(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 721 307**

(51) Int. CI.:

G06F 21/62 (2013.01)
H04W 8/18 (2009.01)
H04W 12/08 (2009.01)
H04W 4/50 (2008.01)
H04W 4/60 (2008.01)
H04W 8/20 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **21.02.2013 PCT/EP2013/053465**

(87) Fecha y número de publicación internacional: **29.08.2013 WO13124358**

(96) Fecha de presentación y número de la solicitud europea: **21.02.2013 E 13707582 (6)**

(97) Fecha y número de publicación de la concesión europea: **21.11.2018 EP 2817989**

(54) Título: **Método de personalización de un elemento de seguridad que coopera con un equipo**

(30) Prioridad:

21.02.2012 EP 12305197

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
30.07.2019

(73) Titular/es:

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

(72) Inventor/es:

TUILIER, EDMOND y
QUIRICONI, JEAN-RÉMI

(74) Agente/Representante:

CASANOVAS CASSÁ, Buenaventura

DESCRIPCION

Método de personalización de un elemento de seguridad que coopera con un equipo.

El campo de la invención es el de las telecomunicaciones y se refiere en particular a un método para personalizar un elemento de seguridad que coopera con un equipo, tal como una máquina. Se entiende por personalización de un elemento de seguridad la descarga de datos confidenciales en el elemento de seguridad que permite diversificarlo de los otros elementos de seguridad y así garantizar la singularidad de los secretos e identificadores cargados en cada elemento de seguridad.

El elemento de seguridad es típicamente una tarjeta tipo SIM (en GSM) o USIM (en UMTS), genéricamente llamada UICC, destinada a cooperar con un equipo. El elemento de seguridad no tiene que ser necesariamente extraíble del equipo, tal como una tarjeta SIM convencional, y puede cooperar con este equipo (o con la parte del módem que forma parte de este equipo). Este elemento de seguridad también puede igualmente presentarse en forma de un circuito integrado soldado en un dispositivo (o en cooperación con un equipo), en el caso de aplicaciones M2M (Máquina a Máquina), el elemento de seguridad se llama e-UICC y realiza las mismas funciones que una tarjeta UICC clásica. Aquí se entiende por "funciones" la autenticación del abonado en una red de telecomunicaciones, por ejemplo celular, lo que permite establecer de manera segura comunicaciones con los elementos conectados a la red del operador. Dicho elemento de seguridad incluye, en particular, una IMSI (International Mobile Subscriber Identity) y una clave Ki que le permite autenticarse en la red del operador. La IMSI y la clave Ki son, en el resto de esta descripción, datos relacionados con una suscripción a una red de un operador de radiotelefonía móvil y son parte de los elementos de seguridad de la suscripción.

El equipo puede ser un terminal de telecomunicaciones como un teléfono portátil, una tableta digital o un teléfono inteligente. También puede tratarse de una máquina más grande, tal como un vehículo automóvil, un contador (de gas o electricidad, por ejemplo), un dispensador de bebidas que en este caso está equipado con un módem de comunicación (GSM o UMTS).

Generalmente, cuando una persona desea suscribirse a un operador, se dirige a un centro de ventas del operador quien, después de solicitar los documentos relacionados con su cuenta bancaria y su lugar de residencia, le da una tarjeta UICC. La tarjeta UICC ya contiene los identificadores que le permiten conectarse casi inmediatamente a la red del operador (el HLR del operador está pre-aprovisionado con estos identificadores).

El inconveniente de esta solución es que requiere el desplazamiento del usuario a un punto de venta de suscripción del operador de radiotelefonía móvil.

Además, esta solución no es aplicable en el caso de que el elemento de seguridad esté integrado de manera fija en un dispositivo, ya que el elemento de seguridad no es insertable en el equipo puesto que es solidario.

Ocurre lo mismo en la solución descrita en la solicitud. WO 93/07697.

Para este propósito, la presente invención propone un método de personalización de un elemento de seguridad que coopera con un equipo, consistente esta personalización en descargar datos relacionados con una suscripción a una red de un operador de radiotelefonía móvil en este elemento de seguridad, consistente el método en:

i- conectar el equipo a un lector de tarjetas;
ii- leer en una tarjeta conectada al lector de tarjeta los datos del operador correspondientes a al menos una suscripción a una red de un operador de radiotelefonía móvil;
iii- transmitir los datos del operador desde el lector a una red del operador;
iv- transmitir desde la red del operador a un administrador de suscripciones una solicitud de transferencia de los datos relacionados con la suscripción a la red del operador de radiotelefonía móvil;
v- transmitir desde el administrador de suscripciones al elemento de seguridad los datos relacionados con la suscripción a la red del operador de radiotelefonía móvil.

Ventajosamente, la etapa -v- consiste en transmitir los datos relacionados con la suscripción a la red del operador de radiotelefonía móvil por medio del lector de tarjetas.

Alternativamente, la etapa -v- consiste en transmitir los datos relacionados con la suscripción a la red del operador de radiotelefonía móvil por medio de la red de Internet a la que está conectado el lector de tarjetas por medio de un ordenador.

La etapa -ii- está precedida preferiblemente por una etapa de verificación de un código de seguridad.

En una implementación ventajosa del método de acuerdo con la invención, la etapa -i- es implementada por un instalador y el método consiste en proponer al instalador varias suscripciones diferentes, eligiendo el instalador por medio de la interfaz hombre-máquina del lector de tarjetas una de las suscripciones propuestas.

El método de acuerdo con la invención puede ser implementado igualmente por un revendedor de tarjetas o un usuario final de la máquina y el código de seguridad corresponde entonces a un código de transferencia de un operador de radiotelefonía móvil.

Otras características y ventajas de la invención aparecerán al leer la siguiente descripción de dos realizaciones de la invención, dadas a título ilustrativo y no limitativo, y las figuras adjuntas que representan dos sistemas que implementan el método según la presente invención, en la que:

- La figura 1 representa un sistema de personalización según la invención en el que la personalización de un elemento de seguridad es realizada por un integrador;
- la figura 2 representa un sistema de personalización según la invención en el que la personalización de un elemento de seguridad es realizada por un usuario final o un vendedor de equipos.

La figura 1 representa un sistema de personalización según la invención en el que la personalización de un elemento de seguridad es realizada por un integrador.

El sistema de personalización de la figura 1 está destinado a personalizar un elemento de seguridad 10, constituido aquí por una e-UICC que coopera con una máquina o un equipo 11. El equipo 11 está aquí constituido por un contador de electricidad o gas que incorpora la e-UICC. La personalización del contador 11 es realizada aquí por un integrador o instalador que dispone de una tarjeta personal 13. Típicamente, este integrador instala físicamente el contador 11 en el domicilio de un particular o de una empresa y la e-UICC no incluye datos que le permiten conectarse a una red de un operador de radiotelefonía móvil.

La personalización del elemento de seguridad 10 consiste, en primer lugar, en conectar el contador 11 a un lector de tarjetas 12 o a un equipo que contiene un lector de tarjetas 12 en el que el integrador puede insertar su tarjeta personal 13. La tarjeta 13 es una tarjeta de tipo PKI que permite autenticar a su operador gracias a un certificado único, proporcionado por su compañía o por un operador. La tarjeta 13 del integrador puede comprender una pluralidad de conjuntos de datos del operador que ofrecen la autorización para contactar con los administradores de suscripciones (SM-SR como se describirá más adelante) del operador. Esta autorización dará la posibilidad de descargar los conjuntos IMSI/Ki correspondientes a las suscripciones de varios operadores de radiotelefonía móvil. Esta tarjeta 13 puede igualmente contener directamente los conjuntos IMSI/Ki correspondientes a las suscripciones de varios operadores.

Después de haber verificado eventualmente un código de seguridad (por ejemplo, un código de cuatro dígitos) introducido por el integrador en el teclado del lector 12, el lector 12 o lee en la tarjeta 13 los datos del operador correspondientes a al menos una suscripción a una red de un operador de radiotelefonía móvil, o interroga a la tarjeta 13 para obtener la autorización para contactar al administrador de suscripciones SM-SR del operador seleccionado.

Como se indicó anteriormente, pueden proporcionarse varios operadores en la tarjeta 13, pudiendo contener cada operador proporcionado un enlace de contacto SM-SR o la suscripción misma. El integrador puede entonces elegir el operador con la red desde la cual la e-UICC podrá entrar en comunicación. En otro modo de implementación, el integrador dispone de varias tarjetas, cada una de las cuales conteniendo datos de un solo operador. Por ejemplo, en Francia, el integrador dispondrá así de una tarjeta para el operador Orange, otra para el operador Bouygues, otra para el operador Free y otra para el operador SFR. Como otro ejemplo, en Francia un integrador dispondría de una única tarjeta que incluiría las 4 IMSI/Ki de Bouygues, Orange, SFR y Free.

El lector 12 incluye un módem capaz de transmitir los datos del operador leídos en la tarjeta 13 a una red de operador 14. Este lector 12 típicamente comprende una interfaz M2M, es decir, una e-UICC y un módem asociado. La red del operador 14 puede ser cualquiera.

Durante una etapa 15, la red del operador 14 transmite a un administrador de suscripciones 16 (denominado SM-SR de Subscription Management - Subscription Routing) una solicitud de transferencia de los datos relacionados con la suscripción seleccionada.

El administrador de suscripciones 16 transmite entonces, durante una etapa 17, los datos relacionados con la suscripción seleccionada, al operador 14. Como se indicó anteriormente, estos datos corresponden a un perfil de operador completo, incluyendo particular mente la pareja IMSI/Ki a cargar en el elemento de seguridad 10 con el fin de que pueda comunicarse con la red del operador seleccionado.

La transmisión de los datos relacionados con la suscripción seleccionada se efectúa por medio del lector 12 que recibe estos datos del operador 14. Los datos recibidos por el lector 12 se escriben entonces en el elemento de seguridad 10. Este último puede entonces comunicarse con la red del operador 18 seleccionada.

En el caso de que los perfiles del operador estén pre-aprovisionados en la tarjeta 13, el proceso anteriormente detallado sigue siendo válido, realizado por el integrador en sentido ascendente antes de realizar su recorrido in situ para instalar el equipo.

En una segunda implementación de la presente invención, representada en la figura 2, la personalización de un elemento de seguridad es realizada por un usuario final o un vendedor de equipos.

Este modo de implementación está destinado al comprador de un equipo, tal como una consola de juegos 21, provisto de una e-UICC 10. Durante su compra, como anteriormente con referencia a la figura 1, la e-UICC 10 no incluye datos que permitan la autenticación a una red de operador 18.

La personalización del elemento de seguridad 10 funciona de la siguiente manera, cuando es implementada por el usuario final (normalmente el comprador de la consola 21): el usuario final compra, con la consola 21 o por separado, una tarjeta 24 que comprende los datos del operador correspondientes a un enlace de suscripción único a una red de un operador de radiotelefonía móvil. Por lo tanto, es preferencial la elección del operador que administrará su consola de juegos 21. Una vez en casa, el usuario inserta su tarjeta 24 en un lector 23 conectado a un ordenador 22 o integrado a éste. El usuario, equipado con un CD 26 de instalación de un software ad-hoc, se conecta entonces mediante la red de Internet 25 al administrador de suscripciones 16 (por medio de una dirección URL) y le transmite, durante una etapa 15, los datos relacionados con la suscripción que figura en su tarjeta 24. Es posible que se solicite un código de seguridad, previamente proporcionado al usuario final, para que se efectúe esta transferencia. El administrador de suscripciones 16 transmite de vuelta, en forma segura, los datos relacionados con la suscripción seleccionada (perfil completo que contiene la pareja IMSI/Ki). Estos datos pasan por el ordenador y la consola 21 para ser escritos en la e-UICC 10. Esta e-UICC 10 puede entonces conectarse a la red 18 del operador cuyos datos figuran en la tarjeta 24.

Se establece así, por medio de una tarjeta 24, una relación física entre el usuario y su operador. La tarjeta 24 materializa de esa manera la relación que el usuario tiene con su operador, lo que tiene ventajas a nivel de marketing: el usuario tiene, en el momento de la compra, la tarjeta del operador que ha seleccionado. El usuario tiene, por tanto, la impresión de encontrarse en la misma situación que cuando realiza una suscripción a un operador para obtener una tarjeta SIM que insertar en su equipo, mientras que la e-UICC que personaliza en el contexto de la presente invención no se puede extraer del equipo 21 que la contiene.

Cuando la invención es implementada por un vendedor de equipos, como las consolas 21, por ejemplo, el método de acuerdo con la presente invención se desarrolla como se describió anteriormente con referencia a la figura 2, con las siguientes diferencias: la tarjeta 24 del vendedor comprende varios enlaces de suscripción a un operador único o a varios enlaces de suscripción a diferentes operadores. Una vez que su tarjeta 24 se inserta en el lector 23, introduce un código confidencial que le ha sido proporcionado por el operador seleccionado por el usuario final. Con la ayuda de este código, los datos del operador correspondientes a una suscripción se transfieren a través de Internet 25 al SM-SR 16, que le devuelve el perfil completo (integrando la pareja IMSI/Ki), lo que permite personalizar la e-UICC 10. Este perfil es entonces cargado en el e-UICC 10 del equipo 21 del usuario.

En las dos situaciones mencionadas con referencia a la Figura 2, el código de seguridad introducido por el usuario final o el vendedor se corresponde en la práctica con un código de transferencia de un perfil de operador de radiotelefonía móvil. Este código de transferencia es de un solo uso para cada suscripción cargada en el elemento de seguridad 10, a fin de evitar que una suscripción sea instalada en varios dispositivos. El operador es informado por el SM-SR 16 de la activación de una suscripción y éste puede entonces proporcionar los identificadores IMSI/Ki en su HLR.

REIVINDICACIONES

1. Un método de personalización de un elemento de seguridad (10) que coopera con un dispositivo (11, 21), consistente dicha personalización en descargar datos relacionados con una suscripción a una red de un operador de radiotelefonía móvil en dicho elemento de seguridad (10), **caracterizado porque** consiste en:

i- conectar dicho equipo (11, 21) a un lector de tarjetas (12, 23);
ii- leer en una tarjeta (13, 24) conectada a dicho lector de tarjeta (12, 23) los datos del operador correspondientes a al menos una suscripción a una red de un operador de radiotelefonía móvil;
iii- transmitir dichos datos del operador desde dicho lector (12, 23) a una red del operador (14);
iv- transmitir desde dicha red del operador (14) a un administrador de suscripciones (16) una solicitud de transferencia de dichos datos relacionados con dicha suscripción a dicha red del operador de radiotelefonía móvil;
v- transmitir desde dicho administrador de suscripciones (16) a dicho elemento de seguridad (10) dicho datos relacionados con dicha suscripción a dicha red del operador de radiotelefonía móvil.

2. Método según la reivindicación 1, **caracterizado porque** la etapa de -v- consiste en transmitir dichos datos relacionados con dicha suscripción a dicha red de operador de radiotelefonía móvil por medio de dicho lector de tarjetas (12, 23).

3. Método según la reivindicación 1, **caracterizado porque** la etapa -v- consiste en transmitir dichos datos relacionados con dicha suscripción a dicha red de operador de radiotelefonía móvil por medio de la red de Internet (25) a la que está conectado dicho lector de tarjetas (23) por medio de un ordenador (22).

4. Método según una de las reivindicaciones 1 a 3, **caracterizado porque** la etapa -ii- está precedida por una etapa de verificación de un código de seguridad.

5. Método según una de las reivindicaciones 1, 2 y 4, **caracterizado porque** la etapa -i es implementada por un instalador y **porque** consiste en proponer a dicho instalador varias suscripciones diferentes, seleccionando dicho instalador por medio de la interfaz hombre-máquina de dicho lector de tarjetas (12) una de las suscripciones propuestas.

6. Método según una de las reivindicaciones 1, 3 y 4, **caracterizado porque** es implementado por un vendedor de tarjetas o un usuario final de dicha máquina y **porque** dicho código de seguridad corresponde a un código de transferencia de un operador de radiotelefonía móvil.

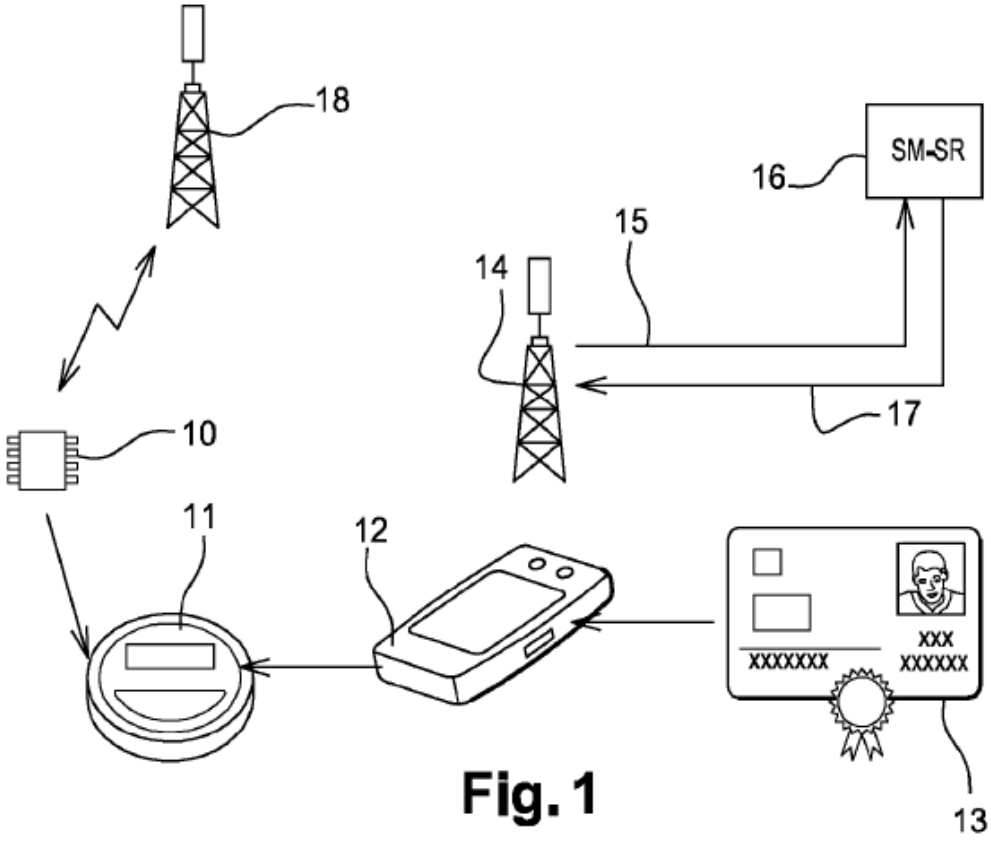
18
SM-SR
16
15
14
17
10
11
12
XXXXXXX
XXX
XXXXXX
13

Fig. 1

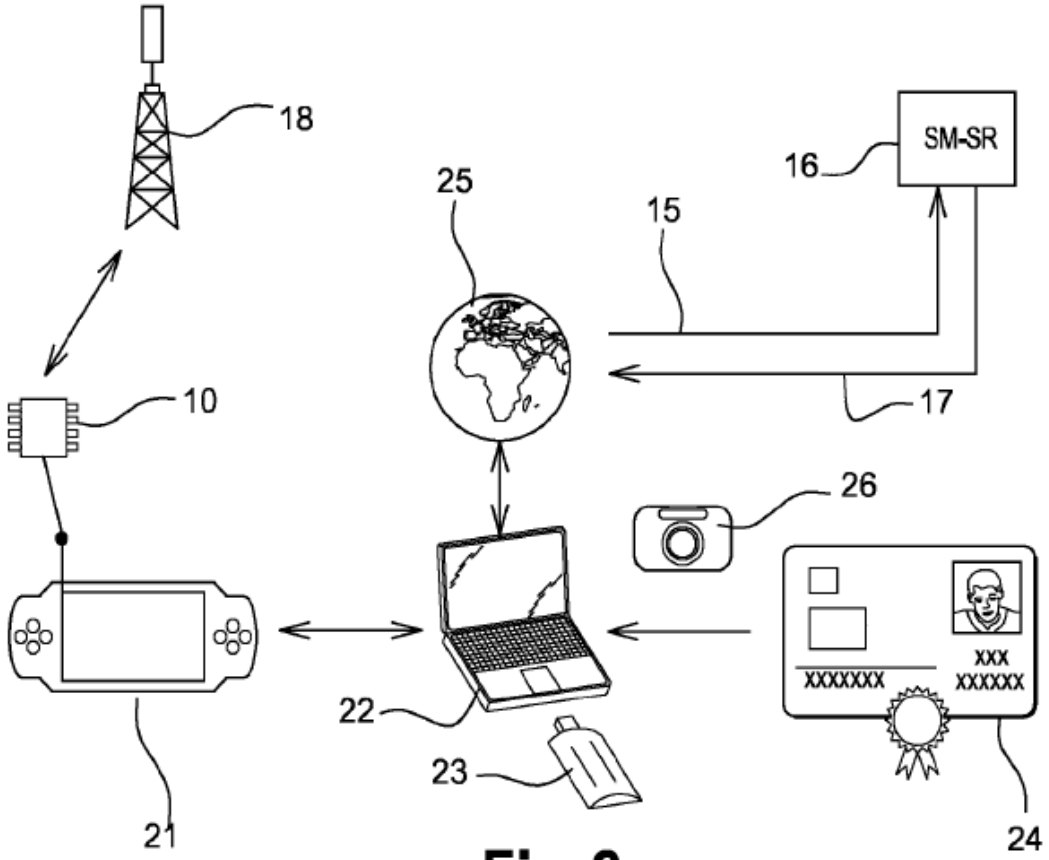
18
SM-SR
16
25
15
17
10
26
22
23
XXXXXXX
XXX
XXXXXX
21
24

Fig. 2