(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 562 765**

(51) Int. CI.:

H04L 29/08 (2006.01)
H04W 8/20 (2009.01)
G06F 21/00 (2013.01)
H04L 29/06 (2006.01)
H04L 9/08 (2006.01)
H04W 12/04 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **02.12.2011 E 11794687 (1)**

(97) Fecha y número de publicación de la concesión europea: **16.09.2015 EP 2649829**

(54) Título: **Método para descargar una subscripción en una UICC incorporada en un terminal**

(30) Prioridad:

06.12.2010 EP 10306359

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
08.03.2016

(73) Titular/es:

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

(72) Inventor/es:

BRADLEY, PAUL

(74) Agente/Representante:

ISERN CUYAS, María Luisa

DESCRIPCIÓN

Método para descargar una subscripción en una UICC incorporada en un terminal.

La presente invención se refiere a un método para descargar una subscripción en una UICC (Tarjeta Universal de Circuito Integrado) incorporada en un terminal, por ejemplo un terminal móvil (teléfono móvil) o una máquina (para aplicaciones M2M (Máquina a Maquina)).

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 lodo 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 mas tarde con una red escenario como la L TE, 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 COMA, 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 funcionara 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 necesito 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.

La presente invención se aplica 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 maquinas. 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 tacto 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 aplicara a las UICCs o los elementos de seguridad que son extraíbles con dificultad.

La presente invención concierne a UICCs incorporadas (no extraíbles).

En una primera realización, la invención trata sobre un método que utiliza NFC para seleccionar y descargar una aplicación (U)SIM incorporada (o generalmente una aplicación UICC completa) en un terminal que incluye dicha UICC incorporada segura. El terminal es, por ejemplo, un teléfono móvil.

En una segunda realización, la invención trata sobre un método que utiliza un código de barras para identificar una aplicación (U)SIM (o generalmente una aplicación UICC completa) a descargar en un terminal capaz de tomar una fotografía de ese código de barras.

Tal como ya se ha explicado en la introducción, en el futuro, cuando haya SIMs blandas o SIMs incorporadas en el interior de dispositivos, será necesario seleccionar la información de subscripción apropiada para descargarla en el dispositivo. La experiencia del usuario podría mejorarse otorgando una etiqueta NFC de un solo uso que identifique la subscripción a descargarse en el dispositivo.

Dicho de otro modo, en un mundo donde la información de subscripción ya no sea almacenada en un formato extraíble seguro como las UICCs de hoy en día y en lugar de almacenarse como "SIM blanda" o elemento seguro soldado (por ej., un elemento seguro VQFN8 / DFN8), entonces existe la necesidad de seleccionar la correcta subscripción para descargar en el dispositivo.

La Patente Internacional WO 2009/103623 A2 describe un sistema y un método para asociar un dispositivo inalámbrico "genérico", como por ejemplo un dispositivo que no es reprogramado con credenciales de subscripción correspondientes a un operador particular, con un operador domestico designado por el propietario del dispositivo. El sistema incluye un servidor de registro para el mantenimiento de los datos de registro electrónicos para una pluralidad de dispositivos inalámbricos y para dirigir dispositivos inalámbricos nuevamente activados a un servidor para descargar credenciales de subscripción "permanentes", como una USIM descargable. El informe técnico 3GPP TR 33.812 V1.0.0 (Divulgación 8) estudia cómo hacer posible proveer a la red de control remoto de la aplicación USIMIJSIM en un equipo M2M de manera segura en un sistema 3GPP.

La invención propone un método para descargar una subscripción en una UICC incorporada en un terminal, consistente el citado método en:

- transferir un ICCID al terminal;
- enviar el ICCID sobre un enlace IP a una bóveda segura;
- seleccionar en la bóveda segura una subscripción correspondiente al ICCID;
- transmitir la subscripción al terminal sobre el enlace IP;
- almacenar la subscripción en la UICC.

El ICCID es transferido preferentemente junto con un código de activación secreto del ICCID y la bóveda segura verifica el emparejamiento del ICCID y el código de activación secreto antes de transmitir la subscripción al terminal.

En una primera realización, el ICCID esta contenido en un token y el ICCID es transferido al terminal a través de la NFC.

El token puede estar constituido por una etiqueta NFC.

En una segunda realización, el ICCID esta contenido en un código de barras para ser fotografiado por el terminal.

De acuerdo con la primera realización de la presente invención, se utiliza un terminal NFC.

La descarga de la subscripción podría realizarse a través de una interfaz de usuario o en forma de impulso. Sin embargo, para terminales que están desbloqueados existe la necesidad (para procesos MNO con flujos legales) de tener una etiqueta física/tarjeta NFC para distribución similar a las tarjetas SIM físicas de la actualidad. Esta etiqueta contendría una referencia al ICCID (con un código seguro de activación conocido para el

sistema de aprovisionamiento y ligado a un ICCID individual). Una vez el ICCID es remitido al sistema de aprovisionamiento con el código de activación correcto, el servicio de aprovisionamiento remoto puede iniciar la transferencia segura del software correcto (perfil SIM, información de subscripción) al elemento seguro incorporado.

Si por ejemplo, un usuario tiene un dispositivo pre-activado X y quiere contratar una subscripción con un operador A, el flujo seria el siguiente:

- El dispositivo X se pone en contacto con el token NFC Y. El token contiene el ICCID y preferiblemente también el código de activación del ICCID. El Dispositivo X lee el ICCID del token Y así como (preferiblemente) código de activación secreto del ICCID, wl cual es único (este código previene la adivinación por la fuerza de la petición del ICCID al centro de aprovisionamiento).

- El Dispositivo X envía este ICCID sobre un enlace IP a la bóveda segura. La bóveda segura verifica el ICCID / código de activación secreto emparejado y si es valido empaqueta de forma segura, cifra y firma el guión de personalización entero para la UICC incorporada (conteniendo la aplicación SIM, la aplicación USIM, la aplicación ISIM, la aplicación CSIM, cualquier otra solicitud de autenticación de red, así como cualquier aplicación SIM, aplicación de Instrumentos y Sistema de Operación de Adaptación/Mecanismo relacionados con ese MNO especifico), así como la información de subscripción relevante como la IMSI, K, Opc, IMPU y constantes algorítmicas. Los contenidos del perfil serian conocidos por la bóveda segura utilizando el rango ICCID o alternativamente, un código de perfil podría ser remitido al sistema.

- La bóveda segura transmite el guión de personalización de arriba al dispositivo X cifrado para el elemento seguro incorporado del Dispositivo X (y con un mecanismo contador anti-repetición incluido) sobre el enlace IP.

- El Dispositivo X (incluyendo su elemento seguro incorporado) descifra y ejecuta el guión de personalización, proveyendo así la subscripción en el elemento seguro incorporado).

El Dispositivo X puede ahora acceder a la red de radio utilizando la subscripción.

En una segunda realización el ICCID esta incluido en un código de barras para que sea fotografiado por el terminal. Después de haber tomado una fotografía del código de barras, el terminal la envía a la bóveda segura. La bóveda segura compara entonces el código de barras recibido con el código de barras pre-registrado o decodifica el código de barras para recuperar el ICCID. Se emprende entonces el m1smo proceso tal como se menciona arriba.

La invención permite la selección de subscripción así como la variación remota del perfil y hace fácil la experiencia del usuario.

REIVINDICACIONES

1. Método para descargar una subscripción en una Tarjeta Universal de Circuito Integrado, UICC, incorporada en un terminal, consistiendo el citado método en:

- transferir un ICCID a dicho terminal;
- enviar dicho ICCID sobre un enlace IP a una bóveda segura:
- seleccionar en dicha bóveda segura una subscripción correspondiente a dicho ICCID;
- transmitir dicha subscripción a dicho terminal sobre dicho enlace IP;
- almacenar dicha subscripción en dicha UICC.

2. Método de acuerdo con la reivindicación 1, en el que dicho ICCID es transferido junto con código de activación secreto de ICCID, y en dicha bóveda segura verifica el emparejamiento del ICCID y el código de activación secreto antes de transmitir dicha subscripción a dicho terminal.

3. Método de acuerdo con las reivindicaciones 2 o 3, en el que dicho ICCID está contenido en un token y que dicho ICCID es transferido a dicho terminal a través de NFC.

4. Método de acuerdo con la reivindicación 3, en el que dicho token es una etiqueta NFC.

5. Método de acuerdo con cualquiera de las reivindicaciones 1 a 2, en que dicho ICCID está contenido en un código de barras para que sea fotografiado por dicho terminal.