(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 620 028**

(51) Int. CI.:

H04W 12/06 (2009.01)
H04W 48/18 (2009.01)
H04W 88/06 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **22.08.2013 PCT/EP2013/002529**

(87) Fecha y número de publicación internacional: **27.03.2014 WO2014044348**

(96) Fecha de presentación y número de la solicitud europea: **22.08.2013 E 13752837 (8)**

(97) Fecha y número de publicación de la concesión europea: **28.12.2016 EP 2898714**

(54) Título: **Módulo de identidad para la autentificación de un abonado en una red de comunicación**

(30) Prioridad:

19.09.2012 DE 102012018540

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.06.2017

(73) Titular/es:

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

(72) Inventor/es:

HARTEL, KARL, EGLOF;
HUBER, ULRICH y
NITSCH, NILS

(74) Agente/Representante:

DURÁN MOYA, Luis Alfonso

DESCRIPCIÓN

Módulo de identidad para la autentificación de un abonado en una red de comunicación

La invención se refiere a un módulo de identidad de abonado para la autentificación de un abonado en una red de comunicación, a un procedimiento para la gestión de un módulo de identidad de abonado con un primer juego de datos de identidad de abonado y un segundo juego de datos de identidad de abonado, a un uso del módulo de identidad de abonado, así como a un sistema constituido por el módulo de identidad de abonado y a una instancia de servidor remota.

Los datos de identidad de abonado sirven para identificar y/o autentificar un abonado de forma unívoca en una red de comunicación, por ejemplo una red de telefonía móvil digital. Mediante estos datos de identidad de abonado, a un operador de una red de comunicación le es posible asociar de forma unívoca el uso de un servicio ofrecido por el operador de red, por ejemplo, de un servicio de voz y/o datos, con cada abonado de la red de comunicación. Además, al operador le es posible facilitar un acceso a la red, es decir, el ingreso en la red de comunicación, en cuanto ha tenido lugar una autentificación del abonado o negar el acceso a la red si no es posible una autentificación del abonado.

Estos datos de identidad de abonado están almacenados en un módulo de identidad de abonado, también denominado Subscriber Identity Modul, (SIM). Habitualmente cada terminal se equipa con un módulo de identidad de abonado de este tipo, para poder usar los servicios de la red de comunicación.

Si un abonado se registra en una red de comunicación, entonces mediante los datos de identidad de abonado se constata si el abonado es conocido en la red de comunicación y qué servicios puede usar en la red. Un abonado no identificable o autentificable de forma unívoca no está autorizado para el uso de los servicios y se rechaza por la red.

Se conoce la instalación en un módulo de identidad de abonado de al menos un primer juego y un segundo juego de datos de identidad de abonado, entre los que se puede conmutar. Los módulos de identidad de abonado de este tipo también se designan como Dual-IMSI, Multi-IMSI y/o Auto-Roamer SIM.

La gestión de los datos de identidad de abonado, así como la conmutación del primer juego de datos de identidad de abonado al segundo juego de datos de identidad de abonado en el módulo de identidad de abonado se realiza generalmente mediante una instancia de servidor remota, por ejemplo una instancia de red para la gestión de los datos de identidad de abonado, también denominada gestor de subscripciones (Subscription Manager). La instancia de servidor remota envía para ello los comandos de gestión y conmutación correspondientes al módulo de identidad de abonado respectivo. La gestión y conmutación las realiza luego el sistema operativo del módulo de identidad de abonado. Alternativamente, la gestión y conmutación las realiza un código de aplicación equiparable casi al sistema operativo del módulo de identidad de abonado.

Lo problemático de ello es que en el módulo de identidad de abonado no están implementadas estrategias de conmutación o sólo están implementadas estrategias de conmutación estáticas, por ejemplo, en el caso de falta de cobertura de red, red sobrecargada o criterios de emplazamiento específicos, como funciones de código de conmutación. Estas funciones son un componente fijo del módulo de identidad de abonado y están implementados de manera que no se pueden modificar. Por consiguiente, el módulo de identidad de abonado no es capaz de reaccionar de forma adecuada a las alteraciones actuales que se produzcan en el entorno, en la red, en los terminales, etc. Por consiguiente, el módulo de identidad de abonado no se puede gestionar a base de especificaciones individuales, parámetros de red y/o propiedades de terminales actuales. En lugar de ello, se llama siempre a las mismas funciones de gestión y conmutación estáticas implementadas y se terminan completamente.

Es imposible detectar y tener en cuenta todas las particularidades o alteraciones posibles, que se deben considerar en la gestión y/o conmutación del módulo de identidad de abonado, incluidas ya dentro de las funciones del sistema operativo, debido a la multiplicidad de alteraciones posibles relativas a la red, al terminal, a la ubicación momentánea, así como a la multiplicidad de comandos de gestión. Además, en el ciclo de vida del módulo de identidad de abonado pueden aparecer adicionalmente efectos de aprendizaje que posibilitan una gestión mejorada, en particular la conmutación. Además, también puede que se desarrollen métodos mejores posteriormente a la comercialización del módulo de identidad de abonado, que luego no sea posible aplicar a todos los módulos de identidad de abonado en uso o, que si se aplican, requieran una costosa sustitución de los módulos.

En el documento de solicitud de patente de Francia FR 2941585 A1 se presenta un dispositivo de comunicación con al menos dos interfaces, permitiendo la primera interfaz un intercambio de datos entre un terminal y el dispositivo de conmutación y permitiendo la segunda interfaz un intercambio de datos entre el dispositivo de comunicación e Internet.

De la solicitud de patente de Alemania presentada el 14 de agosto de 2012 ante la Oficina alemana de patentes y marcas, con número de solicitud DE 10201206166.2 del presente solicitante, se conoce adaptar la conmutación en función de los parámetros de red, a fin de garantizar un ingreso en la red lo más satisfactorio posible después de la

conmutación. Basándose en la solución descrita, la presente invención tiene el objetivo de flexibilizar aún más la gestión del módulo de identidad de abonado. En este documento se hará referencia a la divulgación del documento DE 102012016166.2.

El objetivo de la invención se consigue mediante las medidas descritas en las reivindicaciones independientes de distintas categorías. Las configuraciones ventajosas están descritas en las respectivas reivindicaciones dependientes.

El objetivo se consigue, en particular, mediante un módulo de identidad de abonado para la autentificación de un abonado en una red de comunicación, presentando el módulo de identidad de abonado un primer juego de datos de identidad de abonado para la autentificación del abonado y al menos un segundo juego de datos de identidad de abonado para la autentificación del abonado, diferenciándose el primer juego de datos de identidad de abonado del segundo juego de datos de identidad de abonado. Además, el módulo de identidad de abonado presenta un medio para la gestión del primer y segundo juegos de datos de identidad de abonado, realizándose la gestión mediante funciones de gestión estáticas. El procedimiento se caracteriza porque el medio para la gestión presenta además un código de aplicación de gestión y este código de aplicación de gestión posibilita una gestión variable mediante adaptación de las funciones de gestión estáticas a los parámetros de entorno del módulo de identidad de abonado.

El procedimiento según la invención se basa en la división del medio para la gestión de los datos de identidad de abonado en funciones de gestión estáticas y código de aplicación de gestión variable, preferentemente código de aplicación Java. A este respecto, las funciones de gestión estáticas están implementadas de forma fija como componente del módulo de identidad de abonado. Para adaptar las funciones de gestión a la condición ambiental correspondiente, éstas se activan y ejecutan de forma variable según la invención a través del código de aplicación de gestión, preferentemente código de aplicación Java. El código de aplicación de gestión fija así, por ejemplo, el instante real de la conmutación para la conmutación mediante funciones de conmutación estáticas.

Como parámetros de entorno se consideran según la invención todas las alteraciones y circunstancias en el entorno del módulo de identidad de abonado. A modo de ejemplo se mencionan parámetros de red, indicaciones de estado de red, actualizaciones de archivos del módulo de identidad de abonado, parámetros del terminal en el que es operativo el módulo de identidad de abonado.

Por funciones de gestión estáticas se entienden, en particular, funciones del sistema operativo y/o un código de programa implementado equiparable casi al sistema operativo. A este respecto se entiende, en particular, por función de conmutación estática la adaptación del sistema de archivos al segundo juego de datos de identidad de abonado. Por función de gestión estática se entiende, en particular, la sustitución de los datos de autentificación (también denominados terceto / quinteto) del primer juego de datos de identidad de abonado, por ejemplo el algoritmo de autentificación A3, A5 y/o A8, así como la clave de autentificación Ki, por los datos de autentificación correspondientes del segundo juego de datos de identidad de abonado. Por función de conmutación estática se entiende además, en particular, la sustitución de una clave OTA específica al abonado para la comunicación OTA con la red de comunicación. Por función de gestión estática se entiende además en particular la sustitución de aplicaciones específicas al abonado, por ejemplo, applets Java específicas de los datos de identidad de abonado. Las funciones de gestión estáticas están previstas para la carga, la activación, la conmutación, la desactivación y/o el borrado de los datos de identidad de abonado.

La gestión variable se realiza en particular a través de primeras funciones del código de aplicación de gestión. Estas funciones están diseñadas para evaluar individualmente parámetros de la red de comunicación, indicaciones de estado relativas a la red de comunicación, al terminal y/o al módulo de identidad de abonado, las indicaciones de estado del terminal, así como indicaciones de estado a través de condiciones de entorno como ubicación visitada, escenarios de roaming, etc. y adaptar el comportamiento de cada módulo de identidad de abonado y de los datos de identidad de abonado correspondientes. Por ejemplo, una primera función es la función “check_Network_Status” para la verificación del registro principal en la primera o segunda red en función de los datos de identidad de abonado o para la verificación de una pérdida de la conexión de red pese al registro satisfactorio anterior en esta red. Por ejemplo, una primera función es la función “check_MCC” para la verificación de la ubicación visitada del módulo de identidad de abonado. Por ejemplo, una primera función es la función “set_waitingtime” para establecer un tiempo de espera individual para el módulo de identidad de abonado. Por ejemplo, una primera función es la función “check_Time-out” para la verificación de la expiración del tiempo de espera en el caso de un intento de registro sin éxito o una falta de confirmación de la red después del registro realizado.

La gestión variable comprende, en particular, también la carga de otros juegos de datos de identidad de abonado en el módulo de identidad de abonado. A este respecto, mediante las primeras funciones se analiza el comando de carga, en particular, qué mecanismo de carga especial está implementado en el módulo de identidad de abonado y qué mecanismo de carga se ha seleccionado por parte de la red. En base al análisis se inicializa luego el módulo de identidad de abonado mediante las primeras funciones, a fin de poder cargar correctamente los datos de identidad de abonado. Los datos confidenciales, como informaciones de autentificación, claves de autentificación, claves OTA y similares se instalan en el módulo de identidad de abonado por medio de las primeras funciones mediante una capa de seguridad adicional del estándar GSM 03.48.

La gestión variable también comprende, en particular, la activación de los datos de identidad de abonado, es decir, de un juego de datos de identidad de abonado. La activación es necesaria para poder usar los datos de identidad de abonado en el módulo de identidad de abonado para la autentificación / identificación del abonado en la red de comunicación. Al hacer la activación, el estado del juego de datos de identidad de abonado cambia de «nuevo» a «activado». Con la activación se confirma, por un lado, la integridad de los datos del juego de datos de identidad de abonado. A este respecto, la integridad de los datos se verifica mediante las primeras funciones, en particular mediante una suma de comprobación CRC. Los datos de identidad de abonado sólo se activan si la suma de comprobación CRC de los datos de identidad de abonado almacenados a activar es igual a una suma de comprobación CRC enviada por la red y recibida por el módulo de identidad de abonado. Con la activación se bloquea, por otro lado, el juego activado hasta ahora de los datos de identidad de abonado para otras actualizaciones del lado de red.

La gestión variable también comprende, en particular, la desactivación de los datos de identidad de abonado, es decir, de un juego de datos de identidad de abonado. A este respecto, se emite un comando de desactivación en el lado de red y se recibe por el módulo de identidad de abonado. Al desactivarlos los datos de identidad de abonado en el módulo de identidad de abonado ya no se pueden usar para una autentificación / identificación del abonado en la red de comunicación. Al hacer la desactivación, el estado de los datos de identidad de abonado, es decir, del juego de datos de identidad de abonado, cambia de «activado» a «desactivado». Antes de la desactivación, las primeras funciones verifican el estado de los datos de identidad de abonado. Si el juego de datos de identidad de abonado a desactivar es el único juego activado de datos de identidad de abonado en el módulo de identidad de abonado, la desactivación se impide para seguir garantizando la comunicación entre la red y el módulo de identidad de abonado.

La gestión variable también comprende, en particular, la conmutación variable de primeros datos de identidad de abonado a segundos datos de identidad de abonado, es decir, de un primer juego de datos de identidad de abonado a un segundo juego de datos de identidad de abonado. A este respecto, en principio se pueden conmutar todos los juegos de datos de identidad de abonado contenidos en el módulo de identidad de abonado. Si, por ejemplo, están presentes un primer, segundo y tercer juegos de datos de identidad de abonado en el módulo de identidad de abonado, se puede conmutar de forma flexible entre los tres datos de identidad de abonado, es decir, entre los tres juegos de datos de identidad de abonado. A este respecto, siempre estará activado sólo el primer, el segundo o el tercer juego de datos de identidad de abonado.

La gestión variable también comprende en particular el borrado variable de datos de identidad de abonado. A este respecto, se libera el espacio de almacenamiento que se podrá usar para la carga / almacenamiento de nuevos datos de identidad de abonado.

Un módulo de identidad de abonado, según invención, es un módulo de tamaño y recursos escasos, que presenta un microcontrolador y al menos una interfaz de datos para la comunicación con un terminal. Este módulo de identidad de abonado presenta un espacio de almacenamiento seguro, en el que los datos de identidad de abonado están instalados de forma segura para impedir intentos de manipulación y/o uso indebido durante la identificación y/o autentificación en la red. El módulo de identidad de abonado es operativo gracias al terminal.

El módulo de identidad de abonado es, por ejemplo, una tarjeta inteligente, UICC o tarjeta SIM, en una red de telefonía móvil con datos de identidad de abonado legibles por una máquina y almacenados en un chip. Dichos módulos de identidad de abonado se operan en un terminal mediante unidades de lectura de tarjetas estando previstos, en particular, para poder extraerse del terminal para su sustitución o para su uso en un segundo terminal.

Alternativamente, el módulo de identidad de abonado es un componente integral del terminal móvil, por ejemplo, un módulo electrónico cableado no reprogramable. Dichos módulos de identidad de abonado también se denominan UICC embebidos (*embedded eUICC* eUICC). Con ese diseño, estos módulos de identidad de abonado no están previstos para una extracción del terminal y en principio no se pueden sustituir de forma sencilla. Dichos módulos de identidad de abonado también pueden ser elementos de seguridad embebidos*, embedded Secure Elements,* es decir, componentes de hardware seguros en el terminal móvil.

Alternativamente, el módulo de identidad de terminal es un módulo M2M. Estos módulos sirven para la supervisión, control y mantenimiento remotos de terminales: máquinas, instalaciones y sistemas. Alternativamente, también se pueden usar para unidades de conteo, como contadores eléctricos o contadores de agua caliente.

Alternativamente, el módulo de identidad de abonado es un componente de software de una parte de confianza de un sistema operativo, un así denominado entorno de ejecución de confianza (*Trusted Execution Environment*, TEE) del terminal. En ese caso, el módulo de identidad de abonado está incluido, por ejemplo, dentro de un entorno en tiempo de ejecución protegido en forma de programas que se ejecutan en él, denominados *Trustlets*.

Los datos de identidad de abonado según la invención son, por un lado, los datos que identifican un abonado de forma unívoca en la red de comunicación, por ejemplo, la identidad internacional de abonado móvil (*International*

Mobile Subscriber Identity, IMSI) y/o datos específicos al abonado. La IMSI es el dato de identidad de abonado unívoco en una red de comunicación de telefonía móvil. Se compone del código de país MCC (*Mobile Country Code*), el código de red MNC (*Mobile Network Code*) y un número correlativo que da el operador de la red. Los datos de identidad de abonado comprenden adicionalmente indicaciones de estado, pudiendo ser el estado de los datos de identidad de abonado: «activo», «inactivo» y/o «usado».

Además, los datos de identidad de abonado pueden ser datos que autentifican un abonado de forma unívoca en la red de comunicación, por ejemplo, un algoritmo de autentificación, parámetros específicos del algoritmo, una clave criptográfica de autentificación y/o una clave criptográfica *por el aire* (inalámbrica) (*Over-The-Air*, OTA).

El número de juegos de datos de identidad de abonado del módulo de identidad de abonado no está limitado. Cabe imaginarse que en el futuro en un módulo de identidad de abonado estén presentes treinta o más juegos de datos de identidad de abonado.

Un abonado según la invención es, por ejemplo, una persona que quiera acceder a los servicios de la red de comunicación mediante el terminal. Por abonado también se puede entender un terminal en un entorno M2M.

Una red de comunicación según la invención es un dispositivo técnico en el que tiene lugar la transmisión de señales tras la identificación y/o autentificación del abonado que realiza la comunicación, mediante las que se ofrecen los servicios. La red de comunicación está desplegada preferiblemente por celdas de telefonía móvil, dependiendo el tamaño de una celda de radio de las condiciones meteorológicas y geográficas, así como de las antenas de radio usadas. En particular, en esta invención se entiende por red de telefonía móvil, por ejemplo, el sistema global para comunicaciones móviles, *Global System for Mobile Communications*, abreviadamente GSM como tecnología representativa de la segunda generación o el servicio general de paquetes vía radio, *General Packet Radio Service*, abreviadamente GPRS o sistema universal de telecomunicaciones móviles, *Universal Mobile Telecommunications System*, abreviadamente UMTS, como tecnología representativa de la tercera generación o la evolución a largo plazo, *Long Term Evolution*, abreviadamente, LTE, como tecnología representativa de la cuarta generación.

En una realización preferida, el código de aplicación de gestión se puede actualizar y/o intercambiar a través de una interfaz por aire de la red de comunicación. Mediante esta configuración se mantiene el medio para la gestión en el estado más actual y eventualmente también se puede adaptar a corto plazo, por ejemplo, en el marco de un escenario de roaming, a los nuevos parámetros y condiciones. De este modo, también se puede adaptar a una modificación de acuerdos de roaming. De este modo, también se puede adaptar a las modificaciones en el terminal, por ejemplo, en el marco de la actualización del sistema operativo del terminal.

En una realización preferida, las funciones de gestión estáticas son segundas funciones, accediendo las primeras funciones del código de aplicación de gestión mediante una interfaz de programación a estas segundas funciones. Por consiguiente, las segundas funciones implementadas de forma dura siempre son operativas y se pueden utilizar de forma adaptativa con la interfaz de programación. La interfaz de programación proporciona así la funcionalidad para la gestión mediante las segundas funciones, mientras que las primeras funciones evalúan el comando de gestión correspondiente, supervisan el éxito de la gestión y proyectan / aplican una estrategia de reconmutación adaptativa. Los comandos de gestión son, en particular, el comando de carga para la carga de nuevos datos de identidad de abonado, el comando de activación para la activación de los datos de identidad de abonado, el comando de conmutación para la conmutación de los primeros a los segundos datos de identidad de abonado (es decir, de un primer juego de datos de identidad de abonado a un segundo juego de datos de identidad de abonado), el comando de desactivación para la desactivación de los datos de identidad de abonado y/o el comando de borrado para el borrado de los datos de identidad de abonado.

En una realización preferida, las primeras funciones comprenden la supervisión de parámetros de ubicación actuales. Si cambia en particular la ubicación visitada, lo que se indica a través de un código de país de red móvil, *Mobile Country Code*, abreviadamente, MCC, de la red, el medio para la gestión tiene que esperar, en su caso, a la redirección de los servicios de red que realiza la red de comunicación visitada. En particular la conmutación y reconmutación a los (primeros) datos de identidad de abonado ocurriría con algún desfase temporal.

En una realización preferida, las primeras funciones comprenden la generación de periodos de espera. Así, en función de la disponibilidad de servicios de red se coordinan el borrado, activación, desactivación y/o conmutación o reconmutación, por lo que se evita una implementación dura con conmutación o reconmutación, en su caso, temprana y resultando el proceso amigable para el usuario.

En una realización preferida, las primeras funciones comprenden la reconmutación adaptativa entre el primer juego de datos de identidad de abonado y el segundo juego de datos de identidad de abonado. Las funciones de gestión estáticas prevén una reconmutación estática si fracasase el registro en la nueva red con los datos de identidad de abonado conmutados. Por circunstancias de la red se desea realizar, eventualmente, la reconmutación sólo después de la expiración de un tiempo de espera definido. Para ello, una primera función se ocuparía de establecer un tiempo de espera en función de los parámetros de red, así como del nuevo análisis de la situación de red tras la expiración del tiempo de espera antes de que se reconmutara. La reconmutación, entonces, sería en sí parte de las segundas

funciones, el análisis, el establecimiento del tiempo de espera y el nuevo análisis son entonces parte de las primeras funciones.

En una realización de la invención, las funciones de gestión variables comprenden la generación de mensajes de confirmación a petición de la instancia de servidor remota.

En una realización alternativa, las primeras funciones comprenden la conmutación adaptativa entre los primeros datos de identidad de abonado y los segundos datos de identidad de abonado, es decir, el primer juego de datos de identidad de abonado y el segundo juego de datos de identidad de abonado, iniciándose la conmutación por la instancia de servidor remota mediante un comando de conmutación. En este caso, se conmuta inmediatamente mediante funciones de gestión estáticas. Las primeras funciones verifican ahora el estado de la conmutación dura, para reconmutar de nuevo cuando no se haya conectado, por ejemplo, con la red tras expirar un tiempo de espera predefinido. Si el segundo proveedor de red eliminase el segundo juego de datos de identidad de abonado de sus bases de datos, ya no sería posible un registro del módulo de identidad de abonado en la segunda red conmutada después de la conmutación dura. Las primeras funciones del código de aplicación Java tienen adicionalmente una función para la reconmutación a los datos de identidad de abonado válidos más recientes, por lo que se puede reconmutar al perfil de abonado válido más reciente. Por consiguiente, el código de aplicación de gestión variable para proteger los primeros datos de identidad de abonado los almacena y los marca como datos de identidad de abonado válidos más recientes.

El módulo de identidad de abonado tiene que reconmutarse luego al estado de partida, lo que se denomina en este documento reconmutación. Si la reconmutación la controlan las primeras funciones, se pueden examinar otros parámetros de red para garantizar la reconmutación.

Según la invención, el objetivo también se consigue mediante un procedimiento para la gestión de un módulo de identidad de abonado con un primer juego de datos de identidad de abonado y un segundo juego de datos de identidad de abonado. El procedimiento comprende las etapas de: obtención de un comando de gestión en el módulo de identidad de abonado; gestión del primer juego de datos de identidad de abonado y del segundo juego de datos de identidad de abonado mediante el comando de gestión. El procedimiento se caracteriza porque antes de la etapa de la gestión se inicia el código de aplicación de gestión en el módulo de identidad de abonado, porque tras la etapa de la gestión por el código de aplicación de gestión se evalúan los parámetros de red de comunicación y porque en función de la evaluación se adapta la etapa de gestión.

Además, según la invención está previsto el uso de un módulo de identidad de abonado descrito anteriormente en un terminal de comunicación móvil para conseguir el objetivo planteado. A este respecto, el terminal de comunicación está configurado para hacer operativo el módulo de identidad de abonado.

Un terminal según la invención es en principio un aparato o un componente de aparato que presenta medios para la comunicación con la red de comunicación, a fin de poder usar los servicios de la red de comunicación. Por ejemplo, el término englobaría un terminal móvil, como un Smartphone, una tableta, un ordenador portátil o una PDA. Por terminal también se puede entender, por ejemplo, terminales multimedia, como marcos de fotos digitales, equipos de audio, televisores o libros electrónicos que presenten igualmente medios para la comunicación con la red de comunicación. Por ejemplo, el término «terminal» también comprende cualquier tipo de máquinas, máquinas automáticas, vehículos y dispositivos que presenten medios, en particular módems de telefonía móvil, para la comunicación con la red de comunicación.

Además, según la invención está previsto un sistema que se compone de al menos un módulo de identidad de abonado descrito anteriormente y una instancia de servidor remota, enviando la instancia de servidor remota al al menos un módulo de identidad de abonado un comando de gestión para la gestión de un primer juego de datos de identidad de abonado y de un segundo juego de datos de identidad de abonado en el módulo de identidad de abonado.

A continuación se explican más en detalle la invención u otras formas de realización y ventajas adicionales de la invención mediante las figuras, describiendo las figuras sólo ejemplos de realización de la invención. Los mismos componentes en las figuras tienen los mismos números de referencia. Las figuras no se deben considerar hechas a escala real; elementos individuales de las figuras pueden estar representados exageradamente grandes o exageradamente simplificados.

Muestran:

la figura 1 un diagrama de bloques de un módulo de identidad de abonado según la invención,

la figura 2 una representación detallada de la jerarquía de programa y de datos en el módulo de identidad de abonado según la invención,

la figura 3 un perfil de abonado según la invención con datos de identidad de abonado,

la figura 4 un diagrama de flujo del procedimiento según la invención,

la figura 5 un esquema de un ciclo de vida de los datos de identidad de abonado, a modo de ejemplo.

En la figura 1 se representa un diagrama de bloques de un módulo de identidad de abonado -1-. El módulo de identidad de abonado -1- presenta una interfaz de datos -3-. Una unidad de cómputo central -4- conecta la interfaz de datos -3- con una memoria -2-, volátil (RAM) o no volátil (ROM, EEPROM, FLASH). En el espacio de almacenamiento -2-, en particular, en el espacio de almacenamiento no volátil, están almacenados los perfiles de abonado -11- que contienen los datos de identidad de abonado o juegos de datos de identidad de abonado -13a, 13b, 13n-. De este modo, se pueden adaptar los datos de identidad de abonado -13a, 13b, 13n- para la red de comunicación respectiva. En particular, resulta posible que los datos de identidad de abonado -13- se puedan instalar tras la comercialización del módulo de identidad de abonado -1- al abonado, por ejemplo, vía OTA u OTI, a través de la interfaz de datos -3-, por lo que resulta posible un uso más flexible del módulo -1-. En el espacio de almacenamiento -2- se instala además el sistema operativo -5-, con el que se puede hacer funcionar el módulo -1-. En la figura 2 está representada una pila de capas, a modo de ejemplo, de la jerarquía de programa y de datos de un módulo de identidad de abonado -1- según la invención. En el espacio de almacenamiento -2- del módulo de identidad de abonado -1- está instalado un sistema operativo -5-. El sistema operativo -5- accede a los recursos de hardware del módulo de identidad de abonado -1-. En el módulo de identidad de abonado -1- está instalada a su vez una máquina virtual, en este caso una máquina virtual *Java Card*, abreviadamente JCVM. La JCVM a su vez facilita un entorno de tiempo de ejecución -6-, también denominado JCRE. Dentro del JCRE está configurado un espacio seguro -7-, en el que el creador del módulo puede incluir, en particular, una clave única del módulo y aplicaciones únicas del módulo. Este espacio seguro -7- es inaccesible para los operadores de las redes de comunicación. Además, en el JCRE están implementadas funciones de gestión -8-. Estas funciones de gestión acceden a las interfaces de programación típicas de módulos de identidad de abonado, como la API de plataforma abierta, la SIM-API, USIM-API y/o la API Java Card. Estas interfaces facilitan paquetes de funciones que utilizan los programas del módulo de identidad de abonado -1-.

Las funciones de gestión -8- son segundas funciones según lo que se ha ido describiendo y sirven para desactivar un perfil activo, activar un perfil inactivo, borrar un perfil desactivado, cargar un nuevo perfil y/o conmutar entre perfiles. Estas segundas funciones son componentes fijos del módulo de identidad de abonado -1- y están implementadas de forma que no se puedan modificar. La gestión mediante estas funciones de gestión estáticas -8- se realiza después de introducir un comando de gestión S2 (véase la figura 4) desde una instancia de servidor remota y no es adaptativa en el estado de la técnica actual. Sin embargo, esto es desfavorable en muchos casos o escenarios de uso, dado que según el entorno hay que aplicar diferentes estrategias durante la gestión.

Por ejemplo, en algunos casos se debe hacer una conmutación dura a los segundos datos de identidad de abonado -13b-, aunque se haya confirmado la cobertura de red en la nueva red para los segundos datos de identidad de abonado -13b-. El módulo de identidad de abonado -1- no debería aplicar entonces, a ser posible, ninguna estrategia de reconmutación.

Alternativamente, se debe reconmutar (S11) a veces inmediatamente a los primeros datos de identidad de abonado -13a-, cuando no se ha confirmado la cobertura de red S7 en la nueva red. En este caso se debería realizar una reconmutación lo antes posible para facilitarle al usuario un acceso lo más rápido posible.

En otros casos, sólo se debe intentar durante un tiempo el registro en la nueva red (S7 en conjunción con S8, S9) antes de que se reconmute (S10, S11).

Para posibilitar estas gestiones adaptativas, según la invención se proporciona un código de aplicación de gestión -9-, preferentemente en forma de código de aplicación Java o un applet Java. Este código de aplicación de gestión -9- presenta primeras funciones que se pueden sustituir, cargar a posteriori y/o actualizar, al contrario que las segundas funciones -8-, durante el ciclo de vida del módulo de identidad de abonado -1-. Para ello se usa o bien una interfaz por aire (OTA) o bien una interfaz basada en internet (OTI), introduciéndose el código de aplicación de gestión -9- cargado a posteriori o actualizado a través de la interfaz de datos -3- en el espacio de almacenamiento -2-.

El código de aplicación de gestión -9- está programado de forma individual. El código de aplicación de gestión -9- presenta en particular las siguientes primeras funciones:

- recepción y evaluación del comando de gestión de la instancia remota (etapa S4 en la figura 4);

- supervisión de la gestión iniciada;

- supervisión de los parámetros de red MCC, MNC (etapa S7 de la figura 4) y generación de información de gestión a partir de estos parámetros;

- implementación de una estrategia de retorno adaptativa (etapa S10 de la figura 4);

- facilitación de períodos de espera durante la conmutación (etapas S8, S9 de la figura 4).

Para que el código de aplicación de gestión -9- pueda modificar las segundas funciones de gestión (estáticas) -8-, está prevista una interfaz de programación -10- adicional, una API de gestión. Ésta activa las verdaderas funciones de gestión -8-, en particular la conmutación entre los primeros datos de identidad de abonado -13a- y los segundos datos de identidad de abonado -13b-, la carga de los datos de identidad de abonado -13-, la activación / desactivación de datos de identidad de abonado -13- y el borrado de datos de identidad de abonado -13-.

El código de aplicación de gestión -9- accede así a través de la interfaz de programación -10- a las funciones de gestión estáticas -8-, que acceden a su vez directamente al sistema operativo -5-, representado mediante flechas. Gracias a esta estructura es posible una gestión más flexible, así como la implementación de estrategias de gestión alternativas, según se describe de forma más detallada a continuación al comentar la figura 4.

El módulo de identidad de abonado -1- representado en la figura 2 tiene una multiplicidad de perfiles de abonado -11-. Cada perfil de identidad de abonado -11- de la figura 2 contiene los datos de identidad de abonado -13a, 13b, 13n- (o un juego de datos de identidad de abonado), que identifican y/o autentifican de forma unívoca un abonado en redes de comunicación iguales y/o diferentes. Con dichos módulos de identidad de abonado -1- ya no es forzosamente necesario que un operador de una red genere un nuevo módulo de identidad de abonado -1- para la identificación y autentificación de un abonado en su red por contrato y lo entregue al abonado en forma de tarjeta SIM. En lugar de ello, el operador de red crea un perfil -11- en base al contrato. El perfil -11- se carga entonces en el módulo de identidad de abonado -1- ya instalado en el terminal y pudiendo coexistir con otros perfiles -11-. De este modo, resulta que el módulo de identidad de abonado -1- ya no hace falta que sea desacoplable del terminal, en lugar de ello, los módulos de identidad de abonado -1- pueden tener un cableado fijo abreviadamente eUICCs, en el terminal. Esto ahorra espacio en el terminal, por lo que se pueden implementar otras funcionalidades en él sin tener que aumentar el diseño del terminal. El procedimiento según la invención se debe aplicar en particular a eUICC, dado que aquí un usuario no tiene por qué cambiar el módulo de identidad de abonado -1- a fin de poder usar los servicios de red de un contrato alternativo.

En la figura 3 está representado más en detalle un perfil de abonado -11a-. El perfil -11a- presenta un espacio seguro -111- para el operador de red. El espacio seguro -111- se puede diferenciar del espacio seguro -7-. Además, un perfil tiene código de aplicación -112- específico para él, así como un sistema de archivos -113- específico para dicho perfil también. Cada perfil -11- puede estar activo o inactivo, por módulo de identidad de abonado -1- siempre está activo sólo un perfil -11-, es decir, los datos de identidad de abonado -13- del perfil -11- activo se usan para autentificar y/o identificar a un abonado en una red de comunicación. Solo se pueden conmutar perfiles -11- activos. En principio todos los perfiles son válidos y pueden estar asociados todos a un mismo o a diferentes operadores de red.

Para cada perfil está prevista una clave de perfil propia. Sólo los perfiles -11- activados están implicados en la seguridad del operador de red. El código de aplicación de gestión -9- gestiona estos espacios seguros y actualiza las claves correspondientes.

En una realización del módulo de identidad de abonado -1- todos los datos y parámetros necesarios para un perfil se almacenan en el perfil. La gestión de los datos / parámetros se realiza mediante funciones variables, es decir, el código de aplicación de gestión -9-.

Los datos de identidad de abonado -13- según la figura 2 comprenden en particular una indicación sobre el algoritmo de autentificación usado en el operador de la red (Comp 128-1, Comp 128-2, Comp 128-3, Milenage), la identidad internacional del abonado móvil (*International Mobile Subscriber Identity*, IMSI), las claves de autorización criptográficas usadas para la autentificación, los ajustes de parámetros del algoritmo utilizado, en su caso, las claves OTA específicas del operador de red para posibilitar una comunicación OTA segura, datos específicos del abonado, como nombre, apellido, número de DNI, fecha de nacimiento, lugar de nacimiento, etc.; y/o en su caso datos adicionales, específicos del operador de red, por ejemplo qué servicios están habilitados en la red correspondiente para el abonado, qué algoritmos de *backup* están disponibles y similares. Este listado no es en ningún caso exhaustivo y en otras realizaciones alternativas también pueden comprender menos, más u otros datos.

En la figura 4 está representado un diagrama de flujo de un procedimiento según la invención. En este caso, se parte de que el perfil -13a- está activado y de que se ha usado el primer juego de datos de identidad de abonado -11a- para autentificar el abonado en la primera red. En la etapa S2 se recibe un comando de gestión, que es un comando de conmutación, de una instancia remota, un gestor de subscripción, *Subscription Manager* a través de la primera red de comunicación por la interfaz de datos -3-. Con dicho comando de conmutación S2 se inicia el código de aplicación de gestión -9- en la etapa S3.

En la etapa siguiente S4 se realiza el análisis del comando de conmutación, en particular de los parámetros del comando de conmutación. Los parámetros pueden ser: conmutación dura sin cobertura de red; conmutación sólo si

la nueva red está disponible; conmutación sólo cuando en la red esté disponible un servicio determinado u otros casos similares. A continuación, en la etapa S5 se realiza la conmutación a los segundos datos de identidad de abonado -13b-. A este respecto, el perfil -11- se desactiva y se activa el segundo perfil -11b-. Con los segundos datos de identidad de abonado -13b- del segundo perfil -11b- activado, el módulo de identidad de abonado -1- intenta registrarse en una nueva red de comunicación. Para la etapa S5 se usa la API de conmutación 10 a fin de acceder a las funciones de gestión estáticas -8-.

En la etapa S6 el código de aplicación de gestión -9- supervisa si la nueva red está disponible. Si la nueva red está disponible (caso: sí), el procedimiento queda finalizado, a menos que los parámetros según el análisis de la etapa S4 impongan un tratamiento alternativo, no estando representado ese caso en la figura. Si la nueva red no está disponible (caso: no, en la etapa S6) se realiza un análisis de los parámetros de red en la etapa S7. En particular se realiza la supervisión de los parámetros MNC y MCC, una verificación del archivo EF_Loci, en su caso, la verificación del archivo EF_FPLMN y otros similares. Adicionalmente también se verifican parámetros relativos al terminal, en particular, si el terminal ya estaba listo para la conmutación o no.

En función del análisis de las etapas S4 y S7 se decide entonces en la etapa S8 si se debe ajustar un tiempo de espera. Este tiempo de espera proporciona, por ejemplo, durante un escenario de roaming el lapso de tiempo requerido hasta que la nueva red permite una autentificación mediante los segundos datos de identidad de abonado -13b-. Si en la etapa S8 se necesita un tiempo de espera (caso: sí), se verifica si ha expirado en la etapa S9. Luego se prosigue con la etapa S10. Si en la etapa S8 no se necesita un tiempo de espera (caso: no) se prosigue igualmente con la etapa S10, a saber, en la que se hace una consulta sobre si es necesaria una estrategia de retorno en función de las etapas S4 y S7. Si se necesita una estrategia de retorno (caso: sí en la etapa S10) se realiza una reconmutación al primer perfil -13a- según la API de gestión -10- y las funciones de gestión -8-. Si no se necesita una estrategia de retorno (caso: no en la etapa S10), entonces se vuelve a la etapa S6 y de nuevo se evalúa la disponibilidad de red y se hace un análisis de los parámetros según la etapa 7.

Si en el ciclo de vida del módulo de identidad de abonado -1- una estrategia de gestión resultase muy prometedora, por ejemplo, el ajuste de un tiempo de espera determinado debido a las circunstancias del terminal con el que el módulo de identidad de abonado se comunica mediante la interfaz de datos -3-, entonces esta estrategia se puede aplicar como estrategia estándar.

Alternativamente, también es posible complementar o actualizar el código de aplicación de gestión -9-, a fin de adaptar el módulo de identidad de abonado -1- a condiciones de red modificadas y diseñar una conmutación más flexible debido a ello.

Alternativamente, también es posible sustituir completamente el código de aplicación de gestión -9-, a fin de poder adaptar el módulo de identidad de abonado -1- a condiciones de red modificadas y diseñar una conmutación más flexible debido a ello.

Una parte esencial de las funciones variables, es decir, del código de aplicación de gestión -9-, es la generación de mensajes de confirmación para la instancia de servidor remota. Un mensaje de confirmación se genera, por ejemplo, cuando el módulo de identidad de abonado ha conseguido registrarse de forma satisfactoria en la red usando los datos de identidad de abonado -13- conmutados. Un mensaje de confirmación se genera, por ejemplo, cuando el módulo de identidad de abonado no ha conseguido registrarse de forma satisfactoria en la red usando los datos de identidad de abonado -13- conmutados. Un mensaje de confirmación se genera, por ejemplo, cuando la red ha enviado una consulta al módulo de identidad de abonado. Consultas de este tipo son, en particular, consultas del estado de red, informaciones de emplazamiento y/o informaciones de estado relativas a los perfiles de abonado -11-, generándose las confirmaciones mediante las funciones variables, es decir, el código de aplicación de gestión -9-.

La estrategia de gestión también puede prever que los mensajes de confirmación se le envíen a la instancia de red por comandos de gestión, iniciados por la red, sólo tras expirar un tiempo de espera, a fin de poder retrasar eventualmente los siguientes comandos de gestión de la red.

En una variante no representada en las figuras, el código de aplicación de gestión -9- aplica automáticamente un perfil de seguridad -11- antes de la recepción del comando de conmutación S2, siendo el perfil de seguridad -11- igual al perfil de abonado -11- activado. Si se recibe un comando de conmutación S2 de la instancia remota en el módulo de identidad de abonado -1- y se requiere una conmutación S5 inmediata a los segundos datos de identidad de abonado -13b-, se garantiza que sea posible en cualquier momento una reconmutación S11 a los primeros datos de identidad de abonado -13a- almacenados en el perfil de seguridad -11-.

En la figura 5 está representado el ciclo de vida de los datos de identidad de abonado -13-, es decir, de un juego de datos de identidad de abonado -13-, en un módulo de identidad de abonado -1-. Todo el ciclo de vida se gestiona mediante el código de aplicación de gestión -9- y las funciones de gestión estáticas -8-, en donde según la invención el código de aplicación de gestión -9- controla de forma variable la gestión, es decir, las segundas funciones. A este respecto, los datos de identidad de abonado -13- se almacenan en respuesta a un comando de carga en el espacio de almacenamiento -2- del módulo de identidad de abonado -1-. El comando de carga puede variar en función del

mecanismo de carga, de modo que el código de aplicación de gestión -9- variable gestiona de forma adaptativa el módulo de identidad de abonado -1-. Los datos de identidad de abonado -13- se activan mediante el comando de activación. A este respecto, una suma de comprobación CRC de los datos de identidad de abonado -13- cargados se compara con una suma de comprobación CRC proporcionada por la red antes de la activación. En caso de coincidencia de las sumas de comprobación, se activan los datos de identidad de abonado -13-. Desde este instante se pueden usar en el módulo de identidad de abonado -1-, por ejemplo, mediante el comando de conmutación S2 se puede conmutar a estos datos de identidad de abonado -13-. A este respecto, el código de aplicación de gestión -9- verifica si los datos de identidad de abonado -13- también están activados para una conmutación e impide la conmutación a datos de identidad de abonado inactivos. Si los datos de identidad de abonado -13- ya no han de poder usarse para una autentificación / identificación del abonado en una red, éstos se pueden desactivar mediante un comando de desactivación. Finalmente, los datos de identidad de abonado -13- se pueden borrar mediante un comando de borrado, mediante lo cual el espacio de almacenamiento -2- del módulo de identidad de abonado puede usarse para nuevos datos de identidad de abonado -13-.

Todo el módulo de identidad de abonado -1- se puede desactivar cuando se desactivan y/o borran los últimos datos de identidad de abonado que queden (es decir, el último juego de datos de identidad de abonado que hubiere) -13-. Dicha desactivación del módulo -1- se puede impedir mediante el código de aplicación de gestión -9- variable.

Lista de números de referencia

1	Módulo de identidad de abonado
2	Espacio de almacenamiento
3	Interfaz de datos
4	Unidad de cómputo
5	Sistema operativo
6	Entorno de tiempo de ejecución virtual, JCRE
7	Espacio seguro del fabricante del módulo
8	Funciones de gestión fijas
9	Código de aplicación de gestión Java variable
10	Interfaz de programación de gestión
11a,b,n	Perfiles de abonado, huecos de inserción de abonado
111	Espacio seguro del perfil
112	Código de aplicación individual al perfil
113	Sistema de archivos individual del perfil, datos de identidad de abonado
13a,b,n	Juegos de datos de identidad de abonado
S1-S12	Etapas del procedimiento

REIVINDICACIONES

1. Módulo de identidad de abonado (1) para la autentificación de un abonado en una red de comunicación, en el que el módulo de identidad de abonado (1) presenta:

- un primer juego de datos de identidad de abonado (13a) para la autentificación del abonado;

- al menos un segundo juego de datos de identidad de abonado (13b) para la autentificación del abonado, en el que el primer juego de datos de identidad de abonado (13a) se diferencia del segundo juego de datos de identidad de abonado (13b); y

- un medio para la gestión del primer juego de datos de identidad de abonado (13a) y del segundo juego de datos de identidad de abonado (13b), en el que la gestión se realiza mediante funciones de gestión estáticas (8);

caracterizado porque

- el medio para la gestión presenta además un código de aplicación de gestión (9) y éste código de aplicación de gestión (9) posibilita una gestión variable mediante adaptación de las funciones de gestión estáticas a los parámetros de entorno del módulo de identidad de abonado (1).

2. Módulo de identidad de abonado (1) según la reivindicación 1, en el que el código de aplicación de gestión (9) comprende primeras funciones (S6, S7, S8, S9, S10, S11), mediante las que es posible una conmutación variable entre el primer juego de datos de identidad de abonado (13a) y el segundo juego de datos de identidad de abonado (13b).

3. Módulo de identidad de abonado (1) según una de las reivindicaciones anteriores, en el que el código de aplicación de gestión (9) se puede actualizar y/o sustituir a través de una interfaz por aire de la red de comunicación.

4. Módulo de identidad de abonado (1) según una de las reivindicaciones anteriores, en el que las funciones de gestión estáticas (8) son segundas funciones y en el que las primeras funciones (S6, S7, S8, S9, S10, S11) del código de aplicación de gestión (9) acceden a estas segundas funciones mediante una interfaz de programación (10).

5. Módulo de identidad de abonado (1) según una de las reivindicaciones anteriores, en el que las primeras funciones (S6, S7, S8, S9, S10, S11) comprenden una supervisión de parámetros de emplazamiento (S7) actuales.

6. Módulo de identidad de abonado según una de las reivindicaciones anteriores, en el que las primeras funciones (S6, S7, S8, S9, S10, S11) comprenden una generación de periodos de espera (S8, S9).

7. Módulo de identidad de abonado (1) según una de las reivindicaciones anteriores, en el que las primeras funciones (S6, S7, S8, S9, S10, S11) comprenden una reconmutación (S11) adaptativa a los primeros datos de identidad de abonado (13a).

8. Módulo de identidad de abonado (1) según una de las reivindicaciones anteriores, en el que las funciones de gestión estáticas (8) son funciones de conmutación para la conmutación de los primeros datos de identidad de abonado (13a) a los segundos datos de identidad de abonado (13b).

9. Módulo de identidad de abonado (1) según una de las reivindicaciones anteriores, en el que el código de aplicación de gestión (9) es código de aplicación Java.

10. Procedimiento para la gestión de un módulo de identidad de abonado (1) con un primer juego de datos de identidad de abonado (13a) y un segundo juego de datos de identidad de abonado (13b), con las etapas de:

- recepción (S1) de un comando de gestión en el módulo de identidad de abonado (1);

- gestión (S5) del primer juego de datos de identidad de abonado (13a) y del segundo juego de datos de identidad de abonado (13b) mediante el comando de gestión;

caracterizado porque

- antes de la etapa de la gestión (S5) se inicia (S3) un código de aplicación de gestión (9) en el módulo de identidad de abonado (1);

- después de la etapa de la gestión (S5) realizada por el código de aplicación de gestión (9) se evalúan (S6, S8, S9, S10, S11) los parámetros de red de comunicación (S7); y

- en función de la evaluación (S6, S8, S9, S10, S11) se adapta (S11) la etapa de la gestión (S5) para adaptar la función de gestión estática a los parámetros de entorno del módulo de identidad de abonado (1).

11. Procedimiento según la reivindicación 10, en el que el código de aplicación de gestión (9) accede a las funciones de gestión estáticas (8) del módulo de identidad de abonado (1) a través de una interfaz de programación de gestión (10) para la etapa de la gestión (S5, S11).

12. Procedimiento según una de las reivindicaciones 10 u 11, en el que la evaluación (S6, S7, S8, S9, S10, S11) comprende el análisis del emplazamiento (S7).

13. Procedimiento según una de las reivindicaciones anteriores 10 a 12, en el que la gestión comprende tanto la conmutación, la carga, la activación, la desactivación, así como el borrado de los datos de identidad de abonado (13).

14. Uso de un módulo de identidad de abonado (1) según las reivindicaciones 1 a 9 en un terminal de comunicación móvil.

15. Sistema compuesto por el al menos un módulo de identidad de abonado (1) según las reivindicaciones 1 a 9 y una instancia remota, en el que la instancia remota envía un comando de conmutación (S2) al al menos un módulo de identidad de abonado (1) para la conmutación (S5) de un primer juego de datos de identidad de abonado (13a) a un segundo juego de datos de identidad de abonado (13b).

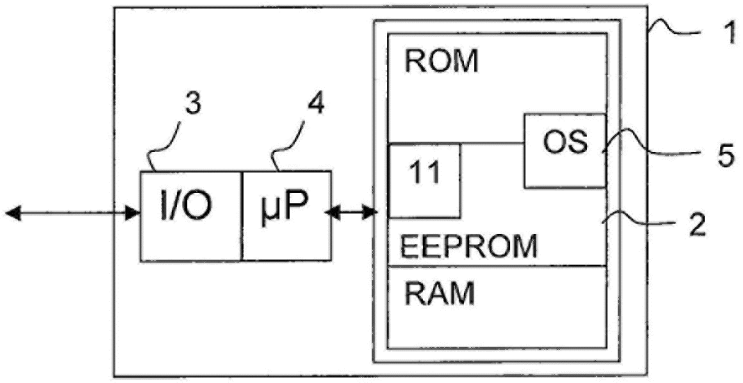

Fig. 1

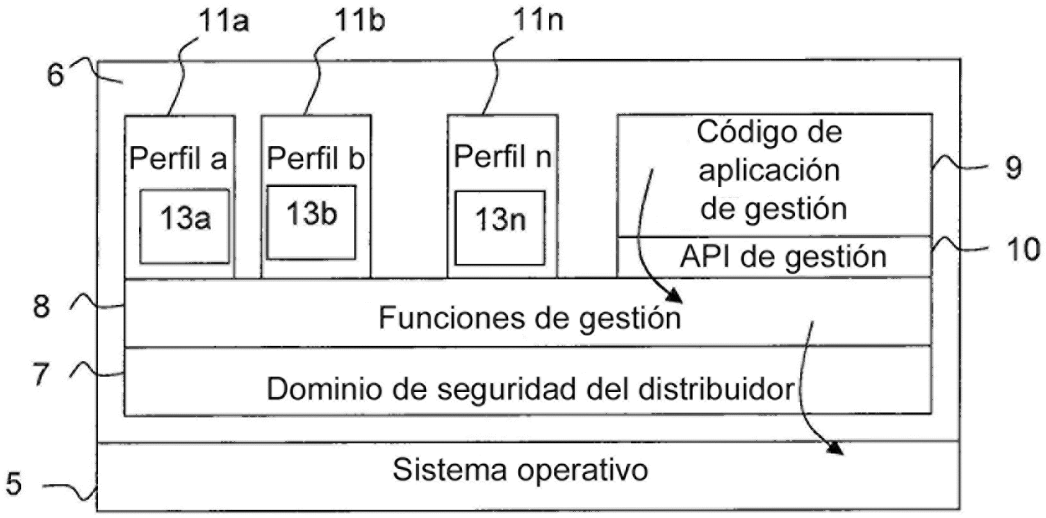

Fig. 2

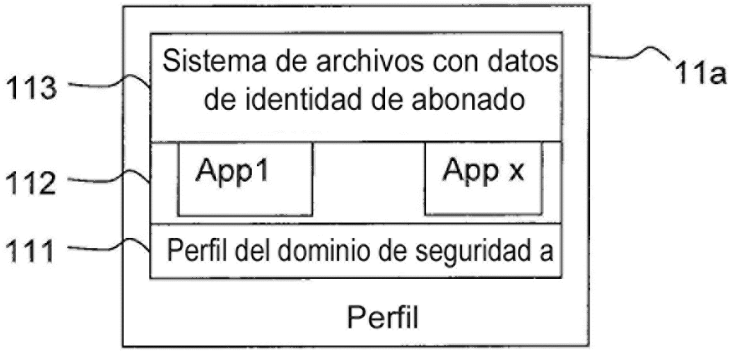

Fig. 3

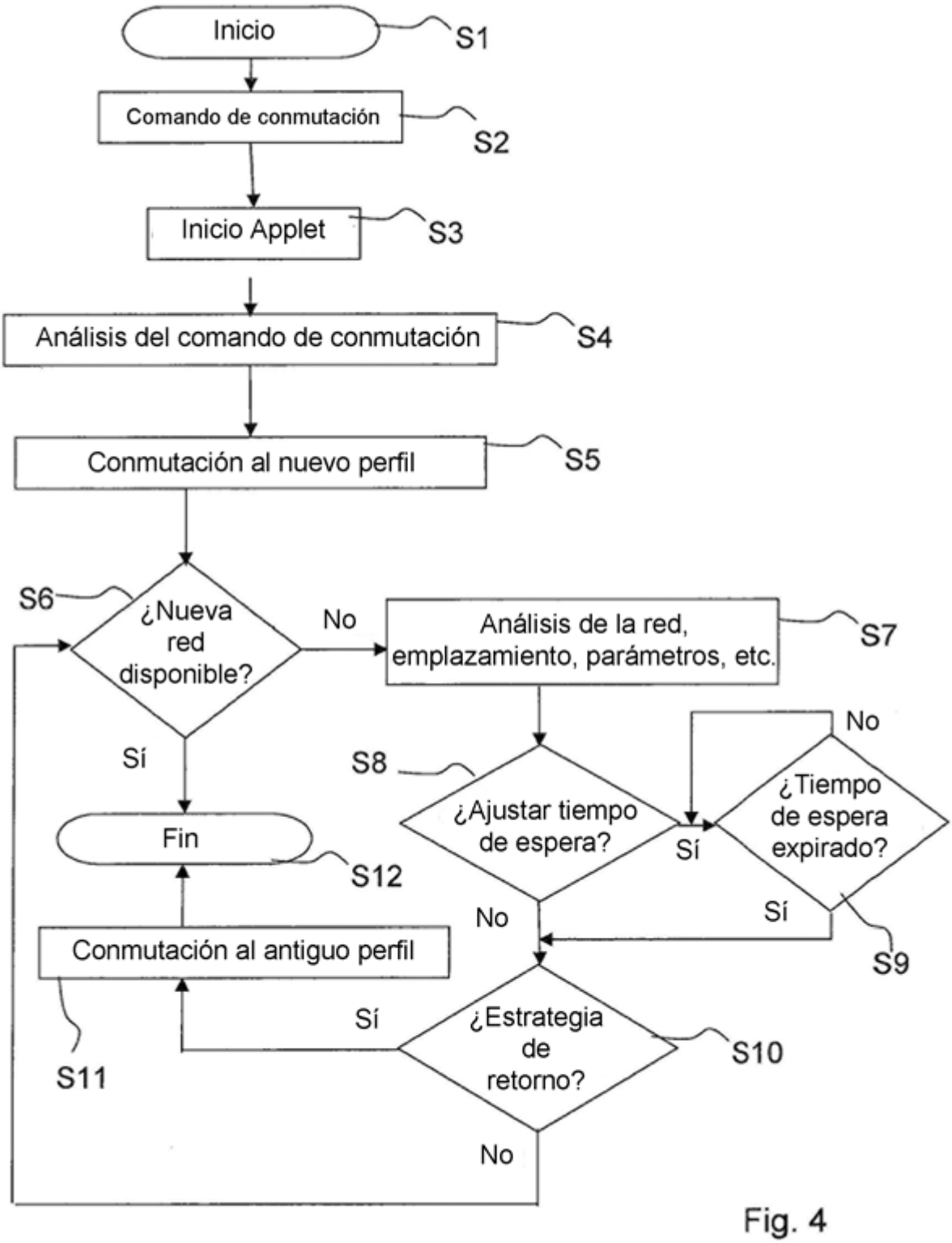
Inicio
S1
Comando de conmutación
S2
Inicio Applet
S3
Análisis del comando de conmutación
S4
Conmutación al nuevo perfil
S5
S6
¿Nueva red disponible?
No
Análisis de la red, emplazamiento, parámetros, etc.
S7
Sí
S8
¿Ajustar tiempo de espera?
Sí
No
¿Tiempo de espera expirado?
Sí
S9
No
Fin
S12
Conmutación al antiguo perfil
S11
Sí
¿Estrategia de retorno?
S10
No

Fig. 4

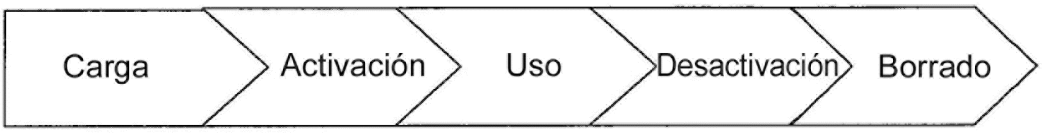

Fig. 5