(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 488 396**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **25.03.2011 E 11290148 (3)**

(97) Fecha y número de publicación de la concesión europea: **07.05.2014 EP 2503754**

(54) Título: **Autenticación en un sistema de comunicaciones**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.08.2014

(73) Titular/es:

AIRBUS DS SAS (50.0%)
ZAC de la Clef Saint Pierre, 1 Boulevard Jean Moulin
78990 Elancourt, FR y
CASSIDIAN FINLAND OY (50.0%)

(72) Inventor/es:

GRECH, SANDRO y
GRUET, CHRISTOPHE

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Autenticación en un sistema de comunicaciones

Campo

La presente invención se refiere a la autenticación de un aparato en un sistema de comunicaciones.

Antecedentes de la técnica

La siguiente descripción de los antecedentes de la técnica puede incluir ideas, descubrimientos, comprensiones o revelaciones, o asociaciones, junto con descripciones no conocidas en la técnica anterior pertinente a la presente invención, pero proporcionados por la invención. Algunas de dichas contribuciones de la invención pueden ser destacadas específicamente más adelante, mientras que otras de dichas contribuciones de la invención serán evidentes a partir de su contexto.

Una de las características principales de los sistemas de telecomunicaciones, especialmente en los sistemas de telecomunicaciones inalámbricas, es la autenticación de un usuario para prevenir un acceso ilegal. La autenticación es un procedimiento en el cual una parte autentica la otra parte según un procedimiento acordado que se basa, típicamente, en contraseñas y/o claves, y que puede ser transparente para el usuario. En las redes móviles, los mecanismos de acceso de seguridad de red incluyen una autenticación mutua de un usuario o, más específicamente, un módulo de identidad de abonado usado por el usuario con un terminal que proporciona interfaces de red, y una red, y la autenticación se basa, típicamente, en un mecanismo basado en pregunta-respuesta que usa criptografía simétrica. En el mecanismo, una clave secreta es almacenada, de manera permanente, en un módulo de identidad de abonado y en un centro de autenticación del entorno doméstico del abonado (red doméstica), en el que la clave raíz permanente es una clave raíz usada por el módulo de identidad de abonado y el centro de autenticación como una entrada en diferentes algoritmos, tal como el cálculo de una respuesta de autenticación, una clave de encriptación, una clave de integridad y/o una clave de anonimato, por ejemplo, en la fase de autenticación. La clave raíz permanente nunca es transmitida pero el centro de autentificación puede calcular un cierto número de vectores de autenticación con los que puede realizarse la autenticación en una red que proporciona servicio al dispositivo del usuario (y, por lo tanto, al usuario), sin la implicación del centro de autenticación tantas veces como vectores de autenticación existentes.

Puede ocurrir que la autenticación sea imposible debido a que la conexión con el centro de autenticación se ha perdido debido a un fallo en la red, y no hay vectores de autentificación disponibles en la red de servicio. En esta situación, el único servicio disponible es una llamada a un centro de emergencia. Sin embargo, hay situaciones en las que sería útil disponer de un servicio un poco más amplio, por ejemplo, una llamada entre dos o más equipos de usuario en la misma red de acceso de radio.

El documento WO 2008/031926 se refiere a una radio móvil profesional denominada Terrestrial Trunked Radio (TETRA), en la que las estaciones móviles pueden comunicarse en un modo directo, es decir, directamente entre sí, o usando la infraestructura truncada denominada infraestructura de conmutación y de gestión (Switching and Management Infrastructure, SwMI). El documento WO 2008/031926 describe una estación móvil que tiene, además de un equipo móvil real, al menos dos módulos de identidad de abonado separados. Un módulo de abonado desconectable y el equipo móvil real pueden autenticarse entre sí por medio de una clave de sistema fuera de servicio almacenada en los módulos de abonado y en el equipo móvil real para propósitos de autenticación entre el módulo de abonado y el equipo móvil real cuando se va a usar un modo directo (un modo en el que la infraestructura truncada no está implicada en la comunicación), o la infraestructura truncada de servicio no está disponible. Si la autenticación con la clave de sistema fuera de servicio tiene éxito, una estación móvil que comprende el módulo de abonado y el equipo móvil real puede formar una conexión directa a otra estación móvil. Sin embargo, esa solución permite sólo llamadas entre estaciones móviles que están suficientemente cerca entre sí de manera que puedan comunicarse directamente entre sí sin el uso de recursos de la red.

El documento WO 2009/045895 describe un procedimiento para autenticar un dispositivo cliente a una red, de manera que la red selecciona un protocolo de autenticación compatible con el dispositivo cliente.

Sumario

De esta manera, un objeto de la presente invención es proporcionar un procedimiento y un aparato para implementar el procedimiento para proporcionar un conjunto restringido de servicios de red si la red no está disponible para la autenticación convencional. El objeto de la invención se consigue mediante procedimientos, un aparato, un producto de programa de ordenador y un sistema que se caracterizan por las afirmaciones en las reivindicaciones independientes. Las realizaciones preferidas de la invención se describen en las reivindicaciones dependientes.

Un aspecto de la invención proporciona, además de un secreto compartido permanente, que sólo está disponible para el módulo de identidad de abonado de un usuario y un centro de autenticación en el entorno doméstico del usuario, un secreto compartido adicional disponible en la red de acceso y en el módulo de identidad de abonado para la autenticación del usuario para el uso restringido de la red de acceso, cuando la autenticación basada en el secreto compartido permanente, es decir, la autenticación convencional, no está disponible.

Una ventaja de la invención es que proporciona un mecanismo para un acceso restringido a una red de acceso para los usuarios con derecho sin poner en riesgo (comprometer) el secreto compartido permanente.

Breve descripción de los dibujos

A continuación, las realizaciones se describirán en mayor detalle con referencia a los dibujos adjuntos, en los cuales

La Figura 1 muestra una arquitectura simplificada de un sistema según una realización;

Las Figuras 2 y 3 son diagramas de bloques de un aparato según las realizaciones;

Las Figuras 4 a 9 son diagramas de flujo que ilustran diferentes realizaciones; y

La Figura 10 es un diagrama de señalización según una realización.

Descripción detallada de algunas realizaciones

Las siguientes realizaciones son ejemplares. Aunque la especificación puede hacer referencia a "un", "una" o "alguna" realización o realizaciones en diversas ubicaciones, esto no significa necesariamente que cada una de dichas referencias corresponda a la misma realización o realizaciones, o que la característica sólo se aplique a una única realización. Las características individuales de las diferentes realizaciones pueden ser combinadas también para proporcionar otras realizaciones.

La presente invención es aplicable a cualquier equipo de usuario, nodo de punto de acceso, componente correspondiente y/o a cualquier sistema de comunicaciones o cualquier combinación de diferentes sistemas de comunicaciones que soportan la autenticación de usuario por medio de un secreto compartido. El sistema de comunicación puede ser un sistema de comunicación fijo o un sistema de comunicación inalámbrico o un sistema de comunicación que utiliza tanto redes fijas como redes inalámbricas. Los protocolos usados, las especificaciones de los sistemas de comunicación, los nodos de punto de acceso y los equipos de usuario, especialmente en la comunicación inalámbrica, se desarrollan rápidamente. Dicho desarrollo puede requerir cambios adicionales para una realización. Por lo tanto, todas las palabras y expresiones deberían ser interpretadas en un sentido amplio y pretenden ilustrar, no restringir, la realización.

En adelante, las diferentes realizaciones se describirán usando, como un ejemplo de una arquitectura de sistema en la que pueden aplicarse las realizaciones, una arquitectura basada en la evolución de sistema de arquitectura (System Architecture Evolution, SAE), especificada en 3GPP (Third Generation Partnership Project, Proyecto de Asociación de Tercera Generación), sin restringir la realización a dicha arquitectura, sin embargo. Otros ejemplos de arquitectura de sistema incluyen WiMax, WiFi, 4 G (cuarta generación) y acceso inalámbrico móvil de banda ancha (Mobile Broadband Wireless, Access, MBWA), iBurst, Flash-OFDMA, IPW, TETRA, 3 G (tercera generación).

Una arquitectura general de un sistema de comunicación que proporciona autenticación basada en secretos compartidos se ilustra en la Figura 1. La Figura 1 es una arquitectura de sistema simplificada que sólo muestra algunos elementos y entidades funcionales, todas ellas unidades lógicas cuya implementación puede ser diferente de la mostrada. Las conexiones mostradas en la Figura 1 son conexiones lógicas; las conexiones físicas reales pueden ser diferentes. Es evidente para una persona con conocimientos en la materia que los sistemas comprenden también otras funciones y estructuras. Debería apreciarse que las funciones, las estructuras, los elementos y los protocolos usados en o para la comunicación de grupo, son irrelevantes para la invención actual. Por lo tanto, no necesitan ser descritos más detalladamente en la presente memoria.

En la realización ilustrada en la Figura 1, el sistema 100 comprende una red 101 de acceso de radio que proporciona acceso al sistema para los equipos de usuario (User Equipment, UE) 300 y 300' por medio de nodos 200 y 200' de punto de acceso, una red 102 central, y un entorno 300 doméstico.

La red central comprende una entidad 121 de gestión de seguridad de acceso (Access Security Management Entity, ACME). La ACME representa aquí cualquier servidor de autenticación que está configurado para recuperar vectores de autenticación desde un centro 131 de autenticación (Authentication Centre, AuC) ubicado en el entorno

103 doméstico del equipo de usuario a ser autenticado. Los ejemplos de ACME incluyen una entidad de gestión de movilidad (Mobility, Management Entity, MME), un registro de localización de visitantes, o nodo de red correspondiente, un nodo de pasarela de servicio por paquetes, y una entidad de conmutación. El equipo de usuario es autenticado por medio de vectores de autenticación desechables calculados por el centro de autentificación usando el secreto compartido y, durante la autenticación, el equipo de usuario calcula las respuestas usando el secreto compartido.

El nodo 200 y 200' de punto de acceso descrito más detalladamente con la Figura 2, puede ser cualquier aparato de cálculo configurado para proporcionar acceso de los equipos de usuario a los servicios de la red central. Los ejemplos de dichos dispositivos incluyen una estación base, un nodo B, un nodo B evolucionado, una estación base multiestándar y un punto de acceso inalámbrico.

El equipo 300 y 300' de usuario, descrito más detalladamente con la Figura 3, puede ser cualquier aparato de cálculo que consiste en un módulo de identidad de abonado (Subscriber Identity Module, SIM) 301 y 301', o información correspondiente, para la identificación de un usuario (o del que ha realizado la suscripción para el usuario), y el terminal 302 y 302' real, que es un equipo o un dispositivo que asocia, o está dispuesto para asociar, el terminal y su usuario con una suscripción y permite a un usuario interactuar con un sistema de comunicaciones. El terminal presenta información al usuario y permite al usuario introducir información. En otras palabras, el terminal de usuario puede ser cualquier aparato o una combinación de diversos aparatos capaz de recibir información desde y/o transmitir información a la red, que puede conectarse a la red inalámbricamente o mediante una conexión fija. El módulo de identidad de abonado incluye los algoritmos y los secretos necesarios en la autenticación y puede incluir además información relacionada con la identificación del abonado, tal como una identidad de abonado móvil internacional (International Mobile Subscriber Identity, IMSI) y una identidad de abonado móvil temporal (Temporary Mobile Subscriber Identity, TMSI) del área de ubicación por medio de los cuales puede evitarse la transmisión de la IMSI a través de la ruta de radiocomunicaciones. El módulo de identidad de abonado, en el que está almacenada la información requerida, puede estar integrado en el terminal, en cuyo caso la información requerida puede ser almacenada en la memoria del terminal. Frecuentemente, sin embargo, el módulo de identidad de abonado se encuentra en un circuito separado a ser conectado/fijado, de manera desconectable, al terminal. Los ejemplos de dichos módulos de identidad de abonado se denominan tarjetas SIM (tarjetas inteligentes) en las que se almacena la información requerida, una tarjeta de interfaz de red y un módem USB (un adaptador o “dongle”). En la presente memoria "equipo de usuario" UE se refiere, en general, a la entidad formada por el módulo de identidad de abonado que identifica al usuario y el terminal real. Los ejemplos de equipos de usuario incluyen un terminal de usuario o estación de trabajo, tal como un ordenador portátil, un netbook, un teléfono inteligente, un ordenador personal, un dispositivo Tablet PC, un dispositivo de lectura electrónica o un asistente digital personal (PDA).

En el ejemplo ilustrado, se supone que los equipos de usuario tienen el mismo entorno doméstico, que no es siempre el caso, y ambos tienen un secreto K1 y K1' compartido diferente para la autenticación convencional, almacenado en la tarjeta SIM 301 y 301' correspondiente y en el centro de autenticación. En adelante, este secreto compartido se denomina clave raíz permanente. Tal como se ha descrito anteriormente, la clave raíz permanente nunca se transmite. Además, en el ejemplo ilustrado, los nodos de punto de acceso y los equipos de usuario (en el ejemplo ilustrado, la tarjeta SIM) comprenden otro secreto K2 compartido, denominado, en adelante, clave raíz adicional, que puede ser usado en lugar de K1 en un procedimiento de autenticación, es decir, como una clave raíz, tal como se describirá más adelante. Las claves son intercambiables, es decir, no se necesitan modificaciones en los algoritmos y los procedimientos de autenticación. En el ejemplo, la clave K2 raíz adicional es la misma para todos, y se almacena en la tarjeta SIM al mismo tiempo que K1 y K1’ y se almacena en una memoria segura de un nodo 200, 200’ de punto de acceso cuando se fabrica, por ejemplo, o se transmite de manera segura sobre la red al nodo de punto de acceso, cuando se hace uso del nodo de punto de acceso, sin restringir la realización a dichas soluciones. Dependiendo de una implementación (y realización), K2 puede ser única para cada UE, o un grupo de UEs, al igual que para todos los UEs servidos por un nodo de punto de acceso, o un grupo de nodos de punto de acceso. K2 puede ser reinicializado por el equipo de usuario o el nodo de punto de acceso, y distribuido a la otra parte si hay un canal seguro fijo/inalámbrico entre las partes (por ejemplo, durante una conexión previa en la que se usó la autenticación convencional basada en clave raíz permanente o usando un canal secundario seguro de otro sistema, tal como WiFi), descargado desde el equipo de usuario o el nodo de punto de acceso a la otra parte a través del canal seguro. Si el nodo de punto de acceso obtiene la clave K2 segura adicional desde el equipo de usuario, el nodo de punto de acceso puede distribuir la clave K2 segura adicional a otros nodos de punto de acceso, como parte de un procedimiento de traspaso, por ejemplo. También es posible combinar los procedimientos descritos anteriormente, por ejemplo, almacenando, durante la fabricación, un valor inicial a K2 y, a continuación, sobreescribirlo con una clave raíz adicional después de una primera autenticación convencional exitosa. Además, el lado de la red puede estar dispuesto para renovar K2 según una política de seguridad predeterminada, por ejemplo, usando una renovación basada en el tiempo. De esta manera, no hay restricciones relativas al aprovisionamiento y actualización de K2, siempre que sean fiables y garanticen

que un tercero no obtenga información de manera ilegal acerca de K2.

La Figura 2 ilustra un diagrama de bloques ejemplar de un aparato que proporciona una funcionalidad de nodo de punto de acceso. En aras de la claridad, el aparato, o un componente correspondiente, se denomina en la presente memoria nodo de punto de acceso. El nodo 200 de punto de acceso es un dispositivo de computación que comprende, no sólo los medios de la técnica anterior, sino también medios para la implementación de la funcionalidad de nodo de punto de acceso descrita con una realización y puede comprender medios separados para cada función separada, o los medios pueden configurarse para realizar dos o más funciones, e incluso para combinar las funciones de las diferentes realizaciones. Estos medios pueden ser implementados mediante diversas técnicas. Por ejemplo, los medios pueden ser implementados en hardware (uno o más aparatos), firmware (uno o más aparatos), software (uno o más módulos), o sus combinaciones. Para un firmware o software, la implementación puede ser mediante unidades/módulos (por ejemplo, procedimientos, funciones, etc.) que realizan las funciones descritas en la presente memoria.

En otras palabras, el nodo 200 de punto de acceso está configurado para realizar una o más de las funcionalidades de cliente descritas más adelante con una realización, y puede ser configurado para realizar funciones de diferentes realizaciones. Para este propósito, el cliente ejemplar ilustrado en la Figura 2 comprende una unidad 21 de detección de modo (decU), una unidad 22 de autenticación (a-U), y al menos una memoria 23 para almacenar una o más (dependiendo de una aplicación) claves K2 raíz adicionales que pueden usarse en lugar de la clave raíz permanente en un modo aislado. El modo aislado significa aquí que la autenticación convencional por medio de la clave raíz no está disponible debido a un fallo del sistema, por ejemplo debido a un fallo de enlace o un fallo de programa o una situación de sobrecarga. Por ejemplo, en el modo aislado, la conexión a ACME puede perderse o es posible que ACME no contenga los vectores de autenticación y haya perdido la conexión con la AuC y, por lo tanto, no pueda obtener más vectores de autenticación y, como consecuencia, no pueda autenticar al usuario. En otras palabras, en el modo aislado la ACME no está disponible para los propósitos de autenticación. En el ejemplo ilustrado, la unidad 22 de autenticación es activada, cuando la unidad 21 de detección de modo detecta un modo aislado, y se desactiva, cuando la unidad 21 de detección de modo detecta de nuevo un modo normal. En la presente memoria, el modo normal significa un modo en el que la autenticación convencional está disponible. Cuando está activada, la unidad 22 de autenticación está configurada para autenticar a los usuarios por medio de la clave raíz adicional, tal como se describirá más detalladamente a continuación, con las Figuras 4 a 6 y 10. La unidad 21 de detección de modo puede ser configurada para detectar los modos por medio de comprobaciones de estado de conexión convencionales, tales como el envío periódico de mensajes tales como "hello" o "alive" y esperando las respuestas durante un tiempo predeterminado.

Además, el nodo de punto de acceso puede comprender otras unidades, tales como una unidad de obtención de clave (no mostrada en la Figura 2) configurada para obtener una clave raíz adicional, si es necesario, y que comprende diferentes unidades de interfaz, tales como una o más unidades 24 de recepción para recibir diferentes entradas, información de control, solicitudes y respuestas, por ejemplo, y una o más unidades 25 de transmisión para enviar diferentes salidas, información de control, respuestas y solicitudes, por ejemplo. Cada una de entre la unidad de recepción y la unidad de transmisión proporciona una interfaz en el nodo de punto de acceso, en el que la interfaz incluye un transmisor y/o un receptor o unos medios correspondientes para la recepción y/o la transmisión de información, y la realización de las funciones necesarias para que el contenido, la información de control, etc., puedan ser recibidos y/o transmitidos. Las unidades de recepción y de envío pueden comprender un conjunto de antenas, cuyo número no está limitado a ningún número en particular.

Dependiendo de la implementación, el nodo de punto de acceso puede estar configurado o no para realizar un procedimiento correspondiente a una re-autenticación desencadena por red que es desencadenada a intervalos predeterminados en un modo normal.

Debería apreciarse que la funcionalidad ACME puede ser proporcionada por un nodo que controla el nodo de punto de acceso, tal como un controlador de red de radio o un controlador de estación base, o que la funcionalidad de nodo de punto de acceso relacionada con la autenticación puede ser realizada por el nodo que controla el nodo de punto de acceso.

La Figura 3 ilustra un diagrama de bloques ejemplar de un aparato que proporciona una funcionalidad de equipo de usuario. En aras de la claridad, el aparato, o una combinación de aparatos/dispositivos, se denomina en la presente memoria equipo de usuario. El equipo de usuario es un dispositivo de computación que comprende no sólo medios de la técnica anterior, sino también medios para la implementación de la funcionalidad de equipo de usuario descrita con una realización y puede comprender medios separados para cada función separada, o los medios pueden ser configurados para realizar dos o más funciones, e incluso para combinar funciones de diferentes realizaciones. Estos medios pueden ser implementados mediante diversas técnicas. Por ejemplo, los medios pueden ser implementados en hardware (uno o más aparatos), firmware (uno o más aparatos), software

(uno o más módulos), o su combinaciones. Para un firmware o software, la implementación puede ser mediante unidades/módulos (por ejemplo, procedimientos, funciones, etc.) que realizan las funciones descritas en la presente memoria.

En otras palabras, el equipo de usuario está configurado para realizar una o más de las funcionalidades de equipo de usuario descritas más adelante con una realización, y puede ser configurado para realizar funciones de diferentes realizaciones. Para este propósito, el equipo de usuario ejemplar ilustrado en la Figura 3 comprende una unidad 31 de supervisión de modo de red (trackU), una unidad 32 de autenticación (aut-T), y al menos una memoria 33 para almacenar al menos una clave K1 raíz permanente, disponible sólo para el módulo de identidad de abonado del usuario y un centro de autenticación en el entorno doméstico del usuario, y la clave K2 raíz adicional y la información de modo. En el ejemplo ilustrado, se supone que el modo es aislado y que se denota mediante i en la memoria 33. Debería apreciarse que la manera en la que se indica la información del modo depende de la implementación y puede usarse cualquier medio para ello. Por ejemplo, la falta de información puede indicar un modo normal. La unidad 31 de supervisión de modo de red está configurada para recibir en un canal de difusión la información acerca del nodo de red y mantener en la memoria información acerca del modo de red actual para la unidad 32 de autenticación, tal como se describirá en detalle, más adelante, con las Figuras 7 a 10.

El equipo de usuario comprende también otras unidades, tal como una unidad de obtención de clave (no mostrada en la Figura 3) configurada para obtener una clave raíz adicional, si es necesario, y que comprende diferentes unidades de interfaz, tales como una interfaz 36 de usuario, y una unidad 34 de recepción para recibir diferentes entradas, información de control, solicitudes y respuestas, por ejemplo, y una unidad 35 de transmisión para enviar diferentes salidas, información de control, respuestas y solicitudes, por ejemplo. Cada una de entre la unidad de recepción y la unidad de transmisión proporciona una interfaz en el equipo de usuario, en el que la interfaz incluye un transmisor y/o un receptor o unos medios correspondientes para la recepción y/o transmisión de información, y la realización de funciones necesarias de manera que el contenido, información de control, etc., puedan ser recibidos y/o transmitidos. Las unidades de recepción y de envío pueden comprender un conjunto de antenas, cuyo número no está limitado a ningún número en particular.

Cada una de las unidades en el nodo de punto de acceso y/o en el equipo de usuario puede ser una unidad separada o integrada con otra unidad, o las unidades pueden estar integradas entre sí. Debería apreciarse que el nodo de punto de acceso y el equipo de usuario pueden comprender otras unidades usadas en o para la comunicación. Sin embargo, son irrelevantes para la invención actual y, por lo tanto, no necesitan ser descritas más detalladamente en la presente memoria.

El nodo de punto de acceso, el equipo de usuario y los aparatos correspondientes que implementan la funcionalidad o algunas funcionalidades según una realización puede incluir generalmente un procesador (no mostrado en las Figuras 2 y 3), un controlador, una unidad de control, un micro-controlador, o similares conectados a una memoria y a diversos interfaces del aparato. Generalmente, el procesador es una unidad central de procesamiento, pero el procesador puede ser un procesador de operación adicional. La unidad 21 de detección de modo y/o la unidad 22 de autenticación y/o la unidad 31 de supervisión de modo de red y/o la unidad 32 de autenticación pueden estar configuradas como un ordenador o un procesador, o un microprocesador, tal como un elemento de computación de un único chip, o como un como un conjunto de circuitos integrados “chipset”, que incluye al menos una memoria para proporcionar un área de almacenamiento usada para una operación aritmética y un procesador de operación para la ejecución de la operación aritmética. La unidad 21 de detección de modo y/o la unidad 22 de autenticación y/o la unidad 31 de supervisión de modo de red y/o la unidad 32 de autenticación pueden comprender uno o más procesadores de ordenador, circuitos integrados de aplicación específica (ASIC), procesadores de señal digital (DSP), dispositivos de procesamiento de señales digitales (DSPD), dispositivos lógicos programables (PLD), arreglos de compuertas programables en campo (FPGA) y/u otros componentes de hardware que han sido programados de manera que realicen una o más funciones de una o más realizaciones. Una realización proporciona un programa informático incorporado en cualquier medio de almacenamiento o unidad o unidades de memoria de datos/distribución, legible por el cliente, o artículo o artículos de fabricación, que comprende instrucciones de programa ejecutables por uno o más procesadores/ordenadores, cuyas instrucciones, cuando se cargan en un aparato, constituyen la unidad 21 de detección de modo y/o la unidad 22 de autenticación y/o la unidad 31 de supervisión de modo de red y/o la unidad 32 de autenticación. Los programas, denominados también productos de programa, que incluyen rutinas de software, fragmentos de programas que constituyen "bibliotecas de programa", subprogramas (“applets”) y macros, pueden ser almacenados en cualquier medio, y pueden ser descargados a un aparato. El medio de almacenamiento de datos o la unidad de memoria puede estar implementado dentro del procesador/ordenador o fuera del procesador/ordenador, en cuyo caso puede acoplarse comunicativamente al procesador/ordenador a través de diversos medios, tal como se conoce en la técnica.

La memoria puede ser memoria volátil y/o no volátil, por ejemplo EEPROM, ROM, PROM, RAM, DRAM, SRAM,

firmware, lógica programable, transistor de efecto de campo de doble puerta flotante, etc., y típicamente almacena contenido, datos o similares, y la memoria puede almacenar también otra información para la autenticación diferente de una o más claves raíz, o secreto compartido correspondiente, tal como información acerca del modo de red actual o información almacenada temporalmente. Además, la memoria puede almacenar código de programa de ordenador, tal como aplicaciones de software (por ejemplo, para la unidad de edición o la unidad de publicación de datos) o sistemas operativos, información, datos, contenidos o similares para que el procesador realice las etapas asociadas con el funcionamiento del nodo de punto de acceso y/o el equipo de usuario según las realizaciones. La memoria puede ser, por ejemplo, memoria de acceso aleatorio, una unidad de disco duro, otra memoria de datos fija o dispositivo de almacenamiento o cualquier combinación de los mismos. Además, la memoria, o parte de la misma, puede ser una memoria extraíble conectada, de manera desconectable, al nodo de punto de acceso y/o al equipo de usuario.

Aunque el nodo de punto de acceso y el equipo de usuario han sido representados como una unidad, diferentes procesadores, controladores, interfaces y/o memorias pueden ser implementados en una o más unidades físicas o lógicas.

Las Figuras 4 y 5 ilustran la funcionalidad de un nodo de punto de acceso según una realización en la que los procedimientos ilustrados se ejecutan en paralelo.

En la etapa 401, el nodo de punto de acceso supervisa si una conexión a una red central está disponible o no para propósitos de autenticación, es decir, si la conexión se ha perdido o no. Si no se ha perdido (es decir, está disponible), el nodo de punto de acceso difunde, en la etapa 402, como parte de una información de sistema o de red en un canal de control de difusión, una indicación de que el nodo de punto de acceso está en un modo normal, y continúa la supervisión (etapa 401).

Si se ha perdido la conexión (etapa 401), es decir, la conexión para el nodo de red central no está disponible para los propósitos de autenticación, el nodo de punto de acceso establece, en la etapa 403, el modo a un modo aislado, y difunde, en la etapa 404, una indicación de que el nodo de punto de acceso está en un modo aislado. En otras palabras, la difusión de la etapa 402 es sustituida por la difusión de la etapa 403. A continuación, el nodo de punto de acceso supervisa, en la etapa 405, si la conexión se ha restaurado o no. Si no, el nodo de punto de acceso pasa a la etapa 404 para difundir información acerca del modo aislado. Si la conexión se ha restaurado (etapa 405), el nodo de punto de acceso establece, en la etapa 406, el modo al modo normal y, si se ha realizado algún tipo de autenticación durante el modo aislado (etapa 407), la información sobre la autenticación o autenticaciones es enviada, en la etapa 408, a la ACME de manera que pueda desencadenar una re-autenticación, si es necesario. A continuación, el procedimiento pasa a la etapa 401 para supervisar la conexión. Si no se realizó ninguna autenticación durante el modo aislado (etapa 407), el procedimiento pasa directamente a la etapa 401 para supervisar la conexión.

La indicación en la difusión puede ser un bit que, cuando está activado, indica el modo aislado y, cuando está inactivado, indica el modo normal, o viceversa.

En algunas otras realizaciones, si hay equipos de usuario autenticados durante el modo aislado, el nodo de punto de acceso puede estar configurado para realizar una autodesconexión con respecto a los mismos antes o después de la etapa 408, o en lugar de ella.

La Figura 5 ilustra una situación en la que el nodo de punto de acceso detecta, en la etapa 501, una solicitud que desencadena la autenticación del usuario. La solicitud puede ser una solicitud de conexión “attach” o de conectividad PDN (red de datos por paquetes) la conectividad, por ejemplo. Por lo tanto el nodo de punto de acceso comprueba, en la etapa 502, si el modo es o no el modo normal. Si el modo es el modo normal, el nodo de punto de acceso reenvía, en la etapa 503, la solicitud (en ese caso, la autenticación es transparente para el nodo de punto de acceso).

Si el modo no es normal, está aislado (etapa 502), y el nodo de punto de acceso autentica, en la etapa 504, el usuario usando la clave K2 raíz adicional. Tal como se ha descrito anteriormente, la autenticación se realiza usando los mismos procedimientos y algoritmos que con la clave K1 raíz permanente, excepto que el propio nodo de punto de acceso usa la información en el vector de autenticación sin enviarlo a otros nodos de la red. Es posible que solo se genere un vector de autenticación cuando se usa la clave K2 raíz adicional. Un ejemplo de un procedimiento de autenticación es un procedimiento de autenticación SAE. En el procedimiento de autenticación SAE, un vector de autenticación comprende los componentes siguientes; un número aleatorio RAND, una respuesta esperada XRES, una clave de encriptación CK, una clave de integridad IK y un testigo (“token”) de autenticación AUTN, y los parámetros RAND y AUTN son enviados al equipo de usuario que comprueba si AUTN puede ser aceptado y, si es así, calcula CK e IK y produce una respuesta RES que es enviada de vuelta a la red, la cual, a su vez, compara la RES recibida con XRES y, si coinciden, la autenticación se considera como exitosa.

Si la autenticación tiene éxito (etapa 505), el nodo de punto de acceso almacena, en la etapa 506, información acerca de la autenticación, la información que está siendo usada, tal como se ha descrito anteriormente, cuando el modo es de nuevo un modo normal, para informar a ACME acerca de las autenticaciones realizadas. El nodo de punto de acceso proporciona también, en la etapa 507, al usuario un acceso restringido a la red de acceso, de manera que los equipos de usuario puedan comunicarse entre sí a través del nodo de punto de acceso, y posiblemente a través de otros nodos de punto de acceso en la misma red de acceso.

Si la autenticación falla (etapa 505), el nodo de punto de acceso rechaza, en la etapa 508, la solicitud.

La Figura 6 ilustra la funcionalidad de un nodo de punto de acceso según otra realización. En la etapa 601, el nodo de punto de acceso supervisa si hay disponible o no una conexión a una red central para propósitos de autenticación, es decir, si se ha perdido o no la conexión. Si se ha perdido la conexión, el nodo de punto de acceso conmuta, en la etapa 602, al modo aislado, y difunde, en la etapa 603, una indicación de que el nodo de punto de acceso está en un modo aislado. En el modo aislado, el nodo de punto de acceso supervisa, en la etapa 604, si se ha recibido o no una solicitud que desencadena una autenticación, y si se recibe dicha solicitud, el nodo de punto de acceso autentica, en la etapa 605, el usuario usando la clave K2 raíz adicional. Tal como se ha descrito anteriormente, la autenticación se realiza usando los mismos procedimientos y algoritmos que con la clave K1 raíz permanente. Si la autenticación tiene éxito (etapa 606), el punto de acceso permite, en la etapa 607, al equipo de usuario autenticado un acceso restringido a la red de acceso de radio. Si la autenticación falla (etapa 606), la solicitud que desencadena la autenticación es rechazada en la etapa 608. Mientras tanto (es decir, si no se recibe ninguna solicitud que desencadena una autenticación en la etapa 604 o después de la etapa 607 o después de la etapa 608), el nodo de punto de acceso supervisa, en la etapa 609, si se ha restablecido o no la conexión. Si no, el nodo de punto de acceso pasa a la etapa 603 para difundir información acerca del modo aislado. Si se ha restablecido la conexión (etapa 609), el nodo de punto de acceso conmuta, en la etapa 610, al modo normal. A continuación, el nodo de punto de acceso difunde, en la etapa 611, una indicación que indica el modo normal, y pasa a la etapa 601, para supervisar si hay disponible o no una conexión a una red central para propósitos de autenticación, y mientras está disponible, realiza la supervisión y la difusión de una indicación acerca del modo normal. Durante el modo normal, el nodo de punto de acceso ignora las solicitudes, dedicándose simplemente a reenviarlas.

Las Figuras 7 y 8 ilustran la funcionalidad de un equipo de usuario según una realización en la que los procedimientos ilustrados se ejecutan en paralelo.

La Figura 7 comienza cuando el equipo de usuario recibe, en la etapa 701, una difusión. A continuación, el equipo de usuario comprueba, en la etapa 702, si el modo de red es normal. Si la difusión indica el modo normal, el equipo de usuario comprueba, en la etapa 703, si la información del modo mantenida en el equipo de usuario indica normal. Si ambas son normales (es decir, etapas 702 y 703), el procedimiento pasa a la etapa 701 para recibir la difusión.

Si la información de modo mantenida en el equipo de usuario indica el modo aislado (etapa 703), la información de modo es establecida, en la etapa 704, para indicar el modo normal. A continuación, se comprueba, en la etapa 705, si en la actualidad el equipo de usuario tiene una conexión de modo aislado con acceso restringido. Si es así, se pregunta al usuario, en la etapa 706, sobre la posibilidad de obtener un acceso completo a la red. Si el usuario desea el acceso completo a la red (etapa 707), se envía una solicitud que desencadena una autenticación (etapa 708) a la red y, a continuación, el procedimiento pasa a la etapa 701 para recibir la difusión.

Si no hay conexión de modo aislado (etapa 705) o el usuario no desea obtener un acceso completo a la red (etapa 707), el procedimiento pasa a la etapa 701 para recibir la difusión.

Si la difusión indica el modo aislado (etapa 702), el equipo de usuario comprueba, en la etapa 709, si la información de modo mantenida en el equipo de usuario indica aislado. Si ambas indican aislado (es decir, etapas 702 y 709), el procedimiento pasa a la etapa 701 para recibir la difusión.

Si la información de modo indica el modo normal (etapa 709), la información de modo se establece, en la etapa 710, para indicar el modo aislado. A continuación, el procedimiento pasa a la etapa 701 para recibir la difusión.

La Figura 8 ilustra la funcionalidad del equipo de usuario cuando se recibe una solicitud de autenticación (etapa 801). En el ejemplo ilustrado, se supone, en aras de la claridad, que las autenticaciones son exitosas, y que se usa el procedimiento de autenticación SAE. Sin embargo, debería apreciarse que puede usarse cualquier otro procedimiento de autenticación, basado preferentemente en el secreto compartido y pregunta-respuesta.

En respuesta a la solicitud de autenticación, el equipo de usuario comprueba, en la etapa 802, si la red funciona o no en el modo normal. Si el modo es normal, los equipos de usuario realizan, en la etapa 803, la autenticación

usando la clave raíz K permanente. Tal como se ha explicado anteriormente, el equipo de usuario verifica la validez del vector de autenticación por medio de un contador recibido en la solicitud, y calcula una respuesta usando la clave raíz permanente y un número aleatorio recibido como una pregunta en las solicitudes de autenticación, enviándose, a continuación, la respuesta a la red en la etapa 809. El equipo de usuario calcula, como parte de la autenticación, las claves usadas para la encriptación y la integridad.

Si el modo es aislado (etapa 802), el equipo de usuario pregunta, en la etapa 804, el usuario acerca del acceso restringido. Si el usuario acepta el acceso restringido (etapa 805), el equipo de usuario realiza, en la etapa 806, la autenticación usando la clave K2 raíz adicional, y almacena temporalmente, en la etapa 807, la información sobre la autenticación en modo aislado para el propósito descrito anteriormente y, a continuación, envía, en la etapa 809, una respuesta de autenticación hacia la red. El procedimiento de autenticación realizado en la etapa 806 es el mismo que el realizado en la etapa 803, siendo la única diferencia la clave usada.

Si el usuario no acepta el modo aislado (etapa 805), los equipos de usuario rechazan, en la etapa 808, la autenticación, y envían, en la etapa 802, como una respuesta de autenticación, un rechazo de autenticación.

La Figura 9 es un diagrama de flujo que ilustra la funcionalidad de un equipo de usuario según otra realización. En la realización, cuando el equipo de usuario recibe, en la etapa 901, una solicitud de autenticación, selecciona una clave a ser usada con la autenticación comprobando, en la etapa 902, si la última difusión recibida indicaba el modo aislado. Si indicaba el modo aislado, se selecciona la clave K2 raíz adicional, en la etapa 903, de lo contrario, se selecciona la clave K1 raíz permanente, en la etapa 904. A continuación, se realiza el procedimiento de autenticación, por ejemplo, un procedimiento tal como se ha descrito anteriormente con la Figura 8, en la etapa 905 usando la clave seleccionada. En el ejemplo ilustrado, si la autenticación de la red tiene éxito (por ejemplo, el testigo se ha verificado con éxito), en la etapa 906, el equipo de usuario envía, en la etapa 907, la respuesta calculada a la red, de lo contrario el equipo de usuario envía, en la etapa 908, un rechazo.

La Figura 10 es un diagrama de flujo de señalización ejemplar según una realización adicional. En el ejemplo ilustrado, los nodos de punto de acceso en la misma red de acceso de radio de SAE son estaciones base multiestándar MSBS1 y MSBS2 que son compatibles con al menos TETRA y acceso de radio SAE y que están configuradas para ser ACMEs para TETRA, en el que un primer equipo de usuario UE1 es un equipo de usuario multiestándar que es compatible con TETRA y SAE, pero un segundo equipo de usuario UE2, al que el primer equipo de usuario UE1 quiere hacer una llamada, sólo es compatible con SAE, y los equipos de usuario están en el área de la misma red de acceso de radio SAE, tal como una red de evolución a largo plazo (LTE) o LTE evolucionado. La mensajería SAE se ilustra mediante líneas sólidas, la mensajería TETRA mediante líneas de trazos.

En el ejemplo ilustrado, se supone que tanto MSBS1 como MSBS2 asumen que están en el modo normal y difunden " indicador de modo normal" en la información del sistema de SAE. Sin embargo, la difusión no se ilustra en la Figura 10. Por lo tanto, cuando UE1 detecta, en el punto 10-1, que el usuario desea llamar a UE2, UE1 envía un mensaje 10-2, en el que el mensaje es una "conexión a SAE", a través de la MSBS1 que da servicio al UE1, a una entidad de gestión de movilidad MME que realiza autenticaciones. En el ejemplo ilustrado, se ha producido un fallo de enlace entre MSBS1 y MME, y la MSBS1 detecta, en el punto 10-3, una situación de "tiempo expirado", es decir, el hecho de que una respuesta a una solicitud enviada no es recibida a tiempo, y conmuta al modo aislado para SAE. Una indicación del modo aislado es difundida por la MSBS1, pero esto no se muestra en la Figura 10. La MSBS2 sigue estando en un modo normal.

En la realización, MSBS1 sabe, en base a la información de terminal incluida en el mensaje 10-2, que UE1 es compatible también con TETRA y, por lo tanto, envía a UE1 el mensaje 10-4 para conexión a TETRA y, en el ejemplo, indica que la conexión a TETRA es para la entrega de la clave K2 raíz adicional con la que UE1 puede realizar la autenticación de acceso restringido. En respuesta al mensaje 10-4, UE1 envía un mensaje 10-5 para conexión a TETRA, el cual, a su vez, desencadena la autenticación TETRA realizada por los mensajes 10-6, en el que la autenticación TETRA usa claves específicas de TETRA. Tal como se ha indicado anteriormente, en el ejemplo ilustrado, se supone que MSBS1 está configurada para actuar como ACME para TETRA. Debido a que la autenticación TETRA es exitosa en el ejemplo ilustrado, hay un canal seguro (canal secundario seguro) sobre el cual se envía la clave K2 raíz adicional para SAE, en el mensaje 10-7, desde UE1 a MSBS1. Debería apreciarse que, en otra implementación, MSBS1 está configurada para enviar dicha K2 través del canal seguro al UE1.

A continuación, UE1 envía de nuevo el mensaje 10-2. Debido a que MSBS1 está en modo aislado, captura, en el punto 10-8, el mensaje y desencadena, en el punto 10-8, la autenticación para el acceso restringido SAE, es decir, la autenticación usando K2. La autenticación es realizada por los mensajes 10-9. En el ejemplo ilustrado, la autenticación es exitosa.

A continuación, UE1 envía el mensaje 10-10 que inicia una llamada a UE2. MSBS1 obtiene, en el punto 10-11,

información de enrutamiento acerca de UE2, y detecta, en el punto 10-11, que UE1 está en acceso restringido pero que UE2 está dentro de la zona de acceso restringido, es decir, en la misma red de acceso de radio para SAE que UE1. Por lo tanto MSBS1 reenvía el mensaje 10-10 a MSBS2 que proporciona servicio a UE2 que, a continuación, reenvía el mensaje a UE2.

En el ejemplo ilustrado, UE2 no está conectado a la red y, por lo tanto, envía el mensaje 10-2' que indica una conexión a la red a MME a través de MSBS2. En el ejemplo ilustrado, UE2 necesita ser autenticado, no hay fallo de enlace entre MSBS2 y MME que contiene vectores de autenticación para UE2, y MME desencadena la autenticación que se realiza en los mensajes 10-12. Después de eso, UE1 y UE2 pueden realizar la llamada (ilustrada en los mensajes 10-13). Aunque no se ilustra, la llamada podría ser una llamada de grupo local entre equipos de usuario en la red de acceso de radio o cualquier otro servicio de comunicación proporcionado por medio de la red de acceso de radio. Otro ejemplo de servicios incluye servicios de mensajería. Típicamente, MSBS1 y MSBS 2 están en la misma red de acceso de radio, pero ese no tiene por qué ser el caso; es suficiente que puedan comunicarse entre sí.

Las etapas/puntos, mensajes de señalización y funciones relacionadas descritos anteriormente en las Figuras 4 a 10 no están en ningún orden cronológico absoluto, y algunas de las etapas/puntos pueden ser realizadas simultáneamente o en un orden diferente del proporcionado. Otras funciones pueden ser ejecutadas también entre las etapas/puntos o dentro de las etapas/puntos y otros mensajes de señalización enviados entre los mensajes ilustrados. Por ejemplo, la etapa 506 puede ser realizada entre las etapas 607 y 609, y la etapa 408 entre las etapas 610 y 611. Algunas de las etapas/puntos o parte de las etapas/puntos pueden omitirse también o sustituirse por una etapa/punto correspondiente o parte de la etapa/punto. Por ejemplo, las etapas 702, 704, 709 y 710 pueden ser sustituidas por una etapa que actualiza, si es necesario, el modo y si es actualizado a normal, pueden realizarse las etapas 705 y 708. Los mensajes de señalización son sólo ejemplares y pueden comprender incluso diversos mensajes separados para transmitir la misma información. Además, los mensajes pueden contener también otra información.

Será obvio para una persona con conocimientos en la materia que, conforme avanza la tecnología, el concepto inventivo puede ser implementado de diversas maneras. La invención y sus realizaciones no se limitan a los ejemplos descritos anteriormente sino que pueden variar dentro del alcance de las reivindicaciones.

REIVINDICACIONES

1. Un procedimiento para un sistema que comprende una red (101) de acceso y un servidor (121) de autenticación configurado para autenticar un usuario por medio de un primer secreto (K1, K1') compartido, en el que el procedimiento comprende:

supervisar (401, 601) si un nodo (200, 200') de punto de acceso está o no en un modo aislado, en el que el servidor de autenticación no está disponible para propósitos de autenticación, o en un modo normal, en el que el servidor de autenticación está disponible para propósitos de autenticación;

difundir (402, 404, 603, 611) información que indica el modo actual; y

durante el modo aislado, autenticar (504, 605) el usuario en el nodo de punto de acceso o en un nodo que controla el nodo de punto de acceso por medio de un segundo secreto (K2) compartido.

2. Procedimiento según se reivindica en la reivindicación 1, en el que el procedimiento comprende además proporcionar (507, 607) al usuario, durante el modo aislado, un acceso de red restringido si la autenticación por medio del segundo secreto (K2) compartido tiene éxito.

3. Procedimiento según se reivindica en la reivindicación 1 o 2, que comprende además:

mantener, durante el modo aislado, información acerca de cada usuario autenticado por medio del segundo secreto;

detectar (405) que el servidor de autenticación está disponible de nuevo para los propósitos de autenticación;

transmitir (408) la información acerca de los usuarios autenticados al servidor de autenticación para su re-autenticación.

4. Un procedimiento para un equipo (300, 300') de usuario configurado para autenticar un usuario del equipo de usuario a una red por medio de un primer secreto (K1, K1') compartido, en el que el procedimiento comprende;

recibir (701) en una difusión una indicación acerca de si la red está en un modo aislado, en el que el servidor (121) de autenticación no está disponible para propósitos de autenticación, o en un modo normal, en el que el servidor de autenticación está disponible para la autenticación por medio del primer secreto (K1) compartido;

recibir (801, 901) una solicitud de autenticación;

si la última difusión indicaba el modo normal, realizar (803, 904-905) la autenticación por medio del primer secreto (K1) compartido; y

si la última difusión indicaba el modo aislado, realizar (806, 903-905) la autenticación por medio de un segundo secreto (K2) compartido.

5. Procedimiento según se reivindica en la reivindicación 4, en el que, si la última difusión indicaba el modo aislado, el procedimiento comprende además:

preguntar (706) al usuario acerca de un acceso de red restringido; y

realizar (806) la autenticación en respuesta a la recepción desde el usuario de una indicación de que el usuario acepta el acceso de red restringido.

6. Procedimiento según se reivindica en la reivindicación 4 o 5, que comprende además:

recibir (701) una difusión que indica el modo normal después de una o más difusiones que indican el modo aislado;

comprobar (707) si en la actualidad existe o no una conexión de modo aislado con un acceso de red restringido; y

enviar (708) una solicitud que desencadena una autenticación de red, si en la actualidad existe una conexión en modo aislado.

7. Procedimiento según se reivindica en la reivindicación 6, en el que si en la actualidad existe una conexión en modo aislado, el procedimiento comprende además:

preguntar al usuario acerca de la posibilidad de obtener un acceso completo a la red; y

enviar la solicitud que desencadena la autenticación de red en respuesta a la recepción desde el usuario de una indicación de que el usuario desea el acceso completo a la red.

8. Procedimiento según se reivindica en cualquiera de las reivindicaciones anteriores, en el que el primer secreto (K1) compartido es una clave raíz permanente que nunca es transmitida, y el segundo secreto (K2) compartido es una clave raíz que puede ser usada en lugar de la clave raíz permanente en los algoritmos de autenticación y que puede ser transmitida a través de una conexión segura.

9. Un aparato que comprende medios para realizar un procedimiento según se reivindica en una cualquiera de las reivindicaciones 1 a 3 y la reivindicación 8, siempre que dependa de cualquiera de las reivindicaciones 1-3.

10. Aparato que comprende medios para realizar un procedimiento según se reivindica en una cualquiera de las reivindicaciones 4-7 y la reivindicación 8, siempre que dependa de cualquiera de las reivindicaciones 4-7.

11. Un sistema de comunicación que comprende:

un centro (131) de autenticación que comprende medios para almacenar, de manera segura, primeros secretos (K1, K1') compartidos específicos de suscripción para la autenticación de los usuarios correspondientes;

un servidor (121) de autenticación configurado para autenticar un usuario por medio de un primer secreto (K1, K1') compartido correspondiente;

una red (101) de acceso configurada para mantener u obtener, de manera segura, un segundo secreto (K2) compartido para la autenticación, para detectar un modo aislado, en el que el servidor de autenticación no está disponible para propósitos de autenticación; en respuesta al modo aislado, autenticar a un usuario por medio del segundo secreto compartido para proporcionar al usuario un acceso restringido; y para difundir información acerca de si la red de acceso está o no en el modo aislado; y

el equipo (300, 300') de usuario comprende medios (33) para almacenar, de manera segura, un primer secreto (k1, K1') compartido para la autenticación del usuario del equipo de usuario, medios (33) para mantener u obtener, de manera segura, un segundo secreto (K2) compartido para la autenticación, medios (34) para recibir información acerca de un modo actual de la red de acceso en difusión, medios (34) para recibir una solicitud de autenticación, medios (31) para seleccionar un secreto a ser usado en una autenticación basada en el modo actual de la red de acceso, en el que los medios (31) de selección están configurados para seleccionar el segundo secreto compartido si el modo actual es el modo aislado, de lo contrario para seleccionar el primer secreto compartido, y medios (32) para realizar la autenticación usando la clave seleccionada.

12. Sistema de comunicación según se reivindica en la reivindicación 11, en el que la red (101) de acceso comprende un nodo (200, 200') de punto de acceso configurado al menos para realizar dicha detección, difusión y autenticación.

13. Sistema de comunicación según se reivindica en la reivindicación 12, en el que

el sistema de comunicación comprende además una segunda red de acceso, en el que la segunda red de acceso es de un tipo diferente que la red de acceso, y

el sistema de comunicación está configurado para establecer un canal secundario seguro entre el equipo de usuario y el nodo de punto de acceso por medio de la segunda red de acceso y para entregar el segundo secreto compartido a través del canal secundario seguro.

14. Sistema de comunicación según se reivindica en la reivindicación 12 o 13, en el que el nodo (200, 200') de punto de acceso es una estación base multiestándar, un nodo B o un nodo B evolucionado.

15. Sistema de comunicación según se reivindica en la reivindicación 11, 12, 13 o 14, en el que el sistema de comunicación está configurado para proporcionar al equipo (300, 3004) de usuario sólo servicios proporcionados por medio de la red (101) de acceso si la autenticación se realiza usando el segundo secreto (K2) compartido.

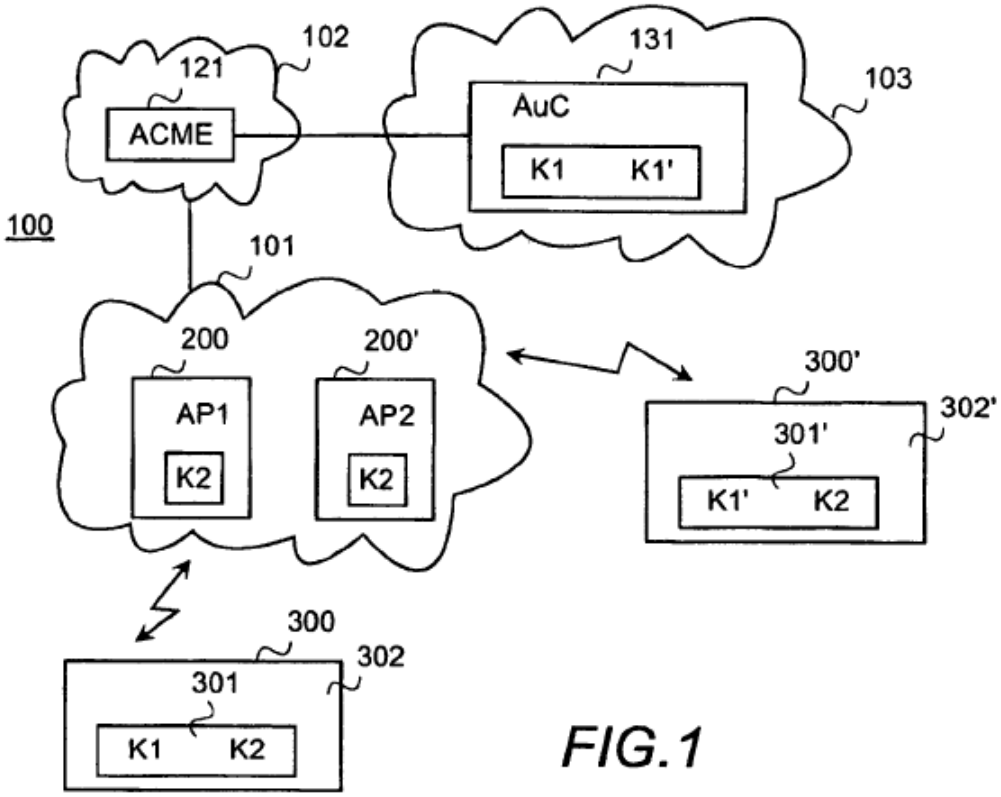

FIG.1

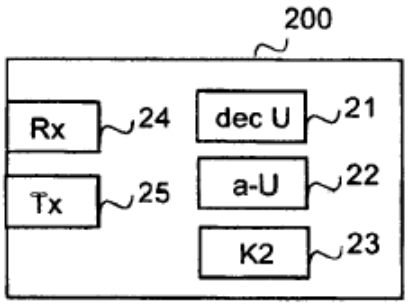

FIG.2

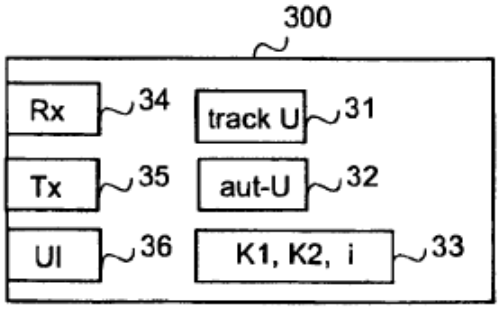

FIG.3

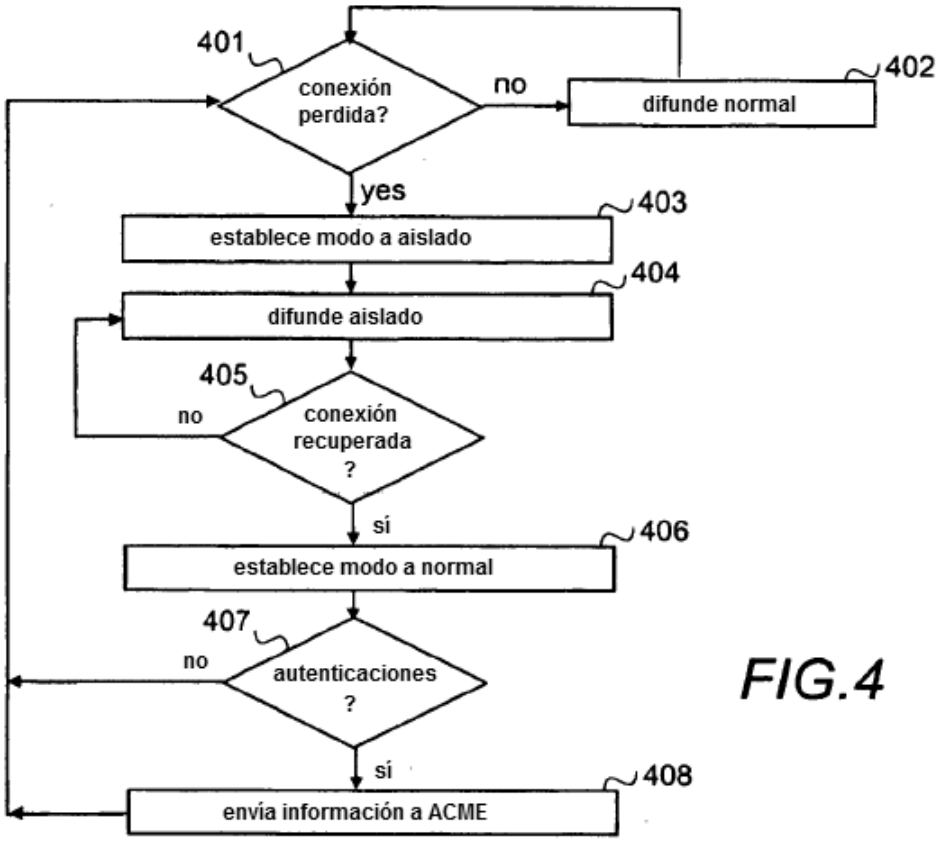
401
conexión perdida?
no
402
difunde normal
yes
403
establece modo a aislado
404
difunde aislado
405
no
conexión recuperada ?
sí
406
establece modo a normal
407
no
autenticaciones ?
sí
408
envía información a ACME

FIG.4

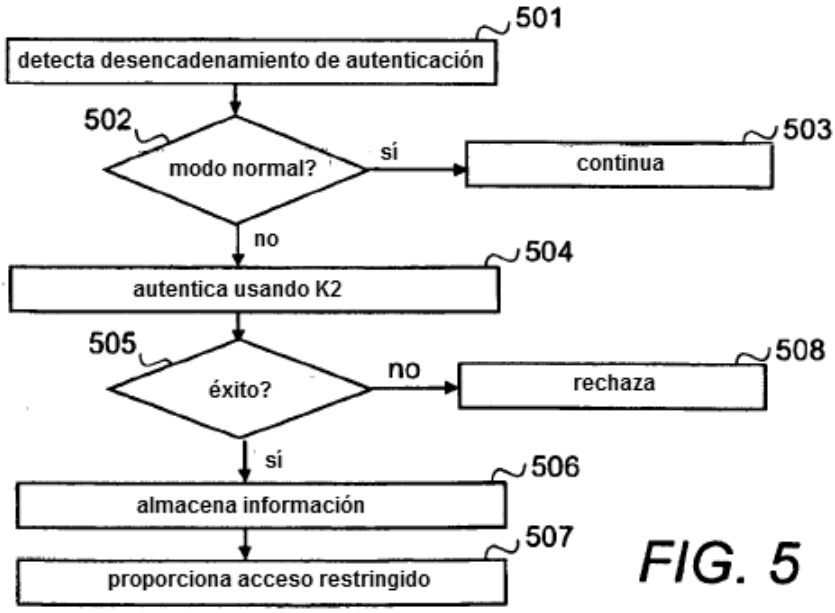
501
detecta desencadenamiento de autenticación
502
modo normal?
sí
503
continua
no
504
autentica usando K2
505
éxito?
no
508
rechaza
sí
506
almacena información
507
proporciona acceso restringido

FIG. 5

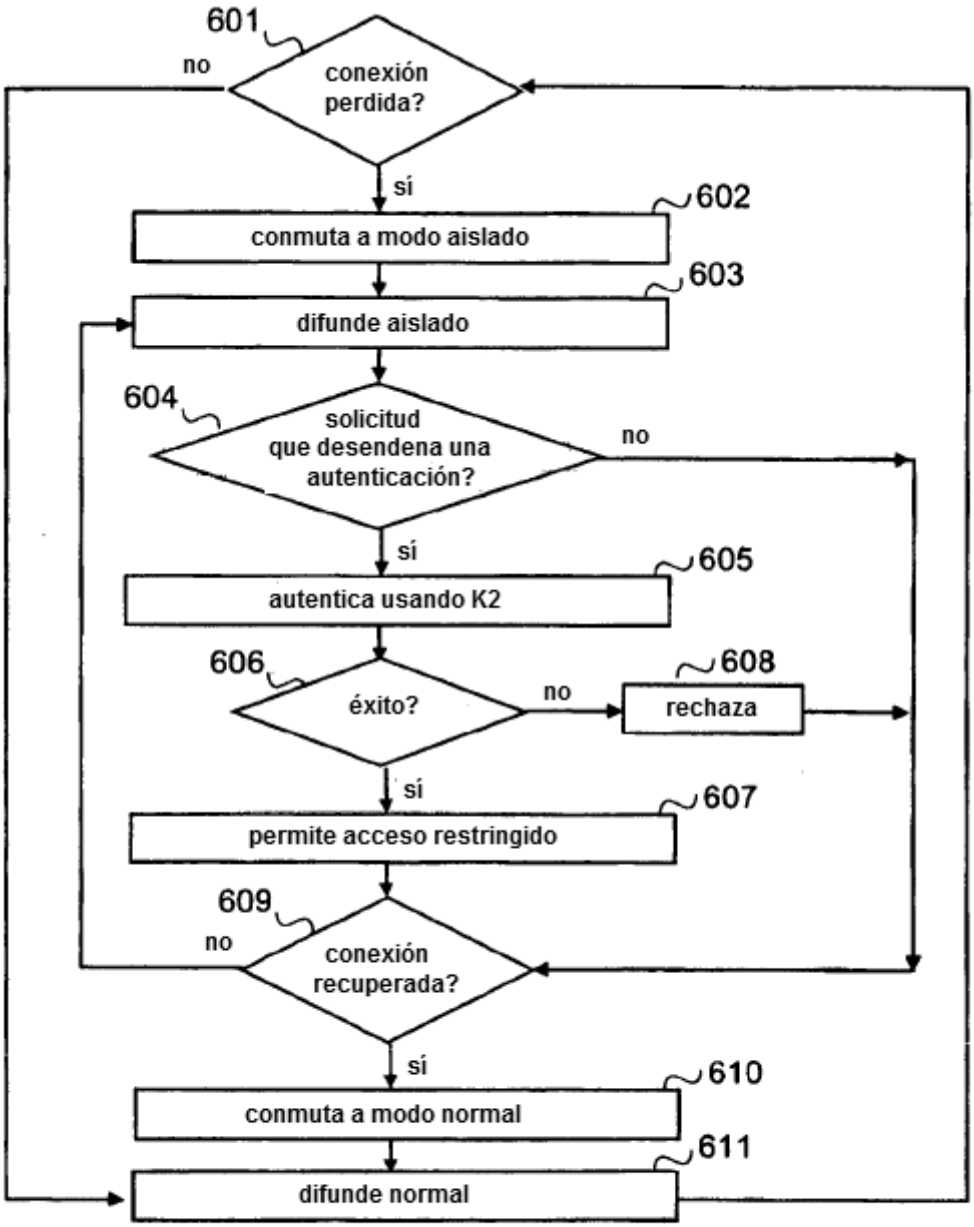
601
conexión perdida?
no
sí
602
conmuta a modo aislado
603
difunde aislado
604
solicitud que desendena una autenticación?
no
sí
605
autentica usando K2
606
éxito?
no
608
rechaza
sí
607
permite acceso restringido
609
conexión recuperada?
no
sí
610
conmuta a modo normal
611
difunde normal

FIG.6

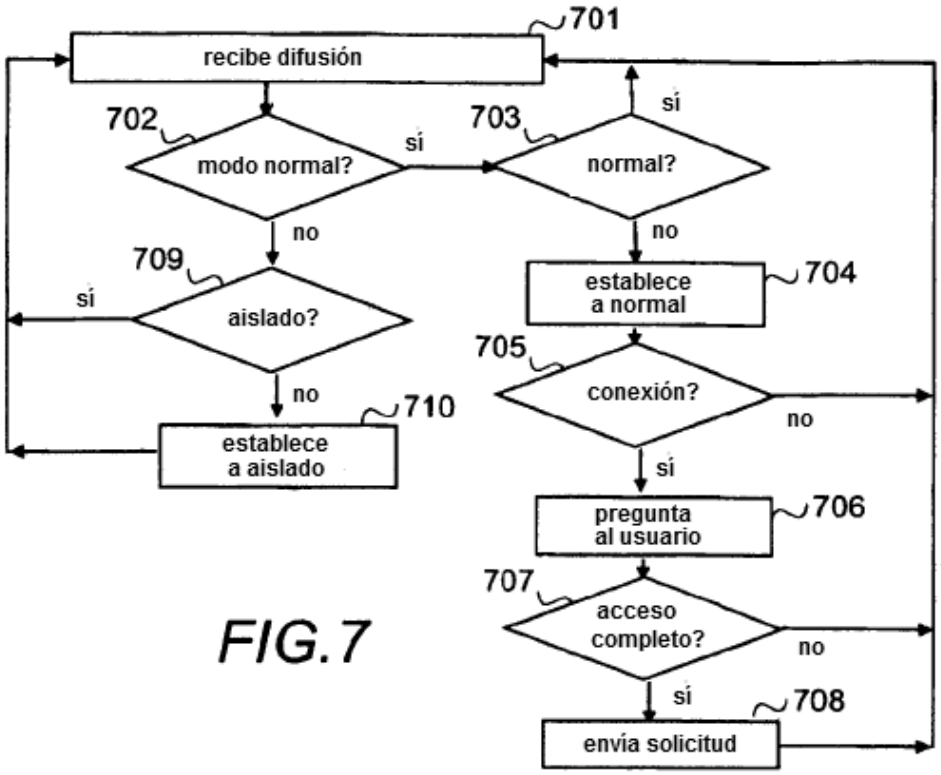
701
recibe difusión
702
modo normal?
sí
703
normal?
sí
no
no
709
aislado?
sí
no
704
establece a normal
705
conexión?
no
sí
710
establece a aislado
706
pregunta al usuario
707
acceso completo?
no
sí
708
envía solicitud

FIG.7

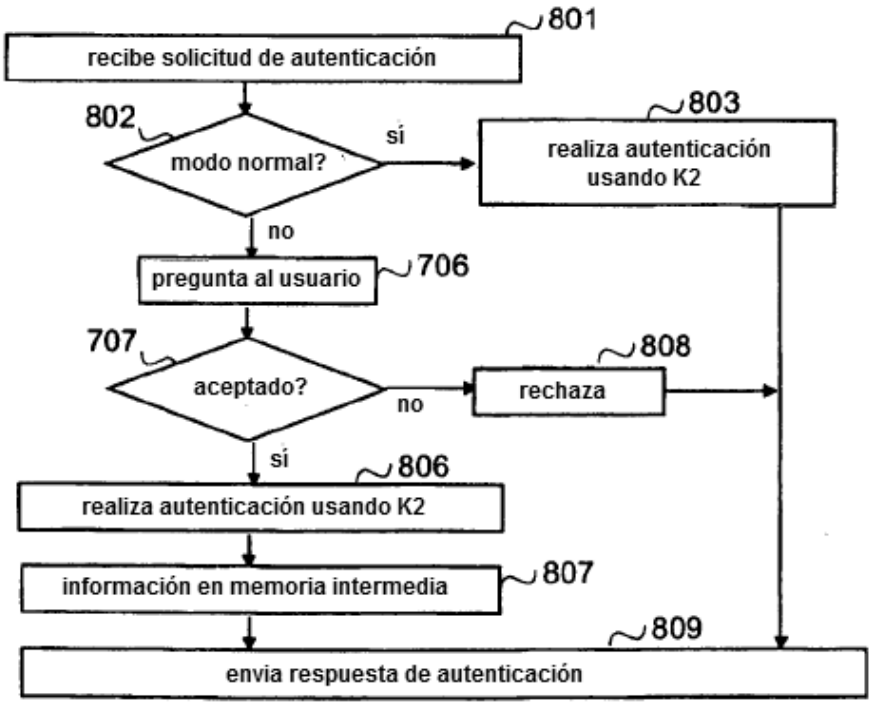
801
recibe solicitud de autenticación
802
modo normal?
sí
803
realiza autenticación usando K2
no
706
pregunta al usuario
707
aceptado?
no
808
rechaza
sí
806
realiza autenticación usando K2
807
información en memoria intermedia
809
envia respuesta de autenticación

FIG.8

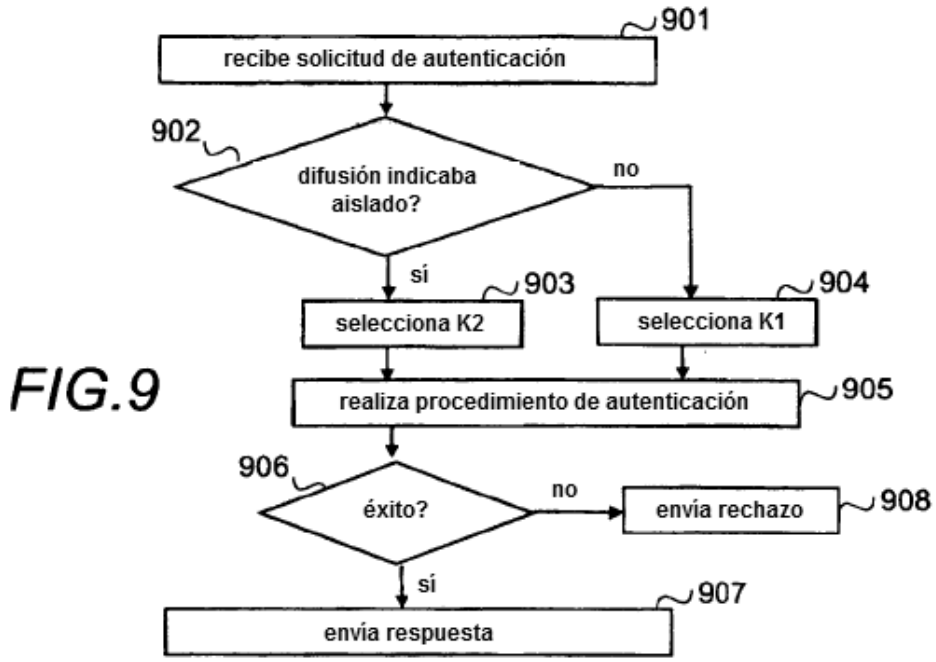
901
recibe solicitud de autenticación
902
difusión indicaba aislado?
no
sí
903
selecciona K2
904
selecciona K1
realiza procedimiento de autenticación
905
906
éxito?
no
envía rechazo
908
sí
907
envía respuesta

FIG.9

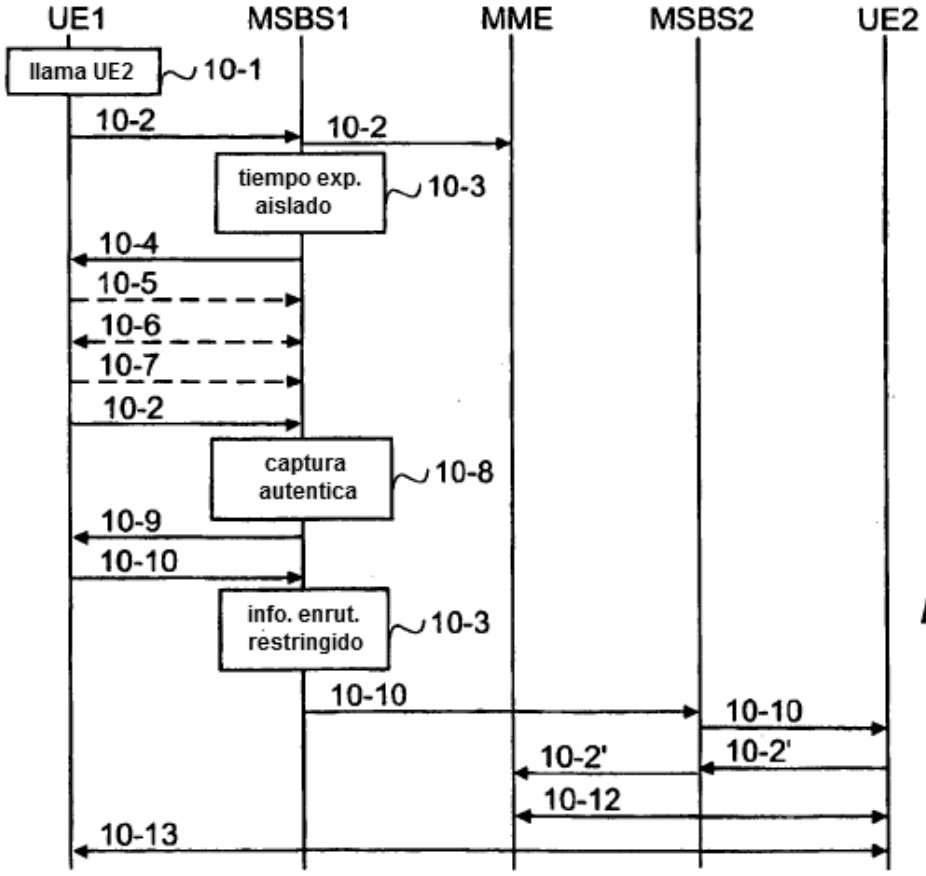
UE1
MSBS1
MME
MSBS2
UE2
llama UE2
10-1
10-2
10-2
tiempo exp. aislado
10-3
10-4
10-5
10-6
10-7
10-2
captura autentica
10-8
10-9
10-10
info. enrut. restringido
10-3
10-10
10-10
10-2'
10-2'
10-12
10-13

FIG.10