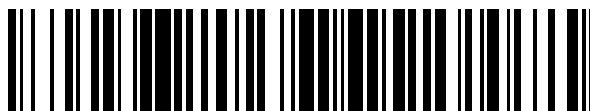


19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 675 770**

51 Int. Cl.:

H04W 12/06 (2009.01)

H04L 29/06 (2006.01)

H04W 8/26 (2009.01)

H04W 8/20 (2009.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **20.04.2009** **PCT/EP2009/002862**

87 Fecha y número de publicación internacional: **17.12.2009** **WO09149788**

96 Fecha de presentación y número de la solicitud europea: **20.04.2009** **E 09761351 (7)**

97 Fecha y número de publicación de la concesión europea: **11.04.2018** **EP 2281404**

54 Título: **Personalización de un SIM mediante un SIM Maestro personalizado inequívoco**

30 Prioridad:

29.05.2008 DE 102008025792

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

12.07.2018

73 Titular/es:

DEUTSCHE TELEKOM AG (100.0%)
Friedrich-Ebert-Allee 140
53113 Bonn, DE

72 Inventor/es:

NEUMANN, PETER y
PAGANO, GIULIO, LEOPOLDO

74 Agente/Representante:

ELZABURU, S.L.P

ES 2 675 770 T3

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

Personalización de un SIM mediante un SIM Maestro personalizado inequívoco

- 5 La invención se refiere a un procedimiento para la puesta en servicio y la personalización de un segundo módulo de identificación, en particular un SIM (*Subscriber Identity Module*), adicional, no personalizado, para el funcionamiento de un equipo terminal de radiotelefonía móvil, existiendo un primer módulo de identificación SIM Maestro (MasterSIM) que contiene un juego de datos personalizado.
- 10 Las tarjetas chip se utilizan, especialmente en la telecomunicación por radiotelefonía móvil, como en particular en las redes de radiotelefonía móvil celulares según el estándar GSM o el estándar UMTS, para una identificación inequívoca y segura de los abonados, así como para la puesta a disposición de distintas funciones especiales y servicios de valor añadido. Las tarjetas chip o aplicaciones de tarjeta chip denominadas UICC, SIM, USIM, R-UIM o también ISIM según la generación y el tipo del estándar de sistema en que se basan llevan con este fin una
- 15 pluralidad de parámetros especiales, claves secretas y otros elementos de los más diversos tipos, por ejemplo con datos del operador, datos del proveedor, datos del producto o datos del abonado. En resumen, estas tarjetas chip y aplicaciones de tarjeta chip se denominan módulo de identificación de abonado o SIM (*Subscriber Identity Module*).
- 20 Otros campos de aplicación de las tarjetas chip son las tarjetas de crédito, tarjetas de débito u otros módulos de identificación, en particular los provistos de chips de memoria integrados en los que está almacenado un juego de datos individual personalizado extraíble. Siempre que a continuación se hable de un juego de datos de abonado, un módulo de identificación de abonado o similar, quiere decirse en cada caso en general juego de datos o módulo de identificación o similar sin una limitación a una aplicación de la invención al campo de la técnica de radiotelefonía móvil. El campo de la técnica de radiotelefonía móvil y en particular la utilización de la invención para la
- 25 personalización de módulos de identificación de abonado de abonados de radiotelefonía móvil para el funcionamiento de equipos terminales de radiotelefonía móvil es solamente un campo de aplicación preferido en el que la invención puede emplearse de manera particularmente ventajosa. Sin embargo, la invención no está limitada a este campo.
- 30 Para la puesta en servicio de un equipo terminal móvil y la participación en el servicio de radiotelefonía móvil, un módulo de identificación de abonado SIM (abreviatura de la denominación inglesa habitual "Subscriber Identity Module") ha de dotarse de un juego de datos de abonado que en particular presente la identificación de abonado (IMSI). Hoy día, tales módulos de identificación de abonado SIM han sido dotados de antemano de los datos correspondientes por el operador de la red de radiotelefonía móvil, para poder identificar al usuario durante el uso de
- 35 los servicios de una red de radiotelefonía móvil. Un SIM no personalizado no es adecuado para la utilización en un equipo terminal de radiotelefonía móvil, es decir que el uso de los servicios de una red de radiotelefonía móvil no es posible con un SIM no personalizado. Los datos específicos, que son necesarios por una parte para el uso de los servicios y por otra parte para la liquidación de los servicios usados, deben identificar inequívocamente al usuario de la red de radiotelefonía móvil, para prevenir un uso indebido.
- 40 En este contexto, una desventaja es que para la utilización de una pluralidad de equipos es necesario un número creciente de tarjetas SIM. Así pues, deben asignarse a un usuario una pluralidad de tarjetas SIM o el usuario, para hacer funcionar distintos equipos terminales de radiotelefonía móvil, ha de cambiar la tarjeta SIM en cada caso entre los equipos, lo que es muy costoso e incómodo.
- 45 Actualmente ocurre que sólo el operador de la red de radiotelefonía móvil puede emitir nuevas tarjetas SIM, lo que acarrea un gran esfuerzo y un gran coste. También en otros campos la emisión de nuevas tarjetas chip está reservada al operador del sistema respectivo.
- 50 La solicitud de patente europea EP 1257106 A1 describe un procedimiento para la concesión de acceso para un equipo terminal de cliente a un módulo de abonado de un equipo terminal de comunicación de servidor, en el que en primer lugar se crea un enlace entre el equipo terminal de cliente y el equipo terminal de comunicación de servidor, a continuación se transmiten mediante este enlace datos relativos al módulo de abonado entre el equipo terminal de comunicación de servidor y el equipo terminal de cliente, después el módulo de abonado autentica el equipo terminal de cliente y finalmente, en función del resultado de la autenticación, se ponen a disposición los datos relativos al
- 55 módulo de abonado.
- 60 En la solicitud de patente europea EP 1 689 199 A1 se describe cómo distintos equipos terminales pueden compartir los datos de una tarjeta SIM, teniendo cada equipo terminal una tarjeta SIM propia, pero presentando un segundo equipo terminal una tarjeta SIM integrada –no extraíble (*built-in*)– y estableciendo el segundo equipo terminal con respecto a un primer equipo terminal un enlace de comunicación de campo próximo a través del cual el primer equipo terminal puede entonces conseguir acceso a la red de radiotelefonía móvil mediante la tarjeta SIM integrada del segundo equipo terminal.

Además, por la solicitud de EE.UU. 2008/0003982 A1 es conocido el conceder a un equipo terminal de cliente acceso a un módulo de identificación de un equipo terminal de servidor, estableciéndose en primer lugar un enlace de comunicación entre el equipo terminal de cliente y el equipo terminal de servidor, transmitiéndose del equipo terminal de servidor al equipo terminal de cliente mediante el enlace de comunicación datos del módulo de identificación relativos al abonado, realizando el módulo de identificación una autenticación del equipo terminal de cliente por medio de un procedimiento de autenticación basado en clave e iniciándose la transmisión de los datos específicos del abonado en virtud del resultado de este procedimiento. El procedimiento posibilita a un "equipo de control remoto" (*remote device = client communications terminal*) una utilización segura del módulo de identificación de otro equipo, para obtener acceso a información o funciones importantes, por ejemplo para conectarse a una red celular. En este contexto, los datos almacenados en el módulo de identificación pueden ser transmitidos del equipo terminal de cliente al equipo terminal de servidor, estando el módulo de identificación del equipo terminal de servidor en condiciones de autenticar una pluralidad de equipos terminales de cliente diferentes. Así pues, el módulo de identificación no autentica otros módulos de identificación, sino más bien equipos terminales. En este contexto, los datos específicos del abonado

El objetivo de la invención es poner a disposición un procedimiento para la puesta en servicio y la personalización de un módulo de identificación, especialmente de un módulo de identificación de abonado SIM para el funcionamiento de un equipo terminal de radiotelefonía móvil, que simplifique la administración, la producción y la utilización de módulos de identificación SIM personalizados.

Este objetivo se logra según la invención mediante un procedimiento según la reivindicación 1.

En las reivindicaciones subordinadas se indican perfeccionamientos ventajosos del procedimiento según la invención.

En el procedimiento según la invención para la puesta en servicio y la personalización de un segundo módulo de identificación, adicional, no personalizado, especialmente para el funcionamiento de un equipo terminal de radiotelefonía móvil, existiendo un primer módulo de identificación SIM Maestro que contiene un juego de datos personalizado, resulta especialmente ventajoso que se lleve o se lleven a cabo una autenticación y/o una comprobación del segundo módulo de identificación y que el juego de datos que ha de almacenarse en el segundo módulo de identificación para la personalización del segundo módulo de identificación sea leído por el primer módulo de identificación SIM Maestro, transmitido al segundo módulo de identificación y almacenado en este segundo módulo de identificación conteniendo en particular una o varias identificaciones de abonado definitivas inequívocas (IMSI).

En este contexto quiere decirse con la denominación "segundo módulo de identificación" no sólo un segundo módulo de identificación, en particular SIM, en sí, sino todo módulo de identificación adicional, dado que con el procedimiento según la invención es posible personalizar una pluralidad, es decir dependiendo de la especificación un número cualquiera, de módulos de identificación adicionales.

Así pues, ya sólo es necesario emitir por una parte un SIM Maestro personalizado, es decir un módulo de identificación o un módulo de identificación de abonado que contiene un juego de datos / juego de datos de abonado personalizado, estando este SIM Maestro equipado correspondientemente y siendo este SIM Maestro adecuado para poner a disposición datos, es decir el juego de datos / juego de datos de abonado personalizado, con el fin de, mediante este juego de datos / juego de datos de abonado, poner a disposición un segundo módulo de identificación, adicional, o un número cualquiera de módulos de identificación adicionales, en particular, así llamadas, tarjetas SIM adicionales, para el funcionamiento de equipos terminales de radiotelefonía móvil adicionales. Así pues, el SIM Maestro crea, por decirlo así, copias de SIM, especialmente para el funcionamiento de equipos terminales de radiotelefonía móvil, pudiendo el SIM Maestro y los SIM adicionales diferenciarse en particular por el hecho de que no es posible crear de nuevo una copia de un SIM adicional, sino que para ello sólo es adecuado el SIM Maestro. Esto puede garantizarse haciendo que el SIM Maestro se dote de una característica o aptitud para la autenticación especial.

Siempre que en el marco de esta descripción o de las reivindicaciones se hable de un juego de datos de abonado, un módulo de identificación de abonado o similar, quiere decirse en cada caso en general juego de datos o módulo de identificación o similar sin una limitación a una aplicación de la invención al campo de la técnica de radiotelefonía móvil. Con la denominación SIM, que es conocida y habitual como abreviatura del concepto inglés "Subscriber Identity Module" para módulo de identificación de abonado, no se realiza ninguna limitación al campo de la comunicación móvil. Se pretende que la abreviatura SIM, o los términos compuestos que contengan la abreviatura SIM, comprenda o comprendan más bien todo tipo de módulo de identificación que presente un juego de datos individual legible o extraíble. El campo de la técnica de radiotelefonía móvil y en particular la utilización de la invención para la personalización de módulos de identificación de abonado de abonados de radiotelefonía móvil para el funcionamiento de equipos terminales de radiotelefonía móvil es solamente un campo de aplicación preferido en el que la invención puede emplearse de manera particularmente ventajosa. Sin embargo, la invención no está limitada a este campo.

Este SIM Maestro puede entonces servir de modelo para todas las demás autenticaciones futuras para tarjetas SIM o equipos terminales de radiotelefonía móvil adicionales con una SIM instalada fijamente, poniéndose al usuario mediante su SIM Maestro en situación de llevar a cabo él mismo la personalización de uno o varios módulos de identificación o módulos de identificación de abonado SIM adicionales.

Existe además la posibilidad de que un primer módulo de identificación SIM Maestro (MSIM) contenga varias identificaciones de abonado (IMSI) y éstas se utilicen para la puesta en servicio y personalización de varios módulos de identificación (VSIM) no personalizados.

Preferiblemente, un módulo de identificación (VSIM) originalmente no personalizado puede también, tras una primera personalización, repersonalizarse varias veces, bien mediante el mismo SIM Maestro (MSIM) original con un juego de datos igual o modificado, bien mediante otro SIM Maestro (MSIM).

Preferiblemente pueden también modificarse sólo partes del juego de datos en los módulos de identificación (VSIM) personalizados, especialmente modificando sólo las identificaciones de abonado (IMSI).

En este contexto, el juego de datos puede transmitirse mediante un radioenlace (por ejemplo OTA *Over-The-Air*) u otro enlace a un dispositivo de lectura/escritura que aloje el segundo SIM o, como alternativa, este juego de datos puede transmitirse dentro de un dispositivo de lectura/escritura que aloje tanto el SIM Maestro como el segundo SIM.

Para la protección del procedimiento, preferiblemente se lleva o se llevan a cabo, antes de llevar a cabo la personalización y la transmisión del juego de datos / juego de datos de abonado del SIM Maestro, una comprobación y/o autenticación del número de serie del segundo SIM y/o del equipo terminal de radiotelefonía móvil por medio del número de identificación de equipo (IMEI), mediante el cual el equipo terminal de radiotelefonía móvil puede identificarse de forma inequívoca, y/o una comprobación de parámetros de seguridad del segundo SIM.

De este modo puede garantizarse que sólo se personalicen los módulos de identificación / módulos de identificación de abonado SIM aún no personalizados que estén previstos para ello, con el fin de prevenir un uso indebido.

Además, como alternativa o de forma acumulativa, para la protección del procedimiento puede o pueden llevarse a cabo, antes de llevar a cabo la personalización y la transmisión del juego de datos / juego de datos de abonado del SIM Maestro, una comprobación y/o una autenticación del SIM Maestro mismo.

De este modo puede aumentarse aún más la seguridad del procedimiento, es decir que en particular no es posible crear, por decirlo así, una copia de cualquier SIM, es decir por ejemplo de cualquier módulo de identificación de abonado para una red de radiotelefonía móvil, sino que esto está realmente reservado a los, así llamados, SIM Maestros.

Así pues, preferiblemente queda excluido crear, por decirlo así, una copia de cualquier módulo de identificación / módulo de identificación de abonado SIM. En este contexto, quiere decirse con "copia" que si bien varios módulos de identificación / módulos de identificación de abonado SIM presentan un número de serie (ICCID) individual respectivo, por lo demás presentan un juego de datos / juego de datos de abonado idéntico para la identificación del abonado de la red de radiotelefonía móvil.

Así pues, mediante la introducción de un SIM Maestro en el sentido de la invención, que se utiliza para personalizar módulos de identificación / módulos de identificación de abonado SIM adicionales, se pone a disposición por una parte un SIM Maestro de una generación parental, mediante el cual pueden crearse una pluralidad de descendientes directos de una generación filial, pero preferiblemente queda excluido crear módulos de identificación de abonado de una segunda generación filial, dado que esto es posible siempre exclusivamente utilizando el SIM Maestro, pero no utilizando un SIM cualquiera y, por lo tanto, tampoco un descendiente del SIM Maestro. De este modo puede ponerse a disposición un procedimiento muy seguro para la personalización de módulos de identificación de abonado SIM adicionales. Por lo tanto, en esta configuración, sólo utilizando un SIM Maestro es posible personalizar un segundo SIM, pero no mediante un SIM cualquiera, como en particular un descendiente del SIM Maestro.

Preferiblemente, el número de serie del segundo SIM se almacena en el SIM Maestro, es decir que preferiblemente se almacena en cada caso en el SIM Maestro una base de datos completa de todas las personalizaciones llevadas a cabo y los números de serie de los descendientes. Preferiblemente, como alternativa o de forma acumulativa, se almacena en el SIM Maestro la fecha de una personalización llevada a cabo de cada módulo de identificación de abonado SIM adicional.

Preferiblemente, el juego de datos / juego de datos de abonado generado durante la personalización y los datos de usuario o datos de abonado correspondientes, en particular el número de serie (ICCID) del segundo SIM, se almacenan en el registro de posiciones base (HLR *Home Location Register*) de la red de radiotelefonía móvil. De

este modo se garantiza una asignación inequívoca de los datos de abonado al usuario respectivo de la red de radiotelefonía móvil.

Preferiblemente se transmite el número de serie (ICCID) del segundo SIM mediante el SIM Maestro a un registro de posiciones base (HLR *Home Location Register*) de la red de radiotelefonía móvil, pudiendo el número de serie del segundo SIM almacenarse entonces en el mismo. Si el número de serie del segundo SIM se transmite al HLR exclusivamente mediante el SIM Maestro, está garantizado que realmente sólo sea posible una personalización de SIM adicionales mediante el SIM Maestro, dado que por otro lado se excluye un inicio de sesión de un SIM adicional en el registro de posiciones base HLR de la red de radiotelefonía móvil. De este modo se logra un aumento adicional de la seguridad del procedimiento y se previene un uso indebido.

Preferiblemente, la transmisión de datos de un juego de datos / juego de datos de abonado del SIM Maestro al segundo SIM se realiza mediante un enlace de datos protegido y en particular la transmisión de datos puede realizarse de manera codificada.

Preferiblemente, una vez recibido y almacenado el juego de datos / juego de datos de abonado en el segundo SIM, se transmite una confirmación al SIM Maestro y/o a la red de radiotelefonía móvil, en particular al registro de posiciones base HLR de la red de radiotelefonía móvil.

Así pues, para la puesta en servicio y la personalización de un módulo de identificación / módulo de identificación de abonado SIM no personalizado, el usuario, es decir por ejemplo el abonado en una red de radiotelefonía móvil, solamente ha de adquirir una única vez un SIM Maestro (MSIM), conteniendo el SIM Maestro una identificación / identificación de abonado inequívoca con un juego de datos / juego de datos de abonado personalizado y presentando además el SIM Maestro parámetros de autenticación correspondientes para una multiplicación. Este SIM Maestro (MSIM) inequívoco puede entonces servir de modelo para una multiplicación para todas las autenticaciones y personalizaciones futuras de módulos de identificación / módulos de identificación de abonado SIM adicionales, independientemente de que se trate de SIM extraíbles como tarjetas o, por ejemplo, SIM instalados fijamente en un equipo terminal de radiotelefonía móvil.

En una forma de utilización preferida del procedimiento según la invención, el primer y/o el segundo módulo de identificación se trata o se tratan de un módulo de identificación de usuario o de un módulo de identificación de abonado para el funcionamiento de un equipo terminal de radiotelefonía móvil.

El juego de datos se trata preferiblemente de un juego de datos de abonado de un usuario de radiotelefonía móvil.

A continuación se explica por medio de las figuras una posible utilización y configuración de la invención. Se muestran:

La Figura 1, el esquema de transmisión de datos de un SIM Maestro MSIM a un descendiente VSIM como SIM adicional;

La Figura 2, un esquema de principio de la transmisión de datos de un SIM Maestro MSIM por radio a un equipo terminal de radiotelefonía móvil con un descendiente VSIM.

Está representado un ejemplo de utilización de la invención en relación con la técnica de radiotelefonía móvil, en el que se emplean módulos de identificación en forma de módulos de identificación de abonado para el funcionamiento de un equipo terminal de radiotelefonía móvil, así llamadas tarjetas SIM (inglés: *Subscriber Identity Module*, abreviado SIM).

El SIM Maestro MSIM se trata de un primer módulo de identificación de abonado SIM Maestro MSIM, que sirve de modelo para todos los módulos de identificación de abonado adicionales VSIM por personalizar del usuario de la red de radiotelefonía móvil. A este respecto puede personalizarse un número predefinido o también un número cualquiera de módulos de identificación de abonado no personalizados adicionales, es decir que se personalizan SIM virtuales VSIM utilizando el SIM Maestro MSIM.

Para ello, mediante cualesquiera circuitos de comercialización, se ofrecen cierto número de tarjetas SIM nuevas y sin usar o también ya usadas o equipos terminales de radiotelefonía móvil con tarjeta SIM integrada nuevos y sin usar o también ya usados. La inicialización y la personalización son realizadas entonces por el usuario de la red de radiotelefonía móvil utilizando el SIM Maestro MSIM inequívoco.

En este contexto queda excluido un uso indebido de los SIM virtuales VSIM aún no personalizados, dado que, sin una personalización efectuada previamente, éstos no son adecuados para el funcionamiento de un equipo terminal de radiotelefonía móvil, de manera que se previene eficazmente un uso indebido.

Por otra parte, el SIM Maestro no ha de ser utilizado necesariamente por el usuario, sino que puede almacenarse en un lugar seguro, por ejemplo en una caja fuerte o en otro lugar seguro, dado que el SIM Maestro no ha de utilizarse

necesariamente para el funcionamiento de un equipo terminal de radiotelefonía móvil, sino que se requiere solamente para la personalización de módulos de identificación de abonado adicionales, es decir SIM virtuales VSIM. De este modo pueden prevenirse eficazmente una pérdida y un posible uso indebido del SIM Maestro, dado que para el funcionamiento de equipos terminales de radiotelefonía móvil han de utilizarse solamente descendientes VSIM.

Para la puesta en servicio y la personalización de un segundo módulo de identificación de abonado VSIM adicional y no personalizado, se conectan entre sí el SIM Maestro MSIM y el SIM virtual VSIM mediante unos medios técnicos correspondientes. Éstos pueden tratarse de un aparato especial en el que se inserten ambas tarjetas SIM. Como alternativa, también es posible establecer un radioenlace entre el SIM Maestro MSIM y el SIM adicional VSIM por personalizar mediante un enlace preferiblemente protegido.

La tarjeta que se ha de inicializar y personalizar debe presentar preferiblemente un determinado certificado, de manera que sean posibles una comprobación y una autorización mediante el MSIM para prevenir un uso indebido. Este certificado es necesario para garantizar un funcionamiento seguro y una realización segura del procedimiento y para garantizar información privada, es decir el juego de datos de abonado del SIM Maestro MSIM, antes de la transmisión del juego de datos de abonado del SIM Maestro MSIM al descendiente VSIM, y prevenir un uso indebido. Con este fin, antes de leer y transmitir al descendiente VSIM los datos del SIM Maestro MSIM, se ejecuta una rutina de inicialización llevando a cabo una comprobación y una autenticación del segundo SIM por personalizar y llevando a cabo además por otra parte una autenticación del SIM Maestro.

También es posible implementar el número de serie del equipo terminal de radiotelefonía móvil que aloja el descendiente VSIM, como está representado esquemáticamente en las Figuras 1 y 2.

También es posible comprobar si la tarjeta chip VSIM por inicializar y personalizar ya estaba en uso o si esa tarjeta SIM es nueva.

También de este modo es posible prevenir un uso indebido.

Como está representado en la Figura 1, el SIM Maestro MSIM dirige una consulta protegida 10 al módulo de identificación de abonado VSIM por inicializar. A continuación se transmite el número de serie del VSIM 20 de vuelta al SIM Maestro MSIM. Una vez realizadas la autenticación y la identificación del VSIM mediante una comprobación del número 20 de serie, se transmiten a continuación los datos 30 de abonado del SIM Maestro MSIM al VSIM y se almacenan los mismos en este último, en el chip 5 de memoria. La comunicación 40 entre el SIM Maestro MSIM y el VSIM por inicializar y personalizar se realiza mediante un enlace protegido.

Como está representado esquemáticamente en la Figura 2, también es posible establecer, mediante un radioenlace protegido, una comunicación con un equipo terminal de radiotelefonía móvil que contenga el SIM VSIM por inicializar. También en este caso se trata de un enlace protegido y el equipo terminal de radiotelefonía móvil es correspondientemente adecuado y está equipado para escribir en un SIM el juego de datos de abonado individual recibido, es decir almacenar el juego de datos de abonado en el VSIM.

Siempre que la rutina de inicialización se haya ejecutado satisfactoriamente y el certificado se haya identificado como válido, la información de abonado individual, es decir el juego de datos de abonado individual, se transmite por consiguiente, como está representado esquemáticamente en las Figuras 1 y 2, del SIM Maestro MSIM al descendiente VSIM por inicializar y personalizar y se almacena en éste. A la inversa, el número de serie del VSIM se almacena en el SIM Maestro MSIM para poder reconstruir en todo momento mediante el SIM Maestro MSIM las inicializaciones, puestas en servicio y personalizaciones de SIM adicionales llevadas a cabo.

Si se pierde o se destruye un descendiente VSIM, pueden utilizarse los datos correspondientes para bloquear tal descendiente VSIM dentro de la red con respecto a su posterior uso.

Un VSIM nuevamente personalizado recibe un número de identificación combinado en forma de un número de identificación de red que contiene por una parte el número de identificación de equipo (IMEI) y además una parte numérica secreta procedente del SIM Maestro MSIM. Así pues, el número de serie del VSIM puede considerarse como una clave pública, que se combina con una clave secreta obtenida del SIM Maestro.

Con este fin, el SIM Maestro está preferiblemente equipado para presentar un campo preprogramado en el que pueden almacenarse números utilizados para la personalización. Estos campos han de mantenerse secretos y se transmiten a un VSIM sólo de un modo seguro, siendo imposible una lectura o una detección de los números, dado que estos números se utilizan como parte secreta de la clave del VSIM. De este modo son posibles una utilización y una asignación inequívocas entre el SIM Maestro MSIM y módulos de identificación de abonado adicionales VSIM que hayan sido personalizados utilizando el SIM Maestro.

Una vez llevada a cabo satisfactoriamente la personalización, puede integrarse el VSIM en un equipo terminal de radiotelefonía móvil y es posible usar a continuación este equipo terminal de radiotelefonía móvil utilizando el VSIM personalizado, es decir que está garantizada la identificación del abonado mediante el VSIM y su identidad en forma del número de serie del VSIM, así como del juego de datos de abonado.

- 5 Así pues, es posible, utilizando el SIM Maestro MSIM, producir una pluralidad de descendientes VSIM y por lo tanto utilizar una pluralidad de equipos terminales de radiotelefonía móvil también con una identificación de abonado idéntica.

REIVINDICACIONES

1. Procedimiento para la puesta en servicio y la personalización de un segundo módulo de identificación (VSIM), no personalizado, para el funcionamiento de un equipo terminal de radiotelefonía móvil en una red de radiotelefonía móvil utilizando un primer módulo de identificación (MSIM) que contiene un juego de datos personalizado con una o varias identificaciones de abonado (IMSI) definitivas inequívocas, en el que se lleva o se llevan a cabo una autenticación y/o una comprobación del segundo módulo de identificación (VSIM), se lee el juego de datos del primer módulo de identificación (MSIM), se transmite el juego de datos al segundo módulo de identificación (VSIM), para la personalización, y se almacena el juego de datos en este último, **caracterizado por que** el juego de datos leído y los datos de usuario o datos de abonado correspondientes y el número de serie del segundo módulo de identificación (VSIM) se almacenan en un registro de posiciones base (HLR) de la red de radiotelefonía móvil.
2. Procedimiento según la reivindicación 1, **caracterizado por que** el primer módulo de identificación (MSIM) contiene varias identificaciones de abonado (IMSI) y éstas se utilizan para la puesta en servicio y la personalización de varios módulos de identificación (VSIM) no personalizados.
3. Procedimiento según la reivindicación 1 ó 2, **caracterizado por que** un segundo módulo de identificación (VSIM) originalmente no personalizado se repersonaliza dos o más veces después de una primera personalización, bien mediante el mismo primer módulo de identificación (MSIM) original con un juego de datos igual o modificado, bien mediante otro primer módulo de identificación (MSIM).
4. Procedimiento según la reivindicación 3, **caracterizado por que** sólo se modifican partes del juego de datos del segundo módulo de identificación (VSIM) personalizado.
5. Procedimiento según una de las reivindicaciones precedentes, **caracterizado por que** el juego de datos se transmite mediante un radioenlace (OTA) a un dispositivo de lectura y escritura que contiene el segundo módulo de identificación (VSIM) o dentro de un dispositivo de lectura y escritura que aloja tanto el primer módulo de identificación (MSIM) como el segundo módulo de identificación (VSIM).
6. Procedimiento según una de las reivindicaciones precedentes, **caracterizado por que**, antes de llevar a cabo la personalización y la transmisión del juego de datos del primer módulo de identificación (MSIM), se lleva o se llevan a cabo una comprobación y/o una autenticación del número de serie (ICCID) del segundo módulo de identificación (VSIM) y/o de un equipo terminal de radiotelefonía móvil por medio del número de identificación de equipo (IMEI), mediante el cual el equipo terminal de radiotelefonía móvil puede identificarse de forma inequívoca, y/o una comprobación de parámetros de seguridad del segundo módulo de identificación (VSIM).
7. Procedimiento según una de las reivindicaciones precedentes, **caracterizado por que**, antes de llevar a cabo la personalización y la transmisión del juego de datos del primer módulo de identificación (MSIM), se lleva o se llevan a cabo una comprobación y/o una autenticación del primer módulo de identificación (MSIM).
8. Procedimiento según una de las reivindicaciones precedentes, **caracterizado por que** el número de serie (ICCID) del segundo módulo de identificación (VSIM) se almacena en el primer módulo de identificación (MSIM).
9. Procedimiento según una de las reivindicaciones precedentes, **caracterizado por que** la fecha de una personalización del segundo módulo de identificación (VSIM) llevada a cabo se almacena en el primer módulo de identificación (MSIM).
10. Procedimiento según una de las reivindicaciones precedentes, **caracterizado por que** el número de serie (ICCID) del segundo módulo de identificación (VSIM) es transmitido mediante el primer módulo de identificación (MSIM) al registro de posiciones base (HLR) de la red de radiotelefonía móvil y almacenado en éste.
11. Procedimiento según una de las reivindicaciones precedentes, **caracterizado por que** la transmisión de datos del juego de datos del primer módulo de identificación (MSIM) al segundo módulo de identificación (VSIM) se realiza mediante un enlace de datos protegido.
12. Procedimiento según una de las reivindicaciones precedentes, **caracterizado por que**, una vez recibido y almacenado el juego de datos en el segundo módulo de identificación (VSIM), se transmite una confirmación al primer módulo de identificación (MSIM) y/o a la red de radiotelefonía móvil.
13. Procedimiento según una de las reivindicaciones precedentes, **caracterizado por que** el primer y/o el segundo módulo de identificación (MSIM, VSIM) se trata o se tratan de un módulo de identificación de usuario o de un módulo de identificación de abonado (VSIM) para el funcionamiento de un equipo terminal de radiotelefonía móvil.
14. Procedimiento según una de las reivindicaciones precedentes, **caracterizado por que** el juego de datos se trata de un juego de datos de abonado de un usuario de radiotelefonía móvil.

15. Procedimiento según la reivindicación 4, **caracterizado por que** sólo se modifica la identificación de abonado (IMSI).

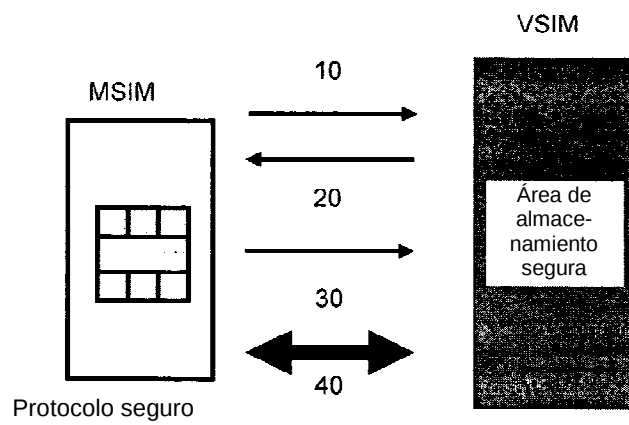


Fig. 1

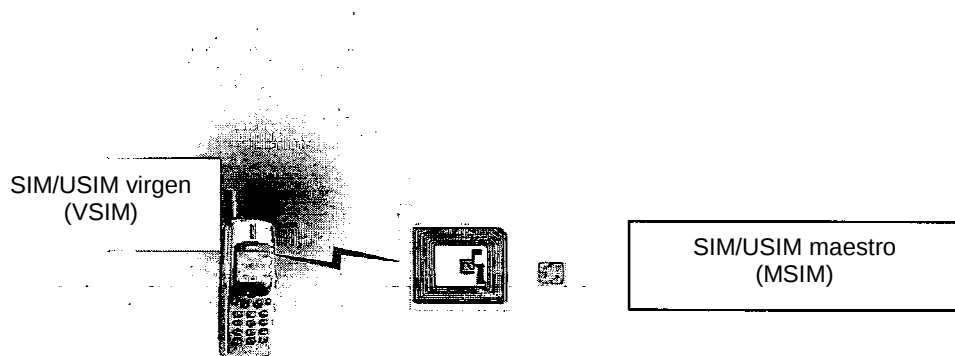


Fig 2