(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 381 552**

(21) Número de solicitud: 200930015

(51) Int. CI.:

H04W 12/06 (2009.01)

(12) PATENTE DE INVENCIÓN B1

(22) Fecha de presentación:

27.03.2009

(43) Fecha de publicación de la solicitud:

29.05.2012

Fecha de la concesión:

23.04.2013

(45) Fecha de publicación de la concesión:

07.05.2013

(73) Titular/es:

UNIVERSIDAD DE MURCIA
AVDA. TENIENTE FLOMESTA, S/N
30003 MURCIA (Murcia) ES

(72) Inventor/es:

MARIN LOPEZ, Rafael;
GOMEZ SKARMETA, Antonio Fernand;
PEREÑIGUEZ GARCIA, Fernando y
BERNAL HIDALGO, Fernando

(74) Agente/Representante:

ELZABURU MARQUEZ, Alberto

(54) Título: **Procedimiento de re-autenticación**

(57) Resumen:

Procedimiento de re-autenticación extensible de autenticación rápido EAP-FRM que se implementa en terminales portables de clientes-abonados a una red de telecomunicaciones inalámbricas y en módulos de autenticación incluidos en puntos de acceso de la red de telecomunicaciones, pudiendo ser los referidos puntos de acceso módulos servidores que ejecutan el protocolo de autenticación extensible EAP, servidor EAP, siendo ejecutado en el terminal-cliente y en el autenticador. En caso de que el módulo autenticador no sea capaz de autorizar el acceso del terminal-cliente al punto de acceso, el módulo autenticador se comunica con un módulo servidor EAP o con un servidor EAP/AAA, AAA autenticación, autorización y auditoria, local de la red de telecomunicaciones a la que es subscrito el terminal-cliente y/o a un servidor EAP/AAA de otra red de telecomunicaciones inalámbricas.

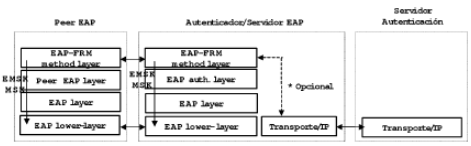

FIG. 1

ES 2 381 552 B1

DESCRIPCIÓN

Procedimiento de re-autenticación.

Objeto de la invención

La presente invención se refiere, en general, a un procedimiento de re-autenticación rápido de una unidad móvil portable itinere y, más particularmente, a un método rápido de re-autenticación de la unidad móvil portable de un abonado en itinerancia o traspaso de un punto de acceso a otro punto de acceso de una red de telecomunicaciones inalámbricas.

Estado de la técnica

Hoy en día, un operador de una red de telecomunicaciones dispone de medios para controlar el acceso de un abonado, propio o en itinerancia, a su red de telecomunicaciones.

El control de acceso se realiza, normalmente, a través de protocolos de autenticación, autorización y auditoria. La aplicación de este tipo de protocolos de comunicación requiere varios intercambios de mensajes, se ha de observar que un intercambio implica un mensaje en cada sentido de la comunicación, entre el terminal del cliente-abonado y un módulo servidor de autenticación y autorización que autentifica y autoriza el acceso del cliente a la red.

Se puede añadir que el referido proceso se complica, es decir, el proceso de autorización de acceso se extiende en el tiempo cuando las redes inalámbricas son heterogéneas.

Un protocolo utilizado para llevar a cabo el antedicho proceso de autenticación y control de acceso a redes inalámbricas, es protocolo de autenticación extensible EAP ejecutado entre el cliente y un servidor a través de un módulo autenticador localizado en el punto de acceso y que actúa como mero transmisor de datos y bloqueador hasta que se autoriza el acceso del cliente a la red de telecomunicaciones sin hilos.

La ejecución del protocolo EAP implica el intercambio de mensajes, en ambos sentidos de la comunicación, entre el terminal del cliente y el servidor de autenticación del operador de la red inalámbrica.

En un proceso de autenticación EAP se generan claves criptográficas como resultado de una autenticación correcta.

Cómo se ha mencionado anteriormente, el referido proceso requiere un período de tiempo al implicar varios intercambios entre el cliente EAP y el servidor EAP a través del autenticador EAP que reenvía los mensajes entre ambos.

El referido proceso se alarga en el tiempo en el caso de que el cliente se encuentre en itinerancia ya que el módulo autenticador y el servidor autenticador físicamente se encuentra a una distancia mayor, por ejemplo, pertenecen a redes inalámbricas de diferentes países y operadores diferentes. Por tanto, el retardo aumenta.

A su vez, cuando el abonado se mueve y se conecta a otro punto de acceso, que implica un diferente autenticador, comienza un nuevo proceso de autorización y control de acceso incluso si aún existe material criptográfico sin expirar.

Se ha de observar que el protocolo Extensible Authentication Protocol EAP permite realizar el proceso de autenticación y control de acceso en diferentes redes de acceso, en particular aquellas cuyo medio de transmisión es inalámbrico.

El protocolo EAP permite llevar a cabo diferentes mecanismos de autenticación llamados métodos EAP. Estos son ejecutados entre el denominado cliente EAP y un servidor EAP. Todo el proceso se realiza a través de un autenticador EAP que simplemente reenvía los paquetes EAP generados por el cliente EAP y un servidor EAP.

Este proceso se puede llevar a cabo incluso cuando el cliente EAP no se encuentra conectado directamente al autenticador en lo que se conoce como pre-autenticación EAP. No obstante, el proceso de pre-autenticación debe estar asistido por el protocolo de transporte entre el cliente EAP y el autenticador.

El autenticador EAP se localiza, generalmente, en puntos de acceso a la red inalámbrica desplegada por el proveedor de servicios de red. Ejemplos de estos dispositivos son puntos de acceso inalámbricos IEEE 802.11, encaminadores, antenas WiMax, etc.

El servidor EAP se puede localizar junto al autenticador o bien en un servidor de autenticación situado en la infraestructura de red inalámbrica del proveedor de servicios de red. De esta forma se centraliza toda la gestión de subscriptores-clientes en un punto central. Si la autenticación EAP finaliza con éxito dos claves son generadas: una Master Session Key MSK y una Extended Master Session Key EMSK. La clave MSK es enviada desde el servidor EAP hasta el autenticador EAP para establecer una asociación de seguridad entre el cliente EAP y el autenticador EAP.

Caracterización de la invención

La presente invención busca resolver o reducir uno o más de los inconvenientes expuestos anteriormente por medio de un procedimiento de re-autenticación rápido como es reivindicado en la reivindicación 1. Realizaciones de la invención son establecidas en las reivindicaciones dependientes.

Un objeto de la presente invención es proporcionar un protocolo rápido de re-autenticación extensible EAP-FRM que reduce el tiempo de autorización y control de acceso a una red de telecomunicaciones inalámbrica al reducir el número de intercambios de mensaje entre un cliente EAP-FRM y un módulo servidor de autenticación, autorización y auditoría, servidor AAA, a través de un módulo de autenticación EAP-FRM en un escenario de itinerancia o traspaso del cliente EAP.

Otro objeto de la invención es incluir, en el módulo autenticador localizable en un punto de acceso de la red, y en un terminal del cliente una capa de método EAP-FRM que ejecuta el protocolo rápido de re-autenticación extensible EAP-FRM, de manera que el autenticador permite autenticar y autorizar el acceso a la red de forma local sin necesidad de comunicarse con el servidor AAA del operador de la red de telecomunicaciones al cual está subscrito el cliente EAP u otro servidor perteneciente a otra red inalámbrica.

Permite al autenticador la posibilidad de tomar decisiones rápidas de autenticación sin necesidad de contactar ningún servidor de autenticación.

No se necesita modificar ni extender el protocolo de comunicaciones estándar EAP, ya que el protocolo EAP transporta cualquier método EAP, en particular, el protocolo EAP-FRM.

En algún escenario se deberá incluir alguna modificiación del protocolo de comunicación existente entre el autenticador y el servidor de autenticación, por ejemplo, si se utiliza un protocolo de Autenticación Autorización y Auditoría AAA del tipo RADIUS y Diameter para la comunicación entre el autenticador y el servidor de autenticación, es necesario un atributo

RADIUS o Diameter para transportar la información del protocolo de autenticación rápida entre el autenticador y el servidor.

Los protocolos RADIUS y Diameter están diseñados de forma modular tales que las extensiones necesarias no afectan a la implementación básica de los protocolos.

Los cambios requeridos en los protocolos RADIUS y Diameter se pueden gestionar a través de actualizaciones de su programación lógica, software, en los clientes AAA y los servidores AAA.

El protocolo rápido de re-autenticación extensible EAP-FRM permite que con un intercambio, dos mensajes, sean necesarios entre autenticador y servidor de autenticación para llevar a cabo el proceso de autenticación.

El autenticador adopta decisiones de autorización de control de acceso sin necesidad de comunicarse obligatoriamente con un servidor de autenticación, permitiendo a los proveedores escoger el protocolo de autenticación rápida que deseen, ya que no requiere modificaciones de los estándares y las tecnologías existentes facilitando con ello el despliegue de la solución. Además habilita la posibilidad de un número intercambio reducido de mensajes entre el autenticador y el servidor. En particular, entre 0 y 2 mensajes. Pudiendo ser el servidor de autenticación local o propio de la red inalámbrica y, por tanto, próximo al cliente.

Breve descripción de las figuras

Ahora serán descritos los dispositivos que materializan la invención, a modo de ejemplo solamente, con referencia a los dibujos adjuntos, en el que:

la figura 1 muestra la relación entre un cliente, un autenticador/servidor EAP y un servidor de autenticación que utilizan el protocolo EAP-FRM de acuerdo a la invención,

la figura 2 muestra el intercambio de menajes del proceso de autenticación rápida de acuerdo a la invención,

la figura 3 muestra el formato del campo de datos de un mensaje EAP-FRM de acuerdo a la invención,

la figura 4 muestra un escenario donde el autenticador resuelve el acceso a la red del terminal-cliente de acuerdo a la invención,

la figura 5 muestra un escenario donde el autenticador no es capaz de autorizar el acceso al terminal-cliente y un servidor autoriza el acceso a la red de acuerdo a la invención,

la figura 6 muestra el formato de un atributo Diameter para transportar la información del protocolo de autenticación rápida entre el autenticador y el servidor de acuerdo a la invención,

la figura 7 muestra un atributo RADIUS para transportar el protocolo de autenticación rápida cuyo tipo se incluye en otro atributo RADIUS de acuerdo a la invención, y

la figura 8 muestra otro atributo RADIUS de acuerdo a la invención.

Descripción de la invención

A continuación, con referencia a las figuras 1 y 2 se encuentra ilustrado el protocolo de autenticación extensible de autenticación rápido EAP-FRM que se implementa en terminales portables de clientes-abonados a una red de telecomunicaciones inalámbricas y en módulos de autenticación incluidos en puntos de acceso de la red de telecomunicaciones, pudiendo ser los referidos puntos de acceso módulos servidores que ejecutan el protocolo de autenticación extensible EAP, servidor EAP.

Es decir, el protocolo EAP-FRM se ejecuta en el terminal-cliente y en el autenticador. En caso de que el módulo autenticador no sea capaz de autorizar el acceso del terminal-cliente al punto de acceso, el módulo autenticador se comunica con un módulo servidor EAP o con un servidor EAP/AAA, AAA autenticación, autorización y auditoria, local de la red de telecomunicaciones a la que es subscrito el terminal-cliente y/o a un servidor EAP/AAA de otra red de telecomunicaciones inalámbricas.

Para poder ejecutar el referido protocolo EAP-FRM, tanto el terminal-cliente como el módulo autenticador incluyen en la parte alta de la pila del protocolo de comunicaciones, según el modelo OSI, un nivel o capa de método EAP-FRM configurado para generar, incluir y extraer información de autenticación rápida relativa al protocolo EAP-FRM.

El intercambio de mensajes, en ambos sentidos de la comunicación, del tipo solicitud, EAP-Request/FRM, respuesta, EAP-Response/FRM; desde el terminal-cliente hacia el autenticador, atraviesan el resto de capas de la pila del protocolo de comunicaciones EAP en sentido descendente-ascendente y, viceversa, descendente-ascendente desde el autenticador hacia el terminal-cliente.

Sin embargo, en el escenario de que en la capa de método EAP-FRM del autenticador no sea capaz de extraer información de autenticación rápida relativa al protocolo EAP-FRM generada por el terminal-cliente; la referida capa de método EAP-FRM del autenticador reenvía la información recibida desde el terminal-cliente hacia una capa de método EAP de servidor de autenticación EAP o servidor EAP/AAA, en adelante, servidor de autenticación propio de la red de telecomunicaciones del terminal-cliente o externo a la referida red de telecomunicaciones.

El intercambio de mensajes del tipo descrito anteriormente se establece desde la capa de método EAP-FRM del autenticador con la correspondiente capa de método EAP del servidor autenticador a través de capas de transporte, por ejemplo, correspondientes a una red IP. De manera que el referido servidor de autenticación se hace responsable de autorizar o denegar el acceso del terminal-cliente, que solicitado originalmente autorización de acceso a la correspondiente red inalámbrica.

Consecuentemente, el autenticador y el servidor de autenticación, propio de la red de telecomunicaciones del terminal-cliente o externo a la referida red de telecomunicaciones, utilizan un protocolo de comunicaciones que permite reenviar información de autenticación originada por el terminal-cliente, y encapsulada, según el protocolo EAP-FRM, en el nivel de método EAP del mismo terminal, previamente enviada al autenticador.

La antedicha comunicación se establece cuando la información originada en el nivel de método del terminal-cliente y transmitida desde el mismo al nivel de método EAP-FRM del autenticador no incluye información de autenticación rápida que puede ser extraída y procesada por el autenticador de forma que autorice el acceso.

Por ejemplo, el terminal-cliente incluye una capa de método EAP, que genera y envía información de re-autenticación relativa al protocolo EAP. Dicha información puede ser leída y por la correspondiente

capa de método EAP-FRM, sin embargo, el referido nivel de método EAP del autenticador no puede extraer información relativa al procedimiento de autenticación rápida EAP-FRM, ya que el paquete recibido no incluye información de autenticación rápida.

En este escenario el autenticador debe reenviar la información recibida al servidor de autenticación. Si el paquete recibido en el autenticador incluye información relativa al protocolo EAP-FRM, esto permite al autenticador tomar decisiones sin contactar con ningún servidor de autenticación situado en cualquier red inalámbrica y, por tanto, reduciendo a cero el número de intercambios de mensajes con la infraestructura de la red inalámbrica.

De hecho, cualquier unidad de datos relativos a un protocolo de autenticación rápida puede ser la información de autenticación que transporten los mensajes del método EAP-FRM. No obstante, es importante resaltar que este modo de operación no cambia el modelo estándar definido en EAP.

Se asume que, de alguna forma inicial, el cliente y el servidor de autenticación disponen de un conjunto de credenciales que les permiten llevar a cabo el protocolo de autenticación rápida. Por ejemplo, estas credenciales pueden ser originadas después de la ejecución de un método EAP cualesquiera que sea capaz de generar material criptográfico, la primera vez que el terminal-cliente se conecta a la red.

Como se ha mencionado anteriormente, la arquitectura genérica para autenticación rápida emplea un protocolo EAP mejorado, denomindado protocolo EAP-FRM, que se instala en la misma capa de método EAP del autenticador y del terminal-cliente, siendo denominadas capas de método EAP-FRM, de manera que una capa de método EAP-FRM es capaz de leer paquetes que transportan información al protocolo EAP, reenviando dicha información al servidor de autenticación situado en la red o a uno externo, p. ej. un servidor AAA, utilizando para ello un protocolo que permite enviar la información del protocolo de autenticación rápida originada por el cliente y encapsulada en EAP-FRM en la comunicación entre el cliente y el autenticador.

Como en el protocolo EAP, en el protocolo EAP-FRM se asume que entre el cliente y el servidor de autenticación existe un secreto compartido que denominaremos credencial EAP-FRM del tipo EMSK, MSK. Esta credencial servirá para construir y diseñar el protocolo de autenticación rápida escogido por el operador.

Para realizar la operación de forma dinámica se utiliza un protocolo de distribución de claves, aunque para generar el material criptográfico inicial es necesario llevar a cabo una vez la denominada fase de bootstrapping. En general, esta fase de bootstrapping permite generar las credenciales EAP-FRM a través del material criptográfico generado tras la ejecución de un método EAP donde el servidor EAP se encuentra localizado en el servidor de autenticación y es capaz de derivar las claves.

Este método es ejecutado cuando el cliente se conecta por primera vez a la red. Una vez que se ejecuta el paso de bootstrapping, la arquitectura está en disposición de utilizar el protocolo EAP-FRM para reducir el tiempo de autenticación en posteriores autenticaciones en la red.

En relación con la figura 2, cuando un terminal-cliente EAP realiza un movimiento, itinerancia o traspaso, del autenticador actual, ubicado en un punto de acceso, a otro autenticador, localizado en otro punto de acceso de una red, o incluso antes del movimiento a un nuevo autenticador a través de un proceso de pre-autenticación EAP, el cliente y el nuevo autenticador comienzan una autenticación basada en el método EAP-FRM, de tal forma que cuando un cliente comienza un proceso de autenticación, el autenticador envía de forma automática un mensaje EAP-Request/FRM, incluyendo en un primer mensaje cualquier información que sea necesaria para llevar a cabo el protocolo de autenticación rápida. Por ejemplo, el servidor que controla dicho autenticador.

Si el cliente no tiene soporte para dicho método EAP-FRM o bien carece de credenciales EAP-FRM para emplear un protocolo de autenticación rápida, envía en el mensaje estándar EAP-Response/Nak. Esto provoca que el autenticador envíe un mensaje EAP-Request/Id para empezar un proceso de autenticación EAP con cualquier otro método. De esta forma, la arquitectura permite aceptar clientes que pudieran no soportar EAP-FRM.

Por el contrario, si el cliente es un terminal-cliente EAP-FRM, responde al mensaje EAP-Request/FRM, con un mensaje EAP-Response/FRM conteniendo datos del protocolo de autenticación rápida. Si el proceso que el cliente inicia es una pre-autenticación EAP activa un bit P en el campo de opciones del paquete, ver figura 3.

El autenticador extrae los datos del protocolo de autenticación rápida contenidos en el mensaje EAP-Response/FRM y, o bien los procesa directamente para autorizar el acceso al servicio de red y derivar las correspondientes claves criptográficas; o bien lo reenvía a un servidor de autenticación, delegando así el proceso de verificación y generación de claves al servidor de autenticación, p. ej. servidor AAA.

En este último caso, la comunicación entre autenticador y servidor se realiza a través otro protocolo que debe ser proporcionado por el operador de la red.

Dicho protocolo debe transportar la información contenida en el campo de datos de EAP-FRM entre el autenticador y el servidor de autenticación. Por tanto, el protocolo lleva la información transportada en el campo de datos, o al menos la parte donde se encuentra contenido el protocolo de autenticación rápida, del mensaje EAP-Response/FRM entre el autenticador y el servidor de autenticación. En general, este protocolo puede ser un protocolo AAA del tipo RADIUS o Diameter, en cuyo caso el servidor de autenticación será un servidor AAA.

Para transportar los datos del protocolo de autenticación rápida contenidos en el mensaje EAP-Response/FRM dentro RADIUS, se define un nuevo atributo RADIUS denominado PAR, Protocolo de Autenticación Rápida, que puede ser transportado en mensajes RADIUS-Access-Request y RADIUS-Access-Accept.

En relación con la figura 6, Diameter existen diferentes alternativas tales como, crear una nueva aplicación Diameter denominada Diameter-FR, y que consta de dos comandos Diameter-FR-Request para transportar el campo de datos del protocolo EAP-FRM desde el autenticador al servidor de autenticación, en el caso de un servidor AAA Diameter.

Diameter-FR-Answer para el mismo propósito en la dirección opuesta. Dicha aplicación también define un atributo Diameter, denominado AVP PAR, para

transportar los datos del protocolo de autenticación rápida en ambos mensajes.

Extender la aplicación Diameter NASREQ para incluir el AVP PAR para transportar el tipo del protocolo de autenticación rápida.

Por tanto, en ambos casos se define un atributo(s) Diameter (AVP) que contendrá el campo de datos del mensaje EAP-Response/FRM en la solicitud desde el autenticador al servidor. Además se utilizará para llevar los datos que serán transportados en el campo de datos del mensaje EAP-Request/FRM desde el servidor al autenticador.

El protocolo EAP-FRM transporta información del protocolo de autenticación rápida en su campo de datos, ver figuras 3, 6, 7 y 8, donde el campo de datos está formado por un octeto para señalar diferentes opciones (8 bits disponibles), un bit (P) se dedica a indicar que la autenticación EAP forma parte de un proceso de pre-autenticación. El resto se deja para uso futuro.

Si el proceso no forma parte de una pre-autenticación el bit P mantendrá siempre el valor 0. Si el proceso forma parte de una pre-autenticación EAP, el bit P se mantendrá a 1 durante todo el proceso. A continuación existe un octeto que indica el tipo de protocolo de autenticación rápida utilizado y que transporta EAP-FRM.

Seguidamente se define una lista de estructuras TLV (Tag [2 octetos], Longitud [2 octetos], Valor [0.65535 octetos]). Dentro del conjunto de TLVs destacan tres principales, aunque se pueden definir más en el futuro.

TLV servidor (opcional): indica en formato NAI (Network Access Identifier) (e.g srv@dom.net) o bien una dirección IP el nombre del servidor de autenticación. Esto es útil para el autenticador a la hora de saber donde iniciar el protocolo de comunicación entre autenticador y servidor. Este servidor puede ser un servidor local al movimiento del cliente.

TLV identidad (opcional): contiene la identidad del usuario en formato NAI, e.g. xxx@domain.es.

TLV protocolo (opcional): contiene los datos del protocolo de autenticación rápida.

Por tanto, la figura 6 muestra un AVP Diameter de tipo agrupado que contiene el tipo del protocolo de autenticación rápida y los datos de dicho protocolo. La figura 7 muestra un atributo RADIUS para transportar el protocolo de autenticación rápida cuyo tipo se incluye en otro atributo RADIUS, ver figura 8.

La figura 4 muestra un escenario donde no se requiere contactar con ningún servidor de autenticación en el momento de autorizar el acceso. El protocolo de autenticación utilizado por el autenticador es Kerberos. Se asume que el cliente dispone de un ticket Kerberos para ser autenticado por el autenticador, siendo enviado el ticket al autenticador (KRB_AP_REQ) a través del protocolo EAP-FRM.

La figura 5 muestra un escenario donde es preciso contactar con un servidor de autenticación mediante el protocolo de autenticación rápida basado en ERP, siendo mostrada la adaptación en la referida figura 5.

El protocolo EAP-FRM lleva un valor tipo PAR de 2. El protocolo ERP define dos mensajes: EAP-Initiate/Re-auth y EAP-Finish/Re-auth. Estos mensajes contienen un número de secuencia para protección contra reenvío y son protegidos por una clave rIK para integridad y compartida entre el cliente y el servidor de autenticación.

La adaptación consiste en transportar la información de autenticación contenida en los mensajes de ERP en mensajes EAP-FRM de la arquitectura propuesta. En particular, cuando el cliente necesita autenticación recibe un mensaje EAP-Request/FRM que contiene la información contenida en el mensaje EAP-Initiate/Re-auth-Start (IRS). Por ejemplo el nombre de dominio al que pertenece el autenticador. A continuación, el cliente envía al autenticador EAP un mensaje EAP-Response/FRM con el contenido especificado en el campo de datos del mensaje EAP-Initiate/Re-auth (IR). Esto incluye un número de secuencia y una etiqueta de autenticación creada con la clave rIK, que puede ser verificada por el servidor de autenticación. El autenticador desencapsula, extrae, dicha información del mensaje EAP-Response/FRM e inicia una conversación Diameter o RADIUS con el servidor de autenticación. En particular, el autenticador envía un mensaje Diameter-FR-Request con el AVP PAR, mostrado en la figura 6, o un mensaje RADIUS-Access-Request con el atributo PAR, ver figura 7, y el atributo Tipo, mostrado en la figura 8 en el caso de uso de RADIUS, que contiene el número de secuencia y la etiqueta de autenticación. Esto es verificado por el servidor que envía un Diameter-FR-Response que contiene un AVP para transportar la clave al autenticador (rMSK en terminología ERP) mientras que el AVP agrupado contiene los datos que el mensaje EAP-Finish/Re-auth (FIR) de ERP puede transportar; por ejemplo, un número de secuencia y otra etiqueta de autenticación ahora generada por el servidor de autenticación.

Esta información que llega a través del mensaje Diameter-FR-Response es extraída por el autenticador, que la encapsula en un mensaje EAP-Request/FRM que envía al cliente. El cliente puede verificar el número de secuencia y la etiqueta de autenticación enviada por el servidor de autenticación. Si todo es correcto, envía un EAP-Response/FRM al cual, el autenticador ya responde con un EAP Success.

REIVINDICACIONES

1. Procedimiento de pre-autenticación rápido EAP-FRM; **caracterizado** por qué comprende las etapas de adición de una capa de método configurado para generar, incluir y extraer información de autenticación rápida relativa a un protocolo EAP modificado, en un terminal-cliente portable de un subscriptor a una red de telecomunicaciones inalámbricas; adición de una capa de método configurado para generar, incluir y extraer información de autenticación rápida relativa a un protocolo EAP modificado, en un módulo de autenticación incluido en puntos de acceso de la referida red de telecomunicaciones, que basándose a la información generada en la capa de método EAP-FRM y enviada por el terminal-cliente a la correspondiente capa de método EAP-FRM del autenticador resuelve autorizar o denegar el acceso del terminal-cliente a una red de telecomunicaciones.

2. Procedimiento de pre-autenticación de acuerdo a la reivindicación 1; **caracterizado** por qué comprende la etapa de reenvío de la información recibida por la capa de método EAP-FRM del autenticador desde la correspondiente capa de método EAP-FRM del terminal-cliente, a un módulo servidor de autenticación para que resuelva autorizar o denegar el acceso del terminal-cliente a una red de telecomunicaciones.

3. Terminal-cliente EAP portable de un clientes-abonado a una red de telecomunicaciones inalámbricas que se comunica con un módulo de autenticación incluido en puntos de acceso de la red de telecomunicaciones; **caracterizado** por qué el terminal-cliente configurado para incluir una capa de método EAP mejorada, capa de método EAP-FRM, intercambia mensajes con la correspondiente capa de método EAP-FRM del autenticador que debe autorizar o denegar el acceso del terminal-cliente a la red de telecomunicaciones basándose con la información que genera, inserta y envía la capa de método EAP-FRM del terminal en un mensaje de respuesta a la capa de método EAP-FRM del autenticador.

4. Módulo de autenticación EAP incluido en puntos de acceso de la red de telecomunicaciones que comunica con un terminal-cliente EAP portable de un clientes-abonado a una red de telecomunicaciones inalámbricas; **caracterizado** por qué el autenticador configurado para incluir una capa de método EAP mejorada, capa de método EAP-FRM, intercambia mensajes con la correspondiente capa de método EAP-FRM del terminal-cliente para autorizar o denegar al mismo el acceso a la red de telecomunicaciones, basándose en la información que genero, inserto y envió la capa de método EAP-FRM del terminal en un mensaje de respuesta a la capa de método EAP-FRM del autenticador.

5. Módulo servidor que ejecuta un protocolo de autenticación extensible EAP de acuerdo a la reivindicación 4; **caracterizado** por qué el autenticador configurado para comunicarse con el servidor EAP en caso de que el autenticador no sea capaz de autorizar el acceso del terminal-cliente a la red inalámbrica, autorice o deniegue el acceso del terminal-cliente a la red inalámbrica en base a la información reenviada por el autenticador desde su capa de método EAP-FRM.

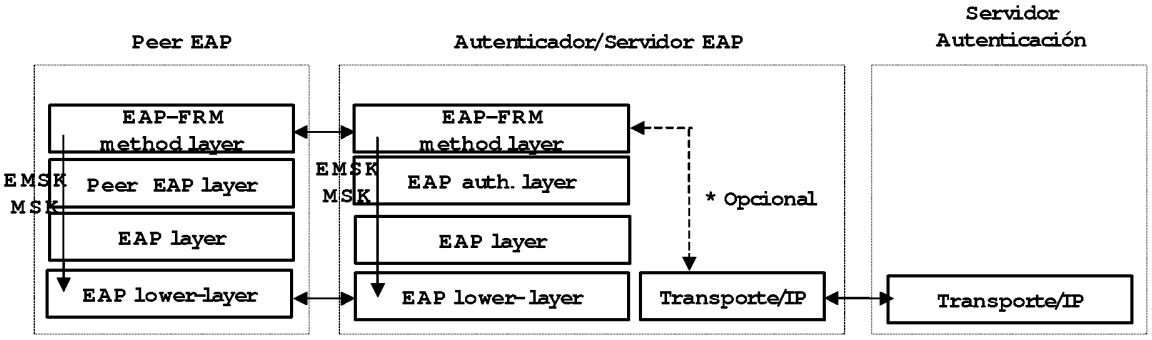

FIG. 1

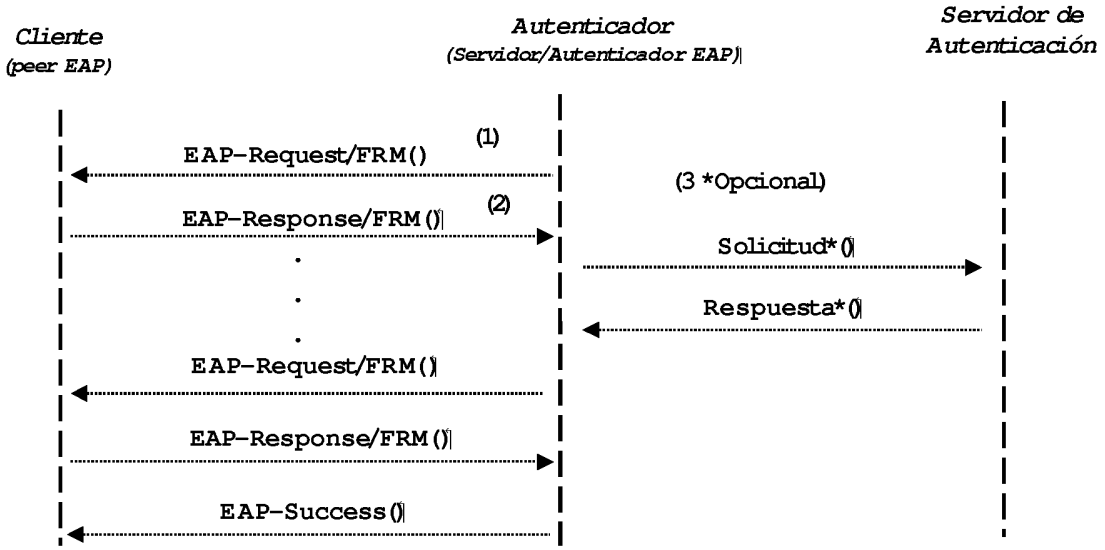

FIG. 2

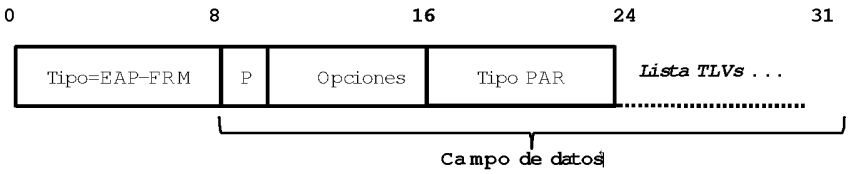

FIG. 3

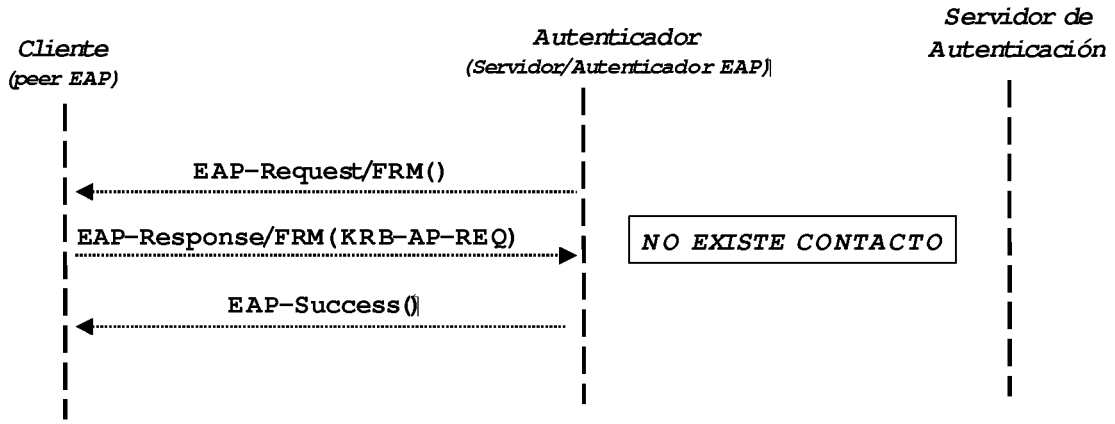
Cliente
(peer EAP)
Autenticador
(Servidor/Autenticador EAP)
Servidor de
Autenticación
EAP-Request/FRM()
EAP-Response/FRM(KRB-AP-REQ)
NO EXISTE CONTACTO
EAP-Success()

FIG. 4

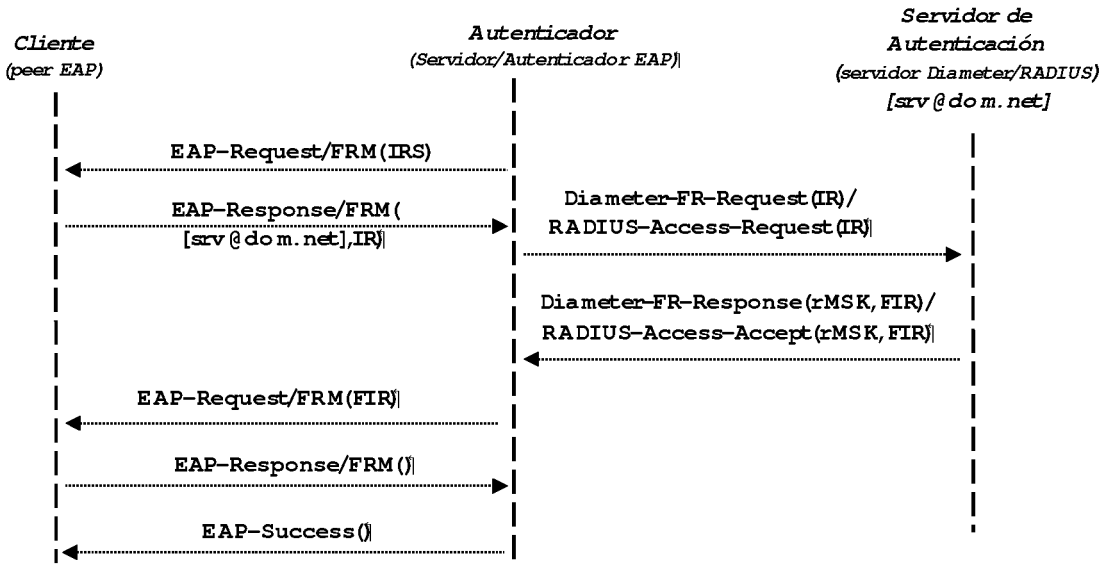
Cliente
(peer EAP)
Autenticador
(Servidor/Autenticador EAP)
Servidor de
Autenticación
(servidor Diameter/RADIUS)
[srv@dom.net]
EAP-Request/FRM(IRS)
EAP-Response/FRM(
[srv@dom.net],IR)
Diameter-FR-Request(IR)/
RADIUS-Access-Request(IR)
Diameter-FR-Response(rMSK,FIR)/
RADIUS-Access-Accept(rMSK,FIR)
EAP-Request/FRM(FIR)
EAP-Response/FRM()
EAP-Success()

FIG. 5

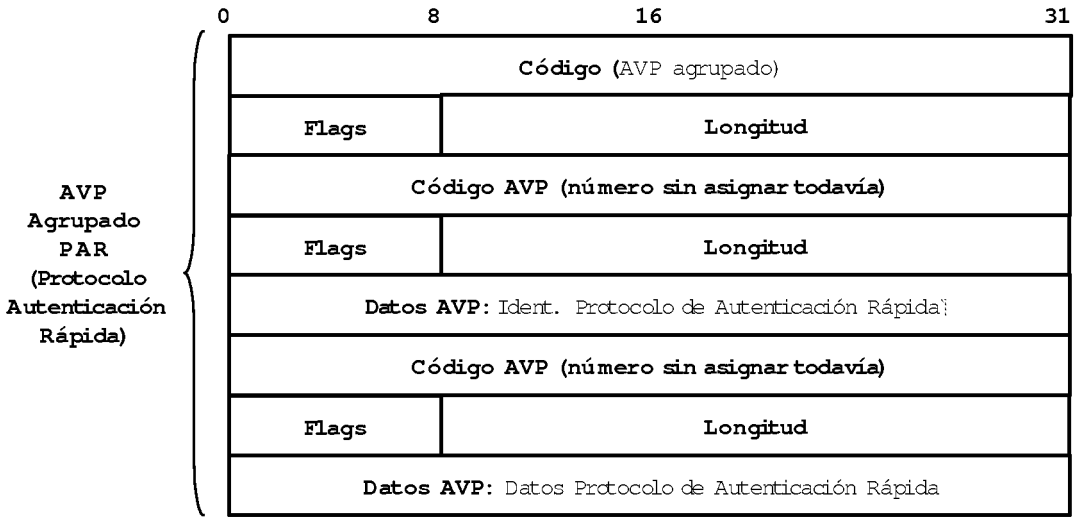

FIG. 6

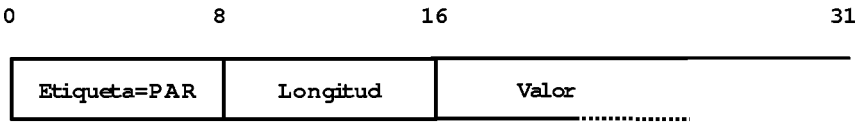

FIG. 7

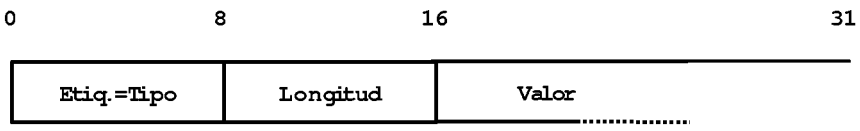

FIG. 8

OFICINA ESPAÑOLA
DE PATENTES Y MARCAS

ESPAÑA

(21) N.º solicitud: 200930015

(22) Fecha de presentación de la solicitud: 27.03.2009

(32) Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TECNICA

(51) **Int. Cl. :** ***H04W12/06*** (2009.01)

DOCUMENTOS RELEVANTES

Categoría	(56) **Documentos citados**	**Reivindicaciones afectadas**
X	"REQUEST FOR COMMENTS (rfc) 5296: EAP Extensions for EAP Re-authentication Protocol (ERP)" NETWORK WORKING GROUP V. NARAYANAN, L. DONDETI AUGUST 2008 http://tools.ietf.org/html/rfc5296.txt	1-5
A	"REQUEST FOR COMMENTS (rfc) 3748: Extensible Authentication Protocol (EAP)" Network Working Group B. ABOBA, L. BLUNK, J. VOLLBRECHT, J. CARLSON, H. LEVKOWETZ JUNE 2004 http://www.ietf.org/rfc/rfc3748.txt	1-5

Categoría de los documentos citados
X: de particular relevancia
Y: de particular relevancia combinado con otro/s de la misma categoría
A: refleja el estado de la técnica
O: referido a divulgación no escrita
P: publicado entre la fecha de prioridad y la de presentación de la solicitud
E: documento anterior, pero publicado después de la fecha de presentación de la solicitud

El presente informe ha sido realizado

☒ para todas las reivindicaciones ☐ para las reivindicaciones nº:

Fecha de realización del informe	**Examinador**	**Página**
10.05.2012	M. Muñoz Sanchez	1/4

Documentación mínima buscada (sistema de clasificación seguido de los símbolos de clasificación)

H04W

Bases de datos electrónicas consultadas durante la búsqueda (nombre de la base de datos y, si es posible, términos de búsqueda utilizados)

INVENES, EPODOC, WPI

Fecha de Realización de la Opinión Escrita: 10.05.2012

Declaración

Novedad (Art. 6.1 LP 11/1986)	Reivindicaciones	1-5	**SI**
	Reivindicaciones		**NO**
Actividad inventiva (Art. 8.1 LP11/1986)	Reivindicaciones		**SI**
	Reivindicaciones	1-5	**NO**

Se considera que la solicitud cumple con el requisito de aplicación industrial. Este requisito fue evaluado durante la fase de examen formal y técnico de la solicitud (Artículo 31.2 Ley 11/1986).

Base de la Opinión.-

La presente opinión se ha realizado sobre la base de la solicitud de patente tal y como se publica.

1. Documentos considerados.-

A continuación se relacionan los documentos pertenecientes al estado de la técnica tomados en consideración para la realización de esta opinión.

Documento	Número Publicación o Identificación	Fecha Publicación
D01	"REQUEST FOR COMMENTS (RFC) 5296: EAP EXTENSIONS FOR EAP RE-AUTHENTICATION PROTOCOL (ERP)"	31.08.2008
D02	REQUEST FOR COMMENTS (RFC) 3748: EXTENSIBLE AUTHENTICATION PROTOCOL (EAP)	30.06.2004

2. Declaración motivada según los artículos 29.6 y 29.7 del Reglamento de ejecución de la Ley 11/1986, de 20 de marzo, de Patentes sobre la novedad y la actividad inventiva; citas y explicaciones en apoyo de esta declaración

Se considera D01 el documento más próximo del estado de la técnica al objeto de la solicitud.

Reivindicaciones independientes

Siguiendo la redacción de la reivindicación 1 el documento D01 (EAP-ER) , divulga un procedimiento de reautenticación rápido que transporta datos de un protocolo de reautenticación, desde un terminal hacia un autenticador mediante una capa de protocolo EAP para que dicho autenticador resuelva autorizar o denegar el acceso a una red de telecomunicaciones. Según el documento D01 se ejecuta este proceso sin añadir la capa adicional reivindicada, diferencia que no produce un efecto técnico resultando solamente una opción de diseño.
Así el documento D01 afecta a la actividad inventiva de la reivindicación 1 según el artículo 8.1 de la Ley de Patentes.

Las reivindicaciones 3,4 y 5 resultan también evidentes para el experto en la materia a la vista del procedimiento reivindicado, al incluir un terminal-cliente, un módulo de autenticación y un servidor que poseen las funcionalidades estrictamente necesarias para la ejecución del procedimiento de la reivindicación 1. Así el documento D01 afecta a la actividad inventiva de las reivindicaciones 3,4 y 5 según el artículo 8.1 de la Ley de Patentes.

Reivindicaciones dependientes

La reivindicación 2 añade solamente el reenvío de la información a un servidor de autenticación como se hace en el documento D01.

Así el documento D01 afecta a la actividad inventiva de la reivindicación 2 según el artículo 8.1 de la Ley de Patentes.