(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 535 386**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04W 12/06 (2009.01)
H04L 9/34 (2006.01)
H04L 9/32 (2006.01)
H04W 8/24 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **08.06.2011 E 11004668 (7)**

(97) Fecha y número de publicación de la concesión europea: **04.03.2015 EP 2533485**

(54) Título: **Procedimientos y dispositivos para gestión durante la comunicación (OTA) de módulos de identificación de abonado**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.05.2015

(73) Titular/es:

GIESECKE & DEVRIENT GMBH (100.0%)
Prinzregentenstrasse 159
81677 München, DE

(72) Inventor/es:

LARSSON, THOMAS

(74) Agente/Representante:

ARPE FERNÁNDEZ, Manuel

DESCRIPCIÓN

Procedimientos y dispositivos para gestión durante la comunicación (OTA) de módulos de identificación de abonado

Campo de la invención

[0001] La invención se refiere en general a comunicaciones móviles y en particular a procedimientos y dispositivos para gestión durante la comunicación de estaciones móviles que contienen un elemento de identificación seguro, preferiblemente un módulo de identificación de abonado, en un sistema de comunicaciones móviles.

Antecedentes de la invención

[0002] El Sistema Global para Comunicaciones Móviles (GSM) es la norma mundialmente más popular para sistemas de comunicaciones móviles. Las características técnicas del GSM se definen por un gran número de especificaciones relacionadas entre sí y mutuamente dependientes publicadas por el organismo de normalización ETSI. En general, para la comunicación con un teléfono móvil a través de una red móvil terrestre pública (PLMN) implementada de acuerdo con las especificaciones GSM requiere un elemento de identificación segura, llamado módulo de identificación de abonado (SIM), por lo general en forma de una tarjeta inteligente. El SIM contiene datos de suscripción para la autenticación y la identificación de abonado de la PLMN, incluyendo, en particular, la Identidad Internacional de Seguridad Móvil (IMSI) y la clave de autenticación Ki. Esta información específica de red es generalmente almacenada en el SIM por el operador PLMN o el fabricante del SIM durante un proceso de personalización de SIM antes de proporcionar al abonado su SIM. Un SIM no personalizado generalmente no es adecuado para su utilización en un teléfono móvil, es decir, la utilización de los servicios proporcionados por una PLNM con un SIM sin no personalizar no es posible.

[0003] De acuerdo con la norma GSM, la IMSI almacenada en el SIM es un número con un máximo de 15 dígitos que permite una identificación única internacional de abonado. Los 3 primeros dígitos del número de IMSI representan el Código Móvil de País (MCC), los siguientes 2 o 3 dígitos representan el código de red móvil (MNC), y los dígitos restantes (hasta 10) representan el número de identificación de la estación móvil (MSIN) asignado por el operador PLMN. El número IMSI permite al operador de la PLMN identificar a un abonado y, proporcionarle aquellos servicios que el abonado haya pagado.

[0004] La clave de autenticación Ki es un elemento de datos de 128 bits para autenticación del SIM contenido en un teléfono móvil con respecto a la PLMN. La clave de autenticación Ki es emparejada con un número IMSI específico durante el proceso de personalización de SIM. Por razones de seguridad la clave de autenticación Ki sólo se almacena en el SIM y en una base de datos de la PLMN, llamada centro de autenticación (AUC).

[0005] El procedimiento de autenticación GSM, que se describe a continuación, es una ejecución de un procedimiento de autenticación puesta a prueba-respuesta general, en el que una de las partes, es decir, la PLMN, presenta una puesta a prueba y un tercero, es decir, el teléfono móvil, debe proporcionar una respuesta válida para ser autenticado. Cuando un teléfono móvil se inicia, recupera el número IMSI de su SIM. El usuario del teléfono móvil generalmente, tiene que introducir un PIN antes que el SIM otorgue acceso al número IMSI. El teléfono móvil envía el número IMSI a través de la interfaz aérea y el subsistema de estación base (BSS) al centro de conmutación móvil (MSC) de una PLMN. El MSC retransmite la IMSI al registro de posiciones base (HLR) y solicita tripletes de autenticación. Cuando el HLR recibe el número IMSI y la petición de tripletes de autenticación, primero comprueba su base de datos para asegurarse de que el número IMSI es válido y perteneciente a la red. Una vez que esto se ha cumplimentado, retransmite el número IMSI y los tripletes de autenticación pedidos al AUC. El AUC utiliza la IMSI para buscar la clave de autenticación Ki asociada con esa IMSI. El AUC también generará un número aleatorio de 128 bits denominado RAND, que, junto con la clave de autenticación Ki se introduce en el algoritmo de cifrado A3. La salida del algoritmo de cifrado A3 es un número de 32 bits llamado Respuesta Firmada (SRES).

[0006] El número RAND y la clave de autenticación Ki se suministran, además, al algoritmo de cifrado A8. La salida es un número de 64 bits denominado Kc. El Kc es la clave de cifrado que se utiliza en el algoritmo de cifrado A5 para cifrar y descifrar los datos que se están transmitiendo sobe la interfaz aérea entre el teléfono móvil y la PLMN.

[0007] El número RAND, la SRES y la clave de cifrado Kc forman un triplete de autenticación que es único para el número IMSI utilizado para la creación de este triplete. Una vez que el AUC ha generado un triplete autenticación tal, se retrasmite al HLR, el cual, a su vez, lo envía al MSC solicitante. El MSC almacena la clave de cifrado Kc y la SRES nada más retrasmite el número RAND como la puesta a prueba del procedimiento de autenticación puesta a prueba-respuesta GSM a la estación móvil y solicita autenticación.

[0008] La clave de autenticación Ki se almacena de forma segura en el SIM del teléfono móvil. Los algoritmos de cifrado A3 y A8 también residen en el SIM. El número RAND recibido desde el MSC a través de la interfaz aérea y la clave de autenticación Ki , se introducen en los algoritmos de cifrado A3 y A8 para generar otra respues firmada SRES* y la clave de cifrado Kc, respectivamente. El teléfono móvil almacena la clave de cifrado Kc en el SIM y envía la respuesta firmada generada SRES* como la respuesta al procedimiento de autenticación puesta a prueba-respuesta GSM de nuevo a la red. El MSC recibe la respuesta firmada SRES * generada por el teléfono móvil y la compara con las respuesta firmada SRES generada por el AUC. Si coinciden, el teléfono móvil (o más bien su SIM) es autenticado.

[0009] Es conocido gestionar, durante la comunicación (OTA), SIMs o dispositivos equipados con tales SIMs utilizando protocolos estandarizados realizados por SMS (servicio de mensajes cortos) o IP (protocolo de Internet)

utilizando canales de comunicación una conexión ya establecida en un sistema de comunicaciones móviles. El documento WO 2010/093312, por ejemplo, describe un procedimiento para la activación OTA y gestión de un SIM usando una application ODA (activación bajo demanda). El procedimiento descrito en el documento WO 2010/093312 está adaptado para activar y gestionar un SIM después de haber sido autenticada en sí con respecto a la PLMN de acuerdo con el procedimiento de autenticación puesta a prueba-respuesta GSM descrito anteriormente.

[0010] Un campo particular de aplicación de los SIM que se espera que crezca rápidamente en los próximos dos años es M2M, es decir, la comunicación entre máquinas en una red de comunicaciones móviles sin intervención humana, también llamado el Internet de las cosas. En M2M se transmiten datos automáticamente entre muchos tipos diferentes de máquinas equipadas con un SIM, tales como sistemas de TV, equipos decodificadores, máquinas expendedoras, vehículos, libros electrónicos, cámaras automáticas, dispositivos sensores y similares. Es previsible que, al menos, para algunos de estos dispositivos no será posible proporcionar, o al menos será muy difícil, el SIM de antemano con un conjunto de datos de suscripción completo, por ejemplo un número IMSI. Esto es porque en algunas aplicaciones M2M el SIM puede ser un dispositivo montado en superficie, que tiene que estar embutido dentro de la máquina respectiva durante el proceso de fabricación de la misma sin la posibilidad de proporcionar el SIM con los datos de suscripción completos de antemano. En consecuencia, desde este ámbito, estas máquinas requieren la provisión de datos de suscripción durante la comunicación.

[0011] El documento US 2009/217038 da a conocer un mecanismo para enlazar un dispositivo M2M inalámbrico desplegado para una suscripción a servicios de red móvil desde un operador de telefonía móvil. El valor de puesta a prueba de autenticación sirve para dos propósitos - como una clave de puesta a prueba para utilizar en un procedimiento estándar de autenticación de acceso a red, y como un portador para la información de dirección. Cuya dirección de servidor es utilizada para obtener las credenciales de suscripción.

[0012] Así, el problema abordado por la presente invención es proporcionar procedimientos y dispositivos que permiten proporcionar a un teléfono móvil que incluye un elemento de identificación segura, tal como un SIM, durante la comunicación, los datos de suscripción y/o instrucción antes de que el teléfono móvil se haya adscrito a una PLMN.

Sumario de la invención

[0013] Este objeto se alcanza de acuerdo con la presente invención mediante el objeto asunto de las reivindicaciones independientes. Las realizaciones preferidas se definen en las reivindicaciones dependientes.

[0014] En general, la presente invención se basa en la idea de utilizar el procedimiento de autenticación de puesta a prueba-respuesta estándar implementado en un sistema de comunicaciones móvil no para su propósito previsto de autenticación, sino para proporcionar, durante la comunicación (OTA), a una estación móvil los datos de suscripción. El procedimiento de autenticación puesta a prueba-respuesta se modifica porque la puesta a prueba se utiliza como un portador OTA para datos de suscripción. Esta puesta a prueba que contiene los datos de suscripción se proporciona a la estación móvil en respuesta a una petición estándar de la estación móvil para permitir el acceso o adscribirse al sistema de comunicaciones móviles, utilizando un elemento de datos indicador de modo, que indica de manera preferida al sistema de comunicaciones móviles que la estación móvil está solicitando datos de suscripción y, por lo tanto, es apropiadamente retrasmitido a una unidad de suministro de datos de suscripción.

[0015] Los datos de suscripcióm transportados por la puesta a prueba comprenden un número IMSI y/o una clave de autenticación Ki.

[0016] Más específicamente, de acuerdo con un primer aspecto, la invención se dirige a un procedimiento para proporcionar datos de suscripción desde una unidad proveedora de datos a una estación móvil según la reivindicación independiente 1.

[0017] De acuerdo con un segundo aspecto de la invención se proporciona un procedimiento para obtener datos de suscripción a partir de una unidad de suministro de datos mediante un elemento de identificación segura, preferiblemente un módulo de identificación de abonado, de una estación móvil para comunicación a través de un sistema de comunicaciones móviles.

[0018] De acuerdo con un tercer aspecto, la invención se dirige a una unidad de suministro de datos para proporcionar a una estación móvil que comprende un elemento de identificación segura, preferiblemente un módulo de identificación de abonado, los datos de suscripción para comunicación a través de un sistema de comunicaciones móviles.

[0019] De acuerdo con un cuarto aspecto, la presente invención proporciona un elemento de identificación segura, preferiblemente un módulo de identificación de abonado, para una estación móvil para comunicación a través de un sistema de comunicaciones móviles.

[0020] De acuerdo con un quinto aspecto, la presente invención proporciona un sistema de comunicaciones móvil que comprende una unidad de suminitro de datos, configurada para proporcionar datos de suscripción y/o una estación móvil con un elemento de identificación segura, preferiblemente un módulo de identificación de abonado, como se describió anteriormente.

[0021] Los datos de suscripción y/o instrucción contenidos en o transportados por la puesta a prueba pueden comprender datos para permitir a la estación móvil adscribirse al sistema de comunicaciones móviles (datos de suscripción) y/o datos conteniendo instrucciones para llevar a cabo determinadas acciones (datos de instrucción), tales como "reintentar la recuperación de datos en 60 segundos" o "utilizar una unidad de suministro de datos diferente".

[0022] Preferiblemente, el elemento de datos indicador de modo hace que el sistema de comunicaciones móviles retransmita la petición de la estación móvil a la unidad de suministro de datos e informa a la unidad de suministro de datos que la estación móvil (es decir, su elemento de identificación segura, preferiblemente su módulo de identificación de abonado) está solicitando datos de suscripción y/o de instrucciones.

[0023] Según realizaciones preferidas, el procedimiento de recuperación de datos de suscripción y/o instrucciones de acuerdo con la presente invención se lleva a cabo antes que de la estación móvil se haya adscrito al sistema de comunicaciones móviles.

[0024] Preferiblemente, los datos de suscripción y/o instrucción transportados por la puesta a prueba están en texto sin cifrar, cifrados o un puntero a datos de suscripción y/o instrucción ya almacenados previamente en la estación móvil, tal como en su elemento de identificación segura, preferiblemente su módulo de identificación de abonado.

[0025] De acuerdo con realizaciones preferidas, el procedimiento de recuperación de datos de suscripción y/o instrucción de acuerdo con la presente invención se puede repetir más de una vez para proporcionar a la estación móvil datos de suscripción y/o instrucción que tienen un tamaño que es mayor que el tamaño de la puesta a prueba del procedimiento de autenticación de puesta a prueba-respuesta llevado a cabo en el sistema de comunicaciones móviles.

[0026] Preferiblemente, los datos de suscripción y/o instrucción transportados por la puesta a prueba dependen de la ubicación de la estación móvil y/o del tipo de la estación móvil.

[0027] De acuerdo con realizaciones preferidas, el sistema de comunicaciones móviles se implementa según la norma GSM. En una realización preferida tal, la puesta a prueba se crea como un número RAND* de 128 bits que transporta los datos de suscripción y/o instrucción, preferiblemente como parte de un triplete de autenticación que comprende además una respuesta firmada SRES y una clave de cifrado Kc de acuerdo con el procedimiento de auemticación puesta a prueba-respuesta GSM.

[0028] Preferiblemente, el elemento de datos indicador de modo es un número IMSI preliminar (PIMSI) que preferentemente define o contiene la dirección de una unidad de suministro de datos y/o tiene el mismo formato que un número IMSI.

[0029] Según la invención, los datos de suscripción transportados por la puesta a prueba permiten a la estación móvil autentificarse a sí misma con respecto al sistema de comunicaciones móviles, utilizando el procedimiento de autenticación puesta a prueba-respuesta llevado a cabo en el mismo. El sistema de comunicaciones móviles se implementa de acuerdo con la norma GSM, los datos de suscripción transportados por la puesta a prueba (RAND*) comprende un número IMSI y/o una clave de autenticación Ki.

[0030] La unidad de suministro de datos puede ser una unidad autónoma dedicada, por ejemplo, un servidor de suministro de datos de suscripción y/o instrucción del sistema de comunicaciones móvil o ejecutado como parte de un registro de posiciones base (HLR) del sistema de comunicaciones móviles que lleva a cabo las funciones de la unidad de suministro de datos de suscripción/instrucción.

[0031] Estas y otras peculiaridades, características, ventajas y objetos de la invención resultarán evidentes a partir de la siguiente descripción detallada de realizaciones preferidas, dadas como ejemplos no restrictivos, en referencia a los dibujos adjuntos. El experto en la técnica apreciará, en particular, que las realizaciones preferidas anteriores se pueden combinar de varias maneras, lo que redundará en realizaciones ventajosas adicionales que son compatibles de forma explícita y cubiertos por la presente invención.

Breve descripcón de los dibujos

[0032]

La figura 1 muestra una vista general esquemática de un sistema de comunicaciones móviles que incorpora aspectos de la presente invención.

La figura 2 muestra un diagrama de señales que ilustra un procedimiento para proporcionar un módulo de identificación de abonado con datos de suscripción y/o instrucción de acuerdo con aspectos de la presente invención.

La figura 3 muestra un diagrama de flujo que ilustra el funcionamiento de una aplicación que se ejecuta en el módulo de identificación de abonado de una estación móvil de acuerdo con aspectos de la presente invención.

La figura 4 muestra una vista general esquemática de un sistema de comunicaciones móviles adicional incorporando aspectos de la presente invención.

Descripción detalla de realizaciones preferidas

[0033] La figura 1 muestra esquemáticamente los componentes de un sistema de comunicaciones móviles 10, así como algunos de los canales de comunicación entre los componentes de este sistema 10 que ilustra diferentes aspectos de la presente invención.

[0034] El sistema de comunicaciones móviles 10 se refiere en general a cualquier sistema de telecomunicaciones en el que el punto de acceso al sistema puede cambiar cuando los abonados se desplazan dentro de la zona de servicio del sistema. A continuación, se describirán realizaciones preferidas de la invención utilizando los términos y elementos de acuerdo con las normas del Sistema Global para Comunicaciones Móviles (GSM), como se especifica en una serie de especificaciones proporcionadas por el ETSI. Sin embargo, los expertos en la técnica apreciarán que la presente invención puede aplicarse ventajosamente también en conexión con otros sistemas de comunicaciones móviles. Tales sistemas incluyen sistemas de comunicación móviles de tercera generación (3GPP),

tales como el Sistema Universal de Telecomunicaciones Móviles (UMTS), así como otros sistemas basados en los sistemas anteriores, tales como GPRS (General Packet Radio Service [servicio general de radicomunicaciones por paquetes]) y CAMEL (Customised Applications for Mobile network Enhanced Logic [aplicaciones personalizadas de lógica mejorada de red móvil]).

[0035] Además en lo que sigue, se describirán las formas de realización preferidas de la invención en el contexto de proporcionar datos de suscripción y/o instrucción a un módulo de identificación de abonado (SIM), al ser el SIM actualmente el tipo más popular de elemento de identificación seguro utilizado en sistemas de comunicaciones móviles para la identificación única y segura de los abonados, así como para la prestación de diferentes funciones especiales y servicios de valor añadido. El experto en la técnica apreciará, sin embargo, que otros tipos de elementos de identificación seguros que, dependiendo de la generación subyacente y tipo de norma de sistema, son designados como UICC, USIM, RUIM o también ISIM, están también englobados en la presente invención.

[0036] En la figura 1, se muestra una estación móvil ejemplar 12 que comprende un terminal móvil 14 y un módulo de identificación de abonado (SIM) 16 insertado en el terminal móvil 14. La estación móvil 12 se comunica a través de la interfaz aérea (o enlace radioeléctrico) con un subsistema de estación base (BSS) 20. Como es bien conocido por la persona experta en la técnica, el subsistema de estación base 20 consta generalmente de una o más estaciones transceptoras base que definen las respectivas células del sistema de comunicaciones móvil 10 y que están conectadas a un controlador de estación base. Generalmente, el controlador de estación base es uno de varios controladores de estaciones base que se comunican con un centro de conmutación móvil (MSC). A menudo, una base de datos local llamada Registro de Localización de Visitantes (VLR) para el seguimiento de los usuarios móviles actualmente situadas dentro de las células cubiertas por un MSC (es decir, el área de servicio MSC) se incorpora en el MSC, en lo sucesivo referido como el MSC/VLR 30 .

[0037] El MSC/VLR 30 proporciona esencialmente la misma funcionalidad que una centralita en una red telefónica conmutada pública y es, además, responsable del procesamiento de llamadas, la gestión de movilidad, y la gestión de recursos de radioeléctricos. El MSC/VLR 30 está además en comunicación con un registro de posiciones base (HLR) 40. El HLR 40 es la base de datos primaria de la PLMN proporcionada por el sistema de comunicaciones móviles 10 que almacena información acerca de los usuarios móviles. Para este fin, el HLR 40 comunica con un centro de autenticación (AUC) 50.

[0038] Como se conoce por el experto en la técnica, los medios de comunicación entre los diferentes componentes del sistema de comunicaciones móviles 10 pueden ser privados o puede utilizar normas abiertas. Los protocolos pueden ser el SS7 o basados en IP. El SS7 es una norma global para telecomunicaciones definida por la Unión Internacional de Telecomunicaciones (UIT) Sector de Normalización (UIT-T). La norma define los procedimientos y el protocolo por el cual los elementos de red de la red telefónica conmutada pública (PSTN) intercambian información sobre una red de señalización digital para efectuar la configuración de llamada inalámbrica (celular) y fija, el encaminamiento y control. La red y protocolo SS7 se utilizan para, por ejemplo, configuración de llamada básica, administración, servicios inalámbricos, itinerancia inalámbrica y autenticación de abonado móvil, es decir, mejoran las funciones de llamada que proporcionan para las telecomunicaciones internacionales eficaces y seguras. Los elementos físicos mediante los cuales los elementos se agrupan o permanecen separados y las Interfaces - ya sea privada o abierta - se dejan al operador PLMN.

[0039] Además, el sistema de comunicaciones móviles 10 mostrado en la figura 1 comprende una unidad de suministro de datos de suscripción y/o instrucción, preferentemente un servidor de datos de suscripción/instrucción dedicado (SIDS) 60. Como se muestra esquemáticamente en la figura 1, el SIDS 60 puede ser una unidad autónoma que está en comunicación con el MSC/VLR 30 y opcionalmente con el HLR 40 y está configurado para proporcionar datos de suscripción y/o instrucción a la estación móvil 12.

[0040] La función del SIDS 60 en combinación con los restantes elementos de los sistemas de comunicaciones móviles 10 mostrados en la figura 1, se describirá ahora haciendo referencia adicional a la figura 2. En la etapa S1 de la figura 2 se inicia un proceso de obtención de datos de suscripción y/o instrucción por medio de la estación móvil 12 que contiene el SIM 16, preferiblemente por un usuario de la estación móvil 12 a partir de una aplicación de recuperación de datos de suscripción/instrucción proporcionada en su estación móvil 12, tal como mediante utilización de una pantalla táctil y/o un teclado del equipo móvil 14. Alternativamente, el proceso de obtención de datos de suscripción y/o instrucción según la presente invención puede iniciarse automáticamente, cuando el usuario inicia la estación móvil 12 y su SIM 16 por primera vez. Es importante tener en cuenta que el proceso de obtención de datos de suscripción y o instrucción que se muestra mediante las etapas S1 a S6 de la figura 2, ventajosamente, se puede realizar OTA (durante la comunicación) antes de haber adscrito con éxito o autenticarse el SIM 16 con respecto a la PLMN proporcionada por el sistema móvil de comunicaciones 10, es decir, mientras que el SIM 16 se encuentra todavía en un modo de pre-adscripción.

[0041] Como resultado de la activación de la sesión de recuperación de datos de suscripción y/o instrucción, la estación móvil 12 retransmite un elemento de datos indicador de modo, preferiblemente en forma de un número IMSI preliminar (en lo sucesivo abreviado como PIMSI), que se almacena en el SIM 16 a través de la interfaz aérea y el subsistema de estación base 20 al MSC/VLR 30 (etapa S2 de la figura 2). Preferiblemente, el número PIMSI tiene el mismo formato que un número IMSI, es decir, el número PIMSI puede tener hasta 15 dígitos. Esto tiene como ventaja que el MSC/VLR 30 maneja el número PIMS como un número IMSI “normal” y emite una petición de "Tripletes de Autenticación de Envío", según el protocolo MAP a partir de este número PIMSI. El MSC/VLR 30 retransmite la petición de "Triplete de Autenticación de Envío" de MAP al SIDS 60 que está direccionado por el número PIMSI (etapa S3 de la figura 2).

[0042] El número PIMSI difiere de un número IMSI "normal" solo en que alguna parte del número PIMSI indica a la unidad que recibe el número de PIMSI desde el MSC/VLR 30 que el SIM 16 no se encuentra en un modo para llevar a cabo un procedimiento de autenticación/adscripción GSM convencional, sino que más bien se encuentra en un modo de recuperación de datos de suscripción/instrucción (preferiblemente pre-adscripción). En consecuencia, es posible que, como en el caso del número IMSI, los 3 primeros dígitos del número de PIMSI representen el código móvil de país y representando los siguientes 2 o 3 dígitos del número de PIMSI, el código de red móvil. Esto tendría como ventaja que, por ejemplo, el operador de una PLMN (que se define únicamente por un cierto código móvil de país y un cierto código de red móvil) podría reservar uno o más números de identificación de la estación móvil sin asignar (es decir, los dígitos restantes del número PIMSI) como indicadores de que el SIM 16 está en un modo de recuperación de datos de suscripción y/o instrucción que solicita datos de suscripción y/o instrucción. Alternativamente, el número PIMSI podría contener un código de país móvil y/o un código de red móvil que no haya sido aún asignado por la Unión Internacional de Telecomunicaciones, por ejemplo un rango permitido de itinerancia global de números IMSI sin asignar. Es importante señalar que, contrariamente a un número IMSI el número PIMSI contenido en un SIM 16 con datos de suscripción incompletos no tiene porque ser único, es decir, de acuerdo con la presente invención varios SIMs pueden proporcionarse con el mismo número PIMSI para la obtención de datos de suscripción (que faltan).

[0043] De acuerdo con la presente invención, es posible que el número PIMSI consista esencialmente en datos de suscripción solo que están presentes inicialmente en el SIM 16 (es decir, antes del primer inicio). Por ejemplo, el número PIMSI puede almacenarse en el SIM 16 durante el proceso de fabricación o de personalización del SIM 16. Todos los restantes datos de suscripción (que faltan), por ejemplo, para realizar el procedimiento de autenticación/adscripción de puesta a prueba-respuesta GSM estándar, se puede proporcionar al SIM 16 por medio de la presente invención.

[0044] En respuesta a la petición MAP del MSC/VLR 30 para proporcionar un triplete autenticación, el SIDS 60 crea tal triplete de autenticación. Sin embargo, contrariamente a lo que sucede en un HLR/AUC convencional durante el procedimiento de autenticación puesta a prueba-respuesta de la norma GSM, el SIDS 60 no creará un número RAND que sea un número aleatorio de de 128 bits, sino un número RAND* con el mismo formato, es decir, también con un tamaño de 128 bits, en el que, al menos, algunos de los bits de dicho número RAND* comprenden datos de suscripción y/o instrucción (etapa S4 de la figura 2). En otras palabras, el SIDS 60 empaqueta o incrusta datos de suscripción y/o de instrucción en el número RAND* que tiene el mismo formato que el número RAND, utilizado en el procedimiento de autenticación GSM convencional. Es decir, el número RAND* es un portador OTA para los datos de suscripción y/o instrucción. Como sólamente el número RAND* será finalmente retransmitido desde el MSC/VLR 30 a la estación móvil 12 por medio de una petición de autenticación DTAP, los valores para la respuesta firmada y la clave de cifrado se puede elegir arbitrariamente, siempre y cuando el formato de estos elementos de datos cumpla con el formato definido por el procedimiento estándar de autenticación puesta a prueba-respuesta GSM y permite una conversión continua del mensaje MAP enviado desde el SIDS 60 al MSC/VLR 30 en la peteción DTAP enviada desde el MSC/VLR 30 a la estación móvil 12.

[0045] Como ya se mencionó anteriormente, de acuerdo con la presente invención es, en principio, es concebible que el número PIMSI que esta presente inicialmente en el SIM 16, consista solo en los datos de suscripción. Los datos de suscripción facilitados por el SIDS 60 en forma de un número RAND* incluyen un IMSI que permite al SIM 16 realizar el procedimiento estándar de autenticación puesta a prueba-respuesta GSM y para autenticarse a sí mismo con relación a la PLMN proporcionada por el sistema de comunicaciones móviles 10. Alternativamente, los datos de suscripción facilitados por el SIDS 60 en forma de un número RAND*, incluyen una clave de autenticación Ki para utilizarse durante el procedimiento de autenticación de puesta a prueba-respuesta GSM estándar. Adicionalmente, los datos de suscripción y/o instrución proporcionados por el SIDS 60 en forma de un número RAND*, incluyen instrucciones para realizar determinadas acciones, tales como "volver a intentar la recuperación de datos en 60 segundos", "utilizar una unidad de suministro de datos diferente" y similares.

[0046] El SIDS 60 puede configurarse para enviar los datos de suscripción/instrucción transportados por el número RAND* como texto sin cifrar. Esta variante se puede utilizar para datos de suscripción y/o instrucción que no son críticos desde una perspectiva de seguridad. Según otra variante, el SIDS 60 puede enviar simplemente un puntero o índice a un elemento específico de una lista, tal como una lista de conjuntos de instrucción diferentes o una lista de parejas de números IMSI y claves de autenticación Ki, o a un perfil de suscripción completo a partir de una lista de perfiles de suscripción disponibles pre-almacenado en el SIM 16. Como estas parejas de números IMSI y claves de autenticación Ki, se encuentra preferiblemente almacenadas también en el AUC 50, resulta posible para el AUC 50, una vez que ha recibido la misma información (es decir, el puntero o índice) desde el SIDS 60 (posiblemente a través del HLR 40), asignar una clave de autenticación Ki al número IMSI recibido desde el SIM 16 en el curso del procedimiento de autenticación de puesta a prueba-respuesta GSM estándar.

[0047] Según otra variante, el SIDS 60 puede estar configurado adicional o alternativamente para cifrar los datos de suscripción y/o instrucción transportados por el número RAND* por medio de una clave de cifrado almacenada en el SIDS 60. Para la extracción de los datos de suscripción/instrucción cifrados a partir del número RAND* recibido por el SIM 16, esta clave de cifrado también tiene que estar presente en el SIM 16. El SIDS 60 también puede configurarse para enviar los datos de suscripción y/o instrucción como un número RAND*, en el que los datos de suscripción y/o instrucción son una función del número RAND* y una clave maestra almacenada en el SIDS 60 y el SIM 16. Por ejemplo, la clave de autenticación Ki puede extraerse a partir de los datos de suscripción y/o instrucción, alimentando el número RAND* enviado por el SIDS 60 y la clave maestra almacenada en la tarjeta SIM 16 a un algoritmo de cifrado.

[0048] Una vez que el SIDS 60 ha creado un triplete de autenticación de la forma anteriormente descrita, será, como un HLR convencional durante el procedimiento de adscripción de puesta a prueba-respuesta GSM estándar, retransmitir al MSC/VLR 30 un mensaje de "Acuse recibo de Tripletes de Autenticación Enviados" de acuerdo con el protocolo MAP, incluyendo datos de suscripción y/o instrucción "enmascarados" como o transportados en un número RAND* (etapa S5 de la figura 2). Como el MSC/VLR 30 considera que el SIM 16 ha solicitado autenticación de acuerdo con el procedimiento de autenticación puesta a prueba-respuesta GSM estándar por medio de su PIMSI, el MSC/VLR 30 retransmite de forma transparente el número RAND* portante de los datos de suscripción/instrucción proporcionados por el SIDS 60 a través del subsistema de estación base 20 y la interfaz aérea OTA a la estación móvil 12 y su SIM 16 por medio de una petición de autenticación DTAP (etapa S6 de la figura 2).

[0049] Como el SIM 16 ha iniciado originalmente la recuperación de datos de suscripción y/o instrucción (etapa 1 de la figura 2), todavía se encuentra en un modo de recuperación de datos de suscripción/intrucción (preferiblemente pre-adscripción) y se considera recibido el número RAND* en la etapa 6 de la figura 2 desde el SIDS 60 conteniendo los datos de suscripción y/o instrucción. Como se describió anteriormente, los datos de suscripción y/o instrucción transportados por el número RAND* pueden estar en texto sin cifrar, cifrados o simplemente ser un puntero. Una vez que el SIM 16 ha extraído los datos de suscripción y/o instrucción del número RAND*, dichos datos extraídos se almacenan en una memoria no volátil del 16 SIM para su posterior utilización y/o ser ejecutadas cualesquiera instrucciones contenidas en el mismo.

[0050] En caso que el volumen o tamaño de los datos de suscripción y/o instrucción a enviar desde el SIDS 60 a la estación móvil 12, sea mayor que el tamaño de la puesta aprueba, por ejemplo, 128 bits en el caso del número RAND* del procedimiento de autenticación de puesta a prueba-respuesta GSM estándar, el procedimiento mostrado en la figura 2 se pueden repetir cuantas veces sea necesario para comunicar los datos de suscripción y/o instrucción transportados por varias puestas a prueba, por ejemplo, varios números RAND*.

[0051] De acuerdo con una realización preferida de la presente invención, en el SIM 16 se ejecuta una aplicación que gestiona el número RAND* de manera diferente, dependiendo de si el SIM 16 se encuentra en modo de recuperación de datos de suscripción/instrucción (preferiblemente pre-adscrito) o el modo "normal" listo para autenticación de acuerdo con el procedimiento de autenticación puesta a prueba-respuesta estándar GSM. La operación preferida de esta aplicación que se ejecuta en la tarjeta SIM 16 se ilustra en la figura 3. La aplicación que se ejecuta en el SIM 16 se inicia preferentemente de forma manual por un usuario de la estación móvil 12 o automáticamente, cuando la estación móvil 12 y el SIM 16 se inician por primera vez. La aplicación inicia la sesión de recuperación de datos de suscripción y/o instrucción mediante el envío del número PIMSI almacenado en el SIM 16 a la PLMN proporcionada por el sistema de comunicaciones móviles 10 (etapa S20 del procedimiento mostrado en la figura 3). En la etapa S21 del procedimiento mostrada en la figura 3, el SIM 16 recibe el número RAND* a partir del SIDS 60 (a través del MSC/VLR 30) y lo pasa a la aplicación que se ejecuta en el SIM 16. La aplicación determina si el SIM 16 se encuentra ya sea en el modo de recuperación de datos de suscripción/instrucción o en el modo normal (etapa S22 del procedimiento mostrado en la figura 3). Cuando la aplicación que se ejecuta en el SIM 16 determina que dicho SIM 16 se encuentra en el modo de recuperación de datos de suscripción/instrucción, la aplicación intentará extraer los datos de suscripción y/o instrucción del número RAND* enviado por el SIDS 60 (etapa S23 del procedimiento mostrado en la figura 3) y almacenar los datos extraídos del SIM 16 (etapa S24 del procedimiento mostrado en la figura 3) o llevar a cabo cualquier instrucción contenida en los mismos. A partir de ahí, la aplicación que se ejecuta en el SIM 16 cambia del modo de recuperación de datos de suscripción/instrucción al modo normal e inicia el procedimiento de adscripción de puesta a prueba -respuesta estándar GSM posiblemente usando un nuevo número IMSI que fue proporcionado por el SIDS 60 por medio del número RAND* (etapa S25 del procedimiento mostrado en la figura 3). Si en la etapa S22 del procedimiento mostrado en la figura 3 la aplicación que se ejecuta en el SIM 16 determina que dicho SIM 16 se encuentra en el modo normal, el número RAND* opcionalmente puede pasarse por el algoritmo de autenticación GSM estándar que se ejecuta en el SIM 16 (etapa S26 del procedimiento mostrado en la figura 3). De acuerdo con una realización preferida, cualquier fallo durante la sesión de recuperación de datos de suscripción/instrucción descrita anteriormente puede volver a inicializar el SIM 16 y la aplicación que se ejecuta en ella al modo de recuperación de datos de suscripción/instrucción. Aunque las etapas mostradas en la figura 3 se han descrito en el contexto de una aplicación que se ejecuta en la tarjeta SIM 16, la persona experta en la técnica apreciará que las mismas etapas podrían ser implementadas por medio de una aplicación que se ejecute en el equipo móvil 14 o dos aplicaciones que interactúan ejecutándose en el SIM 16 y en el equipo móvil 14, respectivamente.

[0052] Como ya se ha descrito anteriormente, una vez que el SIM 16 ha recibido y preferiblemente almacenado los datos de suscripción y/o instrucción proporcionados por el SIDS 60 en forma de un número RAND*, se puede conmutar al modo normal e iniciar el procedimiento de autenticación/adscripción de puesta a prueba-respuesta GSM estándar utilizando los datos de suscripción y/o instrucción proporcionados por el SIDS 60 (etapa S7 de la figura 2) mediante el envío de su (posiblemente nuevo) número IMSI al MSC/VLR 30 (etapa S8 de la figura 2). A partir de este punto, el SIM 16 se comporta como un SIM normal que ha sido provisto con los datos de suscripción obtenidos a partir del SIDS 60 en primer lugar, por ejemplo, durante la fabricación y/o proceso de personalización del mismo.

[0053] En la etapa S9 de la figura 2 el MSC/VLR 30 retransmite el número IMSI al HLR 40 y solicita la verificación de dicho número IMSI. El HLR 40 retransmite el número IMSI al AUC 50 y solicita tripletes de autenticación. Como ya se ha descrito en la sección de antecedentes de la presente invención, para la generación de un triplete de autenticación, por ejemplo, una respuesta firmada (SRES), un número RAND "normal" de 128 bits aleatorio y una clave de cifrado Kc, el AUC 50 necesita saber el número IMSI y la clave de autenticación asociada Ki, que debe ser idéntica a la clave de autenticación Ki que se almacena de forma segura en el SIM 16. Como se describió

anteriormente, esta información está disponible para el AUC 50, porque preferentemente el SIDS 60 ha informado al AUC 50 (posiblemente a través del HLR 40) durante el procedimiento de pre-adscripción sobre la clave de autenticación Ki que se asigna al número IMSI proporcionado al SIM 16.

[0054] El AUC 50 envía el triplete de autenticación junto con el número IMSI de retorno al HLR 40. El HLR 40 valida el número IMSI y luego retransmite el número IMSI y el triplete de autenticación de retorno al MSC/VLR 30 (etapa S10 de la figura 2). El MSC/VLR 30 almacena la SRES y la clave de cifrado Kc y retransmite el número RAND al BSS 20 y ordena al BSS 20 autenticar la estación móvil 12. El BSS 20 envía un mensaje de petición de autenticación a la estación móvil 12, siendo el número RAND el único parámetro que se envía a la estación móvil 12. La estación móvil 12 utiliza el número de RAND para calcular otra respuesta firmada (SRES*), basándose en el mismo algoritmo utilizado por el AUC 50 para calcular la SRES y envía la SRES de retorno al BSS 20, que retransmite la SRES * al MSC/VLR 30. El MSC/VLR 30 compara la SRES generada por el AUC 50 con la SRES* generada por la estación móvil 12. Si los dos números coinciden el SIM 16 se autentica y se conce acceso a la estación móvil 12 a la PLMN, proporcionada por los sistemas de comunicaciones móviles 10 y sus servicios. La clave de cifrado Kc se utiliza para cifrar todas las comunicaciones adicionales entre la estación móvil 12 y la PLMN. Como se apreciará por el experto en la técnica, las etapas finales del procedimiento de autenticación puesta a prueba -respuesta GSM estándar descrito anteriormente se han resumido como etapa S11 de la figura 2. Cabe señalar que las etapas S8 a S11 anteriormente descritas no implican al SIDS 60. En otras palabras, el SIDS 60 es preferiblemente transparente con respecto al procedimiento de autenticación/adscripción de puesta aprueba-respuesta GSM estándar.

[0055] La figura 4 muestra esquemáticamente los componentes de un sistema de comunicaciones móviles adicional 10'que es una variante del sistema de comunicaciones móviles 10 mostrado en la figura 1. El sistema de comunicaciones móviles 10' mostrado en la figura 4, difiere del sistema de comunicaciones móviles 10 mostrado en la figura 1 en que en el sistema de comunicaciones móviles 10', el servidor de datos de suscripción/instrucción se ha implementado junto con el HLR como una sola unidad, a saber, el HLR/SIDS 40'. De acuerdo con realizaciones preferidas, el SIDS se puede implementar en un HLR por hardware adicional y/o software, por ejemplo, como SIDS virtual. Proporcionar un SIDS virtual como parte del HLR tendría como ventaja que no serían necesarias modificaciones esenciales de hardware para implementar la presente invención en la infraestructura de hardware existente de una PLMN de GSM convencional.

[0056] La configuración del HLR y el SIDS como una sola unidad 40', tiene la ventaja sobre la configuración mostrada en la figura 1, donde el HLR 40 y el SIDS 60 son unidades separadas conectadas a través de un canal de comunicación externo adecuado, que no hay información crítica acerca de los datos de suscripción y/o instrucción que el SIDS 60 haya de enviar al SIM 16 en forma de número RAND* a comunicar a lo largo del canal de comunicación externo potencialmente inseguro entre el SIDS y el HLR y/o el AUC. Obviamente, el HLR / SIDS 40' tiene que estar configurado adecuadamente para ser capaz de distinguir entre un número IMSI solicitando un triplete de autenticación conteniendo un número RAND normal y un número PIMSI solicitando un triplete de autenticación con un número RAND* que contiene los datos de suscripción. También es concebible que en variantes adicionales, el SIDS está integrado como parte del AUC o como parte de una implementación del HLR y el AUC en una sola unidad.

[0057] De acuerdo con una realización preferida, la información sobre la sesión de recuperación de datos de suscripción/instrucción, por ejemplo, la ubicación del SIM 16 tal como se define por la Identidad de Área de Ubicación (LAI), puede ser utilizada por el SIM 16 y/o el SIDS 60, HLR/SIDS 40' para seleccionar los datos de suscripción y/o instrucción más adecuados para el SIM 16 a partir de varias opciones de datos de suscripción/instrucción. Alternativa o adicionalmente, el tipo de dispositivo, que podría ser codificado en el PIMSI, puede influir en la selección de un perfil de suscripción y/o un conjunto de instrucciones.

[0058] Aunque se ha descrito anteriormente que la presente invención puede emplearse ventajosamente antes de que el SIM 16 se haya adscrito o autenticado a si misma con éxito con respecto a la PLMN proporcionada por los sistemas de comunicaciones móviles 10 o 10', el experto en la técnica apreciará que la presente invención también se puede emplear después de que el SIM 16 se haya adscrito a la PLMN. Según la presente invención, es concebible que un SIM 16 conteniendo tanto un número IMSI “normal”, como un número PIMSI, como se describió anteriormente. En este caso, una aplicación que se ejecuta en el SIM 16 y/o en el equipo móvil 14 podría permitir a un usuario seleccionar ya sea adscribirse a la PLMN utilizando el número IMSI “normal” o solicitando los datos de suscripción y/o instrucción utilizando el número PIMSI.

[0059] Además, como será apreciado por el experto en la técnica, la presente invención también puede combinarse ventajosamente con otros procedimientos de gestión OTA de un SIM que sólo funciona después de que dicho SIM se haya autenticado en sí con respecto a una PLMN. Por ejemplo, en una primera fase de un proceso de recuperación de datos de suscripción y/o instrucción, el SIM podría por medio de la presente invención obtener esencialmente sólo aquellos de datos de suscripción y/o instrucción que son necesarios para una autenticación satisfactoria con respecto a una PLMN, en particular un número IMSI y/o una clave de autenticación Ki. Después de la autenticación del SIM con respecto a la PLMN, es decir, la adscripción del SIM a la PLMN, a partir de estos datos de suscripción esenciales, el SIM podría obtener más datos de suscripción, utilizando, por ejemplo, la aplicación AOD (On Demand Activation [Activación a petición]) descrita en el documento WO 2010/093312.

[0060] Según la presente invención, también es posible que más de una unidad de suministro de datos de suscripción y/o instrucción esté implicada en el proceso de pre-adscripción de obtención de datos de suscripción/instrucción. Por ejemplo, el SIM podría por medio de un primer PIMSI almacenado inicialmente el SIM, solicitar datos de suscripción y/o instrucción de una primera unidad de suministro de datos de

suscripción/instrucción. En respuesta, la primera unidad de suministro de suscripción/instrucción podría proporcionar un primer conjunto de datos de suscripción y/o instrucción incluyendo un segundo PIMSI refiriéndose a una segunda unidad de suministro de datos de suscripción y/o instrucción. Entonces, el SIM podría solicitar datos de suscripción y/o instrucción adicionales de una segunda unidad de suministro de datos de suscripción / instrucción por medio del segundo PIMSI proporcionado por la primera unidad de suministro de suscripción y/o como parte del primer conjunto de datos de suscripción y/o instrucción. Tal configuración podría realizarse, por ejemplo, por una combinación de las anteriormente descritas realizaciones preferidas primera y segunda, es decir, un sistema de comunicaciones móvil que tiene un primer servidor de datos de suscripción/instrucción (SIDS) 60, así como una unidad 40' que combina las funciones del HLR y un segundo SIDS.

[0061] Uno de los muchos posibles escenarios en donde la presente invención puede emplearse ventajosamente es el siguiente. A menudo, los productos de un fabricante de equipos originales (OEM) que fabrican, por ejemplo, productos de electrónica de consumo que están configurados para comunicarse a través de una red de comunicaciones móviles se venderán por un operador de una red de comunicación móvil de este tipo. En este caso, los conocimientos técnicos sobre los productos y sus características técnicas estará en el lado del OEM, mientras que el operador de la red tendrá información detallada sobre la red móvil. Por lo tanto, usando la presente invención podría ser ventajoso permitir a un OEM intervenir en una primera fase de suministro de datos de suscripción/instrucción y a un operador de red intervenir en una segunda fase subsiguiente al suministro de datos de suscripción/instrucción.En tal escenario el primer proceso de pre-adscripción se dirigirá a un primer SIDS manejado por el OEM, que proporcionará al SIM de un producto, por ejemplo, un nuevo PIMSI que está configurado para obtener más datos de suscripción y/o instrucción de un segundo SIDS manejado por el operador de red. Al hacerlo, el OEM, es decir, el operador de conexión inicial, puede mantenerse ajeno a detalles de suscripción sensibles del SIM (por ejemplo, la clave de autenticación Ki) sólo conocida por el operador de red. Además, otro SIDS puede ser operado por el fabricante del SIM.

[0062] La presente invención ha sido descrita en el contexto de algunas formas de realización ventajosas ejecutadas en una red GSM. Sin embargo, esto no debe ser interpretado como restricción la invención a los detalles de estas realizaciones, que se presentan sólo con fines ilustrativos, ya que la idea general de la presente invención también puede aplicarse en sistemas de comunicaciones móviles que no sean GSM que emplean un procedimiento puesta a prueba-respuesta para autenticar un abonado.

REIVINDICACIONES

1. Procedimiento para proporcionar datos de suscripción desde una unidad de suministro de datos (60; 40 ') a una estación móvil (12) para comunicación a través de un sistema de comunicaciones móviles (10; 10') implementada de acuerdo con norma GSM, en el que dicho procedimiento comprende las siguientes etapas en la unidad de suministro de datos (60; 40'):
recibir una petición desde la estación móvil (12) para iniciar un procedimiento de autenticación puesta a prueba-respuesta llevado a cabo en el sistema de comunicaciones móviles (10; 10'), en el que la petición contiene un elemento de datos indicador de modo;
crear una puesta a prueba que contiene datos de suscripción,
en el que el formato de la puesta a prueba cumple con el procedimiento de autenticación de puesta a prueba-respuesta implementado en el sistema de comunicaciones móviles (10; 10'); y
transmitir la puesta a prueba que transporta datos de suscripción a la estación móvil (12),
caracterizado dicho procedimiento porque los datos de suscripción transportados por la puesta a prueba permiten a la estación móvil (12) autenticarse a si misma con respecto al sistema de comunicaciones móviles (10; 10') utilizando el procedimiento de autenticación de puesta a prueba respuesta GSM y comprendiendo un número de IMSI y/o una clave de autenticación Ki.

2. Procedimiento para obtener datos de suscripción desde una unidad de suministro de datos (60; 40') por medio de un elemento de identificación seguro (16), preferiblemente un módulo de identificación de abonado, de una estación móvil (12) para comunicación a través de un sistema de comunicaciones móviles (10;10') implementado con la norma GSM, en el que dicho procedimiento comprende las siguientes etapas en el elemento de identificación segura (16):
proporcionar un elemento de datos indicador de modo a un equipo móvil (14) de la estación móvil (12),
en el que el equipo móvil (14) emite el elemento de datos indicador de modo como parte de una petición para iniciar un procedimiento de autenticación de puesta a prueba respuesta llevado a cabo en el sistema de comunicaciones móviles (10; 10');
recibir una puesta a prueba que transporta datos de suscripción emitida por la unidad de suministro de datos (60; 40'),
en el que el formato de la puesta a prueba cumple con el procedimiento de autenticación de puesta a prueba-respuesta implementado en el sistema de comunicaciones móviles (10; 10'); y
almacenar los datos de suscripción,
caracterizado dicho procedimiento porque los datos de suscripción transportados por la puesta a prueba permiten a la estación móvil (12) autenticarse con respecto al sistema de comunicaciones móviles (10; 10'), utilizando el procedimiento de autenticación de puesta a prueba respuesta GSM y comprendiendo un número de IMSI y/o una clave de autenticación Ki.

3. Procedimiento de las reivindicaciones 1 o 2, en el que el elemento de datos indicador de modo hace que el sistema de comunicaciones móviles (10; 10') retransmita la petición a la unidad de suministro de datos (60; 40') y/o informe a la unidad de suministro de datos (60; 40') que la estación móvil (12) está solicitando datos de suscripción.

4. Procedimiento de las reivindicaciones 1 o 2, en el que las etapas del procedimiento se llevan a cabo durante la comunicación antes que la estación móvil (12) se haya adscrito al sistema de comunicaciones móviles (10; 10') y,
en el que las etapas del procedimiento se repiten tantas veces como sea necesario, en caso de que el tamaño de los datos de suscripción sea mayor que el tamaño de la puesta a prueba.

5. Procedimiento de las reivindicaciones 1 o 2, en el que la selección de los datos de suscripción transportados por la puesta a prueba depende de la ubicación de la estación móvil (12) y/o del tipo de equipo móvil (14) de la estación móvil (12).

6. Procedimiento de la reivindicación 1, en el que la puesta a prueba se crea como un número RAND* de 128 bits que transporta los datos de suscripción, preferiblemente como parte de un triplete de autenticación que comprende además una respuesta firmada SRES y una clave de cifrado Kc de acuerdo con el procedimiento de autenticación puesta a prueba-respuesta GSM.

7. Procedimiento de la reivindicación 1, en el que el elemento de datos indicador de modo es un número IMSI (PIMSI) preliminar que define la dirección de la unidad de suministro de datos (60; 40') y que tiene el mismo formato que un número IMSI.

8. Unidad de suministro de datos (60; 40') para proporcionar a una estación móvil (12) datos de suscripción para comunicación a través de un sistema de comunicaciones móviles (10,10') implementado de acuerdo con la norma GSM, en el que la unidad de suministro de datos (60; 40') está configurada para:
recibir una petición desde la estación móvil (12) para iniciar un procedimiento de autenticación de puesta a prueba-respuesta implementado en el sistema de comunicaciones móviles (10, 10') y que comprende un elemento de datos indicador de modo;

crear una puesta a prueba que contiene datos de suscripción,
en el que el formato de la puesta a prueba cumple con el procedimiento de autenticación puesta a prueba-respuesta implementado en el sistema de comunicaciones móviles (10, 10'); y
transmitir la puesta a prueba que contiene datos de suscripción a la estación móvil (12), caracterizado dicha unidad de suministro de datos porque
los datos de suscripción transportado por la puesta a prueba permiten a la estación móvil (12) autenticarse con respecto al sistema de comunicaciones móviles (10; 10'), utilizando el procedimiento de autenticación puesta a prueba-respuesta GSM y comprende un número IMSI y/o una clave de autenticación Ki.

9. Unidad de suministro de datos de la reivindicación 8, en la que el elemento de datos indicador de modo hace que el sistema de comunicaciones móviles (10; 10') retrasmita la petición a dicha unidad de suministro de datos (60; 40') y/o informe a dicha unidad de suministro datos (60; 40') que la estación móvil (12) está solicitando datos de suscripción.

10. Unidad de suministro de datos de las reivindicaciones 8 o 9, en la que dicha unidad de suministro de datos (60; 40') es un servidor de datos de suscripción dedicado (60) o parte de un registro de posiciones base (40') del sistema de comunicaciones móviles (10').

11. Elemento de identificación seguro (16), preferiblemente un módulo de identificación de abonado, para una estación móvil (12) para comunicación a través de un sistema de comunicaciones móviles (10; 10'), implementado de acuerdo con la norma GSM, en el que dicho elemento de identificación segura (16) está configurado para:
proporcionar un elemento de datos indicador de modo a un equipo móvil (14) de la estación móvil (12),
en el que el equipo móvil (14) emite dicho elemento de datos indicador de modo como parte de una petición para iniciar un procedimiento de autenticación de puesta a prueba-respuesta implementado en el sistema de comunicaciones móviles (10; 10');
recibir una puesta a prueba que transporta datos de suscripción emitida por una unidad de suministro de datos (60; 40'),
en el que el formato de la puesta a prueba cumple con el procedimiento de autenticación de puesta a prueba-respuesta implementado en el sistema de comunicaciones móviles (10; 10'); y
almacenar los datos de suscripción,
caracterizado dicho elemento de identificación segura porque los datos de suscripción transportados por la puesta a prueba permiten a la estación móvil (12) autenticarse con respecto al sistema de comunicaciones móviles (10; 10'), utilizando el procedimiento de autenticación de puesta a prueba-respuesta GSM y que comprende un número de IMSI y/o una clave de autenticación Ki.

12. Elemento de identificación seguro de la reivindicación 11, en el que el elemento de datos indicador de modo hace que el sistema de comunicaciones móviles (10; 10') retransmita la petición a la unidad de suministro de datos (60; 40') y/o informe a la unidad de suministro de datos (60; 40') que la estación móvil (12) está solicitando datos de suscripción.

13. Sistema móvil de comunicaciones (10; 10') que comprende una unidad de suministro de datos (60; 40') para proporcionar datos de suscripción de acuerdo con las reivindicaciones 8, 9 o 10 y una estación móvil (12) con un elemento de identificación seguro (16), preferiblemente un módulo de identificación de abonado, de acuerdo con las reivindicaciones 11 o 12.

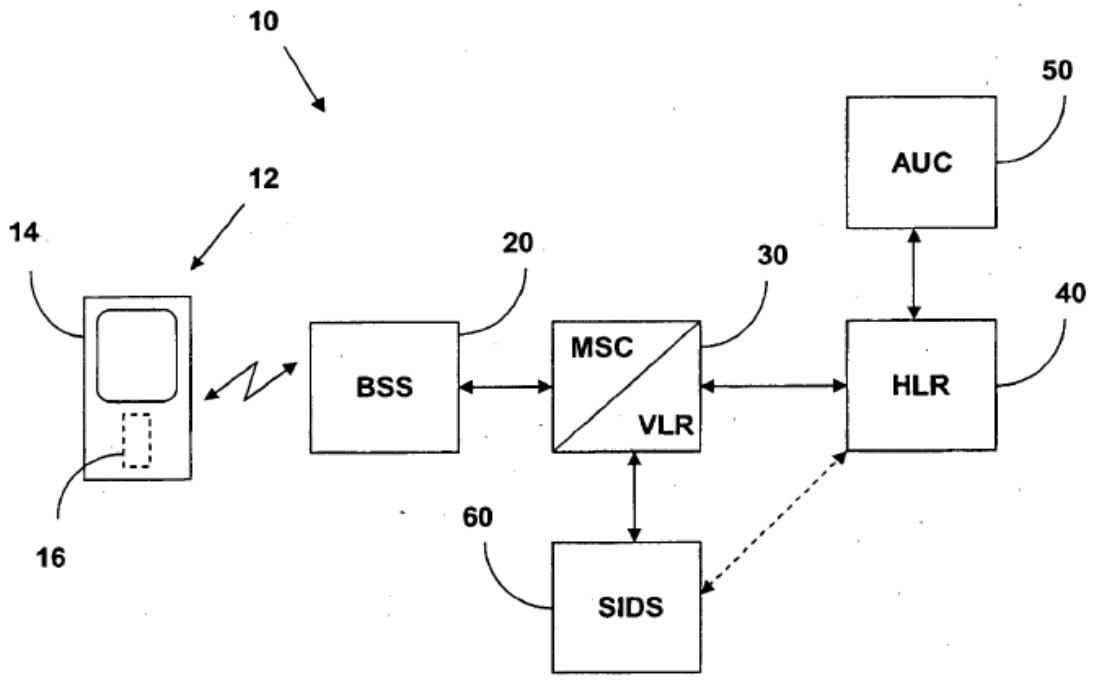

Fig. 1

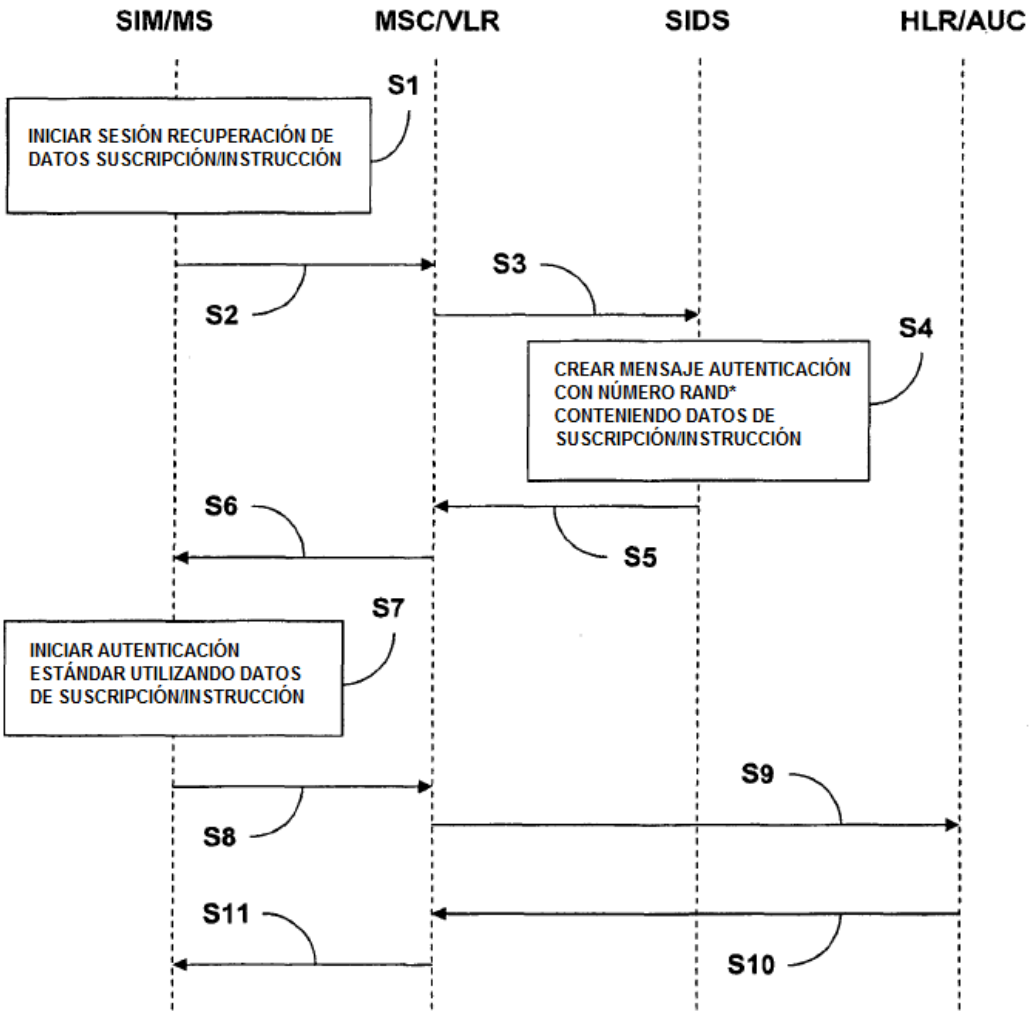
SIM/MS
MSC/VLR
SIDS
HLR/AUC
S1
INICIAR SESIÓN RECUPERACIÓN DE DATOS SUSCRIPCIÓN/INSTRUCCIÓN
S2
S3
S4
CREAR MENSAJE AUTENTICACIÓN CON NÚMERO RAND* CONTENIENDO DATOS DE SUSCRIPCIÓN/INSTRUCCIÓN
S5
S6
S7
INICIAR AUTENTICACIÓN ESTÁNDAR UTILIZANDO DATOS DE SUSCRIPCIÓN/INSTRUCCIÓN
S8
S9
S10
S11

Fig. 2

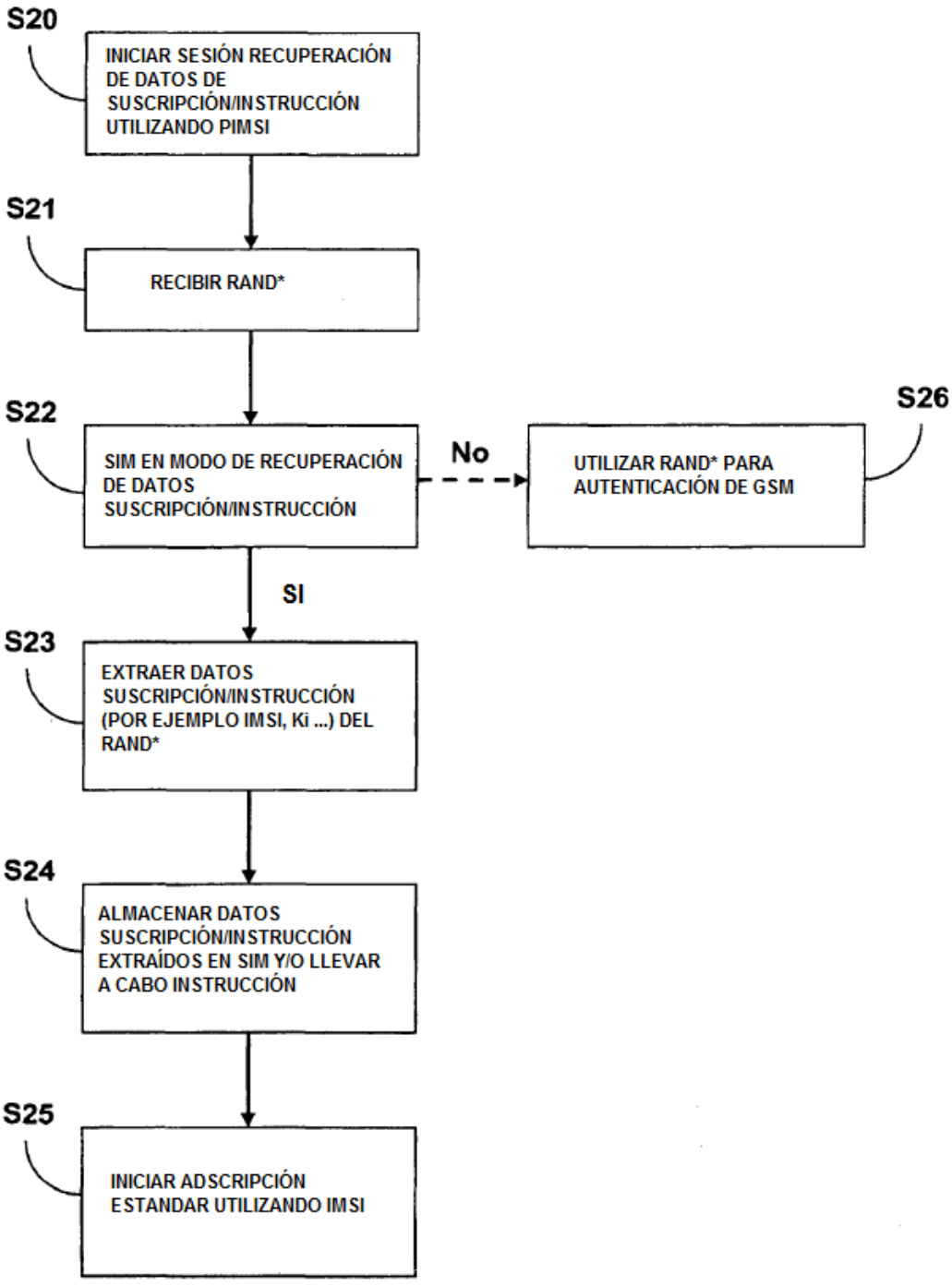
S20
INICIAR SESIÓN RECUPERACIÓN DE DATOS DE SUSCRIPCIÓN/INSTRUCCIÓN UTILIZANDO PIMSI
S21
RECIBIR RAND*
S22
SIM EN MODO DE RECUPERACIÓN DE DATOS SUSCRIPCIÓN/INSTRUCCIÓN
No
S26
UTILIZAR RAND* PARA AUTENTICACIÓN DE GSM
SI
S23
EXTRAER DATOS SUSCRIPCIÓN/INSTRUCCIÓN (POR EJEMPLO IMSI, Ki ...) DEL RAND*
S24
ALMACENAR DATOS SUSCRIPCIÓN/INSTRUCCIÓN EXTRAÍDOS EN SIM Y/O LLEVAR A CABO INSTRUCCIÓN
S25
INICIAR ADSCRIPCIÓN ESTANDAR UTILIZANDO IMSI

Fig. 3

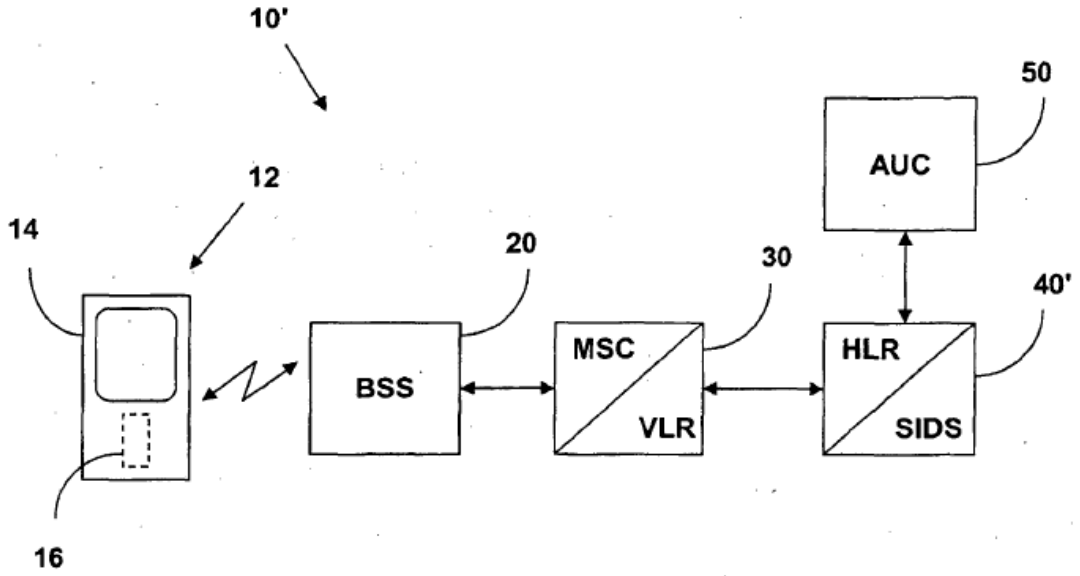

Fig. 4

REFERENCIAS CITADAS EN LA DESCRIPCIÓN

La lista de referencias citada por el solicitante lo es solamente para utilidad del lector, no formando parte de los documentos de patente europeos. Aún cuando las referencias han sido cuidadosamente recopiladas, no pueden excluirse errores u omisiones y la OEP rechaza toda responsabilidad a este respecto.

Documentos de patente citados en la descripción

- WO 2010093312 A **[0009] [0059]**
- US 2009217038 A **[0011]**