(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 633 351**

(51) Int. CI.:

H04W 8/26 (2009.01)
H04W 8/20 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **09.08.2013 E 13003978 (7)**

(97) Fecha y número de publicación de la concesión europea: **21.06.2017 EP 2835994**

(54) Título: **Procedimientos y dispositivos para realizar un cambio de red móvil**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
20.09.2017

(73) Titular/es:

GIESECKE+DEVRIENT MOBILE SECURITY GMBH (100.0%)
Prinzregentenstraße 159
81677 München, DE

(72) Inventor/es:

HUBER, ULRICH y
LARSSON, THOMAS

(74) Agente/Representante:

DURÁN MOYA, Luis Alfonso

DESCRIPCIÓN

Procedimientos y dispositivos para realizar un cambio de red móvil

Sector de la invención

La invención se refiere a las comunicaciones móviles en general y, en particular, a procedimientos y dispositivos para que un terminal móvil que comprende un elemento seguro, tal como un módulo de identidad de abonado (SIM), una tarjeta eUICC/UICC o similares, realice un cambio de un primer perfil de suscripción para conectarse a una primera red móvil a un segundo perfil de suscripción para conectarse a una segunda red móvil.

Antecedentes de la invención

La comunicación por medio de un terminal móvil, tal como un teléfono móvil, a través de una red móvil terrestre pública (PLMN; también denominada una red de comunicaciones móvil o celular en la presente memoria) gestionada por un operador de red móvil (MNO), en general, requiere que el terminal móvil esté equipado con un elemento seguro para almacenar de forma segura datos que identifican unívocamente al usuario del terminal móvil (también denominado abonado). Por ejemplo, en el contexto de un terminal móvil configurado para comunicarse según el Sistema global para comunicaciones móviles (GSM), actualmente el estándar más popular del mundo para sistemas de comunicaciones móviles, el elemento seguro se denomina módulo de identidad de abonado (SIM) y normalmente se proporciona en forma de una tarjeta inteligente. Según el estándar GSM, cuyas características técnicas se definen mediante un gran número de especificaciones interrelacionadas y mutuamente dependientes publicadas por la organización de estandarización ETSI, el SIM contiene las credenciales de la suscripción para autenticar e identificar al usuario del terminal móvil, incluyendo, en particular, una identidad internacional de abonado móvil (IMSI) y una clave de autenticación Ki. En general, el fabricante/proveedor del SIM o el MNO almacenan estas credenciales de la suscripción en el SIM como parte de un perfil de la suscripción durante un proceso de personalización del SIM antes de entregar al usuario del terminal móvil su SIM. Un SIM no personalizado, en general, no es adecuado para usarse en un terminal móvil, es decir, no es posible usar los servicios proporcionados por una PLMN con un SIM no personalizado sin un perfil de suscripción.

Un campo de aplicación particular de los elementos seguros, tales como SIM, eUICC, UICC y similares, que se espera que crezca con rapidez en el futuro, es la comunicación M2M (máquina a máquina), es decir, la comunicación entre máquinas sobre una red de comunicaciones celular sin intervención humana, también denominada Internet de las cosas. En la comunicación M2M los datos se transmiten de forma automática entre muchos tipos diferentes de máquinas equipadas con un elemento seguro en forma de un módulo M2M, tales como sistemas de TV, decodificadores, máquinas expendedoras, vehículos, semáforos, cámaras de vigilancia, dispositivos sensores y similares. Es previsible que al menos para algunos de estos dispositivos no será posible, o al menos será muy difícil, proporcionar con antelación al elemento seguro un perfil de suscripción, incluyendo por ejemplo una IMSI. Esto se debe a que en muchos dispositivos M2M el elemento seguro se implementará muy probablemente en forma de un chip o un módulo de chip montado en la superficie sin posibilidad de proporcionar al elemento seguro un perfil de suscripción con antelación. En consecuencia, una vez sobre el terreno, estos dispositivos M2M y sus elementos seguros no personalizados, en general, necesitarán la provisión de un perfil de suscripción de forma inalámbrica.

Cuando se utilizan los servicios proporcionados por un MNO, en particular la comunicación a través de la PLMN proporcionada por el MNO, normalmente el MNO cobra al usuario de un terminal móvil una determinada tarifa mensual. Si el usuario móvil desea, por ejemplo debido a una tarifa mensual inferior y/o a mejores servicios, cambiar a un MNO diferente, en general debe sustituir manualmente el SIM proporcionado por el MNO actual y que contiene el perfil de suscripción necesario para conectarse a la PLMN del MNO actual por el SIM proporcionado por el nuevo MNO y que contiene el perfil de suscripción necesario para conectarse a la PLMN del nuevo MNO. Ciertamente, sería más sencillo para el usuario, si en lugar de este proceso convencional de cambiar a un nuevo MNO sustituyendo manualmente el SIM fuese posible usar el mismo elemento seguro en forma de un SIM que puede "reprogramarse" de forma inalámbrica.

Se conocen procedimientos convencionales para descargar un perfil de suscripción objetivo de forma inalámbrica en un elemento seguro con un perfil de suscripción ya existente y realizar un cambio del perfil de suscripción ya existente al perfil de suscripción objetivo asociado con una red móvil deseada. Además, se conoce la confirmación del cambio correcto a la red móvil objetivo usando un mensaje SMS o USSD o por medio de un BIP (protocolo independiente de la portadora). Sin embargo, estos medios de comunicación para confirmar un cambio de red móvil no siempre están disponibles, por ejemplo, porque no puede utilizarse el SMS en la red móvil objetivo debido a que todavía no hay crédito. No obstante, también en estos casos es importante saber si el cambio a una red móvil objetivo ha sido correcto, especialmente en el campo de los dispositivos M2M, es decir, dispositivos que no están supervisados directamente por un usuario. Por tanto, existe la necesidad de procedimientos y dispositivos mejorados para que un terminal móvil que comprende un elemento seguro, tal como un módulo de identidad de abonado (SIM), una tarjeta eUICC/UICC o similares, realice un cambio desde una primera red móvil a una segunda red móvil.

El informe final "SIM reprogramables: tecnología, evolución e implicaciones", 2012, da a conocer soluciones para cambiar de utilizar un primer identificador a un segundo identificador para conectarse a una primera y una segunda redes respectivas.

Características de la invención

El objetivo anterior se consigue según la presente invención mediante el contenido de las reivindicaciones independientes. Las realizaciones preferentes de la invención se definen en las reivindicaciones dependientes.

Según un primer aspecto, la invención da a conocer un procedimiento para que un terminal móvil que comprende un elemento seguro realice un cambio desde una primera red móvil (también denominada en la presente memoria red móvil de aprovisionamiento) a una segunda red móvil (también denominada en la presente memoria como red móvil objetivo). El procedimiento comprende las etapas de: (a) conexión a la primera red móvil utilizando un primer mensaje de conexión que contiene un primer elemento de datos de identificación, de un primer perfil de suscripción; y (b) conexión a la segunda red móvil mediante un proceso de conexión que incluye un segundo mensaje de conexión que contiene un segundo elemento de datos de identificación, de un segundo perfil de suscripción, en el que la segunda red móvil está configurada para supervisar, al menos, partes del proceso de conexión, para determinar el segundo elemento de datos de identificación incluido en el mismo y para enviar esta información a un servidor de gestión de la suscripción con el fin de confirmar la conexión correcta del elemento seguro a la segunda red móvil.

Preferentemente, la segunda red móvil está configurada para detectar el segundo mensaje de conexión que contiene el segundo elemento de datos de identificación. Según las realizaciones preferentes de la invención, el procedimiento comprende la siguiente etapa adicional tras la etapa (b): (c) confirmación al elemento seguro de que el cambio ha sido correcto. Preferentemente, en la etapa (c) el servidor de gestión seguro proporciona al elemento seguro el MSIS-DN asignado al segundo elemento de datos de identificación en la segunda red móvil.

Preferentemente, el elemento seguro descarga el segundo perfil de suscripción que incluye el segundo elemento de datos de identificación desde el servidor de gestión de la suscripción, mientras el elemento seguro está conectado a la primera red móvil.

Según las realizaciones preferentes de la invención, la etapa de descargar el segundo perfil de suscripción incluye la etapa adicional de recibir comandos del servidor de gestión de la suscripción para que el elemento seguro los ejecute.

Preferentemente, el procedimiento incluye la etapa adicional de informar a la segunda red móvil del segundo elemento de datos de identificación con el fin de que la segunda red móvil pueda supervisar los procesos de conexión respectivos.

Según las realizaciones preferentes de la invención, la segunda red móvil comprende una unidad de supervisión de la señal que está implementada en hardware y/o software y está configurada para supervisar al menos partes del proceso de conexión, para determinar el segundo elemento de datos de identificación incluido en el mismo y para enviar esta información a un servidor de gestión de la suscripción con el fin de confirmar la conexión correcta del elemento seguro a la segunda red móvil.

Preferentemente, la primera red móvil y/o la segunda red móvil se gestionan según el estándar GSM y el segundo mensaje de conexión es un mensaje "enviar información de autenticación".

Según las realizaciones preferentes de la invención, el primer perfil de suscripción es un perfil de suscripción provisional que se almacena en el elemento seguro durante el proceso de fabricación y/o personalización del terminal móvil y/o el elemento seguro.

Según un segundo aspecto, la invención da a conocer un elemento seguro que realiza las etapas del procedimiento según el primer aspecto de la invención.

Preferentemente, el elemento seguro es un módulo de identidad de abonado (SIM) para la autenticación/identificación de un abonado en la red móvil. Dicho SIM se comunica con el terminal móvil a través de un lector de tarjetas en el mismo y puede retirarse en principio del terminal móvil para sustituirse por un SIM diferente y/o bien para utilizarse en un terminal móvil diferente. De forma alternativa, el elemento seguro es una parte integral del terminal móvil, tal como un módulo de chip cableado. Dichos elementos seguros incorporados se conocen, por ejemplo, como tarjetas de circuitos integrados universales incorporadas (eUICC). Preferentemente, el elemento seguro admite el almacenamiento de múltiples perfiles de suscripción que pueden asociarse con MNO diferentes. En general, solo un perfil de suscripción está activo a la vez.

Según un tercer aspecto, la invención da a conocer un terminal móvil que contiene un elemento seguro según el

segundo aspecto de la invención.

El terminal móvil según la presente invención comprende medios para comunicarse con una red de comunicaciones celular, con el fin de recibir un nuevo perfil de suscripción. Preferentemente, el terminal móvil se implementa en forma de un teléfono inteligente, un PC de tableta, un ordenador portátil, una PDA, o similares. De forma alternativa, el terminal móvil puede ser un dispositivo multimedia tal como un marco de fotos digital, un equipo de sonido, un sistema de TV, un decodificador, un lector de libros electrónicos, etc. A modo de ejemplo, el término "terminal móvil" también incluye cualquier clase de maquinaria, como máquinas expendedoras, vehículos, medidores inteligentes y similares que están configurados para comunicarse a través de un sistema de comunicaciones celular en el contexto de un sistema M2M.

Según un cuarto aspecto, la invención da a conocer un servidor de gestión de la suscripción configurado para interactuar con el elemento seguro según el segundo aspecto de la invención según el procedimiento según el primer aspecto de la invención.

Estas y otras funciones, características, ventajas y objetivos de la invención serán evidentes a partir de la siguiente descripción detallada de las realizaciones preferentes, proporcionadas como un ejemplo no limitativo, haciendo referencia a los dibujos adjuntos. El experto en la materia apreciará, en particular, que las realizaciones preferentes anteriores pueden combinarse de varias formas, que darán lugar a realizaciones ventajosas adicionales que están explícitamente soportadas y cubiertas por la presente invención. En particular, el experto en la materia apreciará que las realizaciones preferentes descritas anteriormente pueden implementarse en el contexto de los diferentes aspectos de la invención mencionados anteriormente.

Breve descripción de los dibujos

La figura 1 muestra una vista general esquemática de un sistema de comunicaciones móviles que ilustra diferentes aspectos de la presente invención; y

la figura 2 muestra un diagrama que ilustra un procedimiento para realizar un cambio de red móvil de una primera red móvil a una segunda red móvil del sistema de comunicaciones móviles de la figura 1 según una realización preferente de la invención.

Descripción detallada de las realizaciones preferentes

La figura 1 muestra esquemáticamente los componentes de un sistema de comunicación -10-, así como algunos de los canales o enlaces de comunicación entre los componentes de este sistema -10- que ilustran diferentes aspectos de la presente invención. Aunque la descripción detallada siguiente se referirá a un terminal "móvil", el experto en la materia apreciará que la presente invención puede implementarse de forma ventajosa en el contexto de cualquier tipo de terminal que esté configurado para comunicarse a través de una red de comunicaciones móvil o celular. En otras palabras, el atributo "móvil" usado en la presente memoria se refiere a la capacidad de un terminal de comunicarse a través de una red de comunicaciones móvil o celular (o red móvil corta), incluyendo también las redes de comunicaciones móviles basadas en IP.

En la figura 1 se muestra un terminal móvil -12- a modo de ejemplo que incluye un elemento seguro -14- para almacenar de forma segura y procesar datos que identifican unívocamente al terminal móvil -12- y/o a su usuario, es decir, el abonado. Como se indica en la figura 1, el terminal móvil -12- es preferentemente un teléfono móvil, un teléfono inteligente o un dispositivo similar. Sin embargo, el experto en la materia apreciará que el terminal móvil -12- según la presente invención puede implementarse también en forma de otros dispositivos, tales como una tableta o un ordenador portátil, un sistema de TV, un decodificador, una máquina expendedora, un vehículo, una cámara de vigilancia, un dispositivo sensor y similares.

Según las realizaciones preferentes de la invención, el elemento seguro -14- está configurado como una tarjeta eUICC o UICC con una aplicación de SIM ejecutándose en la misma, es decir, un elemento seguro que puede estar montado en el terminal móvil -12- y utilizarse en sistemas de comunicaciones celulares para una identificación de abonado única y segura así como para la provisión de diferentes funciones especiales y servicios de valor añadido. De forma alternativa, el elemento seguro -14- podría estar configurado como un módulo de identidad de abonado (SIM) extraíble, siendo el SIM actualmente el tipo de elemento seguro más popular. Sin embargo, el experto en la materia apreciará que también se incluyen en la presente invención otros tipos de elementos seguros que, dependiendo de la generación subyacente y del tipo de estándar del sistema de comunicaciones celular, se designan como USIM, R-UIM, ISIM y similares. Además, el elemento seguro -14- podría ser un módulo M2M o un entorno de ejecución fiable (TEE) implementado como parte del terminal móvil -12-.

El terminal móvil -12- está configurado para comunicarse a través de la interfaz aérea (o enlace de radio) con una primera red de comunicaciones celular o red móvil terrestre pública (PLMN) -30- o una segunda red de comunicaciones celular o red móvil terrestre pública (PLMN) -40- de un sistema de comunicaciones móvil -20-. Preferentemente, la primera PLMN -30- (también denominada en la presente memoria PLMN de aprovisionamiento

-30-) está gestionada por un primer operador de red móvil (MNO) y la segunda PLMN -40- (también denominada en la presente memoria PLMN objetivo -40-) está gestionada por un segundo operador de red móvil (MNO). Preferentemente, se puede acceder a la PLMN de aprovisionamiento -30- y a la PLMN objetivo -40- desde sustancialmente la misma localización física. Según las realizaciones preferentes, la PLMN de aprovisionamiento -30- y/o la PLMN objetivo -40- se gestionan según el estándar GSM.

En lo que sigue, se describirán las realizaciones preferentes de la invención en el contexto de redes de comunicaciones móviles o celulares según los estándares del Sistema global para las comunicaciones móviles (GSM), como se especifica en diversas especificaciones proporcionadas por el ETSI. Sin embargo, el experto en la materia apreciará que la presente invención puede aplicarse también de forma ventajosa en conexión con otros sistemas de comunicaciones celulares. Dichos sistemas incluyen sistemas de comunicaciones celulares de tercera generación (3GPP), tales como el Sistema universal de telecomunicaciones móviles (UMTS), y redes móviles de nueva generación o cuarta generación (4G), tales como Evolución a largo plazo (LTE), así como otros sistemas de comunicaciones celulares.

Como es bien conocido para el experto en la materia, una PLMN configurada según el estándar GSM en general comprende un sub-sistema de estaciones base formado por una o más estaciones base transceptoras que definen celdas respectivas de la PLMN y están conectadas a un controlador de estaciones base. En general, el controlador de estaciones base es uno de varios controladores de estaciones base que se comunican con un centro de conmutación móvil (MSC) común. A menudo, una base de datos local denominada registro de localización de visitantes (VLR) para mantener un seguimiento de los usuarios móviles ubicados actualmente dentro de las celdas cubiertas por un MSC (es decir, el área de servicio del MSC) está incorporada al MSC. El MSC proporciona esencialmente la misma funcionalidad que una central de conmutación en una red telefónica pública conmutada y adicionalmente es responsable del procesamiento de las llamadas, la gestión de la movilidad y la gestión de los recursos de radio. El MSC también está en comunicación con un registro de localización local (HLR), que es la base de datos principal de la PLMN que almacena información sobre sus usuarios móviles requerida para la autenticación. Con este fin, el HLR, en general, está en comunicación con un centro de autenticación (AUC). El experto en la materia apreciará que, aunque los componentes descritos anteriormente de un sistema GSM convencional pueden tener distintos nombres en estándares distintos o consecutivos para redes de comunicaciones móviles, los principios subyacentes utilizados en la presente memoria son sustancialmente similares y, por lo tanto, son compatibles con la presente invención.

Como sabe el experto en la materia, los medios de comunicación entre los componentes descritos anteriormente de una PLMN pueden ser propietarios o pueden utilizar estándares abiertos. Los protocolos pueden ser SS7 o basados en IP.

SS7 es un estándar global para telecomunicaciones definido por el sector de estandarización de telecomunicaciones (ITU-T) de la Unión internacional de telecomunicaciones (ITU). El estándar define los procedimientos y los protocolos mediante los que los elementos de red de la red telefónica pública conmutada (PSTN) intercambian información sobre una red de señalización digital para llevar a cabo el establecimiento, el encaminamiento y el control inalámbrico (celular) y por cable de las llamadas. Por ejemplo, la red y el protocolo SS7 se utilizan para el establecimiento básico de llamadas, la gestión, los servicios inalámbricos, la itinerancia inalámbrica, y la autenticación de abonados móviles, es decir, características mejoradas de las llamadas que proporcionan telecomunicaciones eficientes y seguras a nivel mundial. La forma en que los elementos de red se agrupan o se dejan separados y las interfaces (ya sean propietarias o abiertas) entre estos elementos se deja al MNO.

De los componentes descritos anteriormente de una PLMN solo los siguientes se muestran en el dibujo esquemático de la figura 1 para facilitar la explicación: una estación base transceptora -32- y un HLR -34- a modo de ejemplo para la PLMN de aprovisionamiento -30- y una estación base transceptora -42- y un HLR -44- a modo de ejemplo para la PLMN objetivo -40-. Cada una de la PLMN de aprovisionamiento -30- y la PLMN objetivo -40- están al menos en comunicación temporal con un servidor de gestión de la suscripción -50-, como se describirá con más detalle más adelante. Además, cada una de la PLMN de aprovisionamiento -30- y/o la PLMN objetivo -40- podrían comprender un SMS-C (centro de servicios de mensajes cortos) para almacenar, enviar, convertir y entregar mensajes SMS o estar conectadas a un SMS-C común.

Como se puede deducir a partir de la vista ampliada del elemento seguro -14- en la figura 1, el elemento seguro -14- preferentemente comprende una unidad central de procesamiento (CPU) -15-. Preferentemente, la CPU -15- está configurada de tal manera que al menos una aplicación de gestión de la suscripción -16- (miniaplicación de SM) puede ejecutarse en la CPU -15- proporcionando algunas de las características que se describirán en el contexto de la figura 2 con más detalle más adelante. La aplicación de gestión de la suscripción -16- podría implementarse, por ejemplo, como una miniaplicación Java. Para proporcionar un entorno de ejecución para la aplicación de gestión de la suscripción -16-, un sistema operativo del elemento seguro (no mostrado en la figura 1) se implementa preferentemente en la CPU -15-.

Además, el elemento seguro -14- preferentemente comprende una unidad de memoria -17-, que preferentemente se implementa como una unidad de memoria regrabable no volátil, por ejemplo, una memoria flash. Como se puede

deducir a partir de la figura 1, un primer perfil de la suscripción (SUB) -18a- se almacena en la unidad de memoria -17- del elemento seguro -14-. Este primer perfil de la suscripción -18a- comprende datos que permiten al elemento seguro -14- y al terminal móvil -12- conectarse a la PLMN de aprovisionamiento -30-, es decir, datos tales como credenciales de la suscripción, un algoritmo de autenticación específico del MNO, y similares. Preferentemente, al menos partes de la unidad de memoria -17- del elemento seguro -14- están configuradas para almacenar de forma segura los datos en las mismas, por ejemplo las credenciales de la suscripción que se desean mantener en secreto, tales como una identidad internacional de abonado móvil (IMSI) y/o una clave de autenticación Ki, que son parte del primer perfil de suscripción -18a-. Como se indica en la figura 1, la unidad de memoria -17- preferentemente proporciona varias "posiciones" para acomodar perfiles de suscripción adicionales, tales como un segundo perfil de suscripción (SUB) -18b-, que se proporciona preferentemente mediante el servidor de gestión de la suscripción -50- según el proceso mostrado en la figura 2 y descrito con más detalle más adelante.

Preferentemente, el primer perfil de suscripción -18a- se almacena en la unidad de memoria -17- del elemento seguro -14- durante el proceso de fabricación y/o personalización del terminal móvil -12- y/o su elemento seguro -14-. Especialmente en el contexto de esta realización preferente es concebible que el primer perfil de suscripción -18a- sea sencillamente un perfil de suscripción provisional que solo proporciona servicios básicos que permiten al elemento seguro -14- y al terminal móvil -12- comunicarse con el servidor de gestión de la suscripción -50- a través de la PLMN de aprovisionamiento -30- y descargar un perfil de suscripción más completo que proporciona servicios adicionales, tal como el segundo perfil de suscripción -18b- mostrado en la figura 1. Como un perfil de suscripción provisional, tal como el primer perfil de suscripción -18a- mostrado en la figura 1, en general proporciona solo una funcionalidad limitada, el usuario del terminal móvil -12- en general estará tentado a cambiar a un perfil de suscripción más completo que proporciona servicios adicionales, tal como el segundo perfil de suscripción -18b- mostrado en la figura 1.

Como sabe el experto en la materia, una de las etapas esenciales implicadas en un procedimiento de conexión GSM convencional es que el elemento seguro -14- tiene que proporcionar un elemento de datos de identificación en forma de una IMSI (que es parte de un perfil de suscripción) a la PLMN objetivo -40- con el fin de que la PLMN objetivo -40- pueda identificar al elemento seguro -14-. De forma más específica, el elemento seguro -14- envía un mensaje "enviar información de autenticación" que incluye la IMSI utilizando el protocolo MAP (parte de aplicación móvil) a la PLMN objetivo -40-. En el procedimiento de conexión GSM convencional este mensaje se encamina mediante el centro de conmutación móvil (MSC) de recepción basándose en la IMSI incluida en el mismo al registro de localización local (HLR) -44- de la PLMN objetivo -40- para solicitar tripletas de autenticación.

Cuando el HLR -44- de la PLMN objetivo -40- recibe la IMSI y la petición de tripletas de autenticación, en primer lugar comprueba su base de datos para asegurarse de que la IMSI es válida y está registrada en la red. Una vez que esto se ha conseguido, el HLR -44- de la PLMN objetivo -40- envía la IMSI y la petición de tripletas de autenticación a su 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 denominado respuesta firmada (SRES). El número RAND y la clave de autenticación Ki también se introducen en el algoritmo de cifrado A8. La salida es un número de 64 bits denominado Kc. Kc es la clave de cifrado que se usa en el algoritmo de cifrado A5 para cifrar y descifrar los datos que se están transmitiendo sobre la interfaz aérea al terminal móvil -12-. El número RAND, la SRES y la clave de cifrado Kc forman una tripleta de autenticación que es única para la IMSI utilizada para crear esta tripleta. Una vez que el AUC de la PLMN objetivo -40- ha generado dicha tripleta de autenticación, la envía al HLR -44- que, a su vez, la envía al MSC solicitante. El MSC almacena la clave de cifrado Kc y la SRES pero envía el número RAND como la pregunta del procedimiento de autenticación GSM al elemento seguro -14- del terminal móvil -12- y solicita autenticación.

La clave de autenticación Ki se almacena de forma segura en el elemento seguro -14- del terminal móvil -12-. Los algoritmos de cifrado A3 y A8 también residen en el elemento seguro -14-. El número RAND recibido del MSC de la PLMN objetivo -40- 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 respuesta firmada SRES* y la clave de cifrado Kc, respectivamente. La clave de cifrado Kc se almacena en el elemento seguro -14- y la respuesta firmada generada SRES* se devuelve como la respuesta del procedimiento de autenticación de pregunta-respuesta GSM a la PLMN objetivo -40-. El MSC de la PLMN objetivo -40- recibe la respuesta firmada SRES* generada por el elemento seguro -14- del terminal móvil -12- y la compara con la respuesta firmada SRES generada por el AUC. Si coinciden, el elemento seguro -14- del terminal móvil -12- se autentica y puede comunicarse con la PLMN objetivo -40- y a través de la misma, es decir, el elemento seguro -14- ha cambiado correctamente de la PLMN de aprovisionamiento -30- a la PLMN objetivo -40-.

Según la presente invención el perfil de comunicación asociado con el procedimiento de conexión convencional descrito anteriormente o al menos partes del mismo se usan como una clase de huella o prueba indirecta de que el elemento seguro -14- ha cambiado correctamente de la PLMN de aprovisionamiento -30- a la PLMN objetivo -40-. Con este fin, la PLMN objetivo -40- preferentemente comprende una unidad de supervisión de la señal (SMU) -46- que se ubica de forma apropiada dentro de la PLMN objetivo -40- y está configurada para supervisar el flujo de comunicación MAP/SS7 dentro de la PLMN objetivo -40- y, en particular, entre el MSC y el HLR -44- de la misma. En particular, la SMU -46- está configurada para interceptar el mensaje "enviar información de autenticación"

enviado desde el elemento seguro -14- a la PLMN objetivo -40-. Además, la SMU -46- se configura para extraer del flujo de comunicación MAP/SS7 entre el MSC y el HLR -44- de la PLMN objetivo -40- y, en particular, del mensaje Enviar información de autenticación" la IMSI objetivo proporcionada por el elemento seguro -14-.

El funcionamiento de la SMU -46- combinado con los otros elementos del sistema de comunicaciones -10- mostrado en la figura 1 se describirá a continuación en el contexto de una realización preferente de la invención haciendo referencia a la figura 2 para el caso en el que al principio solo está presente el perfil de suscripción provisional -18a- en el elemento seguro -14-. Sin embargo, a partir de la siguiente descripción detallada, el experto en la materia apreciará que la presente invención también se puede utilizar de forma ventajosa en el caso en el que además del perfil de suscripción provisional -18a- también esté presente ya el perfil de suscripción objetivo -18b- (y posiblemente otros perfiles de suscripción) en el elemento seguro -14-.

En la etapa -S1- de la figura 2 el elemento seguro -14- se autentica en (es decir, se conecta a) la PLMN de aprovisionamiento -30- utilizando su perfil de suscripción provisional -18a- que incluye un primer elemento de datos de identificación en forma de una IMSI provisional. Después de una conexión correcta a la PLMN de aprovisionamiento -30-, el elemento seguro -14- descarga en la etapa -S2- de la figura 2 el perfil de suscripción objetivo -18b- que incluye un segundo elemento de datos de identificación en forma de una IMSI objetivo del servidor de SM -50- para conectarse a la PLMN objetivo -40- y poder utilizar los servicios proporcionados por la misma. De acuerdo con la presente invención es concebible que junto con la descarga del perfil de suscripción objetivo -18b- el servidor de SM -50- proporcione al elemento seguro -14- una pluralidad de comandos a ejecutar por el elemento seguro -14-, tales como comandos para almacenar el perfil de suscripción objetivo descargado -18b- en la memoria no volátil -17- del elemento seguro -14-, borrar el perfil de suscripción provisional -18a- en la memoria no volátil -17- del elemento seguro -14- y similares.

Tras haber descargado el perfil de suscripción para la PLMN objetivo -40- en la etapa -S2- de la figura 2 y tras haberse desconectado de la PLMN de aprovisionamiento -30-, el elemento seguro -14- en la etapa -S3- de la figura 2 se conecta a la PLMN objetivo -40- usando la IMSI objetivo por medio de la sesión de conexión GSM descrita anteriormente. Como la sesión de conexión GSM consta de varias etapas de comunicación únicas, la SMU -46- puede, supervisando el perfil de la señal, determinar que los mensajes/señales correspondientes corresponden a una sesión de conexión y, además, puede extraer la IMSI utilizada en estos mensajes, en concreto la IMSI objetivo para conectarse a la PLMN objetivo -40- (etapa -S4- de la figura 2). Tras haber detectado una sesión de conexión de este tipo y tras haber extraído la IMSI correspondiente, la SMU -46- pasa esta información al servidor de SM -50- en la etapa -S5- de la figura 2.

En la etapa -S6- de la figura 2 el servidor de SM -50- confirma al elemento seguro -14- que ha recibido esta información sobre el cambio de la PLMN de aprovisionamiento -30- a la PLMN objetivo -40-. Además de ser un mensaje de confirmación, el mensaje enviado desde el servidor de SM -50- al elemento seguro -14- en la etapa -S6- de la figura 2 podría comprender comandos a ejecutar por el elemento seguro -14-, tales como eliminar el perfil de suscripción provisional -18a- (en caso de que esto no se haya hecho ya en la etapa -S2- de la figura 2) y similares.

Además, preferentemente el mensaje de confirmación enviado desde el servidor de SM -50- al elemento seguro -14- en la etapa -S6- de la figura 2 comprende el número de teléfono del elemento seguro -14- en la PLMN objetivo -40-, es decir, el MSIS-DN (abonado móvil de ISDN) asignado a la IMSI objetivo. Preferentemente, el servidor de SM -50- obtiene el MSISDN asignado a la IMSI objetivo en la etapa -S5- de la figura 2, ya que tanto la IMSI objetivo y como el MSISDN asignado están disponibles en el HLR -44- de la PLMN objetivo -40-. Proporcionar al elemento seguro -14- el MSISDN asignado a su IMSI, es decir, la IMSI objetivo, podría ser necesario para, al menos, algunas de las aplicaciones implementadas en el elemento seguro -14- y/o el terminal móvil -12- que requieren el MSISDN asignado a la IMSI objetivo para ser capaces de funcionar con la PLMN objetivo -40-.

El experto en la materia apreciará que la SMU -46- puede tomar varias formas y, en general, se puede implementar en hardware y/o software. Por ejemplo, la SMU -46- puede tomar la forma de una rutina de software que reside en el mismo elemento de red que el MSC o el HLR -44- de la PLMN objetivo -40- o puede distribuirse a varias localizaciones apropiadas dentro de la PLMN deseada -40-. Por ejemplo, la SMU -46- podría implementarse como parte del HLR -44- de la PLMN objetivo -40-. De forma alternativa, la SMU -46- puede proporcionarse en forma de una o más unidades de hardware dedicadas.

Aunque la SMU -46- se dispone y se configura preferentemente para supervisar el proceso completo del elemento seguro -14- conectándose a la PLMN objetivo -40-, la presente invención también incluye el caso en el que la SMU -46- solo supervisa partes del mismo, tales como el mensaje de conexión inicial, por ejemplo, el mensaje "enviar información de autenticación", para extraer la IMSI del mismo y como una indicación de que el elemento seguro -14- puede conectarse correctamente a la PLMN objetivo -40- y, por lo tanto, ha cambiado correctamente del perfil de suscripción provisional -18a- al perfil de suscripción objetivo -18b-.

Según una realización preferente de la invención es concebible que el servidor de SM -50- proporcione a la SMU -46- información sobre las IMSI que la SMU -46- debe buscar, cuando supervisa el flujo de comunicación dentro de la PLMN objetivo -40-. De forma más específica, el servidor de SM -50- podría proporcionar a la SMU -46- una lista

de IMSI que son parte de perfiles de suscripción respectivos para conectarse a la PLMN objetivo -40-, pero que todavía no han confirmado que se han conectado correctamente a la PLMN objetivo -40-. Por ejemplo, después de la descarga del perfil de suscripción -18b-, o de forma simultánea a la misma, para la PLMN objetivo -40- en la etapa -S2- de la figura 2 el servidor de SM -50- podría informar a la SMU -46- sobre la IMSI objetivo correspondiente y que esta IMSI objetivo se utilizará muy probablemente en el futuro próximo para intentar conectarse a la PLMN deseada -40-.

A la vista de la descripción detallada anterior, el experto en la materia apreciará que se pueden realizar modificaciones y/o adiciones a los procedimientos, dispositivos y sistemas descritos hasta aquí, que se debe considerar que permanecen dentro del ámbito de la presente invención tal como se define en las reivindicaciones adjuntas.

REIVINDICACIONES

1. Procedimiento para que un terminal móvil (12) que comprende un elemento seguro (14) realice un cambio de una primera red móvil (30) a una segunda red móvil (40), en el que el procedimiento comprende las siguientes etapas:

(a) conexión a la primera red móvil (30) utilizando un primer mensaje de conexión que contiene un primer elemento de datos de identificación, de un primer perfil de suscripción (18a); y

(b) conexión a la segunda red móvil (40) mediante un proceso de conexión que incluye un segundo mensaje de conexión que contiene un segundo elemento de datos de identificación de un segundo perfil de suscripción (18b), en el que la segunda red móvil (40) comprende una unidad de supervisión de la señal (46) que está configurada para supervisar, al menos, partes del proceso de conexión, para determinar el segundo elemento de datos de identificación incluido en el mismo y para enviar esta información a un servidor de gestión de la suscripción (50) con el fin de confirmar la conexión correcta del elemento seguro (14) a la segunda red móvil (40).

2. Procedimiento, según la reivindicación 1, en el que la segunda red móvil (40) está configurada para detectar el segundo mensaje de conexión que contiene el segundo elemento de datos de identificación.

3. Procedimiento, según la reivindicación 1, en el que el procedimiento comprende la siguiente etapa adicional después de la etapa (b):

(c) confirmación al elemento seguro (14) de que el cambio ha sido correcto.

4. Procedimiento, según la reivindicación 3, en el que en la etapa (c) el servidor de gestión seguro (50) proporciona al elemento seguro (14) el MSISDN asignado al segundo elemento de datos de identificación en la segunda red móvil (40).

5. Procedimiento, según la reivindicación 1, en el que el elemento seguro (14) descarga el segundo perfil de suscripción (18b) que incluye el segundo elemento de datos de identificación del servidor de gestión de la suscripción (50), mientras el elemento seguro (14) está conectado a la primera red móvil (30).

6. Procedimiento, según la reivindicación 5, en el que la etapa de descargar el segundo perfil de suscripción (18b) incluye la etapa adicional de recibir comandos del servidor de gestión de la suscripción (50) para que el elemento seguro (14) los ejecute.

7. Procedimiento, según la reivindicación 1, en el que el procedimiento incluye la etapa adicional de informar a la segunda red móvil (40) sobre el segundo elemento de datos de identificación con el fin de que la segunda red móvil (40) pueda supervisar los procesos de conexión respectivos.

8. Procedimiento, según la reivindicación 1, en el que la segunda red móvil (40) comprende la unidad de supervisión de la señal (40) que se implementa en hardware y/o software y está configurada para supervisar, al menos, partes del proceso de conexión, para determinar el segundo elemento de datos de identificación incluido en el mismo y para enviar esta información al servidor de gestión de la suscripción (50) con el fin de confirmar la conexión correcta del elemento seguro (14) a la segunda red móvil (40).

9. Procedimiento, según la reivindicación 1, en el que la primera red móvil (30) y/o la segunda red móvil (40) se gestionan según el estándar GSM.

10. Procedimiento, según la reivindicación 9, en el que el segundo mensaje de conexión es un mensaje "enviar información de autenticación".

11. Procedimiento, según la reivindicación 1, en el que el primer perfil de suscripción (18a) es un perfil de suscripción provisional que se almacena en el elemento seguro (14) durante el proceso de fabricación y/o de personalización del terminal móvil (12) y/o el elemento seguro (14).

12. Procedimiento, según la reivindicación 1, en el que el primer elemento de datos de identificación es una primera IMSI y el segundo elemento de datos de identificación es una segunda IMSI.

13. Sistema adaptado para llevar a cabo un procedimiento según una de las reivindicaciones 1 a 12, comprendiendo el sistema el terminal móvil (12) que contiene el elemento seguro (14), una unidad de supervisión de la señal (46) y el servidor de gestión de la suscripción (50).

14. Sistema, según la reivindicación 13, en el que el elemento seguro (14) es un módulo de identidad de abonado, SIM, extraíble o una parte integrada del terminal móvil (12), tal como una tarjeta de circuito integrado universal incorporada (eUICC).

15. Sistema, según la reivindicación 13, en el que el servidor de gestión de la suscripción (50) está configurado para interactuar con el elemento seguro (14).

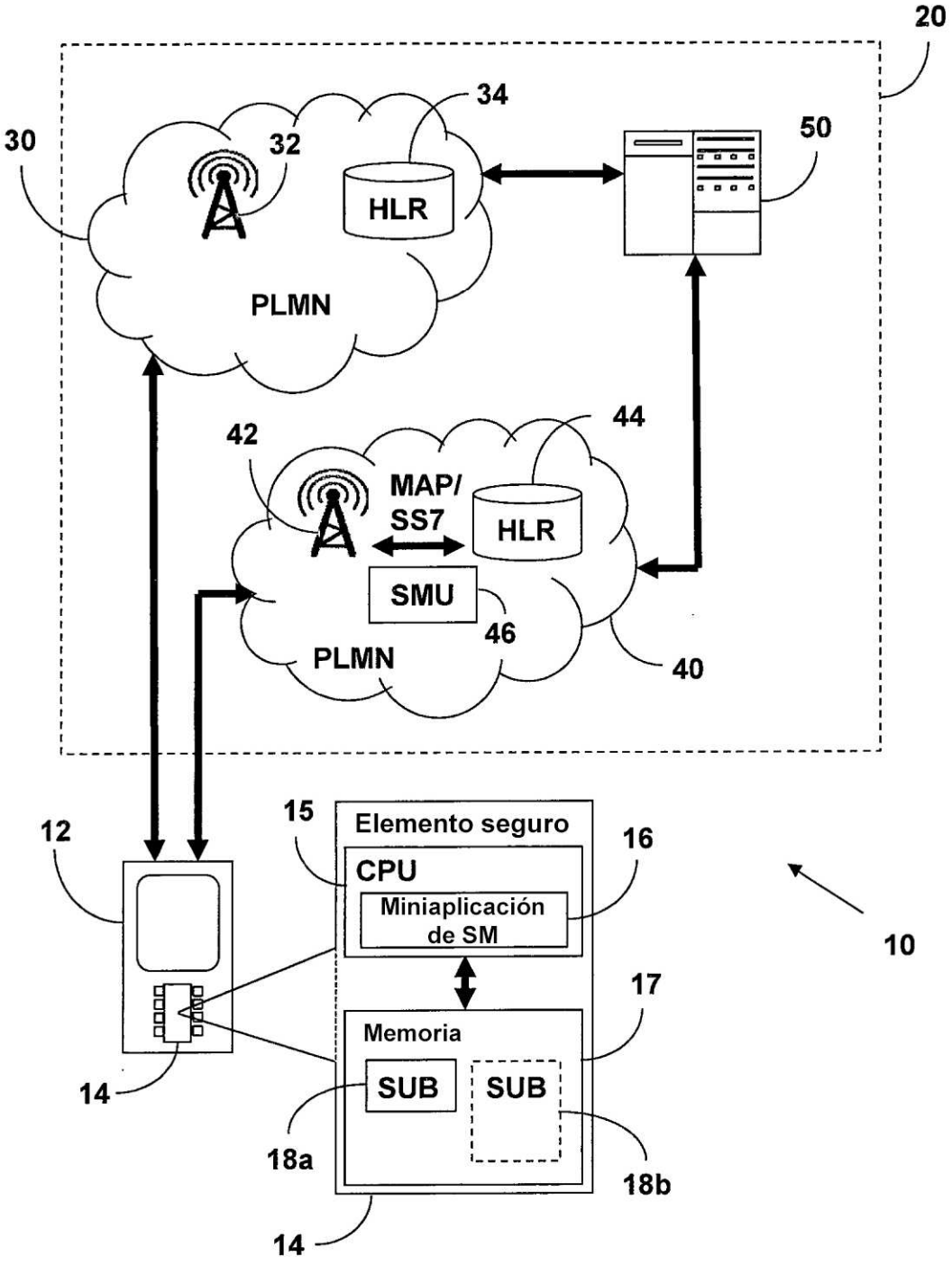
20
30
32
34
HLR
PLMN
50
42
44
MAP/
SS7
HLR
SMU
46
PLMN
40
12
15
Elemento seguro
16
CPU
Miniaplicación
de SM
10
17
Memoria
SUB
SUB
14
18a
18b
14

Fig. 1

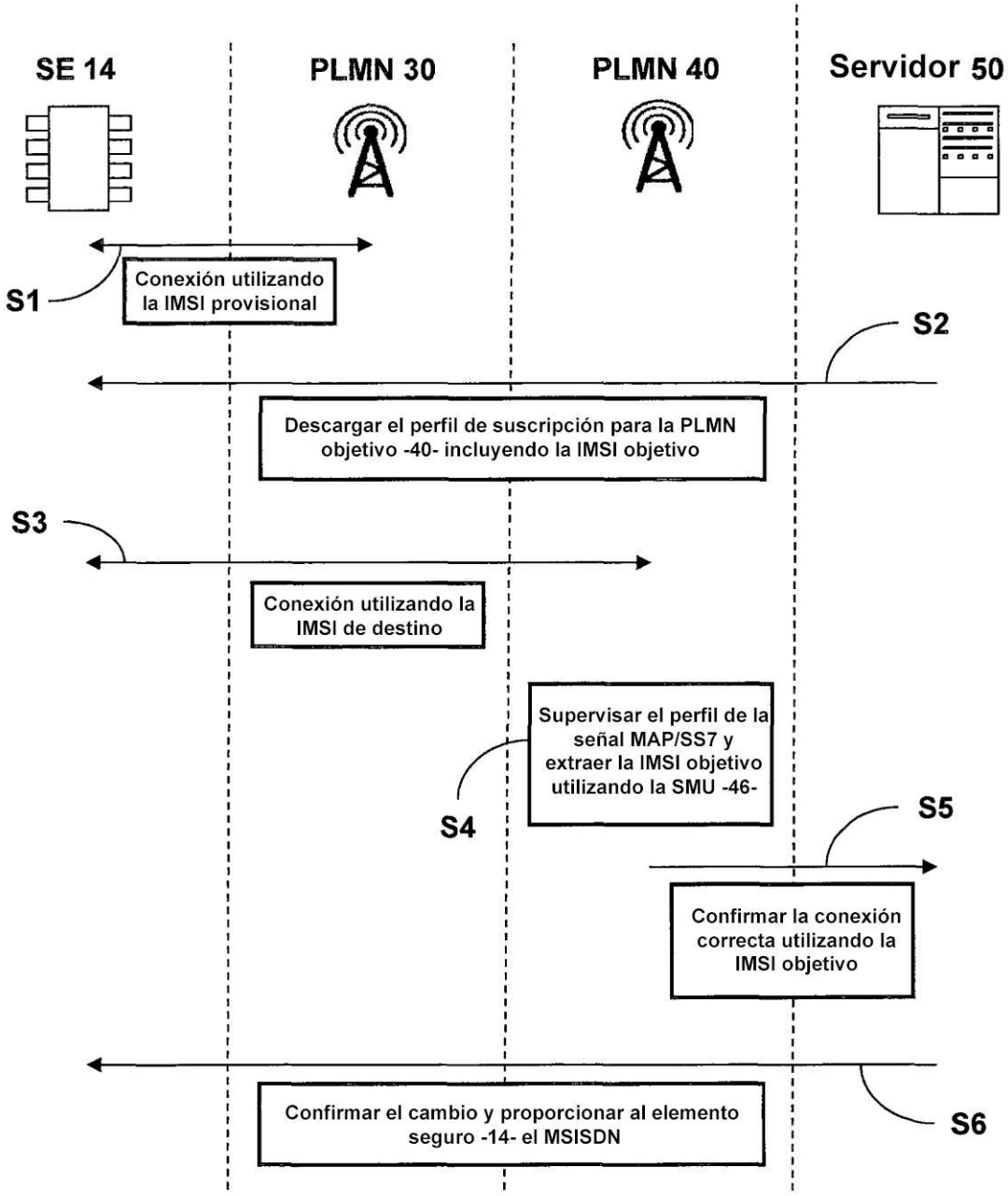
SE 14
PLMN 30
PLMN 40
Servidor 50
S1
Conexión utilizando la IMSI provisional
S2
Descargar el perfil de suscripción para la PLMN objetivo -40- incluyendo la IMSI objetivo
S3
Conexión utilizando la IMSI de destino
Supervisar el perfil de la señal MAP/SS7 y extraer la IMSI objetivo utilizando la SMU -46-
S4
S5
Confirmar la conexión correcta utilizando la IMSI objetivo
Confirmar el cambio y proporcionar al elemento seguro -14- el MSISDN
S6

Fig. 2