

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 729 298**

51 Int. Cl.:

H04W 8/20 (2009.01)

H04W 4/00 (2008.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **24.03.2016 PCT/EP2016/000522**

87 Fecha y número de publicación internacional: **29.09.2016 WO16150574**

96 Fecha de presentación y número de la solicitud europea: **24.03.2016 E 16715451 (7)**

97 Fecha y número de publicación de la concesión europea: **08.05.2019 EP 3275228**

54 Título: **Procedimiento para cargar un perfil**

30 Prioridad:
26.03.2015 DE 102015003977

45 Fecha de publicación y mención en BOPI de la traducción de la patente:
31.10.2019

73 Titular/es:
**GIESECKE+DEVRIENT MOBILE SECURITY GMBH
(100.0%)
Prinzregentenstraße 159
81677 München, DE**

72 Inventor/es:

**NITSCH, NILS y
HUBER, ULRICH**

74 Agente/Representante:

DURAN-CORRETJER, S.L.P

ES 2 729 298 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

Procedimiento para cargar un perfil

5 Campo de la invención

La invención se refiere a un procedimiento para cargar un perfil para una suscripción de telefonía móvil (perfil de suscripción) en un módulo de identificación de abonado.

10 Estado de la técnica

En el marco de la configuración de un módulo de identificación de abonado se debe cargar un perfil de suscripción en el módulo de identificación de abonado. Las solicitudes de modificación del perfil de suscripción (o también abreviado, perfil) requieren proporcionar un perfil de suscripción modificado. En el caso de las tarjetas SIM Plug-In, la modificación puede realizarse intercambiando la tarjeta SIM. Alternativamente, en el módulo de identificación de abonado se carga un nuevo perfil de suscripción, lo que se realiza especialmente para módulos de identificación de abonado soldados de forma fija, que no pueden intercambiarse sin más. La gestión de suscripciones, en particular, mediante la descarga de perfiles de suscripción y datos asociados a una eUICC, se denomina en general también como Subscription Management.

Las especificaciones técnicas [1] 12FAST.13 - Embedded SIM Remote Provisioning Architecture, del 17 de diciembre de 2013, GSMA, y [2] SGP02-Remote-Provisioning-Architecture-for-Embedded-UICC-Technical-Specification-v2.0, del 13 de octubre de 2014, GSMA, describen la descarga y la instalación de un perfil de suscripción en una eUICC. [1] 12FAST.13, cap. 3, describe los roles y funciones mediante los cuales se carga un perfil de un enrutador seguro de gestión de suscripciones SM-SR a una eUICC y se instala en la misma. Una función es un código de programa ejecutable instalado en la eUICC, que se ejecuta mediante un comando correspondiente a la función, que se envía a la eUICC. [2] SGP02, cap. 3, describe el proceso protocolario al descargar e instalar un perfil de suscripción en una eUICC.

Según [1] 12FAST.13 cap. 3.3.1.2.2 "Profile Download and Installation Function", con una función de "Download" se descarga un perfil a la eUICC. Sin embargo, al descargar un perfil a través de "Download" también deben realizarse otras funciones asociadas. Según [1] 12FAST.13 cap. 3.3.1.3.1 "ISD-P Creation Function" y [2] SGP02, cap. 3.1.1 "ISD-P Creation" se utilizan funciones "Create" para crear una estructura de archivos en la eUICC, en particular, la ISD-P. Según [2] SGP02, cap. 3.1.3 "Download and Installation of the Profile", tras la creación de la ISD-P se descarga un perfil y una estructura de archivos, en particular, la ISD-P. Según [1] 12FAST.13 cap. 3.3.1.2.3 "Profile Content Update Function" y 3.3.1.2.4 "Policy Rules Update Function", se utilizan funciones "Update" para realizar actualizaciones conforme al perfil recientemente descargado. Según [1] 12FAST.13 cap. 3.3.1.3.4 "Profile Enabling Function" y [2] SGP02, cap. 3.2 "Profile Enabling", se realizan funciones "Enable" para activar un perfil descargado, en particular, una ISD-P, para convertirla en utilizable para el usuario de la eUICC.

Por tanto, según [1], [2], adicionalmente a la función "Download", con la que se descarga un perfil a una eUICC, deben utilizarse al menos las tres funciones adicionales "Create", "Update" y "Enable". Cada una de estas funciones debe llamarse o enviarse desde el SM-SR a la eUICC a través de una conexión OTA (over-the-air) con cargo. De esto resulta que, para descargar unos 10 kilobytes de datos de perfil a la eUICC, se estima que deben enviarse al menos 20 kilobytes (es decir, aproximadamente el doble) de datos OTA desde el SM-SR a la eUICC.

Lo ideal sería una solución para gestionar los perfiles de suscripción, en la que la cantidad de los datos enviados al módulo de identificación de abonado, en particular, de los datos enviados adicionalmente a los propios datos de perfil, estuviera reducida.

El documento DE 10 2012 018 540 A1 del estado de la técnica da a conocer un módulo de identificación de abonado con dos perfiles de suscripción, entre los cuales se puede conmutar. De este modo es posible realizar un cambio de suscripción en gran medida sin transferencia OTA de datos.

55 Resumen de la invención

La invención se basa en el objetivo de crear un procedimiento para cargar un perfil para una suscripción de telefonía móvil (perfil de suscripción) en un módulo de identificación de abonado que reduzca la cantidad de datos transferidos OTA al módulo de identificación de usuario.

El objetivo se consigue mediante un procedimiento según la reivindicación 1. Las realizaciones preferentes de la invención se indican en las reivindicaciones dependientes.

El procedimiento, según la reivindicación 1, se basa en la idea básica de que el perfil se carga en un módulo de código de programa de ejecución individual en el módulo de identificación de abonado. Tan pronto como un primer comando (de comunicación) APDU llega al módulo de identificación de abonado después de la carga, lo que es

inevitable en algún momento, se ejecuta el módulo de código de programa y se instala el perfil. El envío de comandos de instalación específicos como «Create», «Update» y «Enable» a archivos elementales (Elementary Files, EFs) individuales del módulo de identificación de abonado, mediante lo cual tradicionalmente se instala un perfil, no es necesario.

5 Más precisamente, el procedimiento incluye los pasos: a) Proporcionar un perfil en el servidor de preparación de datos; b) Creación de un módulo de código de programa (Binary Large Object, BLOB) individual y ejecutable del perfil proporcionado según a), que está configurado de forma que mediante ejecución del módulo de código de programa ejecutable se instala el perfil en el módulo de identificación de abonado; c') Carga del módulo de código de programa individual y ejecutable en el módulo de identificación de abonado para cargar el perfil.

Por tanto, según la reivindicación 1, se ha creado un procedimiento para cargar un perfil con una cantidad de datos OTA reducida.

15 Un procedimiento para instalar en el módulo de identificación de abonado un perfil cargado, según la reivindicación 1, comprende correspondientemente los siguientes pasos: d) Envío de un comando APDU (preferentemente un comando que no sea de instalación) del servidor de preparación de datos al módulo de identificación de abonado; en reacción a la recepción del comando APDU en el módulo de identificación de abonado, ejecución del módulo de código de programa ejecutable y, mediante la ejecución, instalación del perfil en el módulo de identificación de abonado.

El módulo de código de programa ejecutable está configurado opcionalmente como programa de aplicación, en particular como Java Applet, en particular como Java Applet en formato cap.file. La CPU del módulo de identificación de abonado, en reacción al primer (o eventualmente también a otro) comando APDU entrante, ejecuta el código de programa e instala de este modo el perfil en el módulo de identificación de abonado.

Alternativamente, el módulo de código de programa ejecutable está configurado como imagen de memoria del perfil, o como una combinación de un código de programa (p. ej. un intérprete universal) instalado en el módulo de identificación de abonado e independiente del perfil, con una imagen de memoria del perfil. En reacción al primer (o eventualmente también a otro) comando APDU entrante se despliega la imagen de memoria y, de este modo, se instala el perfil o el código de programa (p. ej. intérprete) independiente interpreta la imagen de memoria e instala el perfil de este modo.

El paso c') de carga del módulo de código de programa comprende opcionalmente los siguientes subpasos: c'1) Carga del módulo de código de programa ejecutable del servidor de preparación de datos en un enrutador de seguridad (p. ej. Subscription Management Secure Router, SM-SR); c'2) Carga del módulo de código de programa ejecutable del enrutador de seguridad (SM-SR) en el módulo de identificación de abonado.

Opcionalmente, el paso a) está configurado como: a) Proporcionar el perfil de un servidor de operador de red a un servidor de preparación de datos.

Breve descripción de las figuras

A continuación se explica la invención en detalle en base a ejemplos de realización y haciendo referencia a los dibujos, donde muestran:

La figura 1, la imagen [2] cap. 3.1.1 figura 10 del estado de la técnica;

La figura 2, el proceso básico de carga e instalación de un módulo de código de programa BLOB ejecutable para cargar e instalar un perfil, según un modo de realización de la invención.

Descripción detallada de los ejemplos de realización

La figura 1 muestra la imagen [2] cap. 3.1.1 figura 10 del estado de la técnica. Un operador de red MNO descarga un perfil en un módulo de identificación de abonado eUICC a través del SM-DP de preparación de datos SubMan y el enrutador seguro SM-SR SubMan en una pluralidad de pasos con funciones "download" y "create ISDP". Llamando la función "download" también se provoca la ejecución de la función "CreatelSDP" para crear una estructura de archivos, en la que posteriormente pueden descargarse los datos de perfil. [2] cap. 3.1.3 figura 12 muestra la propia descarga de datos de perfil tras la creación de la estructura de archivos ISD-P.

La figura 2 muestra el proceso básico de carga e instalación de un módulo de código de programa BLOB (Binary Large Object) ejecutable para cargar e instalar un perfil P1 en un módulo de identificación de abonado eUICC, según un modo de realización de la invención. El servidor de un operador de red MNO (Mobile Network Operator) proporciona la estructura de perfil y los datos de perfil de un perfil P1 al servidor SM-DP de preparación de datos SubMan, con la solicitud de cargar el perfil P1 en el módulo de identificación de abonado eUICC. El servidor SM-DP de preparación de datos SubMan genera (pseudocódigo Generate) para el perfil P1 un módulo de código de

5 programa BLOB P1 ejecutable y lo envía (pseudocódigo send) al enrutador seguro SM-SR SubMan, que reenvía el módulo de código de programa BLOB P1 ejecutable al módulo de identificación de abonado eUICC. El módulo de identificación de abonado eUICC almacena el módulo de código de programa BLOB ejecutable. En cualquier momento, el enrutador seguro SM-SR SubMan envía un primer comando APDU al módulo de identificación de abonado eUICC. En reacción, se despliega el módulo de código de programa BLOB ejecutable. En función del módulo de código de programa BLOB ejecutable, el despliegue tiene lugar mediante ejecución del Applet (figura 2: pseudocódigo EXE por execute), implementación o interpretación de la imagen de memoria, etc. De este modo se instala el perfil P1 en el módulo de identificación de abonado eUICC.

10 Estado de la técnica citado

[1] 12FAST.13 - Embedded SIM Remote Provisioning Architecture de 17 de diciembre de 2013, GSMA

[2] SGP02-Remote-Provisioning-Architecture-for-Embedded-UICC-Technical-Specification-v2.0, de 13 de octubre de 2014, GSMA

15 [3] DE 10 2012 018 540 A1

REIVINDICACIONES

1. Procedimiento para cargar un perfil (P1) para una suscripción de telefonía móvil de un servidor de preparación de datos (SM-DP) en un módulo de identificación de abonado (eUICC), que comprende los pasos:

- a) Proporcionar un perfil (P1) en el servidor de preparación de datos (SM-DP);
- c) Cargar el perfil (P1) en el módulo de identificación de abonado (eUICC);

caracterizado por los pasos:

b) Crear un módulo de código de programa (BLOB) individual y ejecutable del perfil (P1) proporcionado según a), que está configurado de forma que, en reacción a la recepción del comando APDU en el módulo de identificación de abonado (eUICC) se ejecuta del módulo de código de programa (BLOB) ejecutable, mediante lo cual se instala el perfil (P1) en el módulo de identificación de abonado (eUICC);

c') Realizar el paso c) mediante carga del módulo de código de programa (BLOB) individual y ejecutable en el módulo de identificación de abonado (eUICC).

2. Procedimiento para instalar un perfil (P1) cargado, según la reivindicación 1, en el módulo de identificación de abonado (eUICC), que comprende los pasos:

d) Enviar un comando APDU del servidor de preparación de datos (SM-SP) al módulo de identificación de abonado (eUICC);

e) en reacción a la recepción del comando APDU en el módulo de identificación de abonado (eUICC), ejecutar el módulo de código de programa (BLOB) ejecutable, mediante lo cual se instala el perfil (P1) en el módulo de identificación de abonado (eUICC).

3. Procedimiento, según cualquiera de las reivindicaciones 1 o 2, tal que el módulo de código de programa (BLOB) ejecutable está configurado como programa de aplicación, en particular como Java Applet, en particular como Java Applet en formato cap.file.

4. Procedimiento, según cualquiera de las reivindicaciones 1 o 2, tal que el módulo de código de programa (BLOB) ejecutable está configurado como imagen de memoria del perfil (P1), o como una combinación de un código de programa (intérprete) instalado en el módulo de identificación de abonado (eUICC) e independiente del perfil (P1) con una imagen de memoria del perfil (P1).

5. Procedimiento, según cualquiera de las reivindicaciones 1 a 4, tal que c') comprende los subpasos:

c'1) Cargar el módulo de código de programa (BLOB) ejecutable del servidor de preparación de datos (SM-DP) en un enrutador de seguridad (SM-SR);

c'2) Cargar el módulo de código de programa (BLOB) ejecutable del enrutador de seguridad (SM-SR) en el módulo de identificación de abonado (eUICC).

6. Procedimiento, según cualquiera de las reivindicaciones 1 a 5, tal que el paso a) está configurado:

a) Proporcionar el perfil (P1) de un servidor de operador de red (MNO) al servidor de preparación de datos (SM-DP).

StdT [2] Kap. 3.1.1 Fig. 10

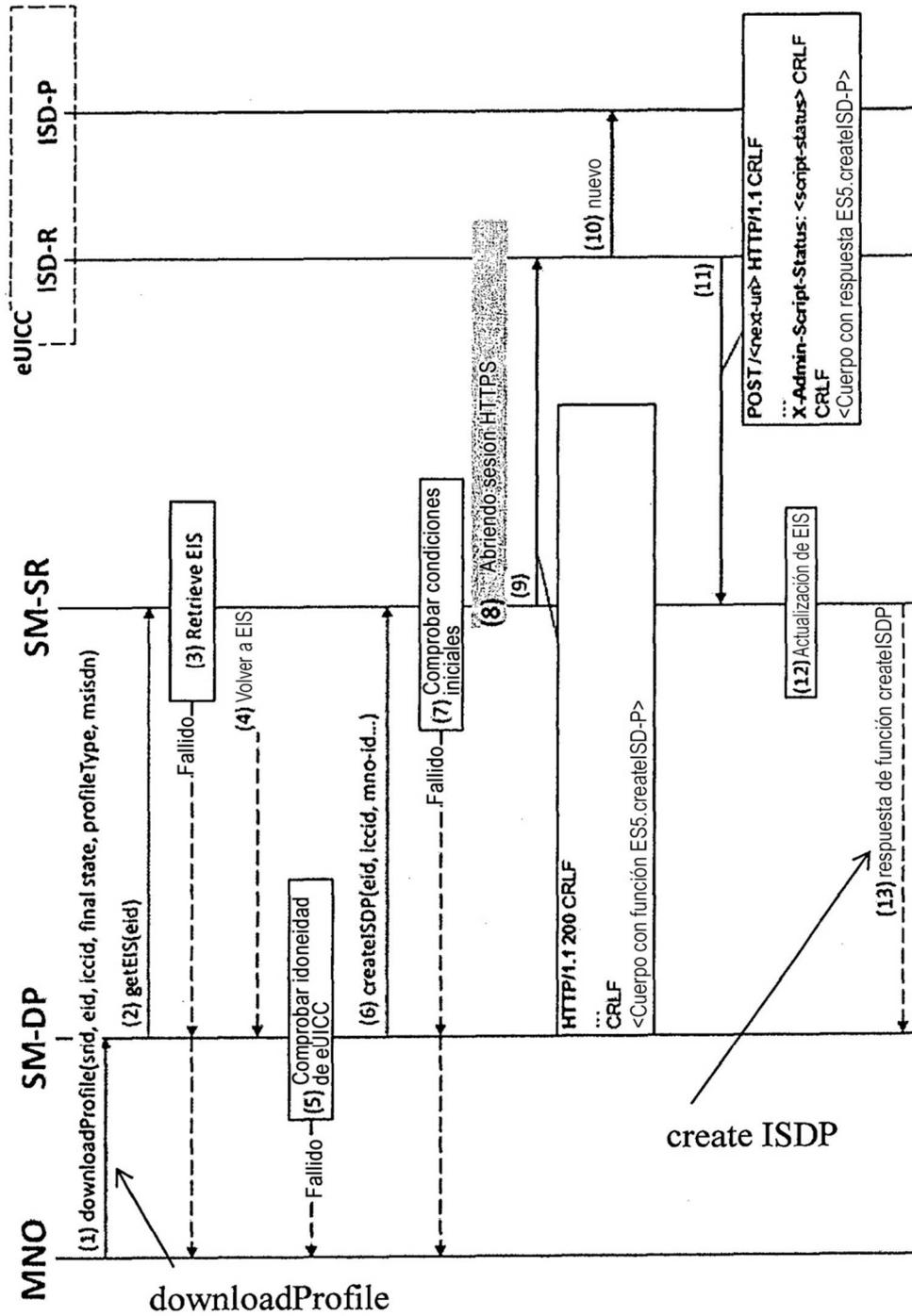


Figura 10: creación de ISD-P

Fig. 1

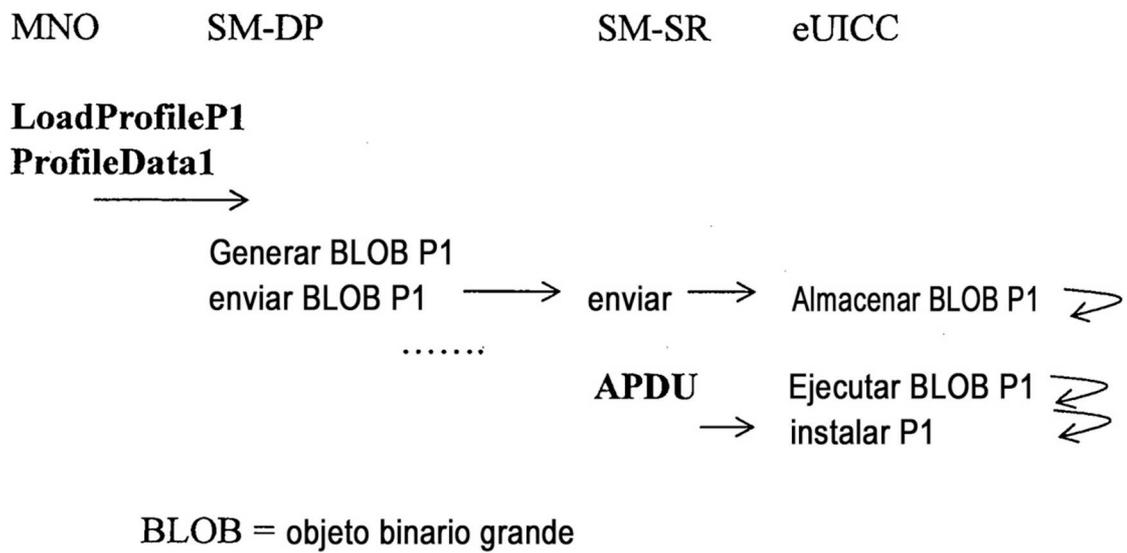


Fig. 2