(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 728 299**

(51) Int. CI.:

H04W 8/14 (2009.01)
H04W 8/18 (2009.01)
H04W 4/50 (2008.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **22.09.2015 PCT/EP2015/001880**

(87) Fecha y número de publicación internacional: **31.03.2016 WO16045786**

(96) Fecha de presentación y número de la solicitud europea: **22.09.2015 E 15777873 (9)**

(97) Fecha y número de publicación de la concesión europea: **06.03.2019 EP 3198903**

(54) Título: **Procedimientos y dispositivos para proporcionar un perfil de suscripción a un dispositivo móvil**

(30) Prioridad:

23.09.2014 DE 102014014078

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
23.10.2019

(73) Titular/es:

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

(72) Inventor/es:

AHRENS, CARSTEN;
MÜLLER, BERND;
DINGER, JENS;
MORAWIETZ, ANDREAS y
HUBER, ULRICH

(74) Agente/Representante:

DURAN-CORRETJER, S.L.P

DESCRIPCIÓN

Procedimientos y dispositivos para proporcionar un perfil de suscripción a un dispositivo móvil

Campo de la invención

La invención se refiere a la comunicación a través de redes de telefonía móvil en general y, en particular, a procedimientos y dispositivos para proporcionar un perfil de suscripción a un dispositivo móvil para la comunicación a través de una red de telefonía móvil.

Antecedentes de la invención

La comunicación mediante un dispositivo móvil, por ejemplo, mediante un teléfono móvil, a través de una red de telefonía móvil (también denominada PLMN [Public Land Mobile Network]), operada por un operador de red (también denominado MNO [Mobile Network Operator]), requiere generalmente que el dispositivo móvil esté equipado con un elemento de seguridad o módulo de identificación de abonado, por ejemplo, en forma de una tarjeta SIM, para el registro seguro de datos de autorización de suscripción ("Subscription Credentials"), que generalmente forman parte de un perfil de suscripción e identifican y autentifican inequívocamente al usuario del dispositivo móvil respecto a la red de telefonía móvil. Este tipo de datos de autorización de suscripción, por ejemplo, una IMSI (International Mobile Subscriber Identity) y una clave de autentificación K_i se almacenaban en el pasado, habitualmente en el marco de una denominada "personalización", en el entorno seguro del fabricante del elemento de seguridad en el elemento de seguridad.

Mientras en el pasado la gran mayoría de los elementos de seguridad en forma de tarjetas SIM en un dispositivo móvil podían sustituirse fácilmente, desde hace algún tiempo existen cada vez más elementos de seguridad que se montan de forma fija en un dispositivo móvil. Un elemento de seguridad de este tipo montado de forma fija en un dispositivo móvil, que el experto conoce, en particular, bajo el término "SIM embebida" (Embedded SIM) o "UICC embebida" [Embedded UICC (eUICC)], generalmente ya no puede personalizarse en un entorno seguro del fabricante del elemento de seguridad, ya que no se conoce previamente, en particular, el campo de aplicación del elemento de seguridad.

Por lo tanto, existe la necesidad de procedimientos y dispositivos mejorados para personalizar un dispositivo móvil, es decir, para proporcionar un perfil de suscripción a un dispositivo móvil, en particular, a su elemento de seguridad.

Del documento EP 2 701 359 A1 se conoce un procedimiento para personalizar un dispositivo no personalizado con datos de identidad de abonado, tal que los datos de identidad de abonado descargados se mantienen en el dispositivo.

El documento US 2014/0057558 A1 se refiere a la transferencia de datos SIM idénticos de un primer dispositivo a un segundo dispositivo. En este caso, los datos SIM no se modifican y se borran del primer dispositivo tras la transferencia.

Resumen de la invención

El anterior objetivo se consigue según la presente invención mediante el objeto correspondiente de las reivindicaciones independientes. En las reivindicaciones dependientes se definen realizaciones preferentes de la invención.

Según un primer aspecto de la invención, se proporciona un procedimiento para proporcionar un perfil de suscripción a un dispositivo móvil para la comunicación a través de una red de telefonía móvil. En este sentido, el procedimiento comprende los siguientes pasos: la conexión de un primer dispositivo móvil con un primer perfil de suscripción a una red de telefonía móvil; la descarga de un segundo perfil de suscripción a través de la red de telefonía móvil al primer dispositivo móvil; y el reenvío del segundo perfil de suscripción del primer dispositivo móvil al segundo dispositivo móvil a través de un canal de comunicación.

Preferentemente, tras el paso del reenvío del segundo perfil de suscripción del primer dispositivo móvil al segundo dispositivo móvil a través del canal de comunicación, el procedimiento comprende el paso adicional de la conexión del segundo dispositivo móvil con el segundo perfil de suscripción a una red de telefonía móvil.

Según modos de realización preferentes de la invención, la red de telefonía móvil a la que se conecta el segundo dispositivo móvil con el segundo perfil de suscripción es la red de telefonía móvil a través de la cual se descargó el segundo perfil de suscripción al primer dispositivo móvil.

Preferentemente, el canal de comunicación entre el primer dispositivo móvil y el segundo dispositivo móvil es un canal de comunicación NFC, un canal de comunicación WiFi, un canal de comunicación Bluetooth, un canal de comunicación óptico y/o un canal de comunicación acústico.

Según modos de realización preferentes de la invención, el segundo perfil de suscripción se descarga de un servidor a través de la red de telefonía móvil al primer dispositivo móvil.

Preferentemente, el canal de comunicación lógico entre el servidor y el segundo dispositivo móvil está protegido criptográficamente.

Según modos de realización preferentes de la invención, el canal de comunicación lógico entre el servidor y el segundo dispositivo móvil está protegido criptográficamente de forma que el segundo perfil de suscripción es cifrado por el servidor con una clave que está almacenada en el servidor en combinación con un identificador del segundo dispositivo móvil y/o un elemento de seguridad del segundo dispositivo móvil.

Según un segundo aspecto de la invención, se proporciona un sistema para proporcionar un perfil de suscripción a un dispositivo móvil para la comunicación a través de una red de telefonía móvil. En este caso, el sistema comprende: un primer dispositivo móvil que está configurado para conectarse con un primer perfil de suscripción a una red de telefonía móvil; un servidor para descargar un segundo perfil de suscripción a través de la red de telefonía móvil al primer dispositivo móvil; y un segundo dispositivo móvil que está configurado para reenviar el segundo perfil de suscripción del primer dispositivo móvil a través de un canal de comunicación al segundo dispositivo móvil.

Como el experto reconoce, las realizaciones preferentes anteriormente descritas pueden implementarse ventajosamente, tanto en el marco del primer aspecto de la invención, es decir, en el marco del procedimiento para proporcionar un perfil de suscripción a un dispositivo móvil para la comunicación a través de una red de telefonía móvil, como también en el marco del segundo aspecto de la invención, es decir, en el marco de un sistema para proporcionar un perfil de suscripción a un dispositivo móvil para la comunicación a través de una red de telefonía móvil.

Otras características, ventajas y objetivos de la invención resultan de la descripción detallada subsiguiente de varios ejemplos de realización y alternativas de realización. Se hace referencia a las figuras, donde muestran:

La figura 1, una representación esquemática de un sistema de comunicación con un sistema de telefonía móvil en comunicación con un primer dispositivo móvil y un segundo dispositivo móvil, que ilustra diferentes aspectos de la presente invención, y

La figura 2, una representación esquemática de un proceso preferente al proporcionar un perfil de suscripción al segundo dispositivo móvil de la figura 1.

La figura 1 muestra una representación esquemática de los componentes de un sistema 10 de comunicación, así como algunas de las conexiones de comunicación entre estos componentes, que ilustra diferentes aspectos de la presente invención. Aunque en la descripción detallada subsiguiente se hace referencia a un dispositivo "móvil", el experto reconocerá que la presente invención puede implementarse ventajosamente en el contexto de cualquier tipo de dispositivo configurado para comunicar a través de una red de comunicación móvil o celular, es decir, también con dispositivos cuya ubicación prácticamente no cambia. En otras palabras: el atributo "móvil" aquí utilizado se refiere a la capacidad del dispositivo de comunicar a través de una red de comunicación móvil o celular.

En la figura 1 están representados a modo de ejemplo un primer dispositivo 20 móvil y un segundo dispositivo 30 móvil. Preferentemente, el primer dispositivo 20 móvil y el segundo dispositivo 30 móvil disponen respectivamente de un elemento 22 o 32 de seguridad ("Secure Element") para el almacenamiento y procesamiento seguro de datos que, por ejemplo, identifican inequívocamente al primer dispositivo 20 móvil y al segundo dispositivo 30 móvil en una red de telefonía móvil. Tal como se da a entender en la figura 1, el primer dispositivo 20 móvil es preferentemente un teléfono inteligente y el segundo dispositivo 30 móvil, una tableta. Sin embargo, el experto reconocerá que el primer dispositivo 20 móvil y el segundo dispositivo 30 móvil según la presente invención también pueden implementarse en forma de otros dispositivos configurados para comunicar a través de una red de telefonía móvil como, por ejemplo, un ordenador portátil, un sistema de TV, un decodificador de televisión, una máquina expendedora, un vehículo, una cámara de vigilancia, un dispositivo sensor y similares.

Según modos de realización preferentes de la invención, el elemento 22 de seguridad y el elemento 32 de seguridad están realizados como una eUICC (Tarjeta de Circuito Integrado Universal embebida) con una aplicación SIM implementada en la misma, es decir, como un elemento de seguridad que es un componente fijo del primer dispositivo 20 móvil o del segundo dispositivo 30 móvil y se utiliza en una red de telefonía móvil para la identificación inequívoca y segura del usuario o abonado y para proporcionar diferentes funciones y servicios de valor añadido. Alternativamente, el elemento 22 de seguridad y/o el elemento 32 de seguridad pueden realizarse como UICC (Tarjeta de Circuito Integrado Universal) o tarjeta SIM (Módulo de Identificación de Abonado) que el experto conoce como una de las formas de elemento de seguridad más habitualmente utilizadas en la actualidad. No obstante, el experto reconocerá que la presente invención también comprende otros tipos de elementos de seguridad que se denominan, en función de la generación y del tipo de estándar de telefonía móvil en que se basan, como USIM, R-

UIM, ISIM y similares.

Según otros modos de realización preferentes de la invención, el elemento 22 de seguridad y/o el elemento 32 de seguridad pueden realizarse como una combinación de componentes de hardware y software en una parte fiable de un sistema operativo de una unidad de procesador central del primer dispositivo 30 móvil o del segundo dispositivo 30 móvil, que el experto conoce también como entorno de tiempo de ejecución seguro ("Trusted Execution Environment"; TEE). El elemento 22 de seguridad y/o el elemento 32 de seguridad pueden realizarse entonces, por ejemplo, dentro de un entorno de tiempo de ejecución seguro de este tipo del primer dispositivo 20 móvil o del segundo dispositivo 30 móvil, en forma de programas que se ejecutan allí, denominados Trustlets®.

El primer dispositivo 20 móvil y el segundo dispositivo 30 móvil están realizados para comunicar a través de la interfaz aérea con una red 50 de telefonía móvil (denominada también como "Public Land Mobile Network" [PLMN]). Para ello, el primer dispositivo 20 móvil y el segundo dispositivo 30 móvil disponen generalmente de respectivamente una antena adecuadamente diseñada (no representada en la figura 1) para enviar y recibir ondas de radio.

A continuación se describen modos de realización preferentes de la invención en relación con una red 50 de telefonía móvil según el estándar GSM (Sistema Global para las comunicaciones Móviles) que está especificado en numerosas especificaciones ETSI. No obstante, el experto reconocerá que la presente invención también puede utilizarse ventajosamente en relación con otras redes de telefonía móvil. Dichas redes comprenden redes de telefonía móvil de la tercera generación (3GPP) como UMTS (Universal Mobile Telecommunications System), redes de telefonía móvil de la cuarta generación (4G) como LTE (Long Term Evolution), así como otras redes de telefonía móvil como CDMA y similares.

Tal como esto es conocido para el experto, una red de telefonía móvil o PLMN construida según el estándar GSM comprende generalmente un BSS ("Base Station Subsystem"), que está compuesto por una pluralidad de BTS ("Base Transceiver Station"), que definen las correspondientes células de telefonía móvil del PLMN y están conectadas con un BSC ("Base Station Controller"). Habitualmente, el BSC consiste en uno de una pluralidad de BSC, que se comunican con un MSC ("Mobile Switching Center") común. Una base de datos local que se denomina VLR ("Visitor Location Register") frecuentemente forma parte del MSC para facilitar información sobre los usuarios de telefonía móvil que se encuentran momentáneamente en las células de telefonía móvil alimentadas por un MSC (es decir, la zona cubierta por un MSC). El MSC proporciona esencialmente la misma funcionalidad que un conmutador telefónico en la red de telefonía fija (publicswitched telephone network; PSTN) y está en comunicación con un HLR ("Home Location Register"), que consiste en la base de datos primaria del PLMN, en la que está almacenada la información para el registro o la autentificación de los usuarios de telefonía móvil. Para ello, el HLR habitualmente tiene acceso a un AUC ("Authentication Center"). Tal como esto es conocido para el experto, las conexiones de comunicación entre los componentes descritos anteriormente de un PLMN pueden basarse en estándares privados y/o abiertos. Los protocolos utilizados pueden basarse, por ejemplo, en SS7 o IP. La forma en que están realizados los componentes de la red como unidades separadas o agrupadas y la forma en que están realizadas las interfaces entre estos componentes es competencia del MNO, por lo que la descripción anterior solo debe entenderse a modo de ejemplo.

El experto reconocerá que, aunque las unidades funcionales descritas anteriormente de una red de telefonía móvil convencional según el estándar GSM pueden presentar otros nombres en estándares de telefonía móvil diferentes o futuros, los principios que sirven de base son esencialmente los mismos y, por tanto, también están cubiertos por la invención. Para mayor claridad, de los componentes descritos anteriormente de una red de telefonía móvil, en la representación esquemática de la figura 1 solo se muestran los siguientes: un BTS 52 a modo de ejemplo, así como un HLR 54 para la red 50 de telefonía móvil.

Como se observa en la figura 1, la red 50 de telefonía móvil se encuentra por momentos en comunicación con un sistema 60 de fondo, preferentemente en forma de un servidor "Subscription Management" (Servidor SM) adecuadamente configurado, tal como se describe a continuación en detalle.

Tal como se observa en las vistas respectivamente aumentadas de los elementos 22 y 32 de seguridad en la figura 1, estos preferentemente comprenden respectivamente una unidad de procesamiento central o un procesador 25 o 35 central ("central processing unit"; CPU). Preferentemente, el procesador 25 o 35 está realizado de forma que en el procesador 25 o 35 pueden ejecutarse aplicaciones que preferentemente proporcionan al menos algunas de las características para proporcionar un perfil de suscripción al segundo dispositivo 30 móvil, tal como se describe a continuación detalladamente en relación con la figura 2. Este tipo de aplicaciones están implementadas preferentemente en forma de Java Applets.

Adicionalmente, preferentemente el elemento 22 de seguridad y el elemento 32 de seguridad comprenden respectivamente una unidad 26 o 36 de almacenamiento que está implementada preferentemente como una unidad de almacenamiento no volátil, de lectura y escritura, por ejemplo, en forma de una memoria Flash. En este sentido, la unidad 26 o 36 de almacenamiento está configurada para contener al menos un perfil de suscripción, por ejemplo, los perfiles SP1 o SP2 de suscripción, tal como se muestra de forma esquemática en la figura 1.

En la representación esquemática de la figura 1, el perfil SP1 de suscripción ya está introducido en la unidad 26 de almacenamiento del elemento 22 de seguridad del primer dispositivo 20 móvil, lo que significa que, en particular y a modo de ejemplo, la CPU 25 del elemento 22 de seguridad puede acceder al perfil SP1 de suscripción. El perfil SP1 de suscripción contiene preferentemente datos que permiten al elemento 22 de seguridad y al primer dispositivo 20 móvil conectarse a la red 50 de telefonía móvil y comunicar a través de esta, es decir, datos como datos de autorización de suscripción ("Subscription Credentials"), un algoritmo de autentificación específico de MNO y/o similares.

En la representación esquemática de la figura 1, la unidad 36 de almacenamiento del elemento 32 de seguridad del segundo dispositivo 30 móvil está listo para contener el perfil SP2 de seguridad, lo que se describe a continuación en detalle, también haciendo referencia a la figura 2. El perfil SP2 de suscripción contiene preferentemente datos que permiten al elemento 32 de seguridad y al segundo dispositivo 30 móvil conectarse a la red 50 de telefonía móvil y comunicar a través de esta, es decir, datos como datos de autorización de suscripción ("Subscription Credentials"), un algoritmo de autentificación específico de MNO y/o similares. Alternativamente, el perfil SP2 de suscripción puede contener datos que permiten al elemento 32 de seguridad y al segundo dispositivo 30 móvil conectarse a otra red diferente a la red 50 de telefonía móvil, por ejemplo, a la red de telefonía móvil de otro operador de red.

La figura 2 muestra un proceso preferente según la invención para proporcionar el perfil SP2 de suscripción al segundo dispositivo 30 móvil.

En el paso S1 de la figura 2, el primer dispositivo 20 móvil se conecta con el perfil SP1 de suscripción existente a la red 50 de telefonía móvil. Esto tiene lugar en el marco del proceso de autentificación utilizando los datos de autorización de suscripción que forman parte del perfil SP1 de suscripción como, por ejemplo, una IMSI y/o una clave K_i de autentificación.

Una vez que el primer dispositivo 20 móvil se ha conectado exitosamente con la red 50 de telefonía móvil y puede comunicar a través de la misma, el primer dispositivo 20 móvil solicita al servidor 60 SM un perfil SP2 de suscripción para el segundo dispositivo 30 móvil a través de la red 50 de telefonía móvil en el paso S2 de la figura 2. Según la invención es posible que, mediante una aplicación ejecutada en el primer dispositivo 20 móvil con una interfaz de usuario gráfica, un usuario pueda desencadenar este proceso y, en particular, seleccionar el perfil S2 de suscripción para el segundo dispositivo 30 móvil.

En respuesta a esta solicitud, en el paso S3 de la figura 2, el servidor 60 SM carga el perfil SP2 de suscripción seleccionado por el usuario para el segundo dispositivo 30 móvil a través de la red 50 de telefonía móvil en el primer dispositivo 20 móvil. En este caso, el servidor 60 SM puede confiar en el primer dispositivo 20 móvil, ya que este se ha autentificado en relación a la red 50 de telefonía móvil.

En el paso S4 de la figura 2 se crea un canal 40 de comunicación entre el primer dispositivo 20 móvil y el segundo dispositivo 30 móvil. Puesto que generalmente tanto el primer dispositivo 20 móvil como también el segundo dispositivo 30 móvil están a disposición del usuario y este puede acercar ambos dispositivos 20, 30 entre sí, el canal 40 de comunicación puede ser un canal de comunicación de corto alcance. Preferentemente, este canal 40 de comunicación es un canal NFC, un canal Bluetooth, un canal WiFi o similar. Alternativamente, también sería posible un canal 40 de comunicación en forma de una transferencia de datos óptica o acústica entre el primer dispositivo 20 móvil y el segundo dispositivo 30 móvil. Por ejemplo, los datos pueden representarse en una pantalla del primer dispositivo 20 móvil, por ejemplo, en forma de un código QR que puede ser registrado mediante una cámara del segundo dispositivo 30 móvil.

Después de que en el paso S4 de la figura 2 se ha creado el canal 40 de comunicación entre el primer dispositivo 20 móvil y el segundo dispositivo 30 móvil, en el paso S5 de la figura 2 se transfiere el perfil SP2 de suscripción del primer dispositivo 20 móvil a través del canal 40 de comunicación al segundo dispositivo 30 móvil.

A continuación, en el paso S6 de la figura 2, el segundo dispositivo móvil o su elemento 32 de seguridad, con el perfil SP2 de suscripción y los datos de autorización de suscripción contenidos en el mismo como, por ejemplo, una IMSI y/o una clave K_i de autentificación, puede conectarse con la red 50 de telefonía móvil. Tal como se ha mencionado anteriormente, la invención también comprende el caso en que los datos de autorización de suscripción del perfil SP2 de suscripción permiten el acceso a otra red de telefonía móvil, por ejemplo, la red de telefonía móvil de otro operador de red.

Si el primer dispositivo 30 móvil se ha conectado exitosamente con la red 50 de telefonía móvil en el paso S6, en el paso S7 de la figura 2, el segundo dispositivo 30 móvil puede enviar al servidor 60 SM una confirmación correspondiente a través de la red 50 de telefonía móvil.

Como reconocerá el experto, para lograr las ventajas proporcionadas por la presente invención no es necesario que los pasos de la figura 2 tengan lugar en el orden allí representado. Por ejemplo, en el marco de la invención sería posible que el paso S4 para crear el canal 40 de comunicación entre el primer dispositivo 20 móvil y el segundo

dispositivo 30 móvil ya tenga lugar antes de descargar el perfil SP2 de suscripción al primer dispositivo 20 móvil.

Los pasos S3 a S5 de la figura 2 para descargar el perfil de suscripción del servidor 60 SM a través de la red 50 de telefonía móvil al primer dispositivo 20 móvil y del primer dispositivo 20 móvil a través del canal 40 de comunicación al segundo dispositivo 30 móvil, pueden considerarse como un canal de comunicación lógico entre el servidor 60 SM y el segundo dispositivo 30 móvil, en el que el primer dispositivo 20 móvil únicamente sirve para reenviar los datos. Preferentemente, el canal de comunicación lógico entre el servidor 60 SM y el segundo dispositivo 30 móvil está protegido criptográficamente.

La protección criptográfica del canal de comunicación lógico entre el servidor 60 SM y el segundo dispositivo 30 móvil puede lograrse, por ejemplo, almacenando preferentemente en el elemento 32 de seguridad del segundo dispositivo 30 móvil una clave secreta que también está almacenada en el servidor 60 SM en combinación con un identificador del segundo dispositivo 30 móvil o del elemento 32 de seguridad, por ejemplo, un ID de chip. En este caso, el segundo dispositivo 30 móvil se identificaría en un paso adicional, no representado en la figura 2, respecto al servidor 60 SM y el servidor 60 SM cifraría el perfil SP2 de suscripción con la clave asignada a este identificador. Como reconocerá el experto, en este caso, el canal 40 de comunicación entre el primer dispositivo 20 móvil y el segundo dispositivo 30 móvil puede crearse en un momento previo para comunicar al primer dispositivo 20 móvil el identificador, por ejemplo, un ID de chip del elemento 32 de seguridad del segundo dispositivo 30 móvil. En este sentido sería posible que el primer dispositivo 20 móvil solicite el identificador del segundo dispositivo 30 móvil o del elemento 32 de seguridad en el marco de la consulta del segundo perfil SP2 de suscripción a través de la red 50 de telefonía móvil al servidor 60 SM (véase paso S2 de la figura 2).

REIVINDICACIONES

1. Procedimiento para proporcionar un perfil (SP2) de suscripción a un dispositivo (30) móvil para la comunicación a través de una red de telefonía móvil, tal que el procedimiento comprende los siguientes pasos:
la conexión de un primer dispositivo (20) móvil con un primer perfil (SP1) de suscripción a una red (50) de telefonía móvil, tal que el primer perfil (SP1) de suscripción contiene datos de autorización de suscripción para la identificación y autentificación inequívocas del primer dispositivo (20) móvil respecto a la red (50) de telefonía móvil; la descarga de un segundo perfil (SP2) de suscripción a través de la red (50) de telefonía móvil al primer dispositivo (20) móvil tras la conexión exitosa a la red (50) de telefonía móvil, tal que el segundo perfil (SP2) de suscripción contiene datos de autorización de suscripción para la identificación y autentificación inequívocas del segundo dispositivo (30) móvil respecto a la red (50) de telefonía móvil o a otra red de telefonía móvil; y
el reenvío del segundo perfil (SP2) de suscripción del primer dispositivo (20) móvil al segundo dispositivo (30) móvil a través de un canal (40) de comunicación.

2. Procedimiento, según la reivindicación 1, tal que el procedimiento, tras el paso del reenvío del segundo perfil (SP2) de suscripción del primer dispositivo (20) móvil al segundo dispositivo (30) móvil a través del canal (40) de comunicación, comprende el paso adicional de la conexión del segundo dispositivo (30) móvil con el segundo perfil (SP2) de suscripción a la red (50) de telefonía móvil o a otra red de telefonía móvil.

3. Procedimiento, según la reivindicación 2, tal que la red de telefonía móvil a la que se conecta el segundo dispositivo (30) móvil con el segundo perfil (SP2) de suscripción es la red (50) de telefonía móvil a través de la cual se descargó el segundo perfil (SP2) de suscripción al primer dispositivo (20) móvil.

4. Procedimiento, según cualquiera de las reivindicaciones anteriores, en el que el canal (40) de comunicación entre el primer dispositivo (20) móvil y el segundo dispositivo (30) móvil es un canal de comunicación NFC, un canal de comunicación WiFi, un canal de comunicación Bluetooth, un canal de comunicación óptico y/o un canal de comunicación acústico.

5. Procedimiento, según cualquiera de las reivindicaciones anteriores, en el que el segundo perfil (SP2) de suscripción se descarga de un servidor (60) a través de la red (50) de telefonía móvil al primer dispositivo (20) móvil.

6. Procedimiento, según la reivindicación 5, en el que el canal de comunicación entre el servidor (60) y el segundo dispositivo (30) móvil está protegido criptográficamente.

7. Procedimiento, según la reivindicación 6, en el que el canal de comunicación entre el servidor (60) y el segundo dispositivo (30) móvil está protegido criptográficamente de forma que el segundo perfil (SP2) de suscripción es cifrado por el servidor (60) con una clave que está almacenada en el servidor (60) en combinación con un identificador del segundo dispositivo (30) móvil y/o un elemento (32) de seguridad del segundo dispositivo (30) móvil.

8. Elemento (22) de seguridad configurado para realizar un procedimiento, según la reivindicación 1, de forma que el segundo perfil (SP2) de suscripción es proporcionado al elemento (22) de seguridad, tal que los pasos de conexión y de descarga se realizan con la ayuda del elemento (22) de seguridad del primer dispositivo móvil.

9. Dispositivo (20) móvil con un elemento (22) de seguridad, según la reivindicación 8.

10. Sistema para proporcionar un perfil (SP2) de suscripción a un dispositivo (30) móvil para la comunicación a través de una red de telefonía móvil, tal que el sistema comprende:

un primer dispositivo (20) móvil que está realizado para conectarse a una red (50) de telefonía móvil con un primer perfil (SP1) de suscripción, tal que el primer perfil (SP1) de suscripción contiene datos de autorización de suscripción para la identificación y autentificación inequívocas del primer dispositivo (20) móvil respecto a la red (50) de telefonía móvil; un servidor (60) para descargar un segundo perfil (SP2) de suscripción a través de la red (50) de telefonía móvil al primer dispositivo (20) móvil tras la conexión exitosa a la red (50) de telefonía móvil, tal que el segundo perfil (SP2) de suscripción contiene datos de autorización de suscripción para la identificación y autentificación inequívocas del segundo dispositivo (30) móvil respecto a la red (50) de telefonía móvil o a otra red de telefonía móvil; y
el segundo dispositivo (30) móvil, que está configurado tal que el segundo perfil (SP2) de suscripción es reenviado del primer dispositivo (20) móvil al segundo dispositivo (30) móvil a través de un canal (40) de comunicación y para conectarse con el segundo perfil de suscripción a la red de telefonía móvil.

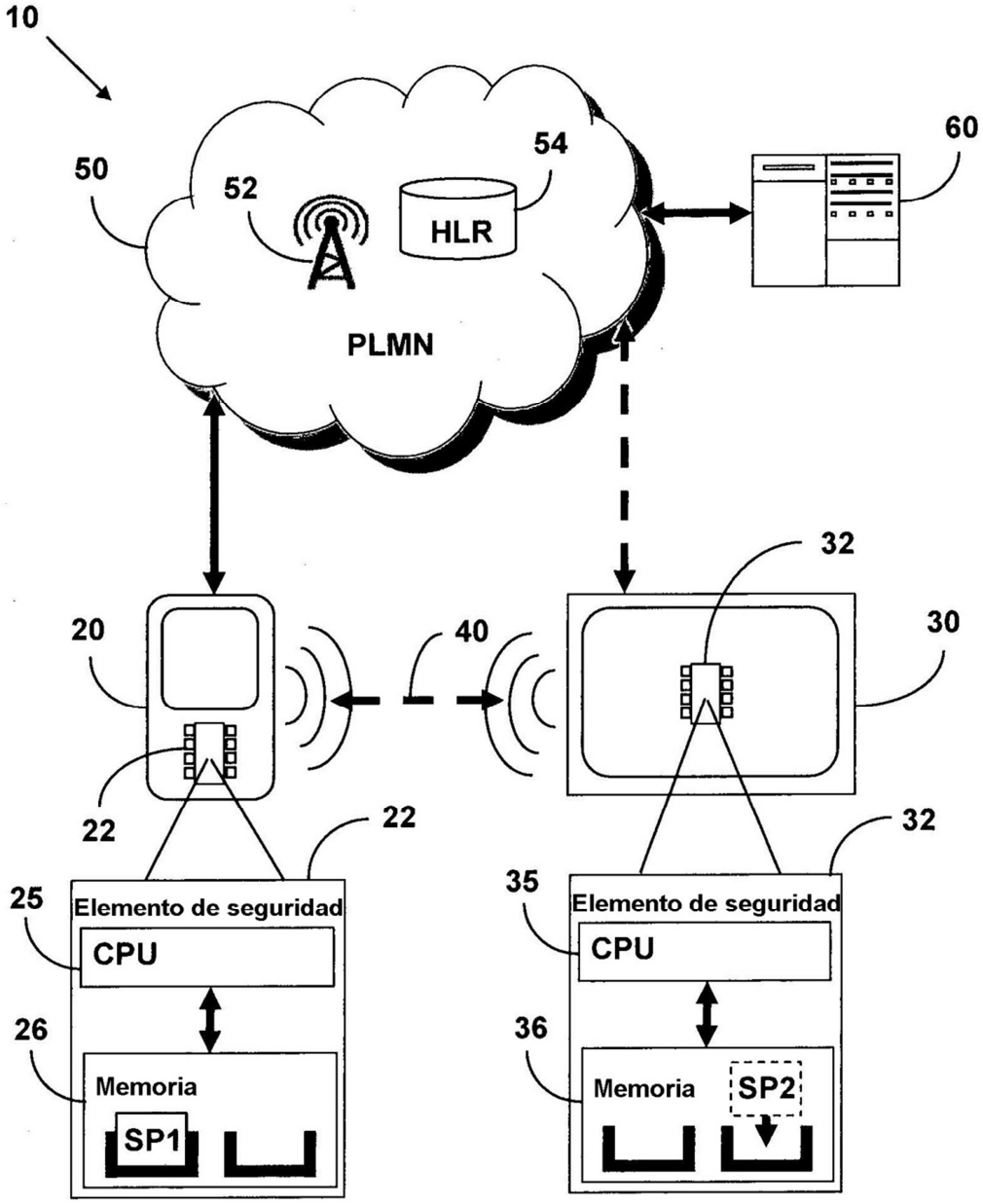
10
50
52
54
HLR
PLMN
60
20
40
32
30
22
22
32
25
Elemento de seguridad
CPU
26
Memoria
SP1
35
Elemento de seguridad
CPU
36
Memoria
SP2

Fig. 1

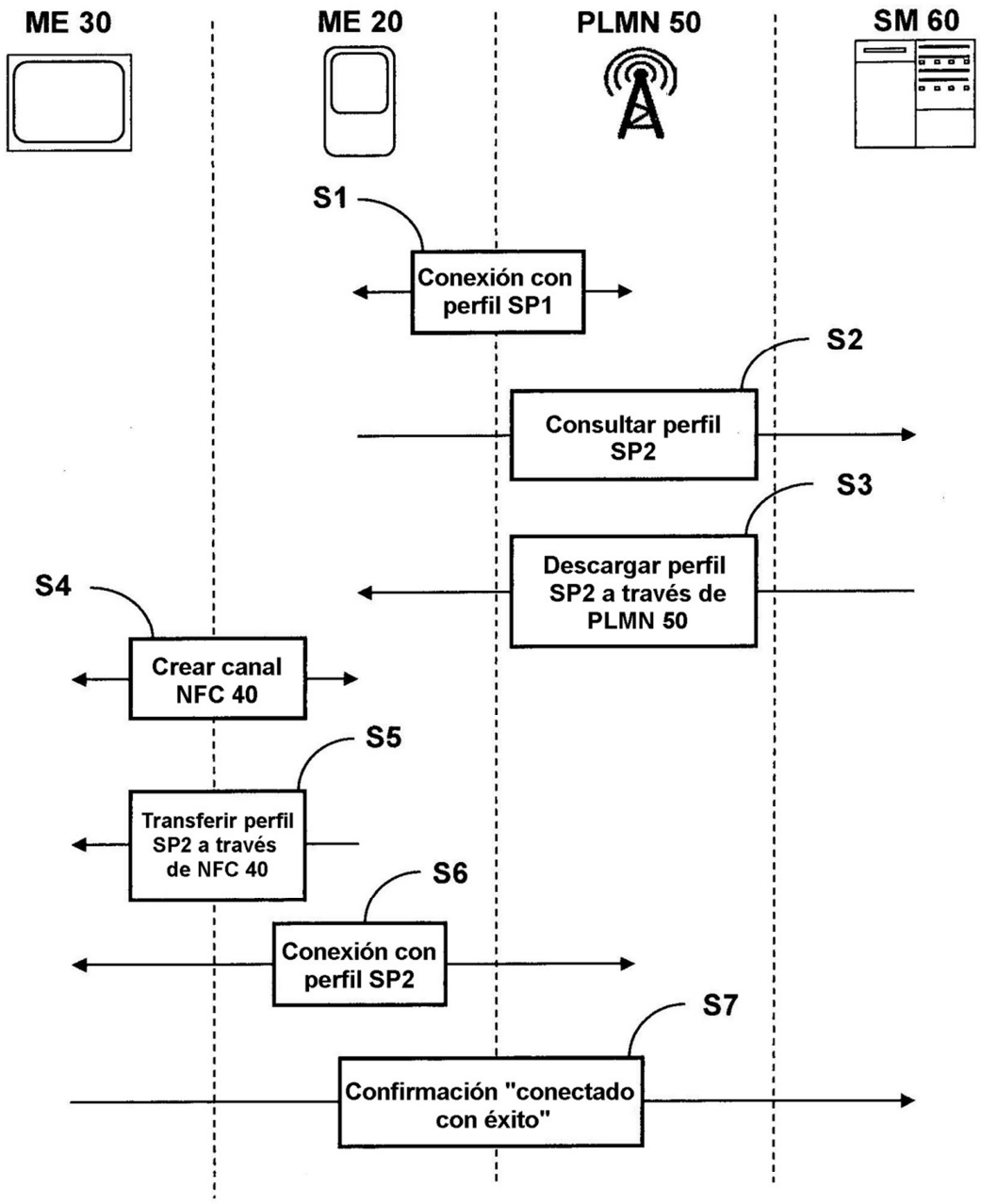
ME 30
ME 20
PLMN 50
SM 60
S1
Conexión con perfil SP1
S2
Consultar perfil SP2
S3
Descargar perfil SP2 a través de PLMN 50
S4
Crear canal NFC 40
S5
Transferir perfil SP2 a través de NFC 40
S6
Conexión con perfil SP2
S7
Confirmación "conectado con éxito"

Fig. 2