(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 647 088**

(51) Int. CI.:

H04W 4/00 (2009.01)
H04W 12/04 (2009.01)
H04W 8/24 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **21.12.2012 E 12008581 (6)**

(97) Fecha y número de publicación de la concesión europea: **04.10.2017 EP 2747466**

(54) Título: **Procedimientos y dispositivos para la gestión de suscripciones OTA**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
19.12.2017

(73) Titular/es:

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

(72) Inventor/es:

WEISS, DIETER;
VEDDER, KLAUS, DR.;
MEYER, MICHAEL;
TAGSCHERER, MICHAEL, DR.;
RUDOLPH, JENS;
DIETZ, ULRICH;
NYHOLM, JARI;
LARSSON, THOMAS y
HULT, JORGEN

(74) Agente/Representante:

DURAN-CORRETJER, S.L.P

DESCRIPCIÓN

Procedimientos y dispositivos para la gestión de suscripciones OTA

Sector de la invención

La invención se refiere a las comunicaciones móviles en general y, en particular, a procedimientos y dispositivos para la gestión de suscripciones de forma inalámbrica (over-the-air, OTA) de terminales móviles que comprenden un elemento seguro, tal como un módulo de identidad de abonado (SIM), una tarjeta eUICC/UICC o similares.

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 durante un proceso de personalización del SIM antes de entregar el SIM al usuario del terminal móvil. 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 las credenciales de suscripción necesarias.

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 próximo, 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 las credenciales de suscripción necesarias, 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 las credenciales de suscripción necesarias con antelación. En consecuencia, una vez sobre el terreno, estos dispositivos M2M y sus elementos seguros no personalizados necesitarán la provisión de las credenciales 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, en particular, las credenciales de suscripción necesarias para conectarse a la PLMN del MNO actual por el SIM proporcionado por el nuevo MNO y que contiene las credenciales de suscripción necesarias 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. Sin embargo, como diferentes MNO a menudo utilizan diferentes algoritmos de autenticación para el proceso de conexión del SIM, en general no es suficiente sencillamente descargar nuevas credenciales de suscripción al SIM. En su lugar, se debe proporcionar al SIM de forma inalámbrica un nuevo perfil de suscripción completo, incluyendo las credenciales de suscripción, las aplicaciones y/o, al menos, partes de un sistema operativo del SIM. En la técnica anterior no se conocen procedimientos para proporcionar esta posibilidad, o en el mejor de los casos son bastante engorrosos.

A la vista de lo anterior, el problema que aborda la presente invención es dar a conocer procedimientos y dispositivos que permitan proporcionar al elemento seguro de un terminal móvil un perfil de suscripción de forma inalámbrica. En el documento U.S.A. 2009/191857 se puede encontrar otro ejemplo.

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 se refiere a un procedimiento para proporcionar un perfil de suscripción a un elemento seguro de un terminal móvil. El terminal móvil está configurado para comunicarse con una red de comunicaciones celular y el perfil de suscripción comprende una parte específica de la red relacionada con la red de comunicaciones celular o una red de comunicaciones celular diferente, y una parte específica del hardware relacionada con el hardware del terminal móvil y/o del elemento seguro. El procedimiento comprende las etapas de: configurar el perfil de suscripción, en donde la parte específica de la red del perfil de suscripción se proporciona mediante un primer servidor y la parte específica del hardware del perfil de suscripción se proporciona mediante un segundo servidor; y proporcionar el perfil de suscripción al elemento seguro de forma inalámbrica.

Como se utiliza en la presente memoria, un "perfil de suscripción" (o, de forma abreviada, una "suscripción") puede comprender, al menos, partes de un sistema operativo del elemento seguro, una o varias aplicaciones, archivos y/o datos, tales como las credenciales de suscripción. Un "perfil de suscripción" según la presente invención comprende, en particular, una parte específica del hardware, es decir, componentes del perfil de suscripción que están relacionados con el hardware del terminal móvil y/o del elemento seguro, y una parte específica de la red, es decir, componentes del perfil de suscripción que están relacionados con los detalles de la red de comunicaciones celular (o una red de comunicaciones celular diferente asociada con el perfil de suscripción).

Como se utiliza en la presente memoria, la expresión "proporcionar un perfil de suscripción al elemento seguro de un terminal móvil" comprende el intercambio completo de un perfil de suscripción antiguo por un perfil de suscripción nuevo, la adición de un perfil de suscripción nuevo a un perfil de suscripción existente, y el intercambio parcial de un perfil de suscripción existente, que puede ser una actualización del perfil de suscripción existente.

Preferentemente, el procedimiento comprende, antes de la etapa de configurar el perfil de suscripción, la etapa adicional de identificar al elemento seguro por medio de un elemento de identificación ID_{se} para determinar una clave de configuración K_{conf} y una clave del elemento seguro K_{se} asociada con el elemento seguro.

Según las realizaciones preferentes de la invención, la etapa de identificar al elemento seguro comprende las etapas de: transmitir el elemento de identificación ID_{se} del elemento seguro al primer servidor; enviar el elemento de identificación ID_{se} del elemento seguro al segundo servidor; y transmitir la clave de configuración K_{conf} determinada basándose en el elemento de identificación ID_{se} del segundo servidor al primer servidor.

Preferentemente, el elemento de identificación ID_{se} se transmite del elemento seguro al primer servidor por medio de un mensaje que incluye el elemento de identificación ID_{se} en forma no cifrada y una versión cifrada del elemento de identificación ID_{se}, cifrado utilizando una clave de configuración K_{conf} almacenada en el elemento seguro.

Según las realizaciones preferentes de la invención, el mensaje transmitido del elemento seguro al primer servidor comprende, además, una versión cifrada de una clave de sesión K_{ses} creada por el elemento seguro y una versión cifrada de una configuración de hardware HW_{conf} del elemento seguro y/o del terminal móvil, ambas cifradas utilizando la clave de configuración K_{conf}.

Preferentemente, el primer servidor descifra la versión cifrada del elemento de identificación ID_{se}, la versión cifrada de la clave de sesión K_{ses} y la versión cifrada de la configuración del hardware HW_{conf} del elemento seguro y/o del terminal móvil utilizando la clave de configuración K_{conf} proporcionada por el segundo servidor, de tal modo que el primer servidor puede verificar la validez de la clave de configuración K_{conf} proporcionada por el segundo servidor verificando que el elemento de identificación ID_{se} enviado de forma no cifrada es idéntico al elemento de identificación ID_{se} resultante de descifrar la versión cifrada del elemento de identificación ID_{se} utilizando la clave de configuración K_{conf}.

Preferentemente, la configuración del hardware HW_{conf} del elemento seguro y/o del terminal móvil se determina sobre la marcha mediante una aplicación de gestión de suscripciones que se ejecuta en el elemento seguro y/o el terminal móvil o se recupera de una unidad de memoria del elemento seguro y/o de una unidad de memoria del terminal móvil.

Según las realizaciones preferentes de la invención, el segundo servidor transmite la clave de configuración K_{conf} determinada basándose en el elemento de identificación ID_{se} al primer servidor solo después de que el primer servidor se haya autenticado correctamente en el segundo servidor o después de una autenticación mutua entre el primer servidor y el segundo servidor.

Preferentemente, la etapa de configurar el perfil de suscripción comprende las etapas de cifrar la parte específica del hardware del perfil de suscripción mediante el segundo servidor utilizando la clave del elemento seguro K_{se}, y cifrar la parte específica de la red del perfil de suscripción mediante el primer servidor utilizando la clave de configuración K_{conf}.

Según las realizaciones preferentes de la invención, el procedimiento comprende, además, la etapa de cifrar la parte específica del hardware cifrada del perfil de suscripción y la parte específica de la red cifrada del perfil de suscripción

utilizando una clave de sesión K_{ses} creada por el elemento seguro.

Preferentemente, la etapa de configurar el perfil de suscripción comprende la etapa adicional de determinar, al menos, un perfil de suscripción que sea compatible con una configuración del hardware HW_{conf} del elemento seguro y/o del terminal móvil.

Según las realizaciones preferentes de la invención, la parte específica del hardware del perfil de suscripción comprende, al menos, partes de un sistema operativo OS para el elemento seguro y/o la parte específica de la red del perfil de suscripción comprende las credenciales de suscripción CREDS, que incluyen preferentemente una IMSI y/o una clave de autenticación Ki, para conectar el elemento seguro a la red de comunicaciones celular o a una red de comunicaciones celular diferente asociada con el perfil de suscripción.

Según un segundo aspecto, la invención da a conocer un elemento seguro que comprende un perfil de suscripción proporcionado al elemento seguro mediante el 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 de comunicaciones celular. 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.

Según un cuarto aspecto, la invención da a conocer un sistema *backend* (en segundo plano) de gestión de suscripciones, que comprende un primer servidor y un segundo servidor, en el que el primer servidor y el segundo servidor están configurados para proporcionar un perfil de suscripción al elemento seguro de un terminal móvil por medio del procedimiento según el primer aspecto de la invención.

Como, en general, la parte relacionada con el hardware de un perfil de suscripción está disponible para el fabricante y/o el proveedor del terminal móvil y/o del elemento seguro, mientras que la parte relacionada con la red está disponible para el MNO de la red de comunicaciones celular, preferentemente el segundo servidor, que proporciona la parte relacionada con el hardware del perfil de suscripción, es gestionado por el fabricante y/o el proveedor del terminal móvil y/o del elemento seguro y el primer servidor, que proporciona la parte relacionada con la red del perfil de suscripción, es gestionado por el MNO de la red de comunicaciones celular (o una red de comunicaciones celular diferente asociada con el perfil de suscripción). De forma alternativa, el primer servidor podría ser gestionado por un proveedor de gestión de suscripciones que sirve a varios MNO diferentes que gestionan diferentes redes de comunicaciones celulares.

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.

Breve descripción de los dibujos

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

la figura 2 muestra un diagrama que ilustra un procedimiento para proporcionar un perfil de suscripción al elemento seguro de un terminal móvil según una realización preferente de la invención.

Descripción detallada de las realizaciones preferentes

La figura 1 muestra esquemáticamente los componentes de un sistema de comunicaciones -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 manera ventajosa en el contexto de cualquier tipo de terminales que estén configurados 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, incluyendo también redes de comunicación móvil basadas en IP.

En la figura 1 se muestra un terminal móvil -12- a modo de ejemplo que incluye un elemento seguro -20- para almacenar de forma segura y procesar datos que identifican de manera única al terminal móvil -12- y/o a su usuario. 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. Además, el sistema de comunicaciones -10- mostrado en la figura 1 comprende un primer servidor -42- y un segundo servidor -44- que son parte de un sistema *backend* de gestión de suscripciones -40- para proporcionar un perfil de suscripción al elemento seguro -20- del terminal móvil -12-. Como se describirá con más detalle más adelante, el primer servidor -42- (en adelante denominado servidor de gestión de suscripciones -42-) y el segundo servidor -44- (en adelante denominado servidor de provisión de suscripciones -44-) del sistema *backend* de gestión de suscripciones -40- pueden ser gestionados por una única entidad o por dos entidades diferentes, por ejemplo, por un operador de red móvil (MNO) y un fabricante/proveedor del terminal móvil -12- y/o del elemento seguro -20-.

Según las realizaciones preferentes de la invención, el elemento seguro -20- se configura como una tarjeta eUICC o UICC con una aplicación 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 la identificación de abonados única y segura así como para la provisión de diferentes funciones especiales y servicios de valor añadido. De forma alternativa, el elemento seguro -20- podría estar configurado como un módulo de identidad de abonado (SIM), 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.

Como ya se ha mencionado anteriormente, el terminal móvil -12- está configurado para comunicarse a través de la interfaz aérea (o enlace de radio) con una red de comunicaciones celular o una red móvil terrestre pública (PLMN) -30-, gestionada preferentemente por un operador de red móvil (MNO) según el estándar GSM, así como con otros terminales móviles conectados con el mismo. En lo que sigue, se describirán las realizaciones preferentes de la invención en el contexto de una red de comunicaciones celular según los estándares del Sistema global para comunicación móvil (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, tales como CDMA, GPRS (Servicio general de paquetes de radio) y similares.

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). 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 mencionados anteriormente de la 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 el protocolo 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.

Como se puede deducir a partir de la vista ampliada del elemento seguro -20- en la figura 1, el elemento seguro -20- preferentemente comprende una unidad central de procesamiento (CPU) -22-. Preferentemente, la CPU -22- está configurada de tal manera que, al menos, una aplicación -24- pueda ejecutarse en la CPU -22- proporcionando características que se describirán en el contexto de la figura 2 con más detalle más adelante. La aplicación -24- podría implementarse, por ejemplo, como una miniaplicación Java. Para proporcionar un entorno de ejecución para la aplicación -24-, un sistema operativo del elemento seguro (no mostrado en la figura 1) se ejecuta preferentemente en la CPU -22-.

Además, el elemento seguro -20- preferentemente comprende una unidad de memoria -26- que preferentemente se implementa como una memoria flash regrabable no volátil. Preferentemente, una primera parte -26a- de la unidad de memoria -26- está configurada para almacenar de forma segura datos secretos en la misma. Como se explicará con más detalle en el contexto de la figura 2, estos datos secretos preferentemente incluyen un elemento de identificación ID_{se} para identificar de manera única al elemento seguro -20-. El elemento de identificación ID_{se} podría ser, por ejemplo, la IC-CID (identidad de la tarjeta de circuito integrado) del elemento seguro -20-. Además, una clave del elemento seguro K_{se} y una clave de configuración K_{conf} se almacenan preferentemente en la primera parte -26a- de la unidad de memoria -26-. El elemento de identificación ID_{se}, la clave del elemento seguro K_{se} y/o la clave de configuración K_{conf} se pueden almacenar en el elemento seguro -20- durante el proceso de fabricación y/o de personalización del elemento seguro -20-. Como se describirá con más detalle más adelante, la clave del elemento seguro K_{se} y la clave de configuración K_{conf} originalmente están disponibles para el elemento seguro -20- así como para el servidor de provisión de suscripciones -44- del sistema *backend* de gestión de suscripciones -40-.

Como se puede deducir a partir de la figura 1, además, un primer perfil de suscripción SUB1 se almacena en la unidad de memoria -26- del elemento seguro -20-, por ejemplo, en una segunda parte -26b- de la misma. Este primer perfil de suscripción SUB1 puede comprender, al menos, partes de un sistema operativo del elemento seguro -20-, una o más aplicaciones, tal como una aplicación de acceso a la PLMN que contiene un algoritmo de autenticación específico del MNO, archivos y/o datos, tales como credenciales de suscripción que permiten al elemento seguro -20- y al terminal móvil -12- conectarse a la PLMN -30-. Preferentemente, también al menos partes de la segunda parte -26b- de la unidad de memoria -26- del elemento seguro -20- están configuradas para almacenar de forma segura los datos en las mismas, por ejemplo cualesquiera credenciales de suscripción que se deben mantener secretas, tales como una Identidad internacional de abonado móvil (IMSI) y/o una clave de autenticación Ki, que son parte del primer perfil de suscripción SUB1. Como se indica en la figura 1, la segunda parte -26b- de la unidad de memoria -26- preferentemente proporciona varias "ranuras" para alojar perfiles de suscripción adicionales, tales como un segundo perfil de suscripción SUB2 que proporcionará el *backend* de gestión de suscripciones -40- según el proceso mostrado en la figura 2 y descrito en más detalle más adelante. En otras palabras, el elemento seguro -20- preferentemente admite el almacenamiento de múltiples perfiles de suscripción. Estos múltiples perfiles de suscripción pueden estar asociados con un MNO o diferentes MNO.

Preferentemente, el primer perfil de suscripción SUB1 puede almacenarse en la unidad de memoria -26- del elemento seguro -20- durante el proceso de fabricación y/o de personalización del terminal móvil -12- y/o de su elemento seguro -20-. En especial, en esta realización preferente es concebible que el primer perfil de suscripción SUB1 sea sencillamente un perfil de suscripción provisional que solo proporciona servicios básicos que permiten al elemento seguro -20- y al terminal móvil -12- comunicarse con el sistema *backend* de gestión de suscripciones -40- y descargar un perfil de suscripción más completo que proporciona servicios adicionales, tal como el segundo perfil de suscripción SUB2 mostrado en la figura 1. Como un perfil de suscripción provisional, tal como el primer perfil de suscripción SUB1 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 SUB2 mostrado en la figura 1.

Como se muestra en la figura 1 y ya se ha mencionado anteriormente, el terminal móvil -12- puede comunicarse a través de la PLMN -30- con el servidor de gestión de suscripciones -42- y el servidor de provisión de suscripciones -44-, que son parte del sistema *backend* de gestión de suscripciones -40-. Una primera base de datos -43- podría comunicarse con el servidor de gestión de suscripciones -42- o implementarse en el mismo. Una segunda base de datos -45- podría comunicarse con el servidor de provisión de suscripciones -44- o implementarse en el mismo.

Aunque el elemento seguro -20- y el terminal móvil -12- se comunican preferentemente a través de la PLMN -30- con el servidor de gestión de suscripciones -42- y/o el servidor de provisión de suscripciones -44-, el experto en la materia apreciará que esta comunicación puede ocurrir también sobre un canal de comunicación diferente, tal como una red LAN, WLAN o WiFi conectada a Internet. El experto en la materia apreciará que la comunicación a través de estos canales de comunicación diferentes y la transferencia de datos del servidor de gestión de suscripciones -42- y/o el servidor de provisión de suscripciones -44- al elemento seguro -20- podría necesitar algunas soluciones técnicas especiales, que, sin embargo, no son objeto de la presente invención.

A continuación se describirá, con referencia adicional a la figura 2, el funcionamiento del servidor de gestión de suscripciones -42- y el servidor de provisión de suscripciones -44- del sistema *backend* de gestión de suscripciones -40- en combinación con los otros elementos del sistema de comunicaciones -10- mostrado en la figura 1.

En la etapa -S1- de la figura 2, que podría iniciarse mediante el elemento seguro -20- solicitando un nuevo perfil de suscripción al sistema *backend* de gestión de suscripciones -40-, el elemento seguro -20- se autentica en el servidor de gestión de suscripciones -42- del sistema *backend* de gestión de suscripciones -40-. Esta autenticación podría realizarse a través de la PLMN -30-, por ejemplo, utilizando los servicios proporcionados por la PLMN -30- o, de forma alternativa, utilizando la PLMN -30- sencillamente como un medio para transportar las credenciales de autenticación. Sin embargo, el experto en la materia apreciará que la autenticación puede realizarse también sobre una red de comunicaciones diferente, tal como una red LAN, WLAN o WiFi conectada a Internet. Según una realización de la presente invención, es concebible que el elemento seguro -20- se autentique en el servidor de gestión de suscripciones -42- utilizando las credenciales de suscripción del perfil de suscripción provisional SUB1 a modo de ejemplo para conectar el elemento seguro -20- a la PLMN -30- que están almacenadas de forma segura en la unidad de memoria -26- del elemento seguro -20-. Por medio de la etapa de autenticación -S1- de la figura 2 el elemento seguro -20- demuestra al servidor de gestión de suscripciones -42- que está autorizado a descargar un perfil de suscripción. Como se utiliza en la presente memoria, "descargar un perfil de suscripción" puede tener el significado de un intercambio completo de un perfil de suscripción antiguo por un perfil de suscripción nuevo, la adición de un nuevo perfil de suscripción a un perfil de suscripción ya existente y un intercambio parcial de un perfil de suscripción existente por una nueva versión del perfil de suscripción existente.

Después de una autenticación correcta del elemento seguro -12-, por ejemplo por medio de las credenciales de suscripción del perfil de suscripción provisional SUB1, una aplicación de gestión de suscripciones (denominada en la figura 2 "SM APP") se puede descargar en la etapa -S2- de la figura 2 del servidor de gestión de suscripciones -42- al terminal móvil -12-. Preferentemente, la aplicación de gestión de suscripciones SM APP puede ejecutarse en el terminal móvil -12-. De manera adicional o alternativa, la aplicación de gestión de suscripciones SM APP puede ejecutarse también en el elemento seguro -20-. Como apreciará el experto en la técnica, la etapa -S2- de la figura 2 podría omitirse, por ejemplo, si la aplicación de gestión de suscripciones SM APP ya se ha descargado e instalado en el terminal móvil -12- y/o el elemento seguro -20- durante una sesión anterior de descarga/actualización del perfil de suscripción.

Preferentemente, la aplicación de gestión de suscripciones SM APP descargada en la etapa -S2- de la figura 2 coordina la actualización del perfil de suscripción según la presente invención. De manera más específica, en caso de que la aplicación de gestión de suscripciones SM APP se esté ejecutando en el terminal móvil -12-, preferentemente proporciona por un lado acceso al servidor de gestión de suscripciones -42- y por otro lado una interfaz con el elemento seguro -20- para proporcionar al elemento seguro -20- un perfil de suscripción nuevo o actualizado.

Una vez que la aplicación de gestión de suscripciones SM APP se ha instalado y se está ejecutando en el terminal móvil -12- y/o en el elemento seguro -20-, la aplicación de gestión de suscripciones SM APP determina en la etapa -S3- de la figura 2 información sobre la configuración del hardware HW_{conf} del terminal móvil -12- y/o de su elemento seguro -20-, tal como el tipo de unidad central de procesamiento (CPU) del elemento seguro -20- y/o del terminal móvil -12-, la cantidad de memoria libre y utilizada en el elemento seguro -20- y similares. Según la presente invención es concebible que, al menos, parte de la información sobre la configuración del hardware HW_{conf} del elemento seguro -20- y/o del terminal móvil -12- ya esté almacenada en la unidad de memoria -26- del elemento seguro -20- y/o en una unidad de memoria del terminal móvil -12- y pueda recuperarse de la misma mediante la aplicación de gestión de suscripciones SM APP. De forma alternativa o adicional, al menos partes de la configuración del hardware HW_{conf} pueden determinarse sobre la marcha mediante la aplicación de gestión de suscripciones SM APP que se está ejecutando en el elemento seguro -20- y/o el terminal móvil -12-. Como se describirá con más detalle más adelante, basándose en la configuración del hardware HW_{conf} del elemento seguro -20- y/o del terminal móvil -12-, solo aquellos perfiles de suscripción que sean compatibles con la configuración del hardware HW_{conf} determinada por la aplicación de gestión de suscripciones SM APP en la etapa -S3- de la figura 2 se ofrecerán al usuario del terminal móvil -12- para su descarga.

En la etapa -S4- de la figura 2, el elemento seguro -20- crea una clave de sesión temporal K_{ses} para asegurar determinadas etapas de la sesión de actualización del perfil de suscripción preferente mostradas en la figura 2. Preferentemente, la clave de sesión K_{ses} es un *nonce*, es decir, un número arbitrario utilizado una sola vez. Esto garantiza que para cada sesión de actualización del perfil de suscripción, tal como la sesión de actualización del

perfil de suscripción mostrada en la figura 2, se utiliza una clave de sesión K_{ses} diferente. Como bien saben los expertos en la materia, dicho *nonce* puede crearse, por ejemplo, utilizando un generador de números pseudoaleatorios, preferentemente un generador de números pseudoaleatorios criptográficamente seguro.

En la etapa -S5- de la figura 2 el elemento de identificación ID_{se} del elemento seguro -20- almacenado en la primera parte -26a- de la memoria -26- del elemento seguro -20- se envía preferentemente junto con la configuración del hardware HW_{conf} determinada en la etapa -S3- y la clave de sesión K_{ses} creada en la etapa -S4- de la figura 2 al servidor de gestión de suscripciones -42-. Con este fin, estos elementos de datos preferentemente se concatenan y la cadena de datos resultante se cifra utilizando la clave de configuración K_{conf} dando lugar al mensaje cifrado $C = ENC(ID_{se}||K_{ses}||HW_{conf}, K_{conf})$, donde el símbolo || denota la operación de concatenación y $ENC(..., K_{conf})$ denota una operación de cifrado utilizando la clave de configuración K_{conf}. Preferentemente, el mensaje cifrado C, se concatena a su vez con el elemento de identificación ID_{se} del elemento seguro -20- dando lugar al mensaje $ID_{se}||ENC(ID_{se}||K_{ses}||HW_{conf}, K_{conf})$. Preferentemente, este mensaje que contiene el elemento de identificación ID_{se} de forma no cifrada y el mensaje cifrado C se envía al servidor de gestión de suscripciones -42- en la etapa -S5- de la figura 2. Como apreciará el experto en la materia, el elemento de identificación ID_{se} puede recuperarse a partir de este mensaje por cualquier destinatario del mismo, mientras que las partes restantes del mismo solo pueden ser leídas por un destinatario que posea la clave de configuración K_{conf}.

Como apreciará el experto en la materia, el orden de los elementos en la concatenación del elemento de identificación ID_{se}, la configuración del hardware HW_{conf} y la clave de sesión K_{ses} es una cuestión de elección y, por lo tanto, no es crítico con respecto a la presente invención, siempre que el emisor y el receptor hayan acordado el mismo orden. Para cifrar la cadena de datos resultante de la concatenación del elemento de identificación ID_{se}, la configuración del hardware HW_{conf} y la clave de sesión K_{ses} puede emplearse cualquier algoritmo de cifrado simétrico utilizando la clave de configuración K_{conf}, tal como AES, DES, 3DES o similares.

Después de haber recibido el mensaje enviado por el elemento seguro -20- en la etapa -S5- de la figura 2, el servidor de gestión de suscripciones -42- extrae el elemento de identificación ID_{se} del mismo, el cual, como se ha descrito anteriormente, se ha enviado de forma no cifrada. Basándose en este elemento de identificación ID_{se} del elemento seguro -20-, el servidor de gestión de suscripciones -42- puede determinar uno o varios servidores de provisión de suscripciones apropiados, por ejemplo el servidor de provisión de suscripciones -44-, que tiene acceso, en concreto, a datos específicos del hardware sobre el elemento seguro -20- y/o el terminal móvil -12- asociados con el elemento de identificación ID_{se} del elemento seguro -20-. Después de haber determinado, al menos, un servidor de provisión de suscripciones apropiado de este tipo, por ejemplo el servidor de provisión de suscripciones -44- mostrado en la figura 1, el servidor de gestión de suscripciones -42- preferentemente envía el elemento de identificación ID_{se} del elemento seguro -20- al servidor de provisión de suscripciones -44-. Preferentemente, el servidor de provisión de suscripciones -44- está gestionado por el proveedor y/o el fabricante del terminal móvil -12- y/o del elemento seguro -20- y tiene acceso a datos específicos del hardware, por ejemplo datos asociados con la configuración del hardware del terminal móvil -12- y/o del elemento seguro -20-.

Con el fin de determinar un servidor de provisión de suscripciones apropiado, una base de datos, tal como la base de datos -43- mostrada en la figura 1, podría comunicarse con el servidor de gestión de suscripciones -42- o implementarse en el mismo, en donde una multitud de diferentes elementos de identificación de elementos seguros, tales como el elemento de identificación ID_{se} del elemento seguro -20-, están vinculados a uno o varios servidores de provisión de suscripciones apropiados, respectivamente. Estos uno o varios servidores de provisión de suscripciones apropiados, tales como el servidor de provisión de suscripciones -44- mostrado en la figura 1, podrían identificarse, por ejemplo, mediante una dirección IP, un URL o similares.

Después de haber recibido el elemento de identificación ID_{se} del elemento seguro -20- en la etapa -S6- de la figura 2, el servidor de provisión de suscripciones -44- en la etapa -S7- de la figura 2 devuelve la clave de configuración K_{conf} asociada con el elemento de identificación ID_{se} del elemento seguro -20- al servidor de gestión de suscripciones -42-. Para recuperar esta clave de configuración K_{conf}, el servidor de provisión de suscripciones -44- podría acceder a la base de datos -45-, en la que una multitud de claves de configuración, tales como la clave de configuración K_{conf}, se almacenan en conexión con una pluralidad de elementos de identificación de elementos seguros, tales como el elemento de identificación ID_{se} del elemento seguro -20-. Como ya se ha mencionado anteriormente, la base de datos -45- podría alojarse en un servidor diferente o implementarse en el propio servidor de provisión de suscripciones -44-.

Preferentemente, el servidor de provisión de suscripciones -44- proporciona al servidor de gestión de suscripciones -42- la clave de configuración K_{conf} solo en caso de que el servidor de provisión de suscripciones -44- pueda confiar en el servidor de gestión de suscripciones -42-. Con este fin, según las realizaciones preferentes de la invención, en concreto, cuando el servidor de provisión de suscripciones -44- y el servidor de gestión de suscripciones -42- están gestionados por entidades diferentes, el servidor de gestión de suscripciones -42- tiene que autenticarse en el servidor de provisión de suscripciones -44- antes de proporcionar la clave de configuración K_{conf} al servidor de gestión de suscripciones -42- en la etapa -S7- de la figura 2.

Utilizando la clave de configuración K_{conf} recibida del servidor de provisión de suscripciones -44- en la etapa -S7- de

la figura 2, el servidor de gestión de suscripciones -42- descifra en la etapa -S8- de la figura 2 la parte del mensaje enviada por el elemento seguro -20- en la etapa -S5- de la figura 2 que se ha cifrado utilizando la clave de configuración K_{conf}. Al hacerlo, el servidor de gestión de suscripciones -42- preferentemente recupera una vez más el elemento de identificación ID_{se} del elemento seguro -20-, la clave de sesión K_{ses} y la configuración del hardware HW_{conf} del elemento seguro -20- y/o del terminal móvil -12-. Comparando el elemento de identificación ID_{se} obtenido descifrando el mensaje proporcionado por el elemento seguro -20- en la etapa -S5- de la figura 2 con el elemento de identificación ID_{se} que se ha transmitido de forma no cifrada como parte de ese mensaje, el servidor de gestión de suscripciones -42- puede verificar que la clave de configuración K_{conf} proporcionada por el servidor de provisión de suscripciones -44- es correcta, es decir, idéntica a la clave de configuración K_{conf} utilizada por el elemento seguro -20- para cifrar el mensaje enviado en la etapa -S5- de la figura 2. En caso de alguna discrepancia, el servidor de gestión de suscripciones -42- podría pedir al elemento seguro -20- que vuelva a transmitir el mensaje enviado en la etapa -S5- de la figura 2 y/o al servidor de provisión de suscripciones -44- que compruebe la clave de configuración K_{conf} proporcionada en la etapa -S7- de la figura 2.

En la etapa -S8- de la figura 2, el servidor de gestión de suscripciones -42- determina adicionalmente, basándose en la configuración del hardware HW_{conf} del elemento seguro -20- y/o del terminal móvil -12-, los perfiles de suscripción que son compatibles con la configuración del hardware del mismo y crea una lista de perfiles de suscripción correspondientes disponibles para el elemento seguro -20- y/o el terminal móvil -12-. A continuación, esta lista se envía en la etapa -S9- de la figura 2 al terminal móvil -12- y, por ejemplo, se muestra en la pantalla del terminal móvil -12- indicando al usuario móvil que seleccione uno de los perfiles de suscripción disponibles. La lista de perfiles de suscripción seleccionables podría comprender para cada perfil de suscripción seleccionable información adicional, tal como los costes mensuales, los servicios adicionales y similares de un perfil de suscripción correspondiente.

Una vez que el usuario del terminal móvil -12- ha seleccionado uno de los perfiles de suscripción disponibles, por ejemplo, mediante una pantalla táctil de su terminal móvil -12-, se informa al servidor de gestión de suscripciones -42- sobre el perfil de suscripción seleccionado (denominado en la figura 2 perfil de suscripción SUB), el cual, a su vez, envía esta información al servidor de provisión de suscripciones -44-. Así pues, tanto el servidor de gestión de suscripciones -42- como el servidor de provisión de suscripciones -44- están informados sobre el perfil de suscripción SUB seleccionado por el usuario del terminal móvil -12-.

Según la presente invención, el perfil de suscripción seleccionado SUB, en general, incluye una parte específica del hardware así como una parte específica de la red de comunicaciones celular. La parte específica del hardware del perfil de suscripción SUB se refiere a cualesquiera componentes del perfil de suscripción que están relacionados con el hardware del terminal móvil -12- y/o del elemento seguro -20-, y preferentemente comprende, al menos, partes de un sistema operativo del elemento seguro (denominado sistema operativo OS en la figura 2) y/o una o varias aplicaciones (denominadas aplicaciones APPS en la figura 2) que dependen de la configuración del hardware HW_{conf} del elemento seguro -20- y/o del sistema operativo OS del mismo. La parte específica de la red del perfil de suscripción SUB se refiere a cualesquiera componentes del perfil de suscripción que están relacionados con los detalles de la PLMN -30- (o una PLMN diferente asociada con el perfil de suscripción SUB), y preferentemente comprende credenciales de suscripción (denominadas en la figura 2 credenciales de suscripción CREDS), tales como una Identidad internacional de abonado móvil (IMSI) y/o una clave de autenticación Ki. El experto en la materia apreciará que la parte específica de la red del perfil de suscripción SUB también puede incluir aplicaciones, por ejemplo, una aplicación de acceso a la PLMN que contiene un algoritmo de autenticación específico del MNO.

Como en general los datos específicos del hardware de un perfil de suscripción están disponibles para el fabricante y/o el proveedor del terminal móvil -12- y/o del elemento seguro -20-, mientras que los datos relacionados con la red están disponibles para el MNO de la PLMN -30- (o una PLMN diferente), preferentemente el servidor de provisión de suscripciones -44- que proporciona los datos específicos del hardware está gestionado por el fabricante y/o el proveedor del terminal móvil -12- y/o del elemento seguro -20- y el servidor de gestión de suscripciones -42- que proporciona los datos específicos de la red está gestionado por el MNO de la PLMN -30- (o una PLMN nueva utilizada por el perfil de suscripción SUB). De forma alternativa, el servidor de gestión de suscripciones -42- podría estar gestionado por un proveedor de gestión de suscripciones que sirve a varios MNO diferentes.

En la etapa -10- de la figura 2 el servidor de gestión de suscripciones -42- solicita al servidor de provisión de suscripciones -44- la parte específica del hardware del perfil de suscripción SUB seleccionado por el usuario del terminal móvil -12- en la etapa -S9- de la figura 2. El servidor de provisión de suscripciones -44- compila y preferentemente cifra estos datos relacionados con el hardware utilizando la clave del elemento seguro K_{se}, que comprende, en particular, al menos partes de un sistema operativo OS del elemento seguro y/o una o varias aplicaciones APPS que dependen de la configuración del hardware HW_{conf} del elemento seguro -20- y/o del nuevo sistema operativo OS del mismo. Según una realización preferente de la invención, estos datos se cifran junto con una suma de verificación de los mismos, dando lugar preferentemente a los siguientes elementos de datos cifrados ENC(OS||CS(OS), K_{se}) y ENC(APPS||CS(APPS), K_{se}), en donde CS(OS) y CS(APPS) denotan una suma de verificación determinada basándose en el sistema operativo OS del elemento seguro y una o varias aplicaciones APPS, respectivamente. El servidor de provisión de suscripciones -44- devuelve los elementos de datos cifrados al servidor de gestión de suscripciones -42-, que no puede descifrar estos elementos de datos, ya que el servidor de gestión de suscripciones -42- no tiene acceso a la clave del elemento seguro K_{se} que es compartida por el elemento

seguro -20- y el servidor de provisión de suscripciones -44- únicamente. Así pues, el servidor de gestión de suscripciones -42- no tendrá acceso a estos datos potencialmente confidenciales.

El servidor de gestión de suscripciones -42- preferentemente concatena los elementos de datos cifrados proporcionados por el servidor de provisión de suscripciones -44- en la etapa -S10- de la figura 2, es decir, ENC(OS||CS(OS), K_{se}) y ENC(APPS||CS(APPS), K_{se}), con la parte específica de la red del perfil de suscripción SUB proporcionado por el servidor de gestión de suscripciones -42- o la base de datos -43- que se comunica con el mismo. Preferentemente, esta parte específica de la red del perfil de suscripción SUB proporcionada por el servidor de gestión de suscripciones -42- incluye credenciales de suscripción (denominadas credenciales de suscripción CREDS en la figura 2), tales como una Identidad internacional de abonado móvil (IMSI) y/o una clave de autenticación Ki, que permite el acceso a la PLMN -30- o a una PLMN diferente admitida por el perfil de suscripción SUB.

Preferentemente, el servidor de gestión de suscripciones -42- cifra la parte específica de la red del perfil de suscripción SUB que incluye las credenciales de suscripción CREDS utilizando la clave de configuración K_{conf} que fue recibida por el servidor de gestión de suscripciones -42- del servidor de provisión de suscripciones -44- en la etapa -S7- de la figura 2 (así como en la forma originalmente cifrada del elemento seguro -20- en la etapa -S5- de la figura 2). También en este caso se prefiere que la parte específica de la red del nuevo perfil de suscripción SUB que incluye las credenciales de suscripción CREDS se cifre junto con una suma de verificación de las mismas dando lugar preferentemente al siguiente elemento de datos cifrado ENC(CREDS||CS(CREDS), K_{conf}), en el que CS(CREDS) denota una suma de verificación determinada basándose en las credenciales de suscripción CREDS.

Preferentemente, el mensaje M resultante de la concatenación de los elementos de datos cifrados, es decir, ENC(OS||CS(OS), K_{se}) y ENC(APPS||CS(APPS), K_{se}), proporcionado por el servidor de provisión de suscripciones -44- en la etapa -S10- de la figura 2 con el elemento de datos cifrado creado por el servidor de gestión de suscripciones -42- basándose en las credenciales de suscripción CREDS, es decir, ENC(CREDS||CS(CREDS), K_{conf}), a su vez, es cifrado por el servidor de gestión de suscripciones -42- utilizando la clave de sesión K_{ses}, es decir, ENC(M, K_{ses}) con M = ENC(OS||CS(OS), K_{se})||ENC(APPS||CS(APPS), K_{se})||ENC(CREDS||CS(CREDS), K_{conf}). La clave de sesión K_{ses} había sido proporcionada al servidor de gestión de suscripciones -42- en forma cifrada mediante el elemento seguro -20- en la etapa -S5- de la figura 2 y ha sido descifrado mediante el servidor de gestión de suscripciones -42- en la etapa -S8- de la figura 2 utilizando la clave de configuración K_{conf} proporcionada por el servidor de provisión de suscripciones -44- en la etapa -S7- de la figura 2.

En la etapa -S11- de la figura 2, el servidor de gestión de suscripciones -42- transmite la versión cifrada del mensaje M al elemento seguro -20- a través del terminal móvil -12-. Después de recibir el mensaje cifrado M, el elemento seguro -20-, a su vez, descifra este mensaje M en la etapa -S12- de la figura 2 utilizando la clave de sesión K_{ses} creada en la etapa -S4- de la figura 2. A partir del mensaje descifrado M, el elemento seguro -20- extrae el sistema operativo OS, una o varias aplicaciones APPS y las credenciales de suscripción CREDS del perfil de suscripción SUB seleccionado por el usuario del terminal móvil -12- en la etapa -S9- de la figura 2. Para descifrar la parte específica del hardware del perfil de suscripción SUB, es decir, el sistema operativo OS y una o varias aplicaciones APPS, el elemento seguro -20- utiliza la clave del elemento seguro K_{se}, mientras que para descifrar la parte específica de la red del perfil de suscripción SUB, es decir, las credenciales de suscripción CREDS, el elemento seguro -20- utiliza la clave de configuración K_{conf}. Además, con el fin de verificar la integridad de los datos proporcionados por el servidor de gestión de suscripciones -42- en la etapa -S11- de la figura 2, el elemento seguro -20- verifica las sumas de verificación correspondientes CS(OS), CS(APPS) y CS(CREDS) determinadas basándose en el sistema operativo OS, una o varias aplicaciones APPS y las credenciales de suscripción CREDS. Si se verifica que los datos son íntegros, es decir, que no se han modificado, el elemento seguro -20- los instala y/o almacena en la unidad de memoria -26- para que estén disponibles para su uso futuro, es decir, para la siguiente conexión a la PLMN -30- o a una PLMN diferente admitida por el perfil de suscripción SUB.

Una vez que el perfil de suscripción SUB se ha implementado correctamente en el elemento seguro -20- en la etapa -S12- de la figura 2, el elemento seguro -20- envía en la etapa -S13- de la figura 2 un mensaje de confirmación al servidor de gestión de suscripciones -42-. Además, en respuesta al mismo, el servidor de gestión de suscripciones -42- preferentemente proporciona al elemento seguro -20- un código de activación para activar el perfil de suscripción SUB en el elemento seguro -20-. Estas etapas podrían coordinarse en el lado del terminal móvil -12- mediante la aplicación de gestión de suscripciones SM APP descargada en la etapa -S2- de la figura 2 o mediante una aplicación similar ejecutándose en el mismo. Después de que el perfil de suscripción SUB se ha activado mediante el elemento seguro -20- utilizando el código de activación proporcionado por el servidor de gestión de suscripciones -42-, en principio es posible eliminar los perfiles de suscripción "antiguos", tales como el perfil de suscripción SUB1 provisional mostrado en la figura 1, de la unidad de memoria -26- del elemento seguro -20- para dejar espacio a perfiles de suscripción adicionales.

En caso de que el perfil de suscripción SUB no pueda implementarse o activarse correctamente en el elemento seguro -20-, el elemento seguro -20- preferentemente vuelve al perfil de suscripción provisional SUB1 que todavía está almacenado en la unidad de memoria -26- y puede reintentar el proceso descrito anteriormente o las etapas específicas del mismo para obtener un perfil de suscripción a través de la PLMN -30- y el sistema *backend* de

gestión de suscripciones -40-.

Antes de la activación del perfil de suscripción SUB en el elemento seguro -20-, o sustancialmente al mismo tiempo de la misma, el servidor de gestión de suscripciones -42- preferentemente envía un mensaje de confirmación al MNO de la PLMN admitida por el perfil de suscripción SUB y, en particular, las credenciales de suscripción CREDS del mismo. En respuesta al mismo, el MNO puede activar las credenciales de suscripción CREDS del perfil de suscripción SUB en su HLR/AUC con el fin de que el terminal móvil -12- y su elemento seguro -20- puedan conectarse a la PLMN utilizando las credenciales de suscripción CREDS del perfil de suscripción SUB.

Aunque anteriormente se ha descrito que una o varias aplicaciones APPS, como parte del nuevo perfil de suscripción SUB, son proporcionadas mediante el servidor de provisión de suscripciones -44-, el experto en la materia apreciará que la presente invención puede implementarse de manera ventajosa en casos en los que dichas aplicaciones, como parte del nuevo perfil de suscripción SUB, se proporcionan de manera adicional o alternativa mediante el servidor de gestión de suscripciones -42-, por ejemplo, una aplicación de acceso a la PLMN que contiene una implementación específica del MNO de un algoritmo de autenticación. Con respecto a la presente invención sencillamente es importante que una parte del perfil de suscripción SUB se proporcione mediante el servidor de provisión de suscripciones -44-, es decir, la parte específica del hardware del mismo, y que otra parte del perfil de suscripción SUB se proporcione mediante el servidor de gestión de suscripciones -42-, es decir, la parte específica de la red del mismo.

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 están dentro del alcance de la presente invención, definida mediante las reivindicaciones adjuntas.

REIVINDICACIONES

1. Procedimiento para proporcionar a un elemento seguro (20) de un terminal móvil (12) un perfil de suscripción (SUB), en el que el terminal móvil (12) está configurado para comunicarse con una red de comunicaciones celular (30) y en el que el perfil de suscripción (SUB) comprende una parte específica de la red relacionada con la red de comunicaciones celular (30) o una red de comunicaciones celular diferente y una parte específica del hardware relacionada con el hardware del elemento seguro (20) y/o del terminal móvil (12), en el que el procedimiento comprende las etapas de:

identificar al elemento seguro (20) por medio de un elemento de identificación (ID_{se}) para determinar una clave de configuración (K_{conf}) y una clave del elemento seguro (K_{se}) asociadas con el elemento seguro, en donde la etapa de identificar al elemento seguro (20) comprende;

transmitir el elemento de identificación (ID_{se}) del elemento seguro (20) al primer servidor (42);

enviar el elemento de identificación (ID_{se}) del elemento seguro (20) al segundo servidor (44); y

transmitir la clave de configuración (K_{conf}) determinada basándose en el elemento de identificación (ID_{se}) del segundo servidor (44) al primer servidor (42), en donde el elemento de identificación (ID_{se}) se transmite del elemento seguro (20) al primer servidor (42) por medio de un mensaje que incluye el elemento de identificación (ID_{se}) de forma no cifrada y una versión cifrada del elemento de identificación (ID_{se}) cifrado utilizando la clave de configuración (K_{conf}) almacenada en el elemento seguro (20), en donde el mensaje comprende, además, una versión cifrada de una clave de sesión (K_{ses}) creada mediante el elemento seguro (20) y una versión cifrada de una configuración del hardware (HW_{conf}) del elemento seguro (20) y/o del terminal móvil (12), ambas cifradas utilizando la clave de configuración (K_{conf});

configurar el perfil de suscripción (SUB), en donde la parte específica de la red del perfil de suscripción (SUB) se proporciona mediante un primer servidor (42) y la parte específica del hardware del perfil de suscripción (SUB) se proporciona mediante un segundo servidor (44); y

proporcionar el perfil de suscripción (SUB) configurado de forma inalámbrica al elemento seguro (20).

2. Procedimiento, según la reivindicación 1, en el que el primer servidor (42) descifra la versión cifrada del elemento de identificación (ID_{se}), la versión cifrada de la clave de sesión (K_{ses}) y la versión cifrada de la configuración del hardware (HW_{conf}) del elemento seguro (20) y/o del terminal móvil (12) utilizando la clave de configuración (K_{conf}) proporcionada por el segundo servidor (44), de tal modo que el primer servidor (42) puede verificar la validez de la clave de configuración (K_{conf}) proporcionada por el segundo servidor (44) verificando que el elemento de identificación (ID_{se}) enviado de forma no cifrada es idéntico al elemento de identificación (ID_{se}) resultante de descifrar la versión cifrada del elemento de identificación (ID_{se}) utilizando la clave de configuración (K_{conf}).

3. Procedimiento, según la reivindicación 1 o 2, en el que la configuración del hardware (HW_{conf}) del elemento seguro (20) y/o del terminal móvil (12) se determina sobre la marcha mediante una aplicación de gestión de suscripciones que se ejecuta en el elemento seguro (20) y/o el terminal móvil (12) o se recupera de una unidad de memoria (26) del elemento seguro (20) y/o de una unidad de memoria del terminal móvil (12).

4. Procedimiento, según cualquiera de las reivindicaciones 1 a 3, en el que el segundo servidor (44) transmite la clave de configuración (K_{conf}) determinada basándose en el elemento de identificación (ID_{se}) al primer servidor (42) solo después de que el primer servidor (42) se haya autenticado correctamente en el segundo servidor (44).

5. Procedimiento, según la reivindicación 1, en el que la etapa de configurar el perfil de suscripción (SUB) comprende las etapas de cifrar la parte específica del hardware del perfil de suscripción (SUB) mediante el segundo servidor (44) utilizando la clave del elemento seguro (K_{se}) y cifrando la parte específica de la red del perfil de suscripción (SUB) mediante el primer servidor (42) utilizando la clave de configuración (K_{conf}).

6. Procedimiento, según la reivindicación 5, que comprende, además, la etapa de cifrar la parte específica del hardware cifrada del perfil de suscripción (SUB) y la parte específica de la red cifrada del perfil de suscripción (SUB) utilizando una clave de sesión (K_{ses}) creada por el elemento seguro (20).

7. Procedimiento, según la reivindicación 1, en el que la etapa de configurar el perfil de suscripción (SUB) comprende la etapa adicional de determinar, al menos, un perfil de suscripción, incluyendo el perfil de suscripción (SUB), que sea compatible con una configuración del hardware (HW_{conf}) del elemento seguro (20) y/o del terminal móvil (12).

8. Procedimiento, según cualquiera de las reivindicaciones precedentes, en el que la parte específica del hardware del perfil de suscripción (SUB) comprende, al menos, partes de un sistema operativo (OS) para el elemento seguro

(20) y/o la parte específica de la red del perfil de suscripción (SUB) comprende credenciales de suscripción (CREDS), que incluyen preferentemente una IMSI y/o una clave de autenticación Ki, para conectar el elemento seguro (20) a la red de comunicaciones celular (30) o a una red de comunicaciones celular diferente.

9. Sistema *backend* de gestión de suscripciones (40), que comprende un primer servidor (42) y un segundo servidor (44), en el que el primer servidor (42) y el segundo servidor (44) están configurados para proporcionar a un elemento seguro (20) de un terminal móvil (12) un perfil de suscripción (SUB) mediante el procedimiento según cualquiera de las reivindicaciones 1 a 8.

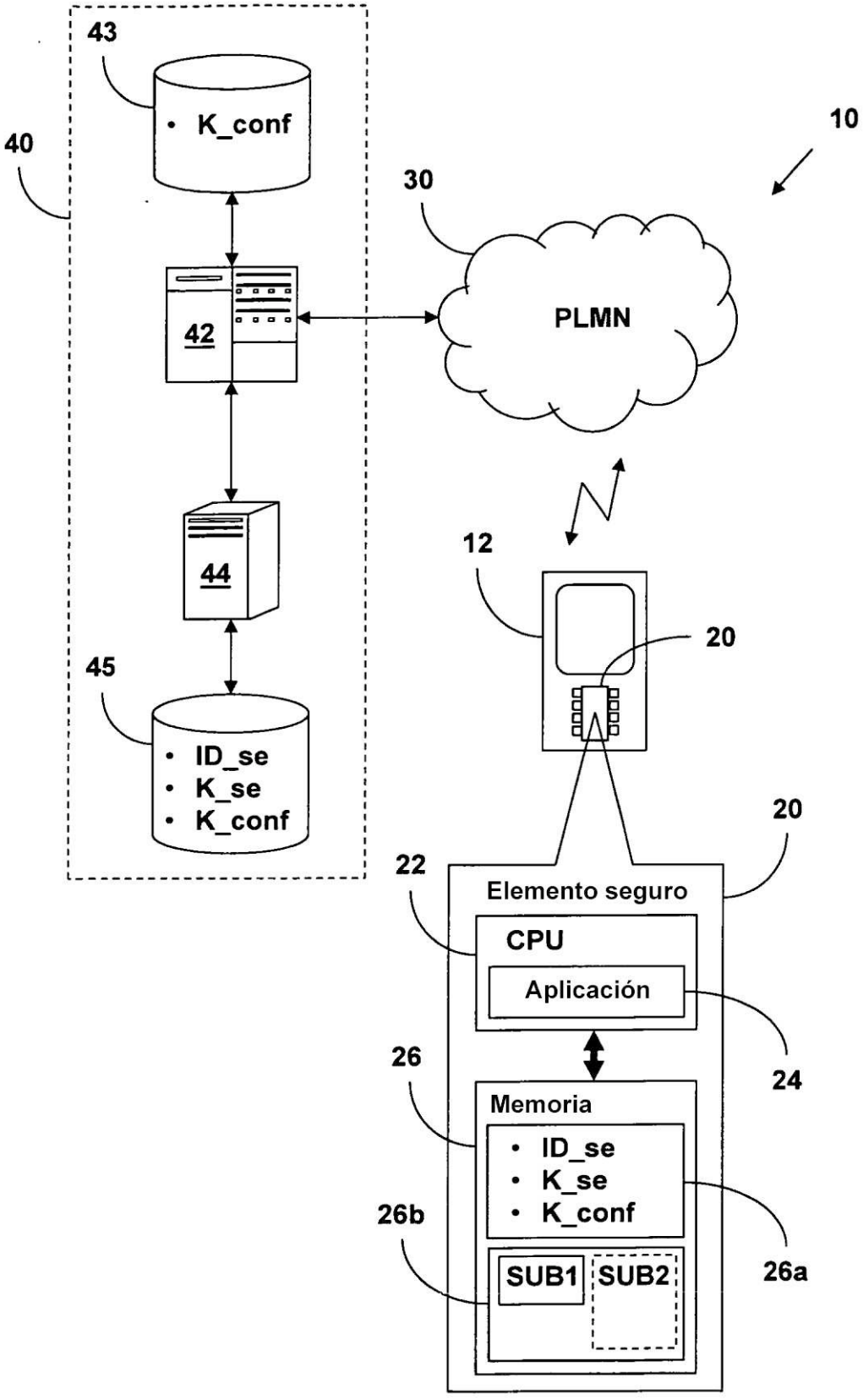
43
• K_conf
40
10
30
PLMN
42
44
12
20
45
• ID_se
• K_se
• K_conf
20
22
Elemento seguro
CPU
Aplicación
24
26
Memoria
• ID_se
• K_se
• K_conf
26b
SUB1
SUB2
26a

Fig. 1

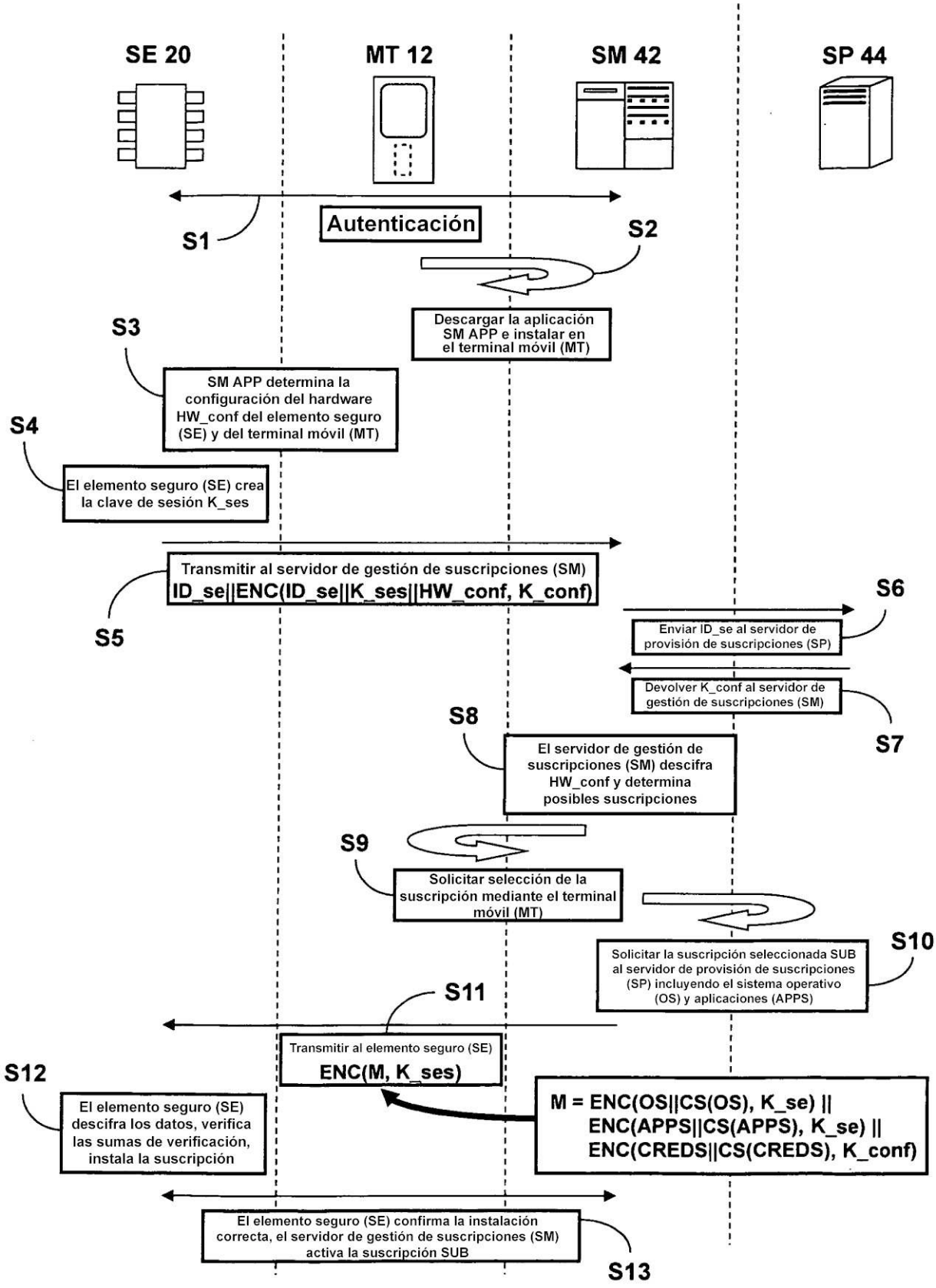
SE 20
MT 12
SM 42
SP 44
S1
Autenticación
S2
Descargar la aplicación SM APP e instalar en el terminal móvil (MT)
S3
SM APP determina la configuración del hardware HW_conf del elemento seguro (SE) y del terminal móvil (MT)
S4
El elemento seguro (SE) crea la clave de sesión K_ses
Transmitir al servidor de gestión de suscripciones (SM)
ID_se||ENC(ID_se||K_ses||HW_conf, K_conf)
S5
S6
Enviar ID_se al servidor de provisión de suscripciones (SP)
Devolver K_conf al servidor de gestión de suscripciones (SM)
S7
S8
El servidor de gestión de suscripciones (SM) descifra HW_conf y determina posibles suscripciones
S9
Solicitar selección de la suscripción mediante el terminal móvil (MT)
S10
Solicitar la suscripción seleccionada SUB al servidor de provisión de suscripciones (SP) incluyendo el sistema operativo (OS) y aplicaciones (APPS)
S11
Transmitir al elemento seguro (SE)
ENC(M, K_ses)
M = ENC(OS||CS(OS), K_se) ||
ENC(APPS||CS(APPS), K_se) ||
ENC(CREDS||CS(CREDS), K_conf)
S12
El elemento seguro (SE) descifra los datos, verifica las sumas de verificación, instala la suscripción
El elemento seguro (SE) confirma la instalación correcta, el servidor de gestión de suscripciones (SM) activa la suscripción SUB
S13

Fig. 2