(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 536 104**

(51) Int. CI.:

H04W 12/06 (2009.01)
H04L 29/06 (2006.01)
H04W 76/02 (2009.01)
H04W 4/22 (2009.01)
H04W 76/00 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **12.03.2008 E 08737617 (4)**

(97) Fecha y número de publicación de la concesión europea: **04.03.2015 EP 2119189**

(54) Título: **Sistema y método para autenticación para servicios de emergencia inalámbricos**

(30) Prioridad:

12.03.2007 US 894443 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
20.05.2015

(73) Titular/es:

NOKIA TECHNOLOGIES OY (100.0%)
Karaportti 3
02610 Espoo, FI

(72) Inventor/es:

SREEMANTHULA, SRINIVAS y
BAJKO, GABOR

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Sistema y método para autenticación para servicios de emergencia inalámbricos

Campo de la invención

La presente invención se refiere en general al campo de la comunicación inalámbrica. Más particularmente, la presente invención se refiere a acceder a servicios de emergencia por un dispositivo inalámbrico.

Antecedentes de la invención

Esta sección pretende proporcionar unos antecedentes o contexto para la invención que se indica en las reivindicaciones. La descripción en el presente documento puede incluir conceptos que podrían conseguirse, pero no son necesariamente los que se han concebido o conseguido anteriormente. Por lo tanto, a menos que se indique de otra manera en el presente documento, lo que se describe en esta sección no es la técnica anterior a la descripción y a las reivindicaciones en esta solicitud y no se admite que sea la técnica anterior por inclusión en esta sección.

Para obtener acceso a servicios de emergencia a través de un dispositivo de usuario inalámbrico, tal como un teléfono portátil, el dispositivo de usuario necesita autenticarse a sí mismo con credenciales apropiados para la red y viceversa. En un sistema IEEE 802.11, esto se hace normalmente proporcionando el dispositivo de usuario la identidad de usuario en mensajes de protocolo de autenticación extensible (EAP) encapsulados en mensajes del protocolo 802.1x a un punto de acceso (AP) de red y a continuación desde el AP a un servidor de autenticación mediante uno cualquiera de diversos protocolos, tal como el Servicio de Autenticación Remota de Marcación de Usuario (RADIUS), para fines de autenticación. Después de un intercambio de EAP satisfactorio, se autentica el dispositivo de usuario, y se genera una clave maestra por pares (PMK) mediante el dispositivo de usuario y el AP. Una toma de contacto de 4 vías entre el dispositivo de usuario y el AP genera claves de sesión (claves transitorias por pares, o PTK). Al final del intercambio de EAP y de la toma de contacto de 4 vías, se completa la autenticación de la entidad para permitir la apertura de los puertos controlados 802.1x en el AP. Además, pueden disponerse servicios de gestión de claves para confidencialidad, autenticidad de origen de datos y de detección de reproducción.

El dispositivo de usuario a continuación puede usar la red inalámbrica para iniciar cualquier servicio, incluyendo llamadas de emergencia que proporciona confidencialidad de enlace, usando las claves generadas. Se lleva a cabo un mecanismo similar para autenticación y gestión de claves en otras tecnologías de enlace inalámbrico (por ejemplo, IEEE 802.16e).

Surgen problemas con el mecanismo anteriormente descrito a la luz de una resolución de la Comisión de Comunicaciones Federal de Estados Unidos que indica que el usuario debe poder realizar llamadas de emergencia y conectarse a puntos de respuesta de seguridad pública locales (PSAP) independientemente de la validez de los credenciales de seguridad del usuario. Para permitir llamadas de emergencia desde clientes con credenciales incorrectos o sin credenciales, la red inalámbrica puede elegir para operar una identificación de servicio de sistema de autenticación abierta (SSID) que no requiere credenciales. Sin embargo, en este caso, no existe implicación de derivaciones de clave de sesión y por lo tanto, no se ofrecen características de seguridad debido al mecanismo de gestión de claves como se ha indicado anteriormente.

Como alternativa, la red inalámbrica puede elegir operar una SSID habilitada con seguridad, tal como Acceso Protegido Wifi (WPA) o WAP2 o cualquier otra certificación de seguridad futura de la Alianza WiFi, que requiere la autenticación mediante el uso de algunos identificadores bien conocidos para que los usen los clientes para obtener acceso de emergencia que se usarán para intercambio de EAP para un mecanismo de autenticación a nivel de emergencia. En este caso, sin embargo, puede no ser posible normalizar los identificadores debido a la ausencia de esta responsabilidad en cualquier cuerpo de normas particular. Sin embargo, el uso de los identificadores en solitario no proporciona todas las características de seguridad sino únicamente una autenticación ficticia. Además, es indeseable proporcionar un identificador para los dispositivos de usuario para uso de emergencia antes de la unión o asociación a la red que podría usarse para una autenticación a nivel de emergencia. Por ejemplo, puede no estar disponible la seguridad de enlace, sino únicamente autenticación para acceder a la red. Adicionalmente, para derivación de claves para seguridad de enlace, debe intercambiarse uno de los mecanismos de autenticación específicos como determina el servidor de autenticación. Sin embargo, existe la posibilidad de que el dispositivo móvil no pueda soportar el mecanismo determinado por el servidor de autenticación.

La publicación de solicitud de patente de Estados Unidos 2006/0154645 desvela un método para controlar acceso de red donde se recibe información de identidad desde un dispositivo de comunicaciones en una red. La información de identidad puede indicar un módulo de identidad relacionado con el dispositivo de comunicaciones y asociarse con una red adicional. La información de identidad puede indicar el dispositivo de comunicaciones.

El documento WO 2005/109830 desvela el uso de un nuevo mensaje que contiene una indicación de que es una llamada de emergencia, siendo esta indicación previamente conocida para el dispositivo móvil.

Sumario de la invención

Estas y otras ventajas y características de diversas realizaciones de la presente invención, junto con la organización y manera de operación de las mismas, se harán evidentes a partir de la siguiente descripción detallada cuando se toman junto con los dibujos adjuntos, en los que elementos similares tienen números similares a lo largo de todos los varios dibujos descritos a continuación.

La presente invención está definida mediante las reivindicaciones independientes adjuntas. Se definen ciertos aspectos más específicos mediante las reivindicaciones dependientes.

En una realización, el procesamiento incluye transmitir el identificador a un servidor de autenticación para obtener acceso a los servicios de emergencia de red.

En una realización, la recepción de una comunicación comprende transmitir una solicitud al servidor de información a través de un punto de acceso de red. La comunicación con el punto de acceso de red puede ser de acuerdo con un protocolo IEEE 802.1x.

En una realización, el identificador está asociado con el tipo del identificador a modo de una tupla formada por el identificador y la indicación del tipo.

En una realización, el tipo de identificador se selecciona tal como que está soportado por el dispositivo de usuario.

En una realización, el identificador es un formato de Tipo-Valor-Longitud (TLV). En otra realización, el identificador es un formato de Marco de Descripción de Recursos (RDF).

Estas y otras ventajas y características de diversas realizaciones de la presente invención, junto con la organización y manera de operación de las mismas, se harán evidentes a partir de la siguiente descripción detallada cuando se toman junto con los dibujos adjuntos, en los que elementos similares tienen números similares a lo largo de los varios dibujos descritos a continuación.

Breve descripción de los dibujos

Las realizaciones de la invención se describen haciendo referencia a los dibujos adjuntos, en los que:

La Figura 1 es un diagrama de bloques que ilustra un sistema en el que pueden implementarse las realizaciones de la presente invención;
La Figura 2 ilustra un identificador de dispositivo de usuario de acuerdo con una realización de la presente invención;
La Figura 3 ilustra un identificador de dispositivo de usuario de acuerdo con otra realización de la presente invención;
La Figura 4 ilustra un identificador de dispositivo de usuario de acuerdo con otra realización de la presente invención;
La Figura 5 ilustra un identificador de dispositivo de usuario de acuerdo con otra realización de la presente invención;
La Figura 6 ilustra un intercambio para completar la adquisición de identificador de autenticación de acuerdo con una realización de la presente invención;
La Figura 7 ilustra un intercambio para completar la adquisición de identificador de autenticación de acuerdo con otra realización de la presente invención;
La Figura 8 ilustra un intercambio para proporcionar acceso de servicios de emergencia para el dispositivo de usuario de acuerdo con una realización de la presente invención;
La Figura 9 ilustra un ejemplo para proporcionar acceso de servicios de emergencia al dispositivo de usuario de acuerdo con una realización de la presente invención;
La Figura 10 es un diagrama de vista global de un sistema en el que pueden implementarse diversas realizaciones de la presente invención;
La Figura 11 es una vista en perspectiva de un dispositivo electrónico que puede usarse junto con la implementación de diversas realizaciones de la presente invención; y
La Figura 12 es una representación esquemática de la circuitería que puede incluirse en el dispositivo electrónico de la Figura 11.

Descripción detallada de las diversas realizaciones

Con referencia ahora a la Figura 1, se ilustra un diagrama de bloques de un sistema 100 en el que pueden implementarse realizaciones de la presente invención. Un dispositivo 112 de usuario, tal como un teléfono portátil, asistente digital personal u otro dispositivo tal, está adaptado para comunicarse con un punto 114 de acceso de red a través de un sistema 110 de comunicación. En una realización preferida, la comunicación entre el dispositivo 112 de usuario y el punto 114 de acceso es de acuerdo con un sistema del IEEE 802.11.

El punto 114 de acceso está adaptado para comunicar con un proveedor de información, tal como un servidor 116 de información. El servidor 116 de información es un servidor interno adaptado para gestionar la asignación de identificadores para información de emergencia. La comunicación entre el punto 114 de acceso y el servidor 116 de información puede ser a través de cualquiera de diversos modos de comunicación. El servidor 116 de información puede mantenerse en la red asociado con el punto 114 de acceso o puede estar fuera de la red.

El punto 114 de acceso está adaptado adicionalmente para comunicar con un servidor 118 de autenticación. Como se ha indicado anteriormente, el servidor 118 de autenticación puede ser un servidor RADIUS que controla y gestiona acceso a servicios de emergencia. La comunicación entre el punto 114 de acceso y el servidor 118 de autenticación puede ser a través de cualquiera de diversos modos de comunicación.

De acuerdo con realizaciones de la presente invención, el establecimiento de identificadores ligados a un tipo de autenticación específico puede indicar cualquiera de tipos de autenticación ficticia, abierta o cualquier otra. Esto puede especificarse en cualquier cuerpo de estandarización o publicarse en algún lugar para uso público. Mientras que los sistemas convencionales no proporcionan maneras para que un dispositivo de usuario conozca el mecanismo de autenticación que debe usar el servidor de autenticación hasta que el servidor de autenticación active un mecanismo específico, las realizaciones de la presente invención proporcionan el tipo de tipo de autenticación específica a través del identificador. Específicamente, el uso del identificador de acuerdo con las realizaciones de la presente invención en los mensajes de autenticación proporciona una elección desde el punto de vista del dispositivo de usuario para indicar específicamente al servidor de autenticación usar un mecanismo o algoritmo de autenticación específico.

Las realizaciones de la presente invención implementan un mecanismo de intercambio de información genérico anterior a la asociación o registro. El mecanismo de intercambio de información proporciona información relacionada con uno o más identificadores para que los dispositivos de usuario los usen cuando tienen unos credenciales incorrectos o no tienen credenciales de seguridad. Los identificadores los usan los dispositivos de usuario para autenticación para obtener acceso de red a servicios de emergencia. Este identificador puede usarse en un intercambio de mensaje de EAP con el servidor de autenticación que determina la necesidad para autenticación para uso de emergencia basándose en este identificador. El servidor de autenticación puede devolver un mensaje de éxito que indica una autenticación ficticia sin intercambios de EAP, o puede activar cualquier mecanismo de EAP que pueda obtener adicionalmente información adicional antes de conceder un acceso autenticado ficticio.

En otras realizaciones, este mecanismo y la provisión de un mecanismo de autenticación asociado a cada identificador se usan como una tupla que indica el uso de un identificador para un mecanismo de autenticación específico. Esto puede ser útil en casos donde el dispositivo de usuario soporta un mecanismo de autenticación específico y elije tener una generación de clave de sesión por razones de seguridad de enlace mediante el uso de este identificador particular. Por ejemplo, pueden proporcionarse dos identificadores, uno para autenticación ficticia y uno de seguridad de capa de transporte de EAP (TLS). La autenticación ficticia da como resultado no seguridad de enlace pero la de para EAP TLS puede ser capaz de generación y distribución de MSK/PMK en el cliente y para el punto de acceso, respectivamente, que da como resultado alguna forma de seguridad de enlace.

Haciendo referencia ahora a la Figura 2, se ilustra un identificador de acuerdo con una realización de la presente invención. En esta realización, el identificador se representa en un formato de Tipo-Longitud-Valor (TLV) para incluir el tipo de identificador 122, longitud del valor 124 y la información 126 de valor de identificador. El tipo de identificador 122 usado para autenticación para obtener acceso para uso de emergencia puede tomar el formato de un Identificador de Acceso de Red (NAI), como se define en RFC 2486. El formato TLV es una definición genérica que puede transportarse a través de cualquier mensaje de protocolo (por ejemplo IEEE 802.21 o RADIUS o Diameter).

En otra realización, ilustrada en la Figura 3, un identificador 130 puede representarse en lenguaje de consultas de Marco de Descripción de Recursos (RDF) (por ejemplo, SPARQL). El lenguaje de consultas de RDF puede ser específico para únicamente ciertos protocolos (por ejemplo, IEEE 802.21).

De acuerdo con realizaciones de la presente invención, el identificador puede etiquetarse con un mecanismo de autenticación. Por ejemplo, el identificador puede etiquetarse con un mecanismo de autenticación para formar una tupla aplicable al identificador, como se describe a continuación con referencia a las Figuras 4 y 5.

Las Figuras 4 y 5 ilustran realizaciones en las que el identificador está asociado con un mecanismo de autenticación específico para formar una tupla. Por ejemplo, la Figura 4 ilustra un identificador en formato TLV de una tupla de este tipo. En este caso, el valor del identificador incluye un tipo 146 de autenticación además del valor del código 148 de autenticación. De manera similar, la Figura 5 ilustra una realización de un identificador 150 en formato de lenguaje de consultas de RDF. En este caso, debería indicarse que una tupla puede repetirse para múltiples identificadores. El tipo de autenticación puede ser cualquiera de los tipos de EAP definidos en el registro de EAP mantenido por el Organismo de Asignación de Números Internet (IANA) en: www.iana.org/assignments/eap-numbers.

Haciendo referencia ahora a la Figura 6, se ilustra un intercambio mediante el cual un dispositivo 112 de usuario puede obtener un identificador en un proceso de pre-autenticación de acuerdo con una realización de la presente invención. El dispositivo de usuario se comunica con un punto de acceso a través de una red IEEE 802.11. A través del intercambio ilustrado, un mecanismo de consulta de pre-asociación para dispositivos cliente tal como el dispositivo 112 de usuario puede consultar información desde un servidor interno, tal como el servidor 116 de información. Como se ha indicado anteriormente, el servidor 116 de información puede contactarse mediante el punto 114 de acceso de red a través de cualquier protocolo. En el intercambio, conforme a una solicitud por el dispositivo 112 cliente, el punto 114 de acceso trasmite una consulta al servidor 116 de información, que identifica la información solicitada. La información de respuesta desde el servidor de información incluye el identificador para información de emergencia, que puede transmitirse al dispositivo 112 de usuario mediante el punto 114 de acceso.

La Figura 7 ilustra otra realización de un intercambio mediante el cual un dispositivo 112 de usuario puede obtener un identificador. De manera similar a la realización ilustrada en la Figura 6, el intercambio ilustrado en la Figura 7 incluye una consulta, o una solicitud, desde el punto 114 de acceso al servidor 116 de información. En la realización de la Figura 7, además del identificador, se incluye un tipo de autenticación en la respuesta desde el servidor de información al punto 114 de acceso. Este par de tipo de autenticación se proporciona al dispositivo 112 de usuario usando comunicación IEEE 802.11. Como se ha indicado anteriormente, el servidor de información puede mantenerse localmente en la red y configurarse para proporcionar esta información en coordinación con los mecanismos e identificadores reconocidos por un servidor de autenticación, tal como un servidor RADIUS o un servidor AAA. En una realización, el servidor 116 de información podría ser un mismo servidor RADIUS (u otro servidor de autenticación).

En la Figura 8, se ilustra una realización de un intercambio con el servidor de autenticación mediante el cual se lleva a cabo una autenticación de “emergencia ficticia”. Este intercambio está asociado con el intercambio ilustrado en la Figura 6, que proporciona al dispositivo 112 de usuario con un identificador. De nuevo, la comunicación entre el dispositivo 112 de usuario y el servidor de autenticación es un intercambio IEEE 802.1x. Conforme a una solicitud desde el dispositivo 112 de usuario, el punto 114 de acceso responde al dispositivo 112 de usuario e inicia un intercambio con el servidor de autenticación usando el identificador de autorización proporcionado por el dispositivo 112 de usuario. El servidor de autenticación acepta la autenticación debido al identificador en la Identidad/Respuesta de EAP (encapsulada en EAPOL-Resp), y proporciona la política o reglas de filtrado para el punto 114 de acceso para indicar cómo manejar el tráfico desde este dispositivo 112 de usuario. Después de la autenticación, los puertos 802.1x se abren para uso de llamada de emergencia. En esta realización, el servidor de autenticación únicamente realiza autenticación de acceso sin ningún procedimiento de gestión de claves requerido para aplicaciones de seguridad de enlace. Debido a la ausencia de un PMK, no se activa intercambio de mensajes de 4 vías, en el dispositivo 112 de usuario y en el punto 114 de acceso.

Haciendo referencia ahora a la Figura 9, la autenticación de “emergencia” se lleva a cabo en un intercambio IEEE 802.1x de acuerdo con otra realización de la presente invención. Este intercambio está asociado con el intercambio ilustrado en la Figura 7, que proporciona al dispositivo 112 de usuario con un identificador así como un tipo de autenticación. En la realización de la Figura 9, conforme a una solicitud desde el dispositivo 112 de usuario, el punto 114 de acceso responde al dispositivo 112 de usuario e inicia un intercambio con el servidor 118 de autenticación usando el identificador de autorización proporcionado por el dispositivo 112 de usuario. El servidor 118 de autenticación acepta la autenticación después de realizar algunos intercambios específicos del tipo de autorización. Estos intercambios son debidos al reconocimiento del identificador desde el dispositivo 112 de usuario en la Identidad/Respuesta de EAP (encapsulada en EAPOL-Resp). El intercambio específico del tipo de autorización da como resultado la generación de una clave por pares. Los expertos en la materia apreciarán que tales intercambios de mensaje de autenticación para la generación de clave por pares sin una clave secreta a largo plazo pueden tomar varias formas, cada una de las cuales se contempla en el alcance de la presente invención. El servidor 118 de autenticación proporciona la clave por pares y la política o reglas de filtrado para el punto 114 de acceso para indicar cómo manejar el tráfico desde este cliente. Después de la autenticación, se abren los puertos 802.1x para uso de llamada de emergencia. En la realización de la Figura 9, se activa una toma de contacto de 4 vías a partir de la disponibilidad de PMK para la derivación de PTK que posibilita aplicaciones de seguridad de enlace.

Por lo tanto, las realizaciones de la presente invención proporcionan el uso de identificadores como indicadores para tipos de autenticación específicos a servidores de autenticación para activar mecanismos de autenticación relacionados. No se requiere anunciar los identificadores en la emisión puesto que pueden ser largos y ser un desperdicio de ancho de banda incluirlos en mensajes de difusión. Los identificadores para uso de emergencia no

necesitan normalizarse y pueden configurarlo de manera flexible los proveedores de servicio de red para diversas tecnologías de enlace y proporcionarse en intercambio de información. Además, los identificadores pueden ser aplicables a más de una tecnología de enlace puesto que se identifican en el nivel de servidor de autenticación que puede tener un alcance administrativo para incluir múltiples tecnologías de enlace.

Las realizaciones de la presente invención son transparentes para el punto 114 de acceso y, por lo tanto, no se requieren cambios para la información de difusión de enlace. Además, no son necesarios cambios para la implementación del AP para permitir este mecanismo y puede ser compatible hacia atrás para versiones más antiguas.

Las realizaciones de la presente invención pueden usar mecanismos de autenticación con credenciales incorrectos o sin credenciales que posibilitarían la generación de PMK e intercambio de gestión de claves adicional para derivar claves de sesión por pares. Además, las realizaciones de la presente invención soportan diferentes mecanismos de autenticación para diferentes niveles de características de seguridad mediante el uso de emparejamientos con combinación de mecanismo de identificador y de autenticación. La distribución de esta información antes de la asociación es beneficiosa para permitir al dispositivo 112 de usuario elegir qué identificador y qué mecanismos usar para autenticación en el usuario de emergencia cuando no están disponibles credenciales. El dispositivo 112 de usuario tiene la elección para seleccionar el identificador y, por lo tanto, el mecanismo de autenticación correspondiente.

La Figura 10 muestra un sistema 10 en el que pueden utilizarse diversas realizaciones de la presente invención, que comprende múltiples dispositivos de comunicación que pueden comunicar a través de una o más redes. El sistema 10 puede comprender cualquier combinación de redes cableadas o inalámbricas incluyendo, pero sin limitación, una red de telefonía móvil, una Red de Área Local (LAN) inalámbrica, una red de área personal Bluetooth, una LAN Ethernet, una LAN de anillo con paso de testigo, una red de área extensa, internet, etc. El sistema 10 puede incluir tanto dispositivos de comunicación cableados como inalámbricos.

Para ejemplificación, el sistema 10 mostrado en la Figura 10 incluye una red 11 de telefonía móvil e internet 28. La conectividad a internet 28 puede incluir, pero sin limitación, conexiones inalámbricas de largo alcance, conexiones inalámbricas de corto alcance y diversas conexiones cableadas incluyendo, pero sin limitación, líneas telefónicas, líneas de cable, líneas de alimentación y similares.

Los dispositivos de comunicación ejemplares del sistema 10 pueden incluir, pero sin limitación, un dispositivo 12 electrónico en la forma de un teléfono móvil, una combinación de asistente digital personal (PDA) y teléfono 14 móvil, un PDA 16, un dispositivo 18 de mensajería integrado (IMD), un ordenador 20 de sobremesa, un ordenador 22 portátil, etc. Los dispositivos de comunicación pueden ser fijos o móviles como cuando se llevan por un individuo que se está moviendo. Los dispositivos de comunicación pueden localizarse también en un modo de transporte incluyendo, pero sin limitación, un automóvil, un camión, un taxi, un autobús, un tren, un barco, un avión, una bicicleta, una motocicleta, etc. Algunos o todos los dispositivos de comunicación pueden enviar y recibir llamadas y mensajes y comunicar con proveedores de servicios a través de una conexión 25 inalámbrica a una estación 24 base. La estación 24 base puede conectarse a un servidor 26 de red que permite comunicación entre la red 11 de telefonía móvil e internet 28. El sistema 10 puede incluir dispositivos de comunicación adicionales y dispositivos de comunicación de diferentes tipos.

Los dispositivos de comunicación pueden comunicar usando diversas tecnologías de transmisión incluyendo, pero sin limitación, Acceso Múltiple por División de Código (CDMA), Sistema Global para Comunicación Móvil (GSM), Sistema Universal de Telecomunicaciones Móviles (UMTS), Acceso Múltiple por División en el Tiempo (TDMA), Acceso Múltiple por División en Frecuencia (FDMA), Protocolo de Control de Transmisión/Protocolo de Internet (TCP/IP), Servicio de Mensajería Corta (SMS), Servicio de Mensajería Multimedia (MMS), correo electrónico, Servicio de Mensajería Instantánea (IMS), Bluetooth, IEEE 802.11, etc. Un dispositivo de comunicación implicado en implementar diversas realizaciones de la presente invención puede comunicar usando diversos medios incluyendo, pero sin limitación, radio, infrarrojos, láser, conexión de cable y similares.

Las Figuras 11 y 12 muestran un dispositivo 12 electrónico representativo en el que puede implementarse la presente invención. Debería entenderse, sin embargo, que la presente invención no pretende limitarse a un tipo particular de dispositivo. El dispositivo 12 electrónico de las Figuras 11 y 12 incluye un alojamiento 30, una pantalla 32, en forma de una pantalla de cristal líquido, un teclado numérico 34, un micrófono 36, un auricular 38, una batería 40, un puerto 42 de infrarrojos, una antena 44, una tarjeta 46 inteligente en la forma de una UICC de acuerdo con una realización, un lector 46 de tarjetas, circuitería 52 de interfaz de radio, circuitería 54 de códec, un controlador 56 y una memoria 58. Los circuitos y elementos individuales son todos de un tipo bien conocido en la técnica, por ejemplo en la gama de Nokia de teléfonos móviles.

Diversas realizaciones descritas en el presente documento se describen en el contexto general de etapas o procesos de método, que pueden implementarse en una realización mediante un producto de programa informático, realizado en un medio legible por ordenador, que incluye instrucciones ejecutables por ordenador, tal como código de programa, ejecutadas por ordenadores en entornos en red. Un medio legible por ordenador puede incluir

dispositivos de almacenamiento extraíbles y no extraíbles incluyendo, pero sin limitación, Memoria de Sólo Lectura (ROM), Memoria de Acceso Aleatorio (RAM), discos compactos (CD), discos versátiles digitales (DVD), etc. En general, los módulos de programa pueden incluir rutinas, programas, objetos, componentes, estructuras de datos, etc., que realizan tareas particulares o implementan tipos de datos abstractos particulares. Las instrucciones ejecutables por ordenador, estructuras de datos asociadas y módulos de programa representan ejemplos de código de programa para ejecutar etapas de los métodos desvelados en el presente documento. La secuencia particular de tales instrucciones ejecutables o estructuras de datos asociadas representa ejemplos de actos correspondientes para implementar las funciones descritas en tales etapas o procesos.

Las realizaciones de la presente invención pueden implementarse en software, hardware, lógica de aplicación o una combinación de software, hardware y lógica de aplicación. El software, lógica de aplicación y/o hardware puede residir, por ejemplo, en un conjunto de chips, un dispositivo móvil, un ordenador de sobremesa, un ordenador portátil o un servidor. El software y las implementaciones web de diversas realizaciones pueden conseguirse con técnicas de programación convencionales con lógica basada en reglas y otra lógica para conseguir diversas etapas o procesos de búsqueda de bases de datos, etapas o procesos de correlación, etapas o procesos de comparación y etapas o procesos de decisión. Diversas realizaciones pueden implementarse también completa o parcialmente en elementos o módulos de red. Debería indicarse que las palabras “componente” y “módulo”, como se usan en el presente documento y en las siguientes reivindicaciones, pretenden abarcar implementaciones que usan una o más líneas de código de software y/o implementaciones de hardware y/o equipo para recibir entradas manuales.

La anterior descripción de realizaciones se ha presentado para fines de ilustración y descripción. La anterior descripción no pretende ser exhaustiva o limitar las realizaciones de la presente invención a la forma precisa desvelada, y son posibles modificaciones y variaciones a la luz de las anteriores enseñanzas. Las realizaciones analizadas en el presente documento se eligen y describen para explicar los principios y la naturaleza de diversas realizaciones y su aplicación práctica para posibilitar a un experto en la materia utilizar la presente invención en diversas realizaciones.

REIVINDICACIONES

1. Un método, que comprende:

transmitir una solicitud, incluyendo la solicitud una consulta para información; y
en respuesta, recibir un identificador, y **caracterizado por** que el identificador indica uno o más mecanismos de autenticación para obtener acceso a servicios de emergencia, y
usar dicho identificador para autenticación para obtener acceso de red para servicios de emergencia.

2. El método de acuerdo con la reivindicación 1, en el que el identificador indica el uno o más mecanismos de autenticación a modo de una tupla formada por el identificador y una indicación del uno o más mecanismos de autenticación.

3. El método de acuerdo con la reivindicación 1 o la reivindicación 2, en el que el uno o más mecanismos de autenticación se seleccionan tal como están soportados por un dispositivo de usuario.

4. El método de acuerdo con cualquiera de las reivindicaciones 1 a 3, en el que el identificador indica un tipo de autenticación ficticia, abierta o cualquier otra.

5. El método de acuerdo con cualquiera de las reivindicaciones 1 a 4, en el que el uso comprende transmitir el identificador para recepción por un servidor de autenticación y recibir una autenticación desde el servidor de autenticación basada al menos en parte en el identificador.

6. Un aparato, que comprende:

al menos un procesador; y
al menos una memoria, incluyendo el código de programa informático la al menos una memoria y el código de programa informático configurados para, con el al menos un procesador, hacer que el aparato realice al menos lo siguiente:

transmitir una solicitud, incluyendo la solicitud una consulta para información; y
en respuesta, recibir un identificador,

dicho aparato **caracterizado por** que el identificador indica uno o más mecanismos de autenticación para obtener acceso a servicios de emergencia; y

la al menos una memoria y el código de programa informático están configurados para, con el al menos un procesador, hacer que el aparato use dicho identificador para autenticación para obtener acceso de red para servicios de emergencia.

7. El aparato de acuerdo con la reivindicación 6, en el que el uno o más mecanismos de autenticación se seleccionan tal como están soportados por un dispositivo de usuario.

8. El aparato de acuerdo con la reivindicación 6 o la reivindicación 7, en el que el uso comprende estar configurados adicionalmente la al menos una memoria y el código de programa informático para transmitir el identificador para recepción por un servidor de autenticación y recibir una autenticación desde el servidor de autenticación basada en el identificador.

9. El aparato de acuerdo con cualquiera de las reivindicaciones 6 a 8, en el que el identificador está adaptado para usarse en un intercambio de protocolo de autenticación extensible (EAP) con un servidor de autenticación.

10. Un método, que comprende:

recibir una solicitud que incluye una consulta para información desde un dispositivo de usuario; y
como respuesta transmitir un identificador,
caracterizado por el identificador indica uno o más mecanismos de autenticación para obtener acceso a servicios de emergencia, en donde dicho identificador es para el dispositivo de usuario para autenticación para obtener acceso de red para servicios de emergencia.

11. El método de acuerdo con la reivindicación 10, en el que la solicitud es recibida por un proveedor de información que es al menos uno de un punto de acceso, un servidor de información o un servidor de autenticación.

12. Un aparato, que comprende:

al menos un procesador; y
al menos una memoria, incluyendo el código de programa informático la al menos una memoria y el código de

programa informático configurados para, con el al menos un procesador, hacer que el aparato realice al menos lo siguiente:

recibir una solicitud que incluye una consulta para información desde un dispositivo de usuario; y
con ello transmitir un identificador, estando caracterizado dicho aparato por que el identificador como respuesta indica uno o más mecanismos de autenticación para obtener acceso a servicios de emergencia y dicho identificador es para el dispositivo de usuario para autenticación para obtener acceso de red para servicios de emergencia.

13. El aparato de acuerdo con la reivindicación 12, en el que la solicitud es recibida por un proveedor de información que es al menos uno de un punto de acceso, un servidor de información o un servidor de autenticación.

14. El aparato de acuerdo con la reivindicación 12, en el que el identificador indica un tipo de autenticación ficticia, abierta o cualquier otra.

15. El aparato de acuerdo con cualquiera de las reivindicaciones 12 a 14, en el que el aparato sirve como un punto de acceso, la al menos una memoria y el código de programa configurados adicionalmente para transmitir una solicitud a un proveedor de información para un identificador para el dispositivo de usuario y recibir un identificador desde el proveedor de información, en donde el identificador indica uno o más mecanismos de autenticación para obtener acceso a servicios de emergencia.

16. Un producto de programa informático realizado en un medio legible por ordenador, el programa informático configurado para controlar un procesador para realizar un método, el método de acuerdo con cualquiera de las reivindicaciones 1 a 5 y 10 a 11.

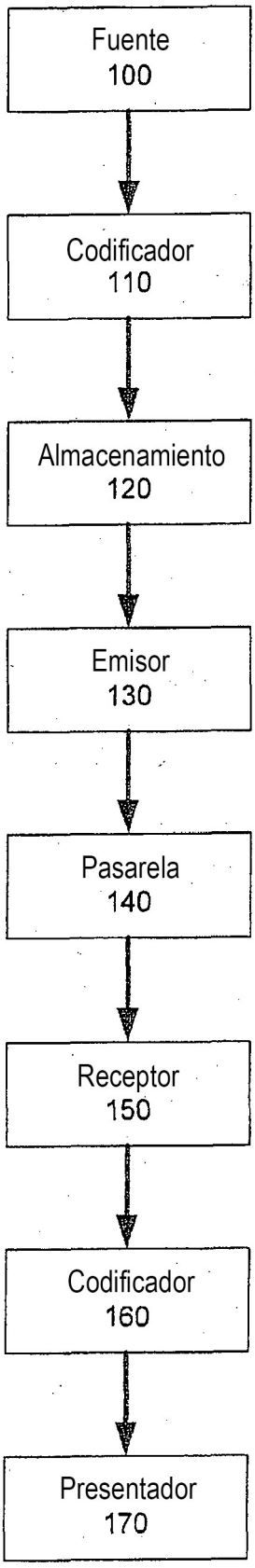
Fuente
100
Codificador
110
Almacenamiento
120
Emisor
130
Pasarela
140
Receptor
150
Codificador
160
Presentador
170

Figura 1

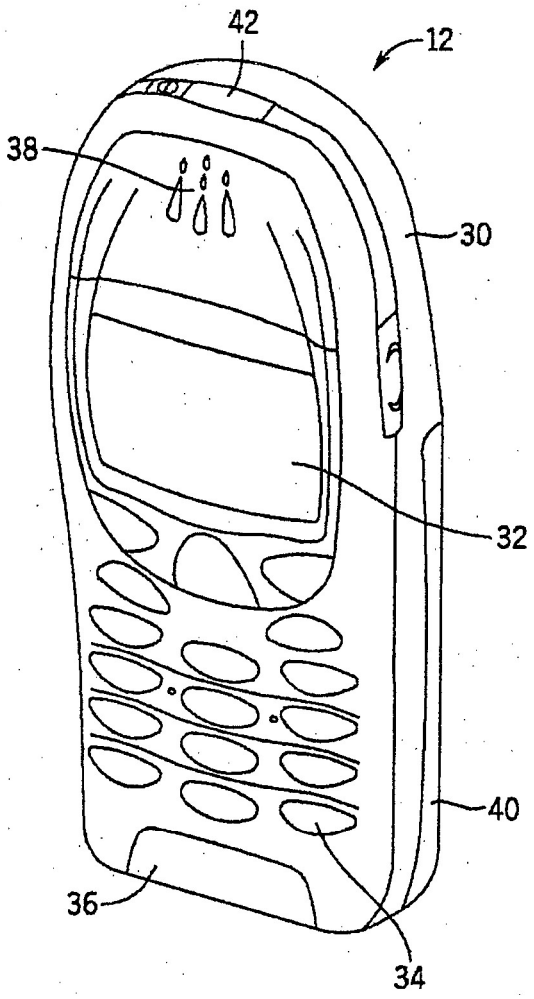

FIGURA 2

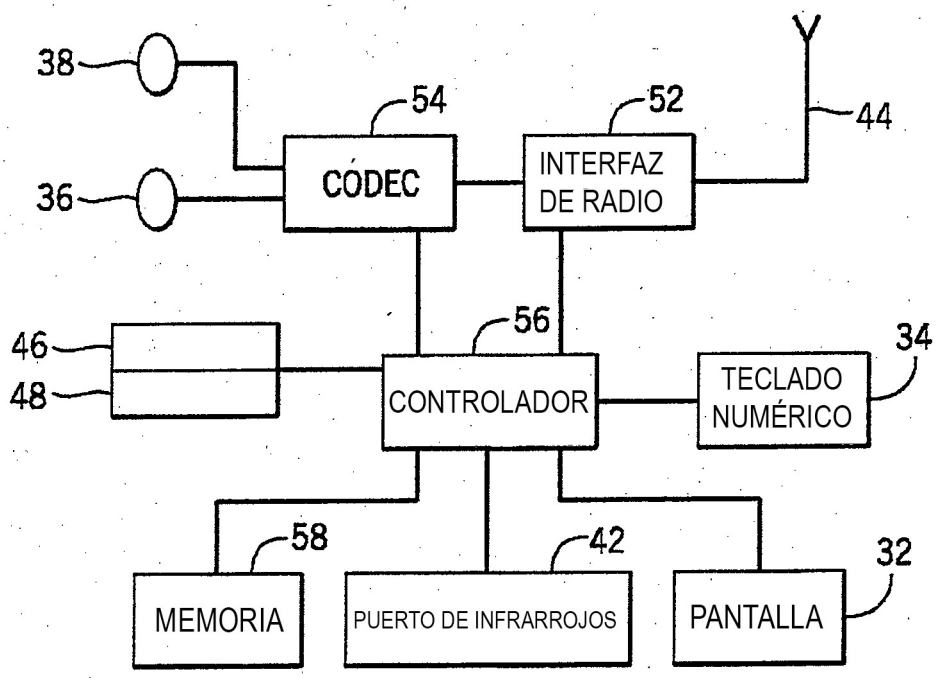
38
36
54
CÓDEC
52
INTERFAZ DE RADIO
44
46
48
56
CONTROLADOR
34
TECLADO NUMÉRICO
58
MEMORIA
42
PUERTO DE INFRARROJOS
32
PANTALLA

FIGURA 3

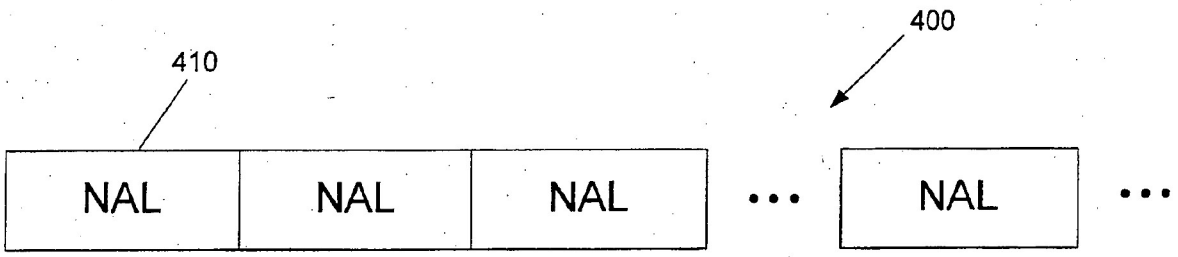

FIGURA 4

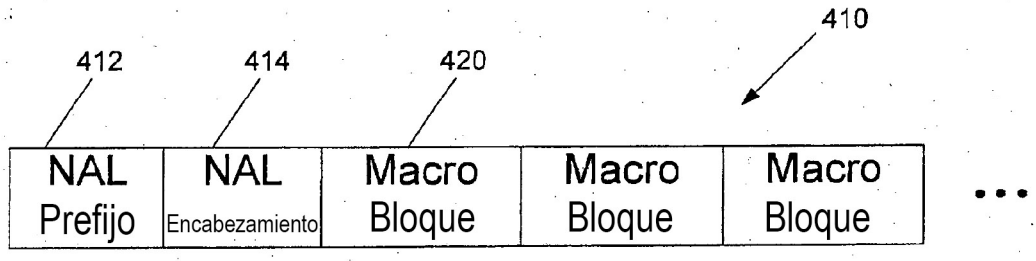

FIGURA 5

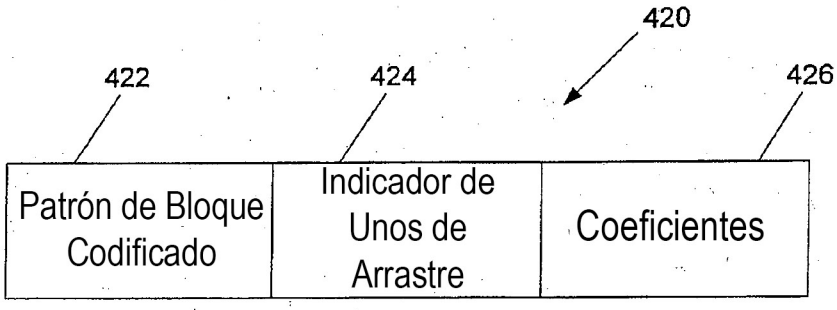

FIGURA 6