(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 524 242**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **04.08.2011 E 11749378 (3)**

(97) Fecha y número de publicación de la concesión europea: **18.06.2014 EP 2601771**

(54) Título: **Sistema y procedimiento para utilizar con total seguridad múltiples perfiles de abonados con un componente de seguridad y un dispositivo de telecomunicación móvil**

(30) Prioridad:

05.08.2010 US 371149 P
05.08.2010 US 371152 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
04.12.2014

(73) Titular/es:

GEMALTO SA (100.0%)
6, rue de la Verrerie
92190 Meudon, FR

(72) Inventor/es:

MERRIEN, LIONEL y
BARBE, SERGE

(74) Agente/Representante:

ISERN CUYAS, María Luisa

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

DESCRIPCIÓN

Sistema y procedimiento para utilizar con total seguridad perfiles de abonados múltiples con un componente de seguridad y un dispositivo de t5elecomunicación móvil.

La presente invención se refiere en general a las telecomunicaciones y más particularmente a la capacidad de proporcionar una aplicación multi-suscripción gestionado por un componente de seguridad tal como una (tarjeta universal de circuito integrado) UICC directamente.

El problema abordado por la presente invención es cómo cambiar de forma segura entre diferentes perfiles y la tecnología de acceso a la red desde un dispositivo móvil, sin límite para el número de perfiles que están soportados.

Un escenario en el que es útil tener varias suscripciones es cuando uno está viajando entre áreas geográficas que cubren diferentes operadores. Esto se conoce generalmente como la itinerancia. En itinerancia en una red visitada, un usuario paga los gastos de itinerancia que por lo general son mucho más caros que los cobrados por cualquiera de la red doméstica o de los operadores de redes visitadas. Para evitar ese problema, los usuarios que con frecuencia se dedican a ese tipo de viajes puede intentar la solución de llevar múltiples dispositivos móviles, por ejemplo, "mi teléfono celular canadiense", "mi teléfono celular francés" o "mi teléfono móvil sueco," utilizando cada teléfono celular con un operador en el país correspondiente. Por supuesto, esta amalgama de varias unidades es muy oneroso en el usuario.

Otra solución es cambiar la UICC. Sin embargo, hay al menos dos problemas con esa solución particular. En primer lugar, el usuario tendría que acordarse de llevar múltiples UICC y saber cuál usar en cada lugar. En segundo lugar, hay una tendencia creciente hacia la UICC incrustada. En un dispositivo móvil con una UICC incrustada no es posible, al menos no a nivel de usuario, acceder fácilmente la UICC y reemplazarla.

Una solución alternativa existente para el problema descrito anteriormente se conoce como la aplicación multi-EVISI, en el que una aplicación dentro de la UICC puede cambiar entre diferentes credenciales, basado en algunas de gatillo externo. Esta solución alternativa tiene dos limitaciones:

- El número de diferentes credenciales para ser apoyada está limitado por la memoria de la UICC.
- Es difícil cambiar los perfiles enteros, principalmente debido a la limitación de la memoria en la UICC. Por lo tanto la aplicación multi-IMSI sólo cambia las credenciales (claves y códigos) y algunos datos seleccionados (por ejemplo, los archivos de itinerancia). El resto del perfil debe ser compartido.

En aplicaciones multi-IMSI, sólo algunos valores de los parámetros de un perfil se conmutan con otros valores, por ejemplo, EVISI y número de teléfono. Sin embargo, no hay un interruptor de un perfil entero.

Una de las limitaciones, por lo tanto, de la solución multi-IMSI es que, debido a que los perfiles enteros no se cambian, los dos operadores deben tener el mismo formato de perfil con el fin de permitir un cambio de perfiles cuando se cambia de un operador a otro. Que a menudo no es el caso, y por lo tanto la solución a menudo no es una solución completa y fiable que permita cambiar de perfiles, por ejemplo en itinerancia.

Hay una necesidad de un método mejorado para proporcionar la capacidad de suministrar aplicaciones multi-IMSI gestionadas directamente por una UICC o dispositivo similar.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La Figura 1 es un diagrama de bloques que ilustra el uso de un dispositivo de telefonía móvil en una ubicación de inicio y en itinerancia en una red móvil visitada.

La Figura 2 es un diagrama de bloques que ilustra una vista de alto nivel de un ejemplo de un dispositivo móvil de la Figura 1 incluyendo una UICC incrustada en el dispositivo móvil.

La Figura 3 es un diagrama de bloques que ilustra un ejemplo de una organización arquitectónica de alto nivel de los componentes de hardware del dispositivo móvil y de la UICC de la Figura 2.

La Figura 4 es un diagrama de bloques que ilustra los programas y datos almacenados en la memoria no volátil de una UICC de las Figuras 2 y 3, incluyendo el almacenamiento de un perfil de abonado.

La Figura 5 es un diagrama de bloques que ilustra un ejemplo de un perfil de abonado monedero para almacenar múltiples perfiles de abonado que pueden ser activados para convertirse en el perfil de abonado actualmente activo.

La Figura 6 es un diagrama esquemático que ilustra varios ejemplos de lugares de almacenamiento para el perfil de abonado monedero de la figura 5.

La Figura 7 es un diagrama de bloques que ilustra los programas y datos almacenados en la memoria no volátil de un UICC de la Figura 4 que incluye el almacenamiento de un perfil de abonado monedero.

La Figura 8 es un diagrama de secuencia de temporización que ilustra un escenario posible para el almacenamiento de perfiles de abonado en el perfil de abonado monedero de las Figuras 5, 6 y 7.

La Figura 9 es un diagrama de temporización que ilustra la secuencia de activación de un perfil de abonado almacenado en el perfil de abonado monedero de las Figuras 5, 6 y 7.

La Figura 10 es un diagrama de flujo que ilustra el uso de la ubicación para desencadenar la activación de un perfil de un abonado a partir del perfil de abonado monedero.

DESCRIPCIÓN DETALLADA DE LA INVENCIÓN

En la siguiente descripción detallada, se hace referencia a los dibujos adjuntos que muestran, a modo de ilustración, realizaciones específicas en las que pueden ponerse en práctica la invención. Estas realizaciones se describen con suficiente detalle para permitir a los expertos en la técnica practicar la invención. Es de entender que las diversas realizaciones de la invención, aunque son diferentes, no son necesariamente excluyentes de manera mutua. Por ejemplo, una característica particular, estructura o característica descrita en este documento en relación con una forma de realización puede ser implementada dentro de otras realizaciones sin apartarse del espíritu y alcance de la invención. Además, es de entender que la ubicación o la disposición de los elementos individuales dentro de cada realización descrita pueden ser modificados sin apartarse del espíritu y alcance de la invención. La siguiente descripción detallada, por lo tanto, no debe tomarse en un sentido limitativo, y el alcance de la presente invención se define sólo por las reivindicaciones adjuntas, interpretadas apropiadamente, junto con el rango completo de equivalentes a los que las reivindicaciones tienen derecho. En los dibujos, los números similares se refieren a la misma o similar funcionalidad en las diversas vistas.

La tecnología presentada en este documento proporciona una solución de gran alcance, de bajo costo, escalable, flexible y universal para permitir que un usuario de un dispositivo móvil seleccione entre diferentes perfiles de abonado. Un escenario en el que esto es útil es la itinerancia. Otra es la de permitir a un operador activar un perfil de administrador o pruebas en un dispositivo móvil para permitir que el operador use un perfil en lugar del perfil propio del suscriptor al hacer tareas administrativas o de prueba de un dispositivo móvil.

La Figura 1 es un diagrama de bloques que ilustra el uso de un dispositivo de telefonía móvil en una ubicación de inicio y en itinerancia en una red móvil visitada. En la parte superior de la figura 1 un usuario 101 está usando un dispositivo móvil 103 conectado a un "Home" teléfono móvil de la red A 105a. La red doméstica puede estar conectada a otras redes a través de, por ejemplo, la red telefónica conmutada públicamente PSTN 107. Una de tales red puede ser una red de teléfono móvil de otro operador B 105b. Mientras está conectado a la red doméstica 105a el suscriptor paga por tiempo “en el aire” y otros servicios por un contrato directamente con el operador de red local A.

En la parte inferior de la Figura 1, el usuario 101' opera el mismo dispositivo móvil 103' que está conectado a una red de telefonía móvil "Visitada" B 105b. Eso suele ocurrir cuando un usuario entra en una zona geográfica no servida por el operador "Inicio". Con el fin de realizar o recibir llamadas telefónicas (u otros datos de comunicación) el abonado paga por tiempo “en el aire” y otros servicios de acuerdo con un contrato de itinerancia con la red Visitada del operador B. Normalmente dichos cargos son mucho más caros que lo que cobra el este último operador a sus propios clientes.

Por lo tanto, sería útil para el usuario 101 si él o ella pudieran entrar en una relación de abonado con múltiples operadores y disponer de un mecanismo para activar el perfil adecuado para suscribirse en cualquier ubicación que el usuario o usuaria se encuentre.

Volviendo ahora a algunos aspectos fundamentales de la tecnología de comunicaciones de telefonía móvil correspondiente a la tecnología actual: la Figura 2 es un diagrama de bloques que ilustra una vista de alto nivel de un ejemplo del dispositivo móvil 103 de la Figura 1 incluyendo una UICC 201 incrustada en el dispositivo móvil 103. Mientras que un lector reconocerá que el dispositivo móvil 103 representado es un teléfono móvil, también denominado con frecuencia teléfono celular, la presente tecnología es aplicable a cualquier dispositivo de comunicaciones móvil, incluyendo pero no limitado a los ordenadores, módems de datos, cámaras, terminales de punto de venta dispositivos, vehículos con comunicación de a bordo, o dispositivos de localización incorporados o acarreados por animales, equipos y los seres humanos.

Tanto la UICC 201 como el dispositivo móvil 103 son ordenadores. Típicamente están conectados el uno al otro en una relación maestro-esclavo en la que el dispositivo móvil 103 es el maestro y la UICC 201 es el esclavo. La UICC 201 ofrece ciertas funciones, tales como el almacenamiento de perfiles de abonado y la realización de operaciones de seguridad de alta prioridad. Las UICC suelen ser resistentes a la falsificación y son por lo tanto dispositivos muy

seguros para el almacenamiento de información sensible, como el perfil de abonado y la información de cuenta, y para proporcionar funciones de seguridad, tales como las operaciones criptográficas.

La Figura 3 es un diagrama de bloques que ilustra un ejemplo de una organización arquitectónica de alto nivel de los componentes de hardware del dispositivo móvil 103 y de la UICC 201 de la Figura 2. Típicamente, la UICC 201 está conectada al dispositivo móvil 103 mediante los conectores 301 en la UICC 201 y los conectores en una ranura de tarjeta (no mostrada) en el dispositivo móvil 103. El dispositivo móvil 103 puede tener una interfaz de comunicaciones 303 para facilitar la comunicación entre los dos dispositivos. En el presente ejemplo, en el extremo de la UICC 201, la comunicación se gestiona directamente por una CPU (Unidad Central de Procesamiento) 305.

La tarjeta CPU 305 está conectada además a un RAM (Random Access Memory) 307 y a una NVM (Memoria No-Volátil) 309. Típicamente, la NVM 309 se utiliza para almacenar información en la UICC 201, esto es persistir a través del ciclo de alimentación de la UICC 201, por ejemplo perfiles de abonado y programas de aplicación de la UICC 201.

El dispositivo móvil 103 también contiene una CPU 311, una RAM 313, y una NVM 315. El dispositivo móvil NVM 313 se puede utilizar para almacenar programas de aplicación del dispositivo móvil 103.

La Figura 4 es un diagrama de bloques que ilustra los programas y datos almacenados en la memoria no volátil 309 de la UICC 201 de las Figuras 2 y 3, que incluye el almacenamiento de un perfil de abonado. Como se ha señalado, la NVM 309 (en el presente documento, "NVM' sin un modificador debería ser utilizada para referirse a la UICC NVM 309 a menos que el contexto indique otra cosa) se utiliza para almacenar datos y programas persistentes. Esto incluye un módulo de criptografía 401 para realizar operaciones criptográficas, por ejemplo, el cifrado de un elemento de datos, descifrado de un elemento de datos cifrado, y la firma criptográfica de un elemento de datos. Estas operaciones criptográficas pueden incluir la criptografía de clave pública o criptografía de clave secreta. En cualquier caso, la UICC 201 habría almacenado en la misma, por ejemplo, en la NVM 309, un (Tarjeta Llave) 403 que sólo es conocida por la UICC 201. (Considerando que es común en la literatura informática usar la terminología antropomórfica tal como "conocido" por un dispositivo, cuando tal uso se emplea en el presente documento debe ser apreciado que este es un uso figurado del término y debe ser tomado en el sentido de que una operación correspondiente se realiza por el dispositivo. Por ejemplo, en este caso "conocido sólo" significa que el elemento de datos en cuestión se almacena sólo en ese dispositivo y no en otros dispositivos o no puede ser recuperado por otros dispositivos) Por lo tanto, la tarjeta llave 403 puede ser utilizada por la UICC 201 para cifrar elementos de datos de tal manera que sólo la UICC 201 puede descifrarlos o puede utilizarse la tarjeta llave 403 por parte de la UICC 201 para firmar criptográficamente un elemento de datos de modo que la UICC 201 (u otros dispositivos) pueden confirmar que la UICC 201 de hecho es el firmante del elemento de datos firmado.

La NVM 309 también contiene perfiles de uno o más de abonado 405 que incluye un perfil de abonado activo 405a (ilustrado aquí con un borde de línea doble). En la mayoría de los casos, la NVM 309 sólo incluiría un perfil de abonado 405, a saber, el perfil de abonado activo 405a. Un perfil de abonado 405 puede incluir un IMSI, un número de teléfono, una clave de autenticación para la autenticación de un abonado a una red particular, las aplicaciones asociadas con el abonado y una red particular, y cualquier otra información que es específica para un abonado y una red particular con la que el perfil de abonado está asociado.

La tarjeta de NVM 309 también puede contener un programa especial 407 utilizado para cambiar perfiles de abonado como se describe aquí a continuación.

La tarjeta de NVM 309 puede contener también una máquina virtual 409 u otro software de sistema operativo para el control de las operaciones de la UICC 201 y otros datos y programas 411.

En una realización de la tecnología presentada en el presente documento, pueden estar asociados múltiples perfiles de abonado 405 con un usuario particular. Un usuario o administrador puede seleccionar un perfil particular de este conjunto de perfiles de abonado 405 asociados con un usuario. La Figura 5 es un diagrama de bloques que ilustra un ejemplo de un mecanismo de almacenamiento para tales perfiles múltiples de abonado, es decir, una perfil de abonado monedero 501 para almacenar múltiples perfiles de abonado 405 asociados con un usuario que puede activarse para convertirse en el perfil de abonado actualmente activo en un usuario de dispositivo móvil 103. En el ejemplo de la figura 5, un abonado particular tiene n perfiles A - N almacenados en un perfil de abonado monedero 501.

La Figura 6 es un diagrama esquemático que ilustra varios ejemplos de lugares de almacenamiento para el perfil de abonado monedero de la figura 5. El perfil de abonado monedero 501 se puede almacenar, por ejemplo, en un ordenador principal 601. Un ejemplo en el que un ordenador principal 601 es una ubicación de almacenamiento útil es el iPhone de Apple Inc., en Cupertino, California, EE.UU.. El iPhone es un dispositivo móvil que se sincroniza normalmente (sincronizado) con un ordenador con el programa iTunes en un Mac o PC. A través de iTunes el contenido en el iPhone se sincroniza con el ordenador principal 601. De esta manera, el ordenador principal 601 puede contener un programa de sincronización 603 para sincronizar contenido con el dispositivo móvil 103. Un plug-

in o de extensión (no mostrado) para que el programa de sincronización puede activar nuevos perfiles de abonado desde el perfil de abonado monedero 501 A.

En otra alternativa, el perfil de abonado monedero B 501 B se almacena en la nube 605. Una aplicación de activación web 607, por ejemplo, invocada a través de un navegador web en el dispositivo móvil 103, puede ser usada para activar un perfil de abonado de perfil de abonado monedero B 501B en la nube 605.

En otra alternativa, el perfil de abonado monedero C 501 C se almacena en la NVM 309 de la tarjeta UICC 201 que se ilustra en la Figura 7. Alternativamente, para un dispositivo móvil multi-UICC, el perfil de abonado monedero puede almacenarse en uno de los UICC en el dispositivo móvil multi-UICC y el perfil de suscriptor activo se puede recuperar del mismo.

La Figura 8 es un diagrama de secuencia de temporización que ilustra un escenario posible para el almacenamiento de perfiles de abonado en el perfil de abonado monedero de las Figuras 5, 6 y 7. En el ejemplo de la Figura 8, el emisor 800 A crea uno o más perfiles de abonado 501, paso 801. Los perfiles se transmiten a la UICC 201, paso 803. La UICC 201 cifra o firma criptográficamente el perfil utilizando la tarjeta llave 403, paso 805, por ejemplo, utilizando el módulo de criptografía 401. La UICC 201 transmite el perfil de abonado cifrado o firmado al perfil de abonado monedero 501, paso 809. El perfil de abonado cifrado o firmado se almacena en el perfil de abonado monedero 501, paso 811.

El proceso anterior se puede repetir para crear perfiles de abonado cifrados o firmados adicionales por parte del emisor, paso 813.

Los pasos anteriores se llevan a cabo de manera ventajosa durante la personalización de tarjetas. Perfiles adicionales pueden además crearse y transferirse a la UICC "por el aire".

En algún momento en el futuro, por ejemplo, un segundo operador B 815 puede crear un perfil de abonado para el usuario, paso 817. Este perfil de abonado asocia el usuario con el operador B 815. El perfil de abonado se transmite a la UICC 201, paso 819. La UICC 201 encripta el perfil de abonado creado por el operador B 815, paso 821, y transmite el perfil de abonado cifrado o firmado al perfil de abonado monedero 501, paso 823. El perfil de abonado cifrado o firmado se almacena en el perfil de abonado monedero 501, paso 825.

La Figura 9 es un diagrama de temporización que ilustra la secuencia de activación de un perfil de abonado almacenado en el perfil de abonado monedero de las Figuras 5, 6 y 7. Un dispositivo móvil, un dispositivo de la computadora huésped o una aplicación web (en conjunto) 901 se acciona para activar un perfil de abonado inactivo almacenado en el perfil de abonado monedero 501, paso 903. Un programa que se ejecuta en el dispositivo móvil 103 puede actuar como una aplicación activadora de perfil. Este programa puede recuperar un perfil de abonado monedero de un perfil de abonado almacenado en el dispositivo móvil, o desde algún otro lugar, por ejemplo, la UICC si se almacena un perfil de abonado monedero o la nube a través de una aplicación web.

El programa -donde se está ejecutando- envía un mensaje de perfil-activo-de recuperación al perfil de abonado monedero 501, paso 905. El perfil de abonado monedero transmite el perfil de abonado activado a la UICC 201, paso 907. En este punto el perfil de abonado está cifrado o firmado criptográficamente. Sólo un perfil de abonado que ha sido cifrado o criptográficamente firmado por la UICC 201 que originalmente cifró o firmó digitalmente el perfil de abonado es aceptado por esa misma UICC 201. En otras palabras, la firma digital o el cifrado mapas de un perfil de abonado particular a una UICC 201 y que la UICC 201 sólo acepta los perfiles de abonado que ella ha firmado o cifrado.

El perfil de abonado monedero 501 transmite el perfil de abonado que está siendo activado para la UICC 201, paso 907. Si bien esto se representa aquí como una transmisión directa desde el perfil de abonado monedero 501 a la UICC 201, la transmisión puede ser a través de uno o más intermediarios, por ejemplo, el dispositivo móvil 103 a la que la UICC 201 está conectado a través de un ordenador central 601.

La UICC 201 descifra el perfil de abonado o verifica que fue firmado por la UICC 201, paso 909. Si la firma o descifrado indica que el perfil de abonado fue firmado o cifrado por la UICC 201, paso 911, la UICC 201 almacena el perfil de abonado recibido como el perfil de abonado activo, paso 913. A la inversa, si el perfil no se verifica como cifrado o firmado por la UICC 201, se puede transmitir un mensaje de vuelta de que la activación del perfil de abonado ha sido rechazada, etapa 915.

En una realización alternativa, a un perfil de abonado asociado con una UICC 201 particular y un operador particular se le da un número de versión. La UICC 201 mantiene una base de datos de perfiles de abonado que ha firmado o cifrado. Por lo tanto, en esta realización, en conjunción con el cifrado o la firma de un perfil, pasos 805 y 821, la UICC 201 registra el número de versión del perfil de abonado para el operador con el que está asociado. En conjunto con la verificación de descifrado o de firma digital, paso 909, la UICC 201 confirma que el perfil de abonado es el perfil de abonado más reciente que la UICC 201 ha procesado para ese operador. La UICC 201 sólo activa el

perfil más reciente abonado para ese operador, evitando así la activación de perfiles de abonado antiguos que, o bien han sido sustituidos o modificados.

En una realización alternativa, la activación de un nuevo perfil se lleva a cabo automáticamente basándose en la ubicación del dispositivo móvil 103. La Figura 10 es un diagrama de flujo que ilustra el escenario para el cambio automático de perfil basado en la ubicación. El dispositivo móvil supervisa continuamente si se está en un lugar "Home" o en una ubicación "Itinerancia", paso 151. Si el dispositivo móvil determina que ha entrado en una situación de itinerancia con respecto al perfil de abonado activo actual 501, paso 153, se selecciona el mejor perfil para utilizar en la nueva red, paso 155, y ese perfil se activa (como se ilustra y describe en relación con la figura 9), paso 157. Por supuesto, si no hay ningún cambio en la red, paso 153, no se hace nada con respecto al perfil de abonado. Alternativamente, los perfiles de abonado en un perfil de abonado monedero pueden estar asociados con ubicaciones geográficas, por ejemplo, países o continentes, y un dispositivo móvil operaría para desencadenar un cambio en el perfil de abonado basado en la ubicación geográfica que se encuentra. Esto podría, por ejemplo, llevarse a cabo en cada puesta en marcha del dispositivo móvil y en cada traspaso a nuevas células mientras se viaja a través de una red.

De lo anterior resulta evidente que se presenta una tecnología en este documento que establece un mecanismo económico, flexible, potente, escalable y seguro para crear, administrar y activar perfiles de abonado de manera que los dispositivos móviles, incluidos los dispositivos móviles con UICC incrustada, se pueden utilizar con múltiples operadores que utilizan suscripciones con cada uno de dichos múltiples operadores. La tecnología puede además ser utilizada para permitir a un operador activar un perfil administrativo en un dispositivo móvil, por ejemplo, para permitir la administración o la prueba del dispositivo móvil.

En una realización alternativa, las funciones de seguridad, por ejemplo, la criptografía y el almacenamiento de claves criptográficas, se puede realizar en una zona segura del dispositivo móvil 103 sin depender de una UICC separada 201 para alojar esa funcionalidad. La tecnología descrita en este documento para proporcionar a un usuario el acceso seguro a múltiples perfiles de abonado que puede estar vinculado cada uno a un operador independiente puede ser implementado en dicha zona segura del dispositivo móvil 103 o en cualquier otra forma en que las funciones de seguridad, como la criptografía y una gestión segura de claves criptográficas, se puede implementar. En este documento, para facilitar la explicación, la función de seguridad se describe como alojada en una UICC 201. Sin embargo, esto debe ser tomado sólo como ilustrativo.

Aunque las realizaciones específicas de la invención se han descrito e ilustrado, la invención no debe ser limitada a las formas o disposiciones de partes específicas así descritas e ilustradas. La invención está limitada sólo por las reivindicaciones.

REIVINDICACIONES

1. Un método para permitir a un dispositivo de telecomunicaciones móviles utilizar varios perfiles de abonado, un perfil de abonado incluyendo el conjunto de datos que asocia un abonado particular a un operador, comprendiendo dicho método:

- operar una función de seguridad para realizar una operación criptográfica en un perfil utilizando una clave de criptografía de la función de seguridad produciendo de este modo un perfil protegido criptográficamente;
- almacenar el perfil de abonado protegido criptográficamente;
- activar el perfil protegido criptográficamente utilizando la función de seguridad para comprobar que el perfil protegido criptográficamente ha sido protegido criptográficamente usando la clave de criptografía de la función de seguridad, y verificar además que el perfil protegido criptográficamente ha sido protegido mediante la clave de criptografía de la función de seguridad, activando el perfil protegido criptográficamente.

2. El método que permite a un dispositivo de telecomunicaciones móviles utilizar múltiples perfiles de la reivindicación 1 en el que la función de seguridad se realiza mediante un dispositivo de seguridad portátil.

3. El método que permite a un dispositivo de telecomunicaciones móviles utilizar múltiples perfiles de la reivindicación 2 en el que el dispositivo de seguridad portátil es una UICC.

4. El método que permite a un dispositivo de telecomunicaciones móviles utilizar múltiples perfiles de la reivindicación 1 en el que la función de seguridad se realiza por una zona segura del dispositivo de telecomunicaciones móvil.

5. El método que permite a un dispositivo de telecomunicaciones móviles utilizar múltiples perfiles de cualquier reivindicación precedente, en el que un perfil comprende las aplicaciones específicas o modificaciones OS específicos para un operador.

6. El método que permite a un dispositivo de telecomunicaciones móvil utilizar múltiples perfiles de cualquier reivindicación precedente en el que la etapa de almacenar el perfil protegido criptográficamente comprende almacenar el perfil protegido criptográficamente en un dispositivo de almacenamiento seleccionado entre el conjunto que incluye un dispositivo de seguridad portátil, el dispositivo de telecomunicaciones móvil, un servidor conectado al dispositivo de telecomunicaciones móvil, y un servidor ubicado en una red accesible por el dispositivo de telecomunicaciones.

7. El método que permite a un dispositivo de telecomunicaciones móviles utilizar múltiples perfiles de la reivindicación 6, que comprende además recuperar el perfil protegido criptográficamente de la función de almacenamiento.

8. El método que permite a un dispositivo de telecomunicaciones móviles utilizar múltiples perfiles de cualquier reivindicación precedente, que comprende además cargar el dispositivo protegido criptográficamente a la función de seguridad durante una fase de pre-uso de un dispositivo que aloja la función de seguridad.

9. El método que permite a un dispositivo de telecomunicaciones móviles utilizar múltiples perfiles de cualquier reivindicación precedente en el que la etapa de activación comprende la restauración de un perfil de abonado creado previamente para convertirse en el perfil de abonado activo.

10. El método que permite a un dispositivo de telecomunicaciones móviles utilizar múltiples perfiles de cualquier reivindicación precedente que comprende la activación de un perfil de administración pre-almacenado.

11. El método que permite a un dispositivo de telecomunicaciones móviles utilizar múltiples perfiles de cualquier reivindicación precedente en el que el proceso criptográfico comprende cifrar el perfil de abonado utilizando una clave secreta de la función de seguridad.

12. El método que permite a un dispositivo de telecomunicaciones móviles utilizar múltiples perfiles de cualquier reivindicación precedente en el que el proceso criptográfico comprende firmar digitalmente el perfil de abonado utilizando una clave secreta de la función de seguridad.

13. El método que permite a un dispositivo de telecomunicaciones móviles a utilizar múltiples perfiles, en el que la etapa de activar un perfil protegido criptográficamente comprende desactivar un perfil actualmente activo.

14. El método que permite a un dispositivo de telecomunicaciones móvil utilizar varios perfiles, que comprende además la determinación de la ubicación del dispositivo móvil y en el que la etapa de activación de un perfil protegido criptográficamente comprende la utilización de la ubicación del dispositivo móvil para determinar qué perfil

protegido criptográficamente activar y activar automáticamente un perfil protegido criptográficamente en caso de cambio de ubicación de un uso dictado de un perfil protegido criptográficamente diferente.

15. Un dispositivo de seguridad que comprende un medio de almacenamiento que almacena instrucciones para ejecutar el método de cualquiera de las reivindicaciones precedentes.

16. Un programa de ordenador almacenado en un medio de almacenamiento de un dispositivo de seguridad para ejecutar cualquiera de las reivindicaciones precedentes.

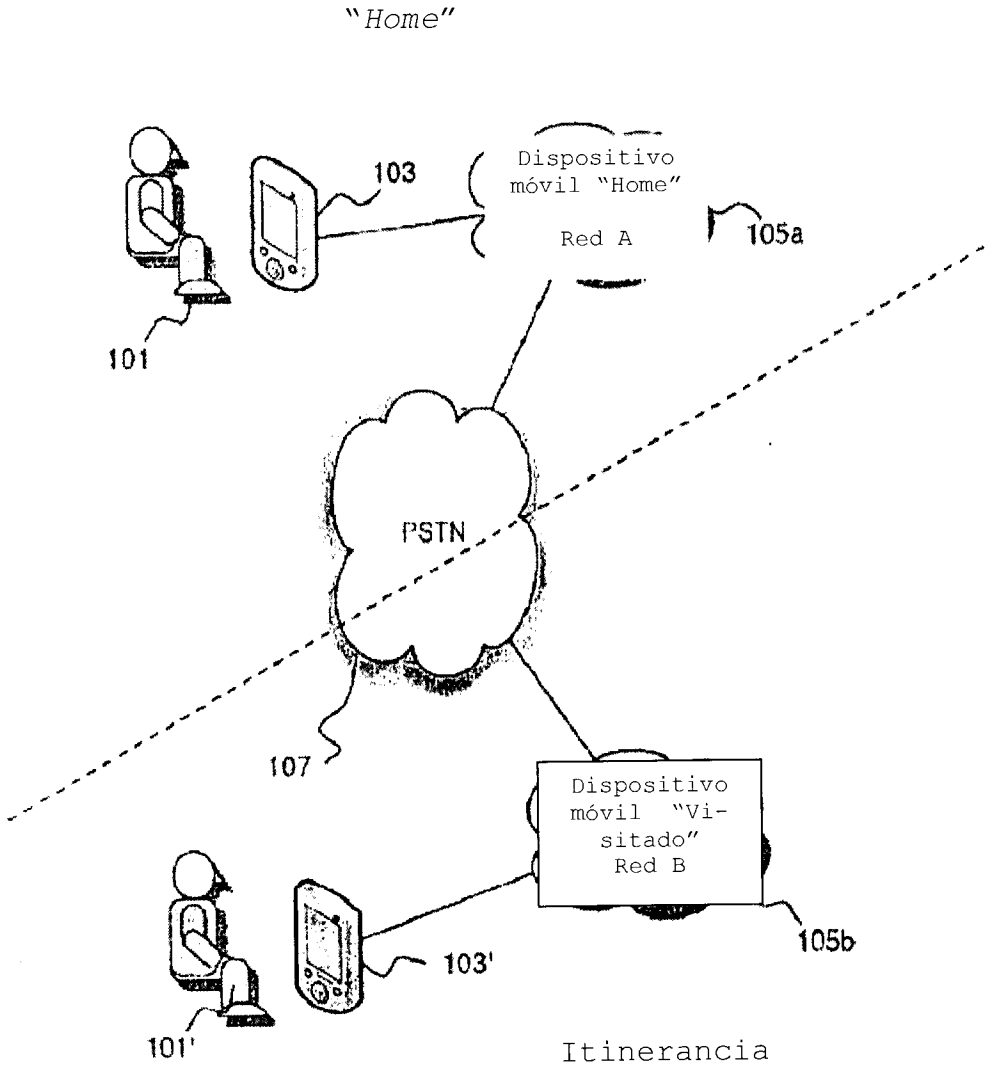
"Home"
103
Dispositivo
móvil "Home"
Red A
105a
101
PSTN
107
Dispositivo
móvil "Visitado"
Red B
105b
103'
101'
Itinerancia

Fig. 1

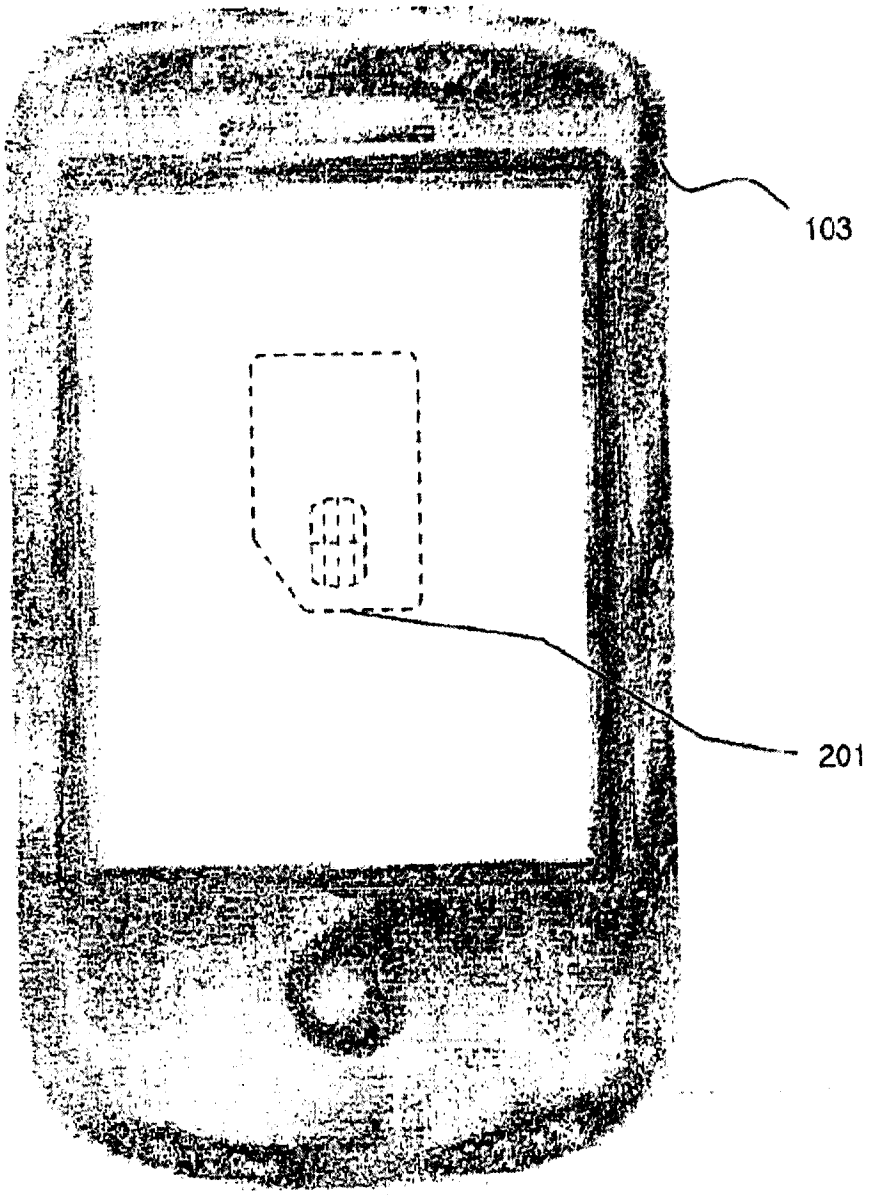

Fig. 2

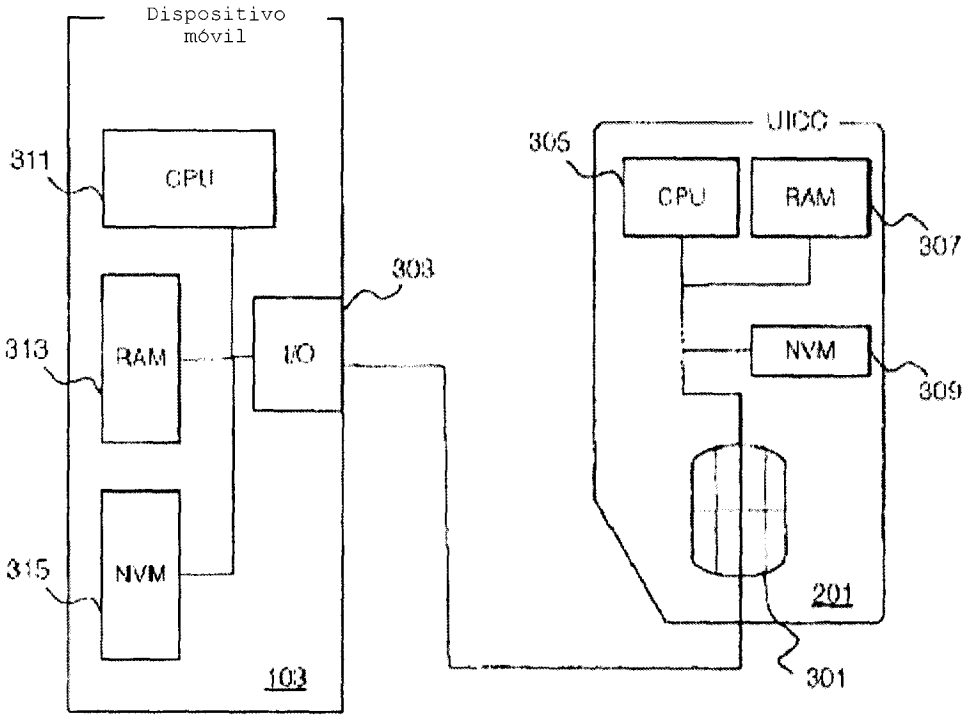
Dispositivo
móvil
311
CPU
313
RAM
315
NVM
303
I/O
103
UICC
305
CPU
RAM
307
NVM
309
201
301

Fig. 3

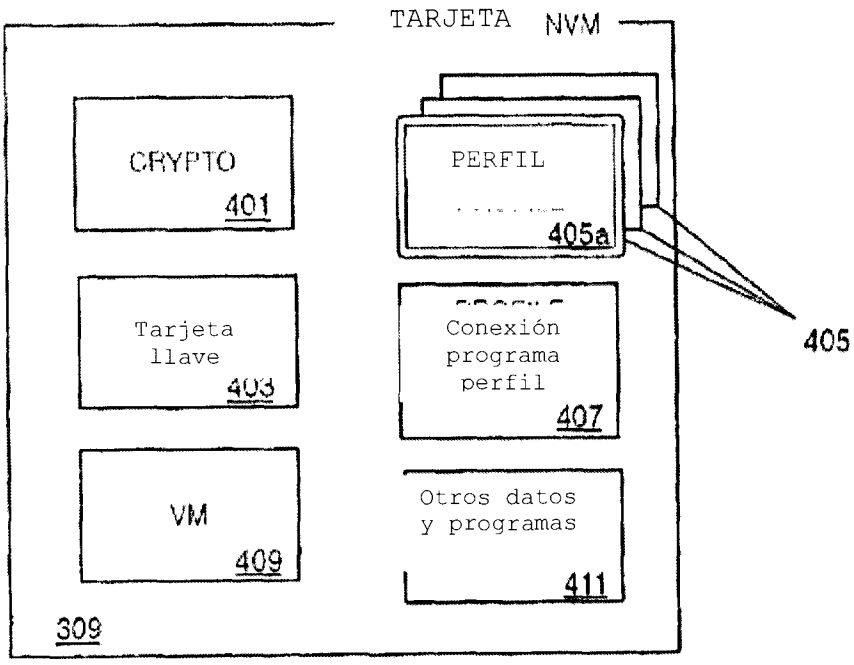
TARJETA NVM
CRYPTO
401
PERFIL
405a
405
Tarjeta
llave
403
Conexión
programa
perfil
407
VM
409
Otros datos
y programas
411
309

Fig. 4

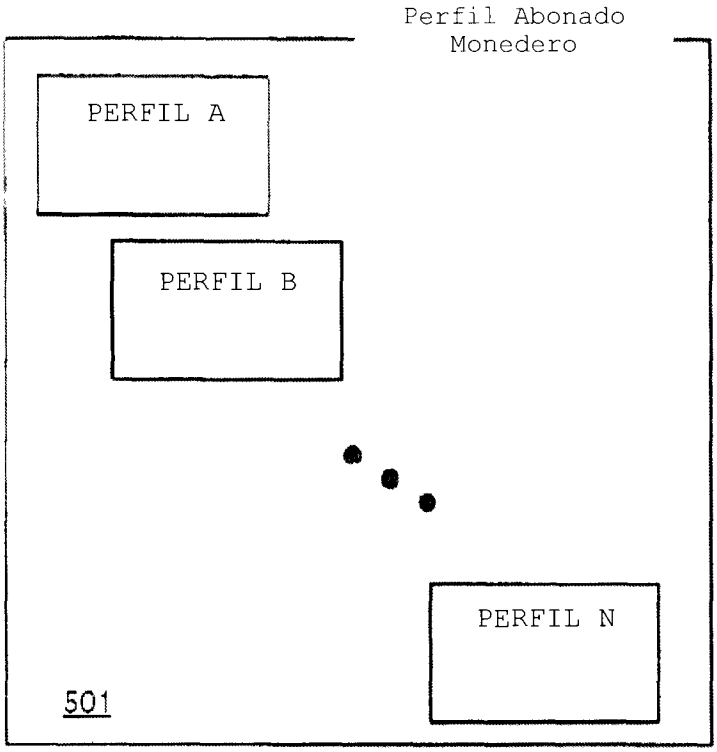

Fig. 5

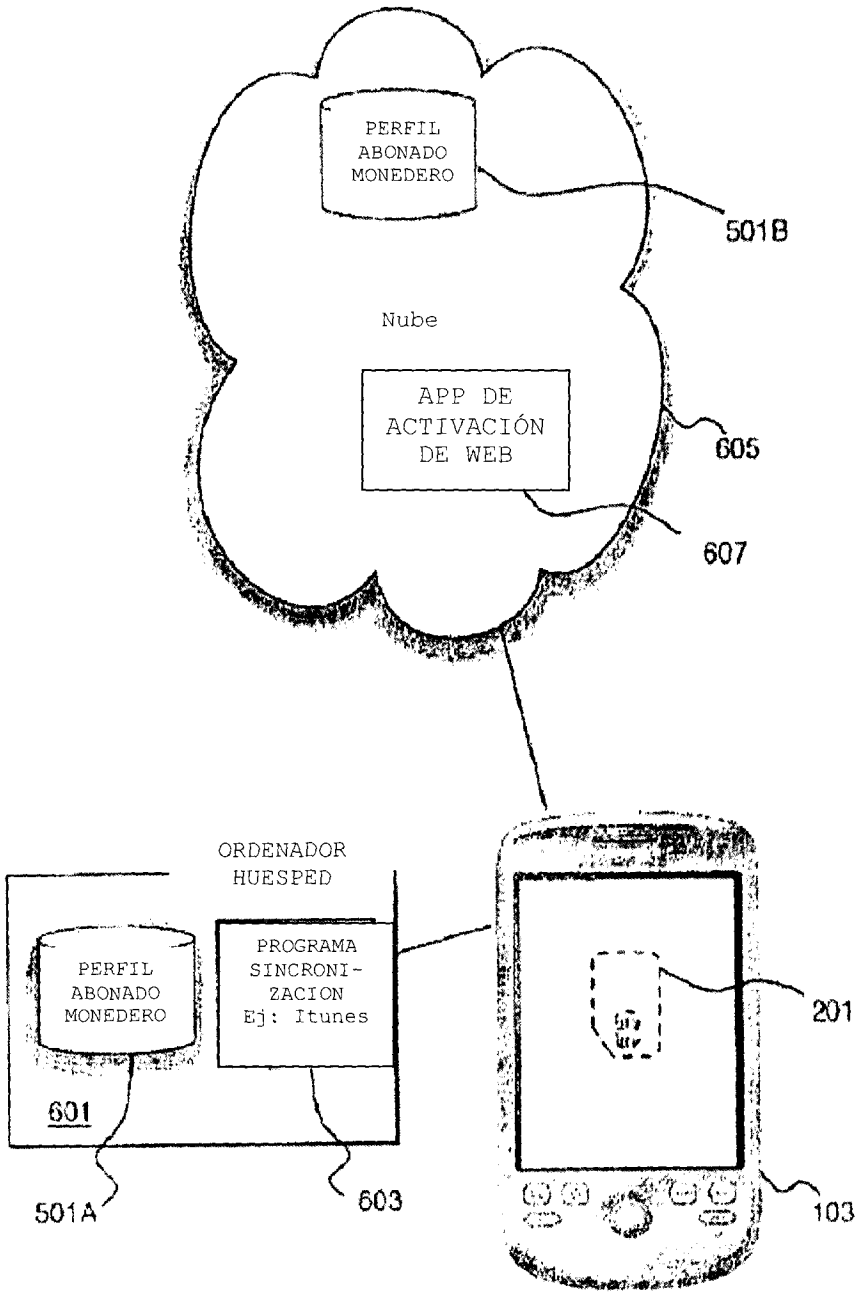
PERFIL ABONADO MONEDERO
501B
Nube
APP DE ACTIVACIÓN DE WEB
605
607
ORDENADOR HUESPED
PERFIL ABONADO MONEDERO
PROGRAMA SINCRONI-ZACION Ej: Itunes
601
501A
603
201
103

Fig. 6

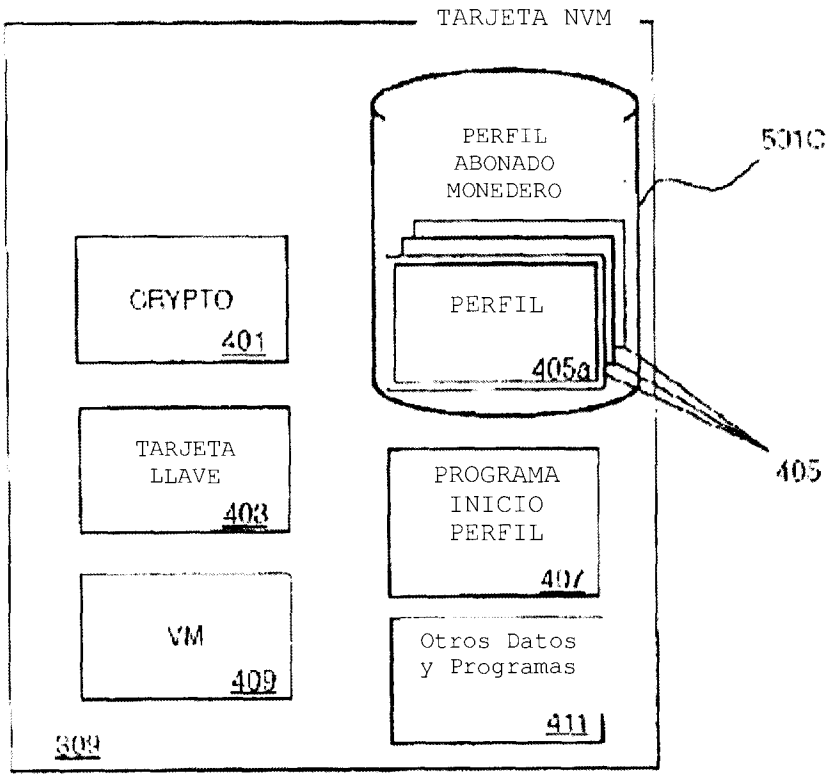
TARJETA NVM
PERFIL
ABONADO
MONEDERO
501C
PERFIL
405a
405
CRYPTO
401
TARJETA
LLAVE
403
VM
409
PROGRAMA
INICIO
PERFIL
407
Otros Datos
y Programas
411
309

Fig. 7

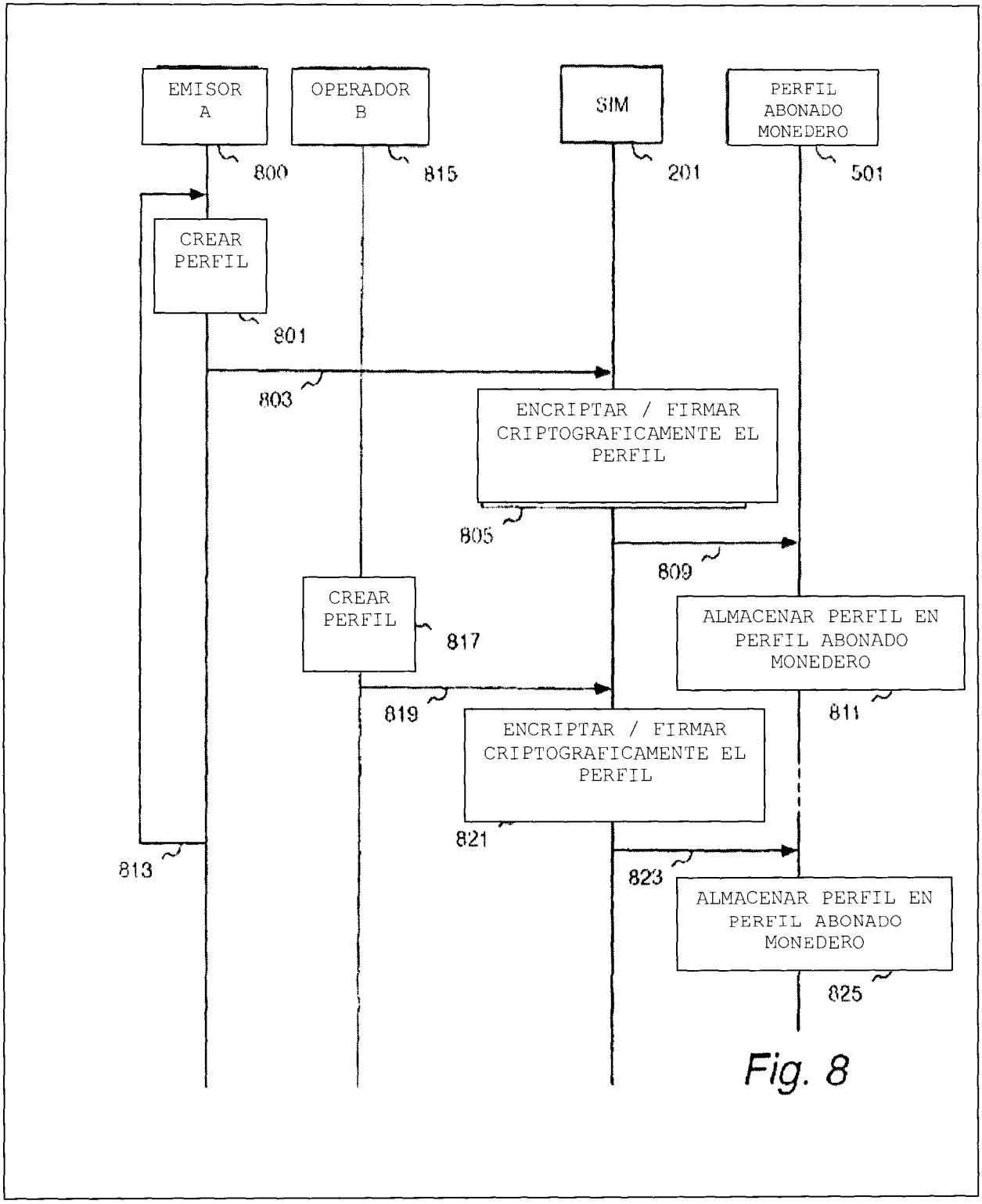
EMISOR A
OPERADOR B
SIM
PERFIL ABONADO MONEDERO
800
815
201
501
CREAR PERFIL
801
803
ENCRIPTAR / FIRMAR CRIPTOGRAFICAMENTE EL PERFIL
805
809
CREAR PERFIL
817
ALMACENAR PERFIL EN PERFIL ABONADO MONEDERO
811
819
ENCRIPTAR / FIRMAR CRIPTOGRAFICAMENTE EL PERFIL
821
813
823
ALMACENAR PERFIL EN PERFIL ABONADO MONEDERO
825

Fig. 8

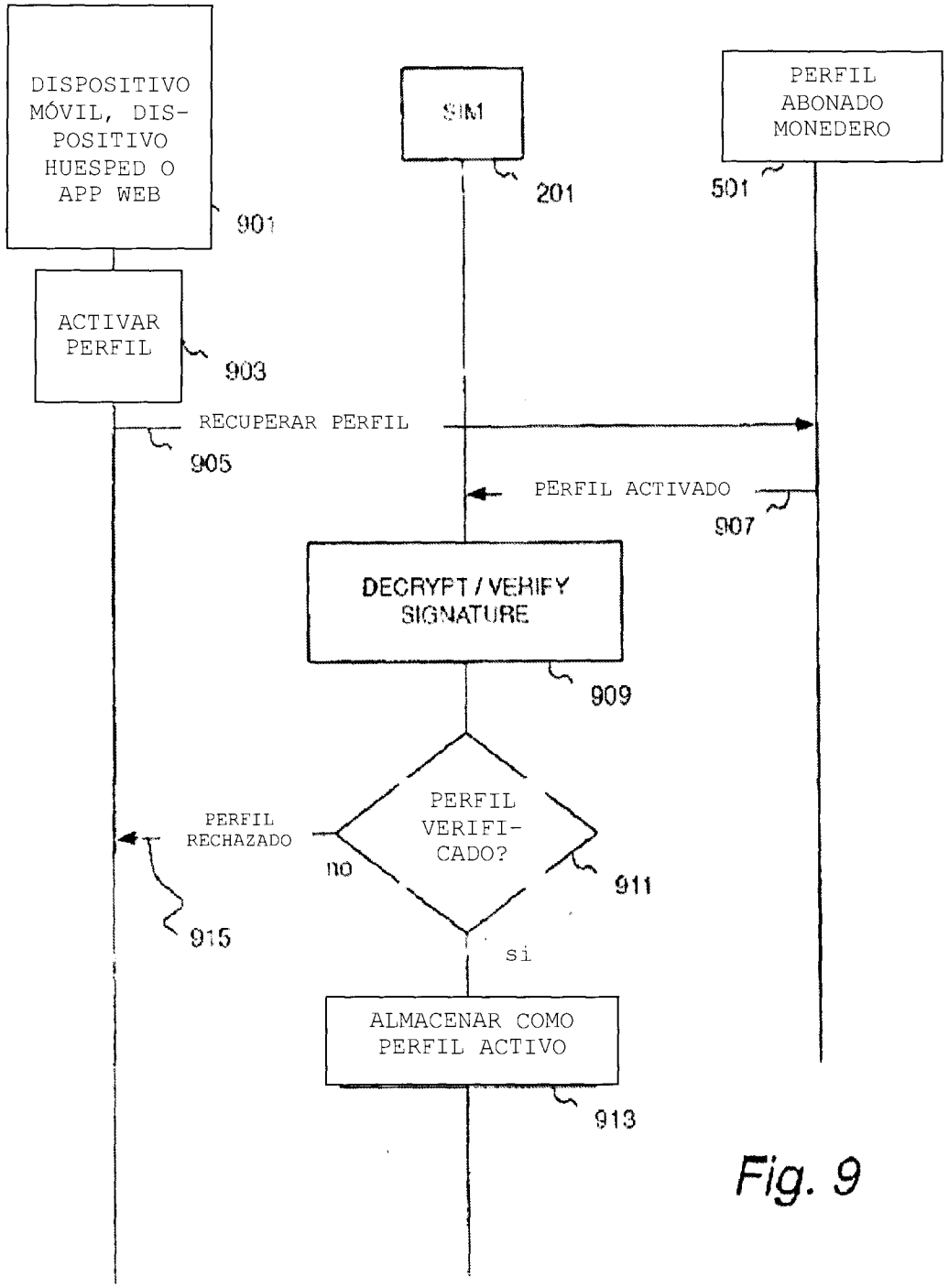
DISPOSITIVO MÓVIL, DISPOSITIVO HUESPED O APP WEB
901
SIM
201
PERFIL ABONADO MONEDERO
501
ACTIVAR PERFIL
903
RECUPERAR PERFIL
905
PERFIL ACTIVADO
907
DECRYPT / VERIFY SIGNATURE
909
PERFIL VERIFICADO?
911
no
PERFIL RECHAZADO
915
si
ALMACENAR COMO PERFIL ACTIVO
913

Fig. 9

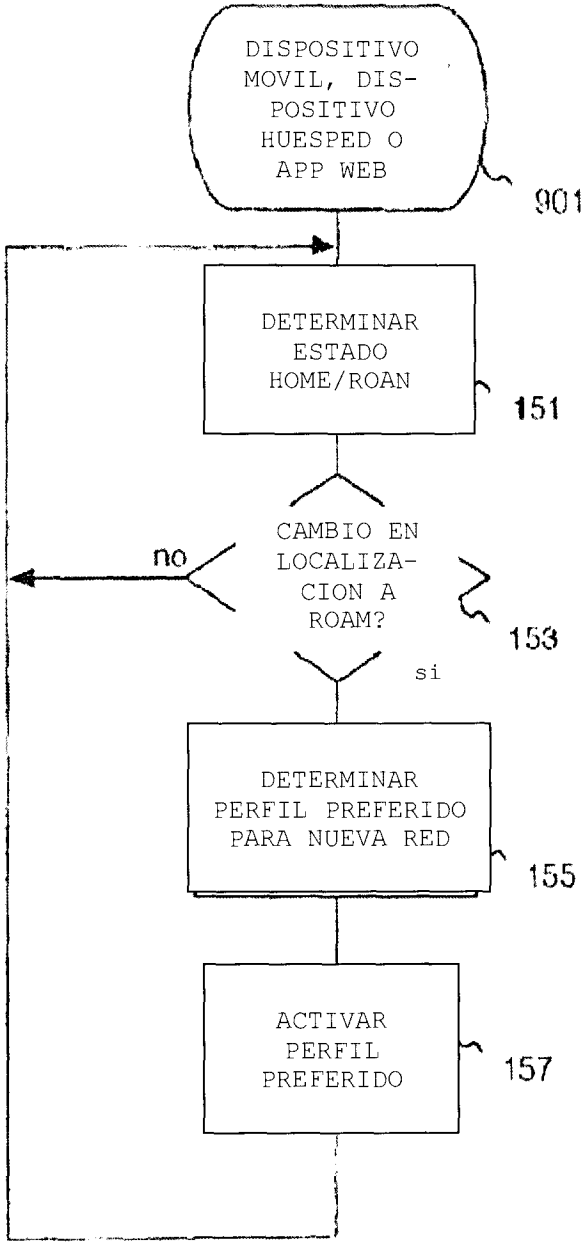
DISPOSITIVO MOVIL, DISPOSITIVO HUESPED O APP WEB
901
DETERMINAR ESTADO HOME/ROAN
151
CAMBIO EN LOCALIZACION A ROAM?
153
no
si
DETERMINAR PERFIL PREFERIDO PARA NUEVA RED
155
ACTIVAR PERFIL PREFERIDO
157

Fig. 10