(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 553 595**

(51) Int. CI.:

H04L 29/08 (2006.01)
H04W 8/20 (2009.01)
G06F 21/00 (2013.01)
H04L 29/06 (2006.01)
H04W 12/06 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **02.12.2011 E 11802008 (0)**

(97) Fecha y número de publicación de la concesión europea: **17.06.2015 EP 2649830**

(54) Título: **Método para trasmitir una aplicación SIM de un primer terminal a un segundo terminal**

(30) Prioridad:

06.12.2010 EP 10306359

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
10.12.2015

(73) Titular/es:

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

(72) Inventor/es:

MERRIEN, LIONEL;
BERARD, XAVIER y
GACHON, DENIS

(74) Agente/Representante:

ISERN CUYAS, María Luisa

DESCRIPCIÓN

Método para transmitir una aplicación Sim de un primer terminal a un segundo terminal.

La presente invención se refiere a un método para transmitir una aplicación Sim de un primer terminal a un segundo terminal.

Una aplicación Sim se instala típicamente en un elemento seguro, como una UICC. El elemento seguro está instalado, de modo fijo o no, en un terminal, como por ejemplo un teléfono móvil. En algunos casos, los terminales están constituidos por máquinas que se comunican con otras máquinas mediante aplicaciones M2M (Máquina a Máquina).

Una UICC (Tarjeta Universal de Circuito Integrado) puede tener el formato de una tarjeta inteligente, o puede estar en cualquier otro formato como por ejemplo, pero no limitado a, un chip de empaquetado como el descrito en la PCT/SE2008/050380, o cualquier otro formato. Se puede utilizar en terminales móviles en redes GSM y UMTS, por ejemplo. La UICC garantiza la autenticación de red, integridad y seguridad de todo tipo de datos personales.

En una red GSM, la UICC contiene principalmente una aplicación SIM y en una red UMTS es la aplicación USIM. Una UICC puede contener varias otras aplicaciones, haciendo posible que la misma tarjeta inteligente pueda dar acceso tanto a la red GSM como a la UMTS, y también proporcionar el almacenamiento de una guía telefónica y otras aplicaciones. También es posible acceder a una red GSM usando una aplicación USIM y es posible acceder a las redes UMTS mediante una aplicación SIM con los terminales móviles preparados para tal fin. Con el UMTS versión 5 y más tarde con una red escenario como la LTE, se requiere una nueva aplicación, el Módulo de Identidad de Servicios Multimedia IP (ISIM) para los servicios en el IMS (Subsistema Multimedia IP). La guía telefónica es una aplicación independiente y tampoco forma parte de ningún módulo de información de suscripción.

En una red CDMA, la UICC contiene una aplicación CSIM, además de aplicaciones SIM y 3GPP USIM.

Una tarjeta con las tres características se llama una tarjeta de identidad de usuario extraíble, o R-UIM. Por lo tanto, la tarjeta R-UIM se puede insertar en terminales CDMA, GSM o UMTS, y funcionará en los tres casos.

En las redes 2G, la tarjeta SIM y la aplicación SIM estaban unidas, por lo que "la tarjeta SIM" podría referirse a la tarjeta física, o cualquier tarjeta física con la aplicación SIM.

La tarjeta inteligente UICC consiste en una CPU, ROM, RAM, EEPROM y circuitos I/O. Las primeras versiones consistían en tarjetas inteligentes de tamaño completo (85 x 54 mm, ISO/IEC 7810 ID-1).

Pronto, la carrera por conseguir teléfonos más pequeños necesitó de una versión más pequeña de la tarjeta.

Dado que la ranura de la tarjeta ha sido estandarizada, un abonado puede mover fácilmente su cuenta inalámbrica y su número de teléfono de un terminal a otro. Esto también transferirá su agenda telefónica y sus mensajes de texto. De similar modo, por lo

general un abonado puede cambiar de operador mediante la inserción de la tarjeta UICC de un nuevo operador en su terminal. Sin embargo, esto no siempre es posible debido a que algunos operadores (por ejemplo, en los Estados Unidos) bloquean el cambio de SIM en los teléfonos que ellos venden, evitando que se puedan utilizar en ellos las tarjetas de los operadores de la competencia.

La integración del marco ETSI y del marco de gestión de aplicaciones de la Plataforma Global se ha estandarizado en la configuración de la UICC.

Las UICCs están estandarizadas por 3GPP y ETSI.

Una UICC normalmente se puede extraer de un terminal móvil, por ejemplo cuando el usuario desea cambiar su terminal móvil. Después de haber insertado su UICC en su nuevo terminal, el usuario mantendrá aún el acceso a sus aplicaciones, contactos y credenciales (operador de red).

También es conocido el hecho de soldar o fijar la UICC a un terminal, con el fin de conseguir que sea dependiente del terminal. Esto se hace en aplicaciones M2M (Máquina a Máquina). Se alcanza el mismo objetivo cuando un chip (un elemento seguro) que contiene las aplicaciones y archivos SIM o USIM está contenido en el terminal. El chip es, por ejemplo soldado a la placa madre del terminal o máquina y constituye una UICC.

Algunas de las mejoras más divulgadas son aplicables a dichas UICCs soldadas o para esos chips que contienen las mismas aplicaciones que los chips contenidos en las UICCs. Se puede realizar una copia de las UICCs que no están totalmente vinculadas a dispositivos, pero que son extraíbles con dificultad porque no están pensadas para ser extraídas, situadas en terminales distantes o profundamente integradas en máquinas. Un factor de forma especial de la UICC (muy pequeña, por ejemplo, y por lo tanto difíciles de manejar) también puede ser una razón para considerarla de facto integrada en un terminal. Lo mismo se aplica cuando una UICC está integrada en una máquina que no está destinada a ser abierta.

En la siguiente descripción, las UICCs soldadas o los chips que contienen o están diseñados para contener las mismas aplicaciones que las UICCs se denominarán generalmente UICCs incrustadas o elementos de seguridad incrustados (en contraste con las UICCs extraíbles o elementos de seguridad extraíbles). Esto también se aplicará a las UICCs o los elementos de seguridad que son extraíbles con dificultad.

La presente invención concierne a la autenticación del usuario final de un terminal durante la transferencia de la aplicación SIM. En un determinado contexto, una aplicación Sim completa (es decir, datos personales, sistema de archivos, aplicaciones Java como aplicaciones bancarias por ejemplo, y secretos) se almacena en una UICC incrustada incorporada en un primer terminal (por ejemplo soldada en un primer teléfono móvil) y un usuario desea transferir esta aplicación SIM completa a otra UICC incrustada incorporada en un segundo terminal (por ejemplo, constituido por un segundo terminal móvil). Esto puede suceder cuando un usuario cambia su teléfono móvil pero no desea perder las aplicaciones, contactos y datos personales, tales como fotografías, vídeos o canciones almacenadas en la UICC de su primer teléfono móvil.

Este problema no ocurre cuando la aplicación Sim es almacenada en una tarjeta SIM que se puede extraer de un teléfono móvil e insertar en otro ya que cuando un elemento de

seguridad como una UICC se suelda en el teléfono móvil, no es posible físicamente cambiar el elemento seguro que contiene la aplicación SIM, de un teléfono móvil a otro.

El proceso general para lograr esta operación de transferencia de la aplicación Sim normalmente podría ser el siguiente:

- El elemento seguro envuelve la SIM instalada de manera que pueda ser reinstalada en otro elemento seguro. Este envase debe resultar seguro, es decir, cifrado con el fin de que sólo el elemento seguro específico sea capaz de leerla, y firmada con el objetivo de asegurar que el envoltorio proviene del elemento seguro inicial;

- La SIM envasada se carga en una bóveda de seguridad en la nube (Internet). Esta operación puede ser necesaria en el caso de que el elemento de seguridad específico no se conozca en el momento de envasado;

- La SIM envasada se descarga en el nuevo elemento de seguridad específico;

- El elemento de seguridad específico realiza la comprobación de seguridad y posteriormente puede instalar la SIM envasada descargada.

El resultado es que la Sim completa inicial ha sido transferida a otro elemento seguro, con todo el entorno del usuario.

Métodos similares se describe en US2005/0266883, EP 2076071 A1 y US2008/261561 A1.

Al comenzar la transferencia inicial desde el elemento seguro inicial hasta la bóveda de seguridad, podemos imaginar que el usuario final está introduciendo un código PIN para autenticarse él mismo y confirmar la operación. Sin embargo, aparece un problema cuando se desea transferir la SIM envasada de nuevo desde la bóveda de seguridad al elemento de seguridad específico: Cómo estar seguro de que la solicitud proviene del mismo usuario final? No hay posibilidad de introducir de nuevo el código PIN, ya que es parte de la aplicación SIM y es necesario para asegurarse de la identidad del usuario final antes de instalar la SIM en el nuevo elemento de seguridad específico. Este problema podría conducir al hecho de que la suscripción realizada con la SIM pudiera ser instalada y reutilizada por otro usuario.

A fin de evitar este problema, podría ser posible instalar primero la SIM en el elemento seguro específico y luego solicitar el PIN para autenticación. Sin embargo, el inconveniente es que la instalación de la Sim se ha realizado y la autenticación no es sólida ya que, para un código PIN de 4 dígitos, después de un máximo de 10.000 intentos, una persona deshonesta podría encontrar el código PIN correcto y utilizar la aplicación Sim de otro usuario (y consecuentemente su suscripción).

La presente invención tiene el propósito de resolver este problema.

A este respecto, la presente invención propone un método para transmitir una aplicación Sim de un primer terminal a un segundo terminal, estando almacenada la aplicación en un elemento de seguridad incluido en el primer terminal, estando bloqueado el acceso a la aplicación Sim por un código PIN.

De acuerdo con esta invención, el método consiste en:

i - la exportación de la aplicación Sim desde el primer terminal a un sitio distante, incluyendo el código PIN así como un código de carga remoto;

ii - pedir al usuario del segundo terminal que introduzca el código de carga remoto en el segundo terminal;

iii - en el caso de que el código de carga remoto introducido por el usuario coincida con el código de carga remoto que ha sido exportado, autorizar la instalación de la aplicación Sim en un elemento de seguridad del segundo terminal, y de no ser así, no instalar la aplicación Sim en el elemento seguro del segundo terminal.

Ventajosamente, la coincidencia del código de carga remoto se comprueba al nivel del sitio distante y la coincidencia lanza la descarga de la aplicación SIM en el elemento de seguridad del segundo terminal y la instalación.

Alternativamente, la coincidencia del código de carga remoto se comprueba al nivel del segundo terminal, después de que la aplicación SIM se haya descargado en el elemento seguro del segundo terminal, la coincidencia lanza la instalación de la aplicación SIM en el elemento de seguridad del segundo terminal.

El código de carga remoto se encuentra preferentemente cifrado.

En una realización preferida, el código de carga remoto consiste en una frase de paso.

Otras características de la mejora se desprenderán de la lectura de la siguiente descripción de una realización preferida dada a modo de ejemplo ilustrativo no limitativo.

La presente invención propone solicitar al usuario final la introducción de un código de carga remoto además del código PIN para confirmar la exportación de la aplicación SIM a un sitio distante (la bóveda segura). El código de carga remoto puede ser, por ejemplo, una frase de paso.

Esta frase de paso está cifrada e incluida en la tarjeta SIM segura envasada que se carga en la bóveda de seguridad en la nube. Así, la bóveda segura almacena la Sim envuelta (la suscripción comprendida en el elemento seguro, el código PIN, el entorno, los secretos de autenticación, las claves aplicativas (Dominio Seguro), las diferentes claves de las diferentes aplicaciones, las claves PKI, la diferentes aplicaciones (NFC, banco, ...), la ISD (Dominio de Seguridad del Emisor), el sistema de archivos, ...) y el código de carga remoto en un único paquete que se puede posteriormente descargado a un nuevo elemento seguro.

Antes de instalar este paquete en el nuevo elemento de seguridad, se pide al usuario del segundo terminal que comprende el elemento seguro que introduzca el código de carga remoto en el segundo terminal.

Si el código de carga remoto introducido por dicho usuario coincide con el código de carga remoto que ha sido exportado, se autoriza la instalación de la aplicación Sim en el elemento seguro del segundo terminal. De lo contrario, la instalación no se realiza.

Se pueden utilizar dos maneras diferentes de funcionamiento: la primera consiste en la comprobación de la coincidencia de los códigos de carga remotos al nivel de la bóveda de seguridad. Si los códigos coinciden, la aplicación Sim se descarga en el elemento seguro y luego se ejecuta.

La segunda consiste en la comprobación de la coincidencia de los códigos de carga remotos a nivel del segundo terminal, después de haber descargado la aplicación Sim en el elemento seguro del segundo terminal. Si los códigos coinciden, la aplicación SIM se instala en el elemento de seguridad del segundo terminal.

Después de haber sido instalada, la aplicación Sim puede ser lanzada por el usuario introduciendo su código PIN.

En una realización preferida, se cifra el código de carga remoto. En la primera realización, la bóveda segura descifra de la frase de paso contenida en la SIM envuelta. En la segunda forma de realización, el elemento de seguro es quien realiza ese descifrado.

La invención permite mejorar la seguridad general de la transferencia de la aplicación Sim ya que asegura que la aplicación SIM es exportada e importada por el mismo usuario final.

El usuario final es normalmente el propietario del terminal, como por ejemplo un teléfono móvil. En las aplicaciones M2M, el usuario final es el instalador, por ejemplo el instalador eléctrico de una máquina eléctrica.

REIVINDICACIONES

1. Método para transmitir una aplicación SIM de un primer terminal a un segundo terminal, estando almacenada dicha aplicación Sim en un elemento de seguridad incluido en el primer terminal,

caracterizado porque

el acceso a dicha aplicación Sim está bloqueado por un código PIN, consistente el método en:

i - la exportación de la aplicación Sim desde el primer terminal a un sitio distante, incluyendo el código PIN así como un código de carga remoto;

ii - pedir al usuario del segundo terminal que introduzca el código de carga remoto en el segundo terminal;

iii - en el caso de que el código de carga remoto introducido por el usuario coincida con el código de carga remoto que ha sido exportado, autorizar la instalación de la aplicación Sim en un elemento de seguridad del segundo terminal, y de no ser así, no instalar la aplicación Sim en el elemento seguro del segundo terminal.

2. Método según la reivindicación 1, en el que la coincidencia de dichos códigos de carga remotos se comprueba al nivel de dicho sitio distante y dicha coincidencia lanza la descarga de dicha aplicación Sim en el elemento de seguro de dicho segundo terminal y dicha instalación.

3. Método según la reivindicación 1, en el que la coincidencia de dichos códigos de carga remotos se comprueban al nivel de dicho segundo terminal, después de que dicha aplicación Sim haya sido descargada en dicho elemento seguro de dicho segundo terminal, lanzando dicha coincidencia la instalación de dicha aplicación Sim en el elemento seguro de dicho segundo terminal.

4. Método de acuerdo con cualquiera de las reivindicaciones 1 a 3, en el que dicho código de carga remoto está cifrado.

5. Método de acuerdo con cualquiera de las reivindicaciones 1 a 4, en el que dicho código de carga remoto es una frase de paso.

6. Método de acuerdo con cualquiera de las reivindicaciones 1 a 5, en el que dicho terminal es una máquina.