(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 607 782**

(51) Int. CI.:

H04W 4/00 (2009.01)
H04W 8/18 (2009.01)
H04W 8/20 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **17.12.2013 E 13005876 (1)**

(97) Fecha y número de publicación de la concesión europea: **02.11.2016 EP 2887702**

(54) Título: **Procedimiento y dispositivo para proporcionar un elemento seguro con un perfil de suscripción**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
04.04.2017

(73) Titular/es:

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

(72) Inventor/es:

DAKSIEWICZ, DANIEL;
ÖSTLING, LEIF y
LARSSON, THOMAS

(74) Agente/Representante:

DURÁN MOYA, Luis Alfonso

DESCRIPCIÓN

Procedimiento y dispositivo para proporcionar un elemento seguro con un perfil de suscripción

Sector técnico de la invención

La invención se refiere a las comunicaciones móviles en general, y en particular a procedimientos y dispositivos para proporcionar un elemento seguro, tal como un módulo de identidad de abonado (SIM, subscriber identity module), una eUICC/UICC o similar, de un terminal móvil con un perfil de suscripción para la comunicación por medio de una red móvil.

Antecedentes de la invención

La comunicación por medio de un terminal móvil, tal como un teléfono móvil, por medio de una red móvil terrestre pública (PLMN, también denominada una red móvil o celular en la presente memoria) gestionada por un operador de red móvil (MNO) requiere por lo general que el terminal móvil esté equipado con un elemento seguro para almacenar de manera segura datos que identifican unívocamente al usuario del terminal móvil (también denominado abonado). Por ejemplo, en el contexto de un terminal móvil configurado para comunicar según el Sistema global para comunicaciones móviles (GSM, Global System for Mobile Communications), actualmente el estándar más popular del mundo para sistemas de comunicaciones móviles, el elemento seguro se denomina módulo de identidad de abonado (SIM, subscriber identity module) y normalmente se proporciona en forma de tarjeta inteligente. De acuerdo con 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, International Mobile Subscriber Identity) y una clave de autenticación Ki. Estas credenciales de la suscripción son almacenadas generalmente por el fabricante/proveedor del SIM o el MNO en el SIM durante el proceso de personalización del SIM antes de entregar su SIM al usuario del terminal móvil. Un SIM no personalizado normalmente no está adaptado para su utilización en un terminal móvil, es decir, la utilización de los servicios proporcionados por una PLMN con un SIM no personalizado no es posible sin las credenciales de la suscripción necesarias.

Un sector técnico de aplicación particular de elementos seguros, tales como SIM, eUICC, UICC y similares, que se espera crezca rápidamente en un futuro próximo, es la comunicación M2M (máquina a máquina), es decir, la comunicación entre máquinas sobre una red móvil sin intervención humana, también denominada Internet de las cosas. En la comunicación M2M los datos se transmiten automáticamente entre muchos tipos diferentes de máquinas equipadas con un elemento seguro en forma de un módulo M2M, tales como sistemas de TV, descodificadores, máquinas expendedoras, vehículos, semáforos, cámaras de seguridad, sensores, dispositivos de medición y similares. Es previsible que por lo menos para algunos de estos dispositivos no será posible o como mínimo será muy difícil proporcionar previamente al elemento seguro las credenciales de la suscripción necesarias, incluyendo por ejemplo una IMSI. Esto se debe a que en muchos de los dispositivos M2M el elemento seguro estará probablemente implementado en forma de un chip montado en superficie o un módulo de chip incorporado, sin la posibilidad de proporcionar previamente al elemento seguro las credenciales de la suscripción necesarias. Por consiguiente, una vez sobre el terreno, estos dispositivos M2M y sus elementos seguros no personalizados requieren el suministro seguro de las credenciales de la suscripción de manera inalámbrica.

Cuando se utilizan los servicios proporcionados por un MNO, en particular la comunicación por medio de la PLMN proporcionada por el MNO, el MNO carga normalmente una determinada tarifa mensual al usuario de un terminal móvil. Si el usuario móvil desea, debido por ejemplo a una menor tarifa mensual y/o a mejores servicios, cambiar a un MNO diferente, normalmente tiene que sustituir manualmente el SIM proporcionado por el MNO actual y que contiene, en particular, las credenciales de la suscripción necesarias para la conexión a la PLMN del MNO actual, por el SIM proporcionado por el nuevo MNO y que contiene las credenciales de la suscripción necesarias para la conexión a la PLMN del nuevo MNO. Ciertamente, para el usuario sería más cómodo que en lugar de este proceso de cambio a un nuevo MNO mediante la sustitución manual del SIM fuese posible utilizar un mismo elemento seguro en forma de un SIM que se pudiese "reprogramar" de manera inalámbrica mediante la descarga de un perfil de suscripción correspondiente incluyendo las credenciales de la suscripción e implementándolas automáticamente en el SIM.

Son conocidos dichos procedimientos para descargar un perfil de suscripción e implementarlo en un elemento seguro. Sin embargo, en la práctica, a menudo ocurrirá que un perfil de suscripción esté proporcionado por una entidad, por ejemplo, un operador de red móvil (MNO), diferente a la entidad que fabricó inicialmente el elemento seguro, es decir, el fabricante del elemento seguro. Dado que normalmente sólo el fabricante del elemento seguro tiene conocimiento de los detalles específicos del elemento seguro, tales como su sistema operativo así como las interfaces de gestión de la suscripción para implementar un nuevo perfil de suscripción en el elemento seguro, por ejemplo en forma de una interfaz de programación de aplicaciones (API, application programming interface) configurada de manera apropiada, que, en particular, por motivos de seguridad, el fabricante del elemento seguro desea mantener en secreto, puede surgir el problema de que el perfil de suscripción proporcionado por un MNO

tenga un formato que no sea compatible con la interfaz de gestión de la suscripción implementada en los elementos seguros.

El documento EP 2 747 466 A1 se refiere a un procedimiento para proporcionar un elemento seguro de un terminal móvil con un perfil de suscripción. El documento define la técnica anterior según el artículo 54(3) EPC.

El documento US 2009/0191857 A1, "Remote Subscription Management of M2M Terminals in 4G Cellular Wireless Networks" ("Gestión remota de suscripciones de terminales M2M en redes inalámbricas celulares 4G", de Isam Abdalla, Local computer networks workshop, así como el documento "GSMA One API Exchange Architecture for cross-operator network APIs Exchange Architecture for cross-operator network APIs" ("Arquitectura de intercambio One API para GSMA para API de redes de varios operadores, Arquitectura de intercambio para API de redes de varios operadores") se refieren a diversos procedimientos para gestionar las suscripciones en dispositivos móviles, en particular en dispositivos M2M.

El documento US 2009/0239503 A1 se refiere a un procedimiento para proporcionar a los dispositivos de comunicación credenciales de la suscripción de red después de la compra del dispositivo de comunicación. Según este documento, sería posible evitar tener que cargar previamente una suscripción temporal por medio de una provisión OTA (Over the Air, inalámbrica) en el dispositivo de comunicación.

Por lo tanto, existe una necesidad de procedimientos y dispositivos mejorados para proporcionar a un elemento seguro, tal como un módulo de identidad de abonado (SIM), una eUICC/UICC o similar, de un terminal móvil un perfil de suscripción para comunicar por medio de una red móvil, en que estos procedimientos y dispositivos traten los problemas descritos anteriormente.

Características de la invención

La necesidad anterior se resuelve 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 de la invención se da a conocer un procedimiento para proporcionar a un elemento seguro que tiene un procesador y una memoria de un terminal móvil un perfil de suscripción objetivo para comunicar por medio de una red móvil objetivo. El procedimiento comprende las etapas de: proporcionar al elemento seguro, como una primera parte del perfil de suscripción objetivo, una interfaz de gestión de la suscripción; implementar la interfaz de gestión de la suscripción en el elemento seguro; y proporcionar al elemento seguro, como una segunda parte del perfil de suscripción objetivo, los datos de la suscripción en un formato definido por el operador de la red móvil objetivo, donde la interfaz de gestión de la suscripción permite al elemento seguro procesar los datos de la suscripción (en el formato utilizado por el operador de la red móvil objetivo) e implementar el perfil de suscripción objetivo en el mismo para permitir el acceso a la red móvil objetivo.

La interfaz de gestión de la suscripción implementa una API estandarizada en el elemento seguro para procesar los datos de la suscripción utilizados por el operador de la red móvil objetivo.

Según las realizaciones preferentes de la invención, el procedimiento comprende, antes de la etapa de proporcionar, como una primera parte del perfil de suscripción objetivo, una interfaz de gestión de la suscripción al elemento seguro, la etapa adicional de conectar a una red móvil soportada por un perfil de suscripción ya presente en el elemento seguro. Este perfil de suscripción ya presente en el elemento seguro podría ser un perfil de suscripción de provisión.

Preferentemente, el procedimiento comprende, antes de la etapa de proporcionar, como una primera parte del perfil de suscripción objetivo, una interfaz de gestión de la suscripción al elemento seguro, la etapa adicional de solicitar el perfil de suscripción objetivo a un sistema en segundo plano de gestión de suscripciones.

Según las realizaciones preferentes de la invención, el procedimiento comprende, después de la etapa de implementar la interfaz de gestión de la suscripción en el elemento seguro, la etapa adicional de enviar un mensaje de confirmación al sistema en segundo plano de gestión de suscripciones. Preferentemente, la etapa de implementar la interfaz de gestión de la suscripción en el elemento seguro comprende la etapa adicional de comprobar la integridad de la interfaz de gestión de la suscripción.

Preferentemente, el procedimiento comprende, después de la etapa de proporcionar al elemento seguro los datos de la suscripción en un formato definido por el operador de la red móvil objetivo, las etapas adicionales de conectar a la red móvil objetivo y enviar un mensaje de confirmación al sistema en segundo plano de gestión de suscripciones.

La presente invención proporciona, entre otras, la ventaja de que la entidad que proporciona el perfil de suscripción objetivo puede seguir utilizando sus procedimientos y formatos propietarios de gestión de la suscripción, mientras que el fabricante del elemento seguro puede seguir utilizando sus procedimientos y formatos de gestión de la suscripción sin revelar ninguna información confidencial.

Tal como se utiliza en la presente memoria, un "perfil de suscripción" (o abreviadamente, una "suscripción") puede comprender como mínimo partes de un sistema operativo del elemento seguro, una o más aplicaciones, archivos y/o datos, tales como credenciales de la suscripción. Tal como se utiliza en la presente memoria, la expresión "proporcionar un perfil de suscripción a un 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 junto a un perfil de suscripción ya existente así como un intercambio parcial de un perfil de suscripción existente, que puede ser una actualización del perfil de suscripción existente.

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 celular de comunicaciones. Dicho SIM se comunica con el terminal móvil por medio de un lector de tarjetas en el mismo y en principio puede ser extraído del terminal móvil para ser sustituido por un SIM diferente y/o utilizado en un terminal móvil diferente. Alternativamente, el elemento seguro es una parte integral del terminal móvil, tal como un módulo de chip cableado. Dichos elementos seguros incorporados son conocidos, por ejemplo, como Tarjetas universales de circuito integrado incorporadas (eUICC, embedded Universal Integrated Circuit Cards). Preferentemente, el elemento seguro soporta el almacenamiento de varios perfiles de suscripción que pueden estar asociados con diferentes MNO. Generalmente, en cualquier momento está activo solamente un perfil de suscripción, ya que el dispositivo móvil sólo se puede utilizar con un perfil de suscripción.

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 comunicar con una red celular de comunicaciones, con el fin de recibir un nuevo perfil de suscripción. Preferentemente, el terminal móvil está implementado en forma de un teléfono inteligente, una tableta, un ordenador portátil, una PDA o similar. Alternativamente, el terminal móvil puede ser un dispositivo multimedia tal como un marco de imágenes digitales, un equipo de sonido, un sistema de TV, un descodificador, un lector de libros electrónicos y similares. A modo de ejemplo, el término "terminal móvil" también incluye cualquier clase de maquinaria, tal como máquinas expendedoras, vehículos, medidores inteligentes y similares que estén configurados para comunicar mediante un sistema de comunicaciones celulares.

Según un cuarto aspecto, la invención da a conocer un sistema en segundo plano de gestión de suscripciones configurado para proporcionar a un elemento seguro de un terminal móvil un perfil de suscripción mediante 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 ejemplo no limitativo, haciendo referencia a los dibujos adjuntos. Los expertos en la materia apreciarán, en particular, que las anteriores realizaciones preferentes se pueden combinar de varias formas, que darán lugar a realizaciones adicionales ventajosas que están explícitamente soportadas y cubiertas por la presente invención. En concreto, los expertos en la materia apreciarán que las realizaciones preferentes descritas anteriormente se pueden implementar en el contexto de los diferentes aspectos de la invención.

Breve descripción de los dibujos

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

La figura 2 muestra un diagrama que ilustra un procedimiento para proporcionar al elemento seguro de un terminal móvil un perfil de suscripción, 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 varios aspectos de la presente invención. Aunque la siguiente descripción detallada se referirá a un terminal "móvil", un experto en la materia apreciará que la presente invención se puede implementar ventajosamente en el contexto de cualesquiera clases de dispositivos que estén configurados para comunicar por medio de una red de comunicaciones móvil o celular. En otras palabras, el atributo "móvil" utilizado en la presente memoria se refiere a la capacidad de un terminal para comunicar por medio de una red de comunicaciones móvil o celular, incluyendo también las redes de comunicación móvil basadas en IP.

En la figura 1 se muestra un terminal móvil a modo de ejemplo -12-, que incluye un elemento seguro -20- para almacenar de forma segura y procesar los datos que identifican unívocamente el elemento seguro -20-, el terminal móvil -12- y/o su usuario. Tal como se indica en la figura 1, el terminal móvil -12- es preferentemente un teléfono móvil, un teléfono inteligente o un dispositivo similar. Un experto en la materia apreciará, sin embargo, que el terminal móvil -12- según la presente invención se puede implementar también en forma de otros dispositivos, tales como, una tableta o un ordenador portátil, un sistema de TV, un descodificador, una máquina expendedora, un vehículo, una cámara de seguridad, un sensor y similares.

Según las realizaciones preferentes de la invención, el elemento seguro -20- está configurado como una eUICC o una UICC con una aplicación de SIM que se ejecuta en el mismo, es decir, un elemento seguro que se puede montar en el terminal móvil -12- y utilizar en sistemas celulares de comunicaciones para la identificación unívoca y segura del abonado así como para la provisión de distintas funciones especiales y servicios de valor añadido. Alternativamente, el elemento seguro -20- se podría configurar como un módulo de identidad de abonado (SIM), siendo actualmente el SIM el tipo de elemento seguro más popular. Sin embargo, un experto en la materia apreciará que la presente invención abarca asimismo otros tipos de elementos seguros que, dependiendo de la generación y del tipo subyacentes del estándar del sistema de comunicaciones celulares, se denominan como USIM, R-UIM, ISIM, CSIM y similares. Además, el elemento seguro -20- podría ser un módulo M2M o un Entorno de ejecución fiable (TEE, Trusted Execution Environment) implementado como parte del terminal móvil -12-.

Tal como se ha mencionado anteriormente, el terminal móvil -12- está configurado para comunicar por medio de la interfaz aérea (o enlace radioeléctrico) con una red celular de comunicaciones o una red móvil terrestre pública (PLMN, public land mobile network) -30-, preferentemente gestionada por un operador de red móvil (MNO) según el estándar GSM, para utilizar los servicios proporcionados por la PLMN -30-, tales como la comunicación con otros terminales móviles conectados con la misma. En lo que sigue, se describirán las realizaciones preferentes de la invención en el contexto de una red celular de comunicaciones según los estándares del Sistema global para comunicación móvil (GSM), según se especifica en diversas especificaciones proporcionadas por ETSI. Sin embargo, un experto en la materia apreciará que la presente invención también se puede aplicar ventajosamente en relación con otros sistemas celulares de comunicación. Dichos sistemas incluyen los sistemas celulares de comunicaciones de tercera generación (3GPP), tal como el Sistema universal de telecomunicaciones móviles (UMTS, Universal Mobile Telecommunications System), y redes móviles de última generación o cuarta generación (4G), tal como Evolución a largo plazo (LTE, Long Term Evolution), así como otros sistemas de comunicaciones.

Como saben bien los expertos en la materia, una PLMN configurada según el estándar GSM comprende normalmente un subsistema de estaciones base que consiste en una o más estaciones base transceptoras que definen celdas respectivas de la PLMN y están conectadas a un controlador de estaciones base. Generalmente, el controlador de estaciones base es uno de varios controladores de estaciones base que se comunican con un centro de conmutación móvil (MSC, mobile switching center) común. Frecuentemente, en el MSC está incorporada una base de datos local denominada Registro de posición de visitantes (VLR, Visitor Location Register) para mantener un seguimiento de los usuarios móviles que están situados actualmente en el interior de las celdas cubiertas por un MSC (es decir, el área de servicio del MSC). El MSC proporciona esencialmente la misma funcionalidad que una central de conmutación principal en una red telefónica pública conmutada y adicionalmente es responsable del procesamiento de las llamadas, de la gestión de la movilidad y de la gestión de los recursos radioeléctricos. Además, el MSC está en comunicación con un Registro de posición local (HLR, home location register), que es la base de datos principal de la PLMN que almacena información sobre sus usuarios móviles necesaria para la autenticación. Con este fin, el HLR generalmente está en comunicación con un centro de autenticación (AUC, authentication center). Un experto en la materia apreciará que aunque los componentes descritos anteriormente de un sistema GSM convencional pueden tener distintos nombres en estándares diferentes o consecutivos para las redes de comunicaciones móviles, los principios básicos utilizados en los mismos son sustancialmente similares y, por lo tanto, compatibles con la presente invención.

De los componentes de la PLMN -30- descritos anteriormente se muestra solamente una estación base transceptora -32- a modo de ejemplo en el dibujo esquemático de la figura 1, para facilitar la explicación. La PLMN -30- está en comunicación, por lo menos temporalmente, con un sistema en segundo plano de gestión de suscripciones -40- para proporcionar al elemento seguro -20- del terminal móvil -12- un perfil de suscripción, que se describirá con más detalle más adelante. La PLMN -30- podría comprender además un SMS-C (Short Message Service Center, Centro de servicio de mensajes cortos) para almacenar, enviar, convertir y entregar mensajes SMS. Dichos mensajes SMS podrían utilizarse para transmitir un perfil de suscripción o como mínimo partes del mismo al elemento seguro -20- del terminal móvil -12-.

Tal como se puede deducir a partir de la vista a mayor escala del elemento seguro -20- en la figura1, en el mismo está implementada la siguiente arquitectura software preferente. Un entorno en tiempo de ejecución Java Card™ (JCRE, Java Card™ runtime environment) -24- está implementado en la parte superior de un sistema operativo (OS, operating system) nativo -22- del elemento seguro -20-. Generalmente el sistema operativo nativo -22- y el entorno en tiempo de ejecución Java Card™ -24- son instalados por el fabricante durante el proceso de fabricación del elemento seguro -20-. El Entorno en tiempo de ejecución Java Card™ -24- comprende una máquina virtual Java Card™ (JCVM, Java Card™ Virtual Machine) -26-, así como por lo menos una interfaz de programación de

aplicaciones (API) Java Card™ 16'. Mediante las API Java Card™, cualesquiera miniaplicaciones que se ejecuten en el elemento seguro -20- pueden ejecutar funciones que están proporcionadas por la máquina virtual Java Card™ -26- y el sistema operativo nativo -22-. En el libro "Java Card™ Technology for Smart Cards" ("Tecnología Java Card™ para tarjetas inteligentes"), de Zhiqun Chen, Addison-Wesley, 2000, por ejemplo, se pueden encontrar más detalles sobre esta arquitectura de software convencional.

Tal como apreciará un experto en la materia, para implementar y ejecutar los componentes de software descritos anteriormente, el elemento seguro -20- comprenderá generalmente una unidad central de procesamiento (CPU, central processing unit) para procesar los datos así como una unidad de memoria para almacenar los datos, que para simplificar la ilustración no se muestran en la figura 1. Preferentemente, la CPU está configurada de tal manera que como mínimo se pueda ejecutar una aplicación en la CPU proporcionando las características que se describirán con más detalle a continuación en el contexto de la figura 2. La aplicación podría implementarse, por ejemplo, como una aplicación Java. Preferentemente, la unidad de memoria se implementa como una memoria flash regrabable y no volátil. Preferentemente, por lo menos una parte de la misma está configurada para almacenar de forma segura datos secretos en la misma, tales como credenciales de la suscripción que son parte de un perfil de suscripción. Preferentemente, la unidad de memoria soporta el almacenamiento de múltiples perfiles de suscripción, por ejemplo en forma de "posiciones" para alojar perfiles de suscripción, tales como un perfil de suscripción que debe ser proporcionado por el sistema en segundo plano de gestión de suscripciones -40- según el proceso mostrado en la figura 2 y descrito a continuación con más detalle. Los múltiples perfiles de suscripción pueden estar asociados con un MNO o con diferentes MNO.

Preferentemente, se puede almacenar un primer perfil de suscripción en la unidad de memoria del elemento seguro -20- durante el proceso de fabricación y/o personalización del terminal móvil -12- y/o de su elemento seguro -20-. Específicamente en esta realización preferente es posible que este primer perfil de suscripción sea solamente un perfil de suscripción provisional que sólo proporcione servicios básicos que permitan al elemento seguro -20- y al terminal móvil -12- comunicar con el sistema en segundo plano de gestión de suscripciones -40- y descargar un perfil de suscripción más completo que proporcione servicios adicionales. Puesto que un perfil de suscripción provisional generalmente proporciona únicamente una funcionalidad limitada, generalmente se incitará al usuario del terminal móvil -12- a cambiar a un perfil de suscripción más completo que proporcione servicios adicionales.

Generalmente, un perfil de suscripción puede comprender como mínimo partes de un sistema operativo del elemento seguro -20-, una o varias aplicaciones, tales como una aplicación de acceso a la PLMN que contiene un algoritmo de autenticación específico del MNO, archivos y/o datos, tales como las credenciales de la suscripción que permiten al elemento seguro -20- y al terminal móvil -12- conectarse a la PLMN -30-, por ejemplo una Identidad internacional de abonado móvil (IMSI) para la identificación y/o una clave de autenticación Ki para la autenticación del elemento seguro -20-.

A continuación se describirá haciendo referencia a la figura 2 una forma preferente de hacer funcionar el sistema en segundo plano de gestión de suscripciones -40-, preferentemente en forma de un servidor de gestión de la suscripción -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, el elemento seguro -20- se conecta a la PLMN -30- utilizando el perfil de suscripción (o uno de los perfiles de suscripción) y, en concreto, las credenciales de la suscripción del mismo almacenadas en la unidad de memoria del elemento seguro -20-. Habiéndose conectado con éxito a la PLMN -30-, el elemento seguro -20- solicita al sistema en segundo plano -40- de gestión de suscripciones en la etapa -S2- de la figura 2 la recuperación de un nuevo perfil de suscripción para acceder a la PLMN objetivo. Tal como apreciará un experto en la materia, esta PLMN objetivo -30- podría ser la PLMN -30- o una PLMN diferente gestionada por un MNO diferente. En respuesta a esta solicitud, el sistema en segundo plano de gestión de suscripciones -40- carga una interfaz de gestión de la suscripción -16- en el elemento seguro -20- en la etapa -S3- de la figura 2.

Después de haber descargado del sistema en segundo plano de gestión de suscripciones -40- la interfaz de gestión de la suscripción -16- en la etapa -S3- de la figura 2, la interfaz de gestión de la suscripción -16- se implementa en el elemento seguro -20- en la etapa -S4- de la figura 2. Antes de implementar la interfaz de gestión de la suscripción -16- esta etapa podría incluir la etapa adicional de comprobar la integridad de la interfaz de gestión de la suscripción -16- mediante el elemento seguro -20-, por ejemplo calculando una suma de verificación. La interfaz de gestión de la suscripción -16- podría implementarse como una aplicación que, junto con las API Java Card™ 16' ya presentes en el elemento seguro -20-, proporcione una API que permita interactuar con, y procesar un perfil de suscripción con un formato utilizado por el MNO de la PLMN objetivo.

Preferentemente, el elemento seguro -20- envía en la etapa -S5- de la figura 2 un mensaje de confirmación al sistema en segundo plano de gestión de suscripciones -40- indicando que la interfaz de gestión de la suscripción se ha implementado correctamente. En respuesta a este mensaje de confirmación, el sistema en segundo plano de gestión de suscripciones -40- carga en el elemento seguro -20- los datos de la suscripción -18- en el formato proporcionado por el MNO de la PLMN objetivo (etapa -S6- de la figura 2).

Habiendo recibido los datos de la suscripción en el formato proporcionado por el MNO de la PLMN objetivo, el elemento seguro procesa en la etapa -S7- de la figura 2 estos datos de la suscripción -18- utilizando la interfaz de gestión de la suscripción -16- implementada en el elemento seguro -20- en la etapa -S4- de la figura 2. De este modo, el elemento seguro -20- implementa el perfil de suscripción objetivo.

Una vez que el perfil de suscripción objetivo se ha implementado correctamente en el elemento seguro -20-, el elemento seguro -20- puede intentar conectarse a la PLMN objetivo (etapa -S8- de la figura 2). En caso de una conexión con éxito a la PLMN objetivo, el elemento seguro -20- envía preferentemente un mensaje de confirmación al sistema en segundo plano de gestión de suscripciones -40- (etapa -S9- de la figura 2).

Antes o de manera sustancialmente simultánea a la implementación del perfil de suscripción objetivo en el elemento seguro -20-, el sistema en segundo plano de gestión de suscripciones -40- envía preferentemente un mensaje de confirmación al MNO de la PLMN objetivo. En respuesta al mismo, el MNO puede activar las credenciales de la suscripción del perfil de suscripción objetivo en su HLR/AUC para que el terminal móvil -12- y su elemento seguro -20- puedan conectarse a la PLMN objetivo utilizando las credenciales de la suscripción del perfil de suscripción objetivo.

A la vista de la descripción detallada anterior, un experto en la materia apreciará que se pueden realizar modificaciones y/o adiciones a los procedimientos, dispositivos y sistemas descritos en lo anterior, que se debe considerar que quedan dentro del alcance de la presente invención, tal como se define mediante las reivindicaciones adjuntas. En particular, un experto en la materia apreciará que la presente invención no se limita al número y la secuencia de etapas mostradas en la figura 2. Por ejemplo, las etapas -S3- y -S6- de la figura 2 podrían incorporarse en una sola etapa.

REIVINDICACIONES

1. Procedimiento para proporcionar a un elemento seguro (20) que tiene un procesador y una memoria de un terminal móvil (12) un perfil de suscripción objetivo para comunicar por medio de una red móvil objetivo, en el que el procedimiento comprende las etapas de:

proporcionar al elemento seguro (20), como una primera parte del perfil de suscripción objetivo, una interfaz de gestión de la suscripción (16);

implementar la interfaz de gestión de la suscripción (16) en el elemento seguro (20) y, a continuación, enviar un mensaje de confirmación a un sistema en segundo plano de gestión de suscripciones (40), y comprobar la integridad de la interfaz de gestión de la suscripción (16) mediante el elemento seguro (20)

proporcionar al elemento seguro (20), como una segunda parte del perfil de suscripción objetivo, los datos de la suscripción (18) en un formato definido por el operador de la red móvil objetivo,

en el que la interfaz de gestión de la suscripción (16) permite al elemento seguro (20) procesar los datos de la suscripción (18) e implementar el perfil de suscripción objetivo en el mismo para permitir el acceso a la red móvil objetivo, y en el que la interfaz de gestión de la suscripción (16) implementa una interfaz de programación de aplicaciones estandarizada en el elemento seguro (20) para procesar los datos de la suscripción (18) utilizados por el operador de la red móvil objetivo.

2. Procedimiento, según la reivindicación 1, en el que el procedimiento comprende, antes de la etapa de proporcionar como una primera parte del perfil de suscripción objetivo una interfaz de gestión de la suscripción (16) al elemento seguro (20), la etapa adicional de conectar a una red móvil soportada por un perfil de suscripción ya presente en el elemento seguro (20).

3. Procedimiento, según la reivindicación 2, en el que el perfil de suscripción ya presente en el elemento seguro (20) es un perfil de suscripción de provisión.

4. Procedimiento, según la reivindicación 1, en el que el procedimiento comprende, antes de la etapa de proporcionar como una primera parte del perfil de suscripción objetivo una interfaz de gestión de la suscripción (16) al elemento seguro (20), la etapa adicional de solicitar el perfil de suscripción objetivo a un sistema en segundo plano de gestión de suscripciones (40).

5. Procedimiento, según la reivindicación 1, en el que el procedimiento comprende, después de la etapa de proporcionar al elemento seguro (20) los datos de la suscripción (18) en un formato definido por el operador de la red móvil objetivo, las etapas adicionales de conectar a la red móvil objetivo y enviar un mensaje de confirmación a un sistema en segundo plano de gestión de suscripciones (40).

6. Elemento seguro (20), que comprende un perfil de suscripción proporcionado al elemento seguro (20) mediante el procedimiento según cualquiera de las reivindicaciones anteriores.

7. Elemento seguro (20), según la reivindicación 6; en el que el elemento seguro (20) está configurado como un módulo de identidad de abonado (SIM) o una Tarjeta de circuito integrado universal incorporada (eUICC).

8. Terminal móvil (12) que contiene un elemento seguro (20) según las reivindicaciones 6 o 7.

9. Sistema en segundo plano de gestión de suscripciones (40) configurado para proporcionar a un elemento seguro (20) de un terminal móvil (12) un perfil de suscripción mediante el procedimiento según cualquiera de las reivindicaciones 1 a 5.

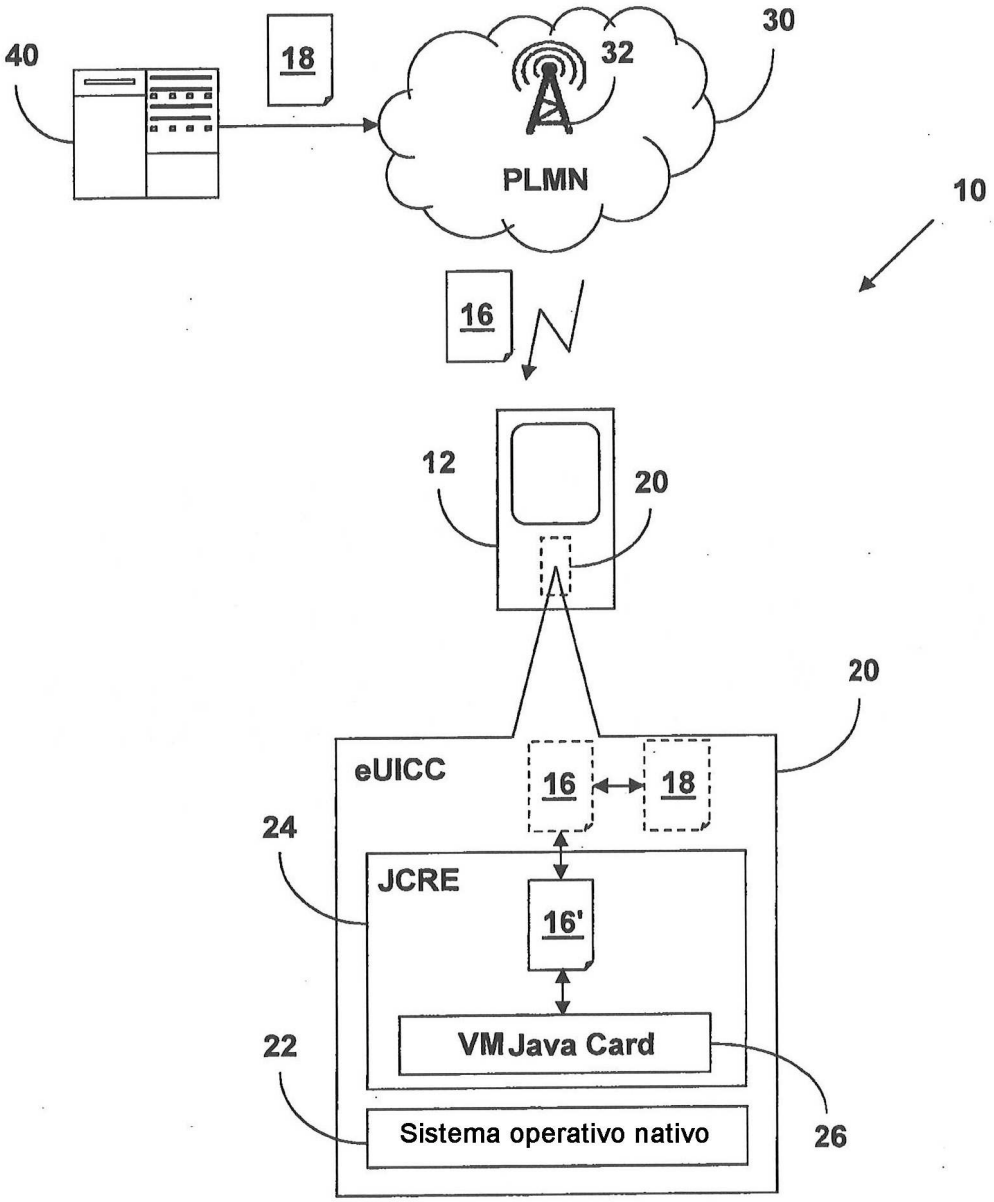
40
18
30
32
PLMN
10
16
12
20
20
eUICC
16
18
24
JCRE
16'
22
VM Java Card
26
Sistema operativo nativo

Fig. 1

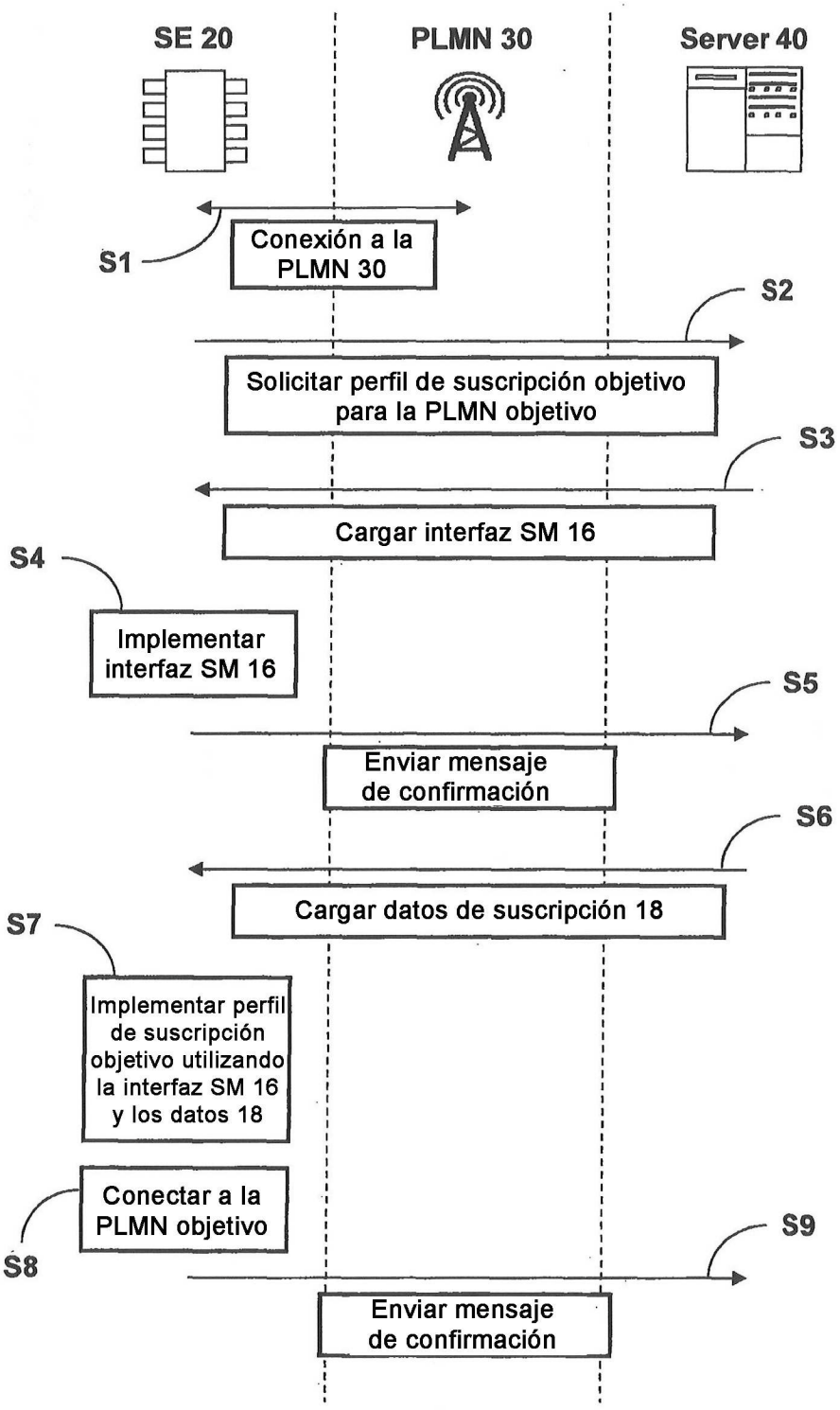
SE 20
PLMN 30
Server 40
S1
Conexión a la PLMN 30
S2
Solicitar perfil de suscripción objetivo para la PLMN objetivo
S3
Cargar interfaz SM 16
S4
Implementar interfaz SM 16
S5
Enviar mensaje de confirmación
S6
Cargar datos de suscripción 18
S7
Implementar perfil de suscripción objetivo utilizando la interfaz SM 16 y los datos 18
Conectar a la PLMN objetivo
S8
S9
Enviar mensaje de confirmación

Fig. 2