadas falsas. Si un atacante usa otra dirección de IP en la misma AN de WLAN, esto se detectará. Como alternativa, también se puede usar una combinación a la que se ha aplicado función de troceo de la dirección de IP local + ID de AN de WLAN.

Cuando una UE se conecta a AN de WLAN para tener una conexión de escenario 2, puede usar un identificador de usuario en la etapa 3, por ejemplo, userID@sos.w-apn.mnc012.mcc345.pub.3gppnetwork.org. Es decir, en un mensaje inicial (etapa 3), el terminal de abonado usa el identificador de usuario. En respuesta a esto, el servidor de AAA puede conseguir la dirección de MAC / IP de la UE y la información de AN de WLAN a partir de la AN de WLAN. Por lo tanto, en respuesta a esto, en la etapa 5, el servidor de AAA puede formar la ID del usuario a partir del MAC / IP (y la información de AN de WLAN) recibida de AN de WLAN.

Cuando la UE establece la conexión de escenario 3 con la PDG, debido a que la parte de dominio en su NAI puede indicar a la PDG que la solicitud de conexión es para llamada de emergencia y quiere usar EAP sobre IKEv2, y ya existe clave compartida (MSK) entre la UE de WLAN y un servidor de AAA, la UE de WLAN puede generar el parámetro de AUTH y enviar este a la PDG. La PDG puede obtener la MSK a partir del servidor de AAA para comprobar la AUTH. De este modo ya no se necesitan más etapas como en el escenario 3 normal.

Por lo tanto, de acuerdo con la presente realización, un método de autenticación tal como el método de autenticación de EAP-TLS, que puede pasar por alto una autenticación de cliente, se usa en I-WLAN para usuarios sin UICC en el caso de llamada de emergencia.

De este modo, todavía se proporciona una autenticación de servidor. La autenticación de servidor permite la generación de MSK compartida entre la UE de WLAN y el servidor de AAA para usar EAP sobre IKE2.

Por lo tanto, la autenticación es solo para el servidor, no para el cliente. De este modo, la red no rechazará la llamada de emergencia (llamada de EM). Existen dos fines de la autenticación. Uno es mantener la AN de WLAN sin cambios. De otro modo, la AN de WLAN ha de comprobar el NAI de la UE para identificar si este es para llamada de EM. El otro fin es generar la MSK que se va a usar en el procedimiento de escenario 3.

Además, es posible establecer un túnel codificado a la PDG si el Servidor de AAA no tiene vectores de autenticación para este terminal (= caso sin UICC). En concreto, tal como se ha descrito en lo que antecede, la MSK se puede generar a partir del secreto maestro de TLS tal como se especifica en el documento RFC 4346 en la UE y el servidor de AAA. La PDG puede conseguir la MSK a partir del Servidor de AAA de 3GPP. De este modo, el túnel codificado se puede establecer entre la UE y la PDG.

No se necesita cambio en la AN de WLAN. El servidor de AAA necesita formar la ID de usuario a partir de MAC / IP (y la ID de AN de WLAN).

Por lo tanto, se puede establecer una conexión fiable y autenticada en un caso sin UICC.

A continuación se describe una segunda realización de la invención, en la que se considera el caso de que un atacante pueda empezar llamadas de emergencia dobles.

Con detalle, de acuerdo con el documento T533. 234 se permiten sesiones simultáneas tanto en el escenario 2 como en el 3 (es decir, a través del acceso de IP y el acceso de 3GPP), y los números de las sesiones simultáneas se basan en la política de los operadores. La solicitud de tener sesiones simultáneas es válida especialmente en el caso de división de UE de WLAN. Por ejemplo, un usuario puede usar su terminal móvil para visitar un sitio web de operador y usar su bloc de notas para acceder al VPN de su compañía al mismo tiempo.

No obstante, cuando un usuario hace una llamada de emergencia de IMS a través de un terminal sin UICC (tal como se describe en la primera realización, por ejemplo), no es razonable por su parte tener llamadas de emergencia de IMS simultáneas. Si esto ocurre, la segunda puede ser una fraudulenta y puede ser vandalismo hacia el servicio de emergencia. De este modo, las llamadas de emergencia de IMS simultáneas a través de un terminal sin UICC estarán prohibidas.

De acuerdo con la presente realización, en la PDG se lleva a cabo un control correspondiente, es decir, la W-APN para llamada de emergencia, en lugar del servidor de AAA debido a que la UE de WLAN puede no recibir el mensaje de éxito de EAP (en la etapa 12 de la figura 1) y no empieza los procedimientos de escenario 3.

Cuando la PDG recibe la solicitud a partir de la UE de WLAN (en la etapa 14), este debería comprobar si ya hay una sesión para el usuario. Si es así, esta rechazará la nueva solicitud en lugar de aceptar la misma. La razón

fundamental es que es difícil para un atacante saber la ID de la víctima con anticipación, pero puede interceptar esta cuando la UE establece la conexión de escenario 2.

A partir de la ID de UE, la PDG puede saber que esta es una llamada de emergencia de IMS sin UICC.

Por lo tanto, de acuerdo con la presente realización, las llamadas de emergencia dobles se detectan y se evitan de manera fiable.

A continuación, los elementos de red implicados en las realizaciones que se han descrito en lo que antecede se describen haciendo referencia a las figuras 2A a 2D. Se observa que en las figuras 2A a 2D solo se muestran los elementos básicos con el fin de simplificar los dibujos.

La figura 2A muestra la configuración básica de un terminal A de abonado. El terminal A de abonado comprende un controlador A1 y un transceptor A2. El controlador A2 puede incluir una CPU y diferentes tipos de unidades de memoria tales como RAM, ROM o similares. Un programa informático puede almacenarse en la memoria y puede comprender porciones de código de soporte lógico para llevar a cabo el método de acuerdo con las realizaciones. Este programa informático puede almacenarse en un medio de grabación tal como un CD-ROM, por ejemplo, y puede ser susceptible de carga directamente en la memoria de trabajo del controlador. Como alternativa, el programa informático puede cargarse a través de la red en la memoria del controlador.

La figura 2B muestra la configuración básica del servidor de AAA B, que comprende un controlador B1 y un transceptor B2. El controlador B1 puede estar configurado de una manera similar a la del controlador. Es decir, también el controlador B2 puede incluir una CPU y diferentes tipos de unidades de memoria tales como RAM, ROM, un disco duro, un lector de CD o de DVD-ROM o similar. Se puede proporcionar un programa informático al servidor de AAA de una manera similar a como se ha descrito en lo que antecede. El transceptor B2 puede comprender una o más interfaces, por medio de las cuales se puede proporcionar una conexión a través de una red a otros elementos de red.

La figura 2C muestra una configuración básica de la PGD C, que es similar a la configuración del servidor de AAA B, de tal modo que la descripción de la misma no se repite.

La figura 2D muestra una configuración básica de la AN de WLAN, que también es similar a la configuración del servidor de AAA B, de tal modo que la descripción de la misma no se repite.

La invención no está limitada a las realizaciones que se han descrito en lo que antecede, y son posibles varias modificaciones. En particular, el método de autenticación (o procedimiento de autenticación) no está limitado a EAPTLS. En particular, se puede usar cualquier otro método en el que la autenticación de cliente se puede omitir.

Además, el identificador del terminal de abonado no está limitado al IMEI. Es decir, se puede usar cualquier otro identificador que identifique un terminal de manera única.

Además, la secuencia de autenticación y los elementos de red implicados no están limitados a los detalles tal como se muestran en la figura 1 y se han descrito en lo que antecede.

Además, la llamada de emergencia de IMS que se ha mencionado en lo que antecede es solo un ejemplo para una llamada sin UICC. En particular, puede haber otras situaciones en las que se pudiera permitir una llamada sin UICC. Por ejemplo, se podría permitir una llamada sin UICC por una red con el fin de contactar con un operador del proveedor.

REIVINDICACIONES

1. Un método que comprende
iniciar una sesión a partir de un terminal de abonado, en el que el terminal de abonado no comprende un módulo de identificación de usuario específico;
formar una identificación temporal del terminal de abonado;
basándose por lo menos en parte en la identificación temporal, realizar una autenticación de servidor sin realizar autenticación de cliente, en el que
un procedimiento de autenticación aplicado es un protocolo de seguridad de capa de transporte de protocolo de autenticación extensible, EAP / TLS, y se omite una parte de autenticación de cliente del protocolo de seguridad de nivel de protocolo de autenticación extensible.

2. El método de acuerdo con la reivindicación 1, en el que la identificación temporal comprende un identificador de usuario y un dominio, comprendiendo el dominio una indicación específica para una sesión iniciada por el terminal de abonado.

3. El método de acuerdo con la reivindicación 2, en el que el identificador de usuario se crea basándose por lo menos en parte en uno de: un identificador de terminal, una dirección de control de acceso a medios del terminal de abonado y una dirección de protocolo de Internet asignada por un elemento de red de acceso al terminal de abonado.

4. Un método que comprende
enviar una solicitud de autenticación a un terminal de abonado para autenticar una sesión iniciada a partir del terminal de abonado;
recibir una respuesta de autenticación / un mensaje de identidad a partir del terminal de abonado, en el que la respuesta de autenticación / el mensaje de identidad comprende una identificación temporal del terminal de abonado; y
autenticar la sesión basándose por lo menos en parte en la identificación temporal del terminal de abonado, en el que una autenticación de servidor se realiza pero la autenticación de cliente se omite, en el que
un procedimiento de autenticación aplicado es un protocolo de seguridad de capa de transporte de protocolo de autenticación extensible, EAP / TLS, y se omite una parte de autenticación de cliente del protocolo de seguridad de nivel de protocolo de autenticación extensible.

5. El método de acuerdo con la reivindicación 4, que comprende además generar una clave de sesión maestra compartida que puede usarse para el cifrado de datos de usuario.

6. El método de acuerdo con la reivindicación 4, en el que la identificación temporal comprende un identificador de usuario y un dominio, comprendiendo el dominio una indicación específica para la sesión iniciada por el terminal de abonado, en el que el terminal de abonado no comprende un módulo de identificación de usuario específico.

7. El método de acuerdo con la reivindicación 6, en el que el identificador de usuario se forma basándose por lo menos en parte en uno de: una identidad de equipo móvil internacional, una dirección de control de acceso a medios y una dirección de Internet asignada por un elemento de red de acceso al terminal de abonado.

8. El método de acuerdo con cualquiera de las reivindicaciones 4-7, que comprende además
comprobar si ya existe una sesión para el terminal de abonado, y
rechazar una nueva sesión en el caso de que ya exista una sesión.

9. Un aparato, que comprende
por lo menos un procesador; y
por lo menos una memoria que incluye código de programa informático, configurados la por lo menos una memoria y el código de programa informático para, con el por lo menos un procesador, dar lugar a que el aparato realice por lo menos lo siguiente:

iniciar una sesión, en el que el aparato no comprende un módulo de identificación de usuario específico;
formar una identificación temporal; y
basándose por lo menos en la identificación temporal, realizar una autenticación de servidor sin realizar una autenticación de cliente, en el que

un procedimiento de autenticación aplicado es un protocolo de seguridad de capa de transporte de protocolo de autenticación extensible, EAP / TLS, y se omite una parte de autenticación de cliente del protocolo de seguridad de nivel de protocolo de autenticación extensible.

10. El aparato de acuerdo con la reivindicación 9, en el que se genera una clave de sesión maestra que puede usarse para el cifrado de datos de usuario.

11. El aparato de acuerdo con la reivindicación 9, en el que la identificación temporal comprende un identificador de usuario y un dominio, comprendiendo el dominio una indicación específica para una sesión de emergencia iniciada por el aparato.

12. El aparato de acuerdo con la reivindicación 11, en el que el identificador de usuario se crea basándose por lo menos en parte en uno de: una identidad de equipo móvil internacional, una dirección de control de acceso a medios del terminal de abonado y una dirección de Internet asignada por un elemento de red de acceso al terminal de abonado.

13. Un aparato que comprende
por lo menos un procesador; y
por lo menos una memoria que incluye código de programa informático, configurados la por lo menos una memoria y el código de programa informático para, con el por lo menos un procesador, dar lugar a que el aparato realice por lo menos lo siguiente:

enviar una solicitud de autenticación a un terminal de abonado;
recibir una respuesta de autenticación / un mensaje de identidad a partir del terminal de abonado, en el que la respuesta de autenticación / el mensaje de identidad comprende una identificación temporal del terminal de abonado; y
llevar a cabo una autenticación basándose por lo menos en parte en la identificación temporal en el que una autenticación de servidor se realiza pero se omite la autenticación de cliente, en el que
un procedimiento de autenticación aplicado es un protocolo de seguridad de capa de transporte de protocolo de autenticación extensible, EAP / TLS, y se omite una parte de autenticación de cliente del protocolo de seguridad de nivel de protocolo de autenticación extensible.

14. El aparato de acuerdo con la reivindicación 13, en el que la identificación temporal comprende un identificador de usuario y un dominio, comprendiendo el dominio una indicación específica para una sesión iniciada por el terminal de abonado, en el que el terminal de abonado no comprende un módulo de identificación de usuario específico.

15. El aparato de acuerdo con la reivindicación 14, en el que el identificador de usuario se forma basándose por lo menos en parte en uno de: una identidad de equipo móvil internacional, una dirección de control de acceso a medios del terminal de abonado y una dirección de protocolo de Internet asignada por un elemento de red de acceso al terminal de abonado.

16. El aparato de acuerdo con cualquiera de las reivindicaciones 13-15, en el que el procesador está configurado para comprobar si ya existe una sesión para el terminal de abonado, y
para rechazar una nueva sesión en el caso de que ya exista una sesión.

17. Un producto de programa informático incorporado en un soporte legible por ordenador, configurado el programa informático para controlar un procesador para realizar un método, el método de acuerdo con cualquiera de las reivindicaciones 1 a 7.

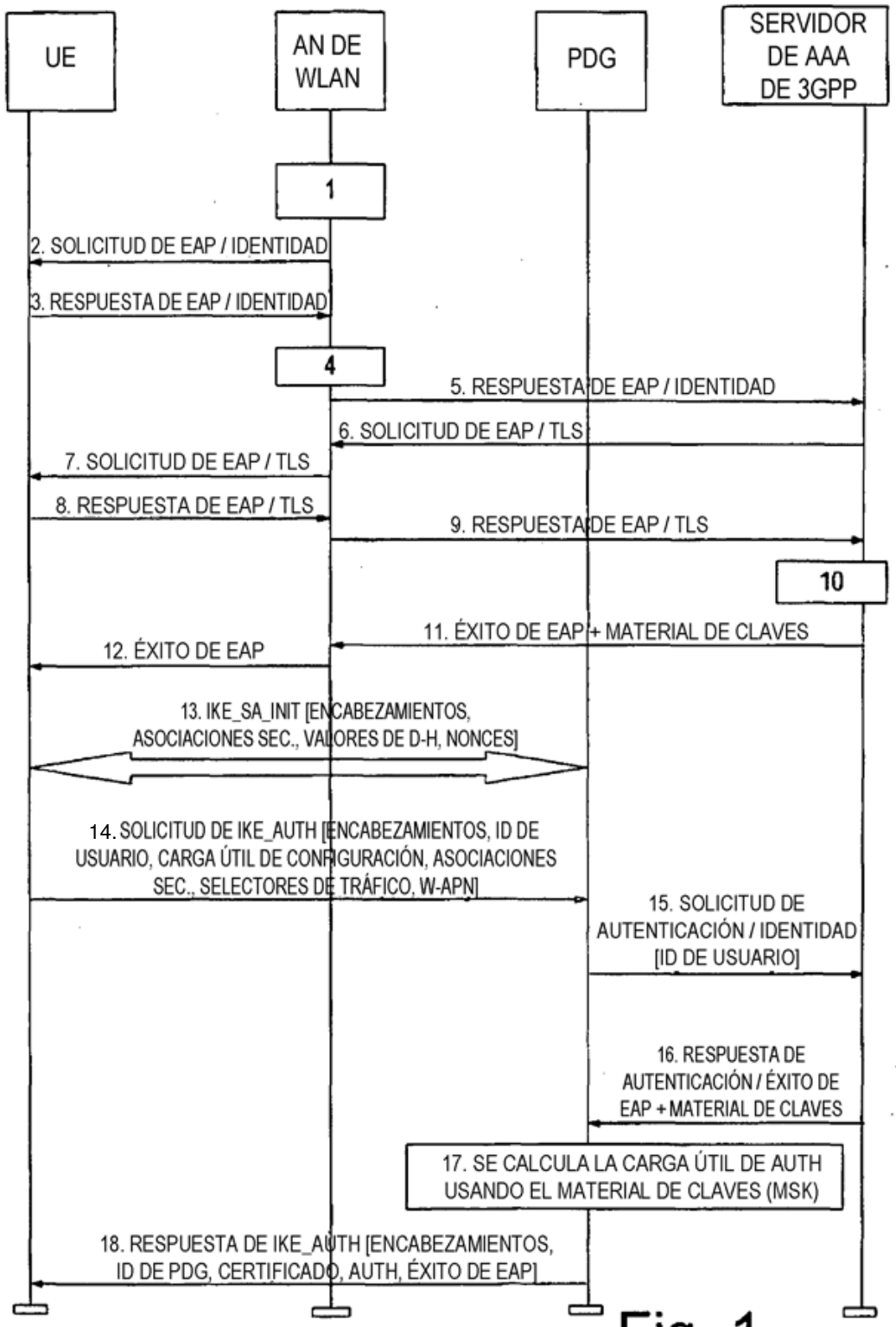
UE
AN DE WLAN
PDG
SERVIDOR DE AAA DE 3GPP
1
2. SOLICITUD DE EAP / IDENTIDAD
3. RESPUESTA DE EAP / IDENTIDAD
4
5. RESPUESTA DE EAP / IDENTIDAD
6. SOLICITUD DE EAP / TLS
7. SOLICITUD DE EAP / TLS
8. RESPUESTA DE EAP / TLS
9. RESPUESTA DE EAP / TLS
10
11. ÉXITO DE EAP + MATERIAL DE CLAVES
12. ÉXITO DE EAP
13. IKE_SA_INIT [ENCABEZAMIENTOS, ASOCIACIONES SEC., VALORES DE D-H, NONCES]
14. SOLICITUD DE IKE_AUTH [ENCABEZAMIENTOS, ID DE USUARIO, CARGA ÚTIL DE CONFIGURACIÓN, ASOCIACIONES SEC., SELECTORES DE TRÁFICO, W-APN]
15. SOLICITUD DE AUTENTICACIÓN / IDENTIDAD [ID DE USUARIO]
16. RESPUESTA DE AUTENTICACIÓN / ÉXITO DE EAP + MATERIAL DE CLAVES
17. SE CALCULA LA CARGA ÚTIL DE AUTH USANDO EL MATERIAL DE CLAVES (MSK)
18. RESPUESTA DE IKE_AUTH [ENCABEZAMIENTOS, ID DE PDG, CERTIFICADO, AUTH, ÉXITO DE EAP]

Fig. 1

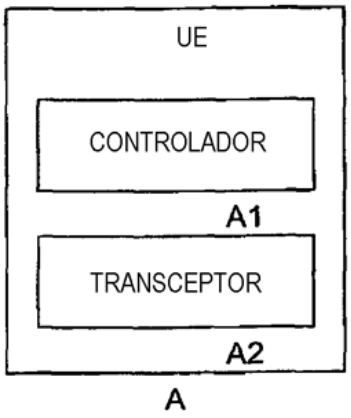

Fig. 2A

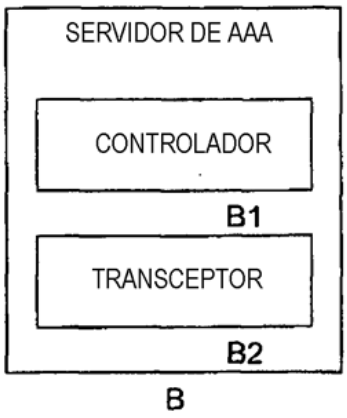

Fig. 2B

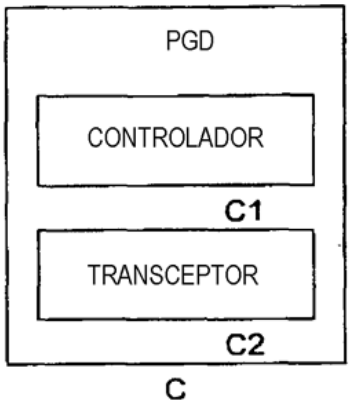

Fig. 2C

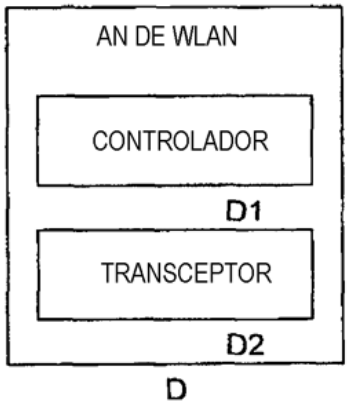

Fig. 2D