(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 667 215**

(51) Int. CI.:

H04W 12/04 (2009.01)
H04W 8/20 (2009.01)
H04L 12/24 (2006.01)
H04L 29/08 (2006.01)
H04W 8/18 (2009.01)
H04L 9/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **06.10.2014 PCT/FR2014/052529**

(87) Fecha y número de publicación internacional: **16.04.2015 WO15052422**

(96) Fecha de presentación y número de la solicitud europea: **06.10.2014 E 14796220 (3)**

(97) Fecha y número de publicación de la concesión europea: **31.01.2018 EP 3056037**

(54) Título: **Procedimiento de personalización de un elemento de seguridad**

(30) Prioridad:

07.10.2013 FR 1359690

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
10.05.2018

(73) Titular/es:

IDEMIA FRANCE (100.0%)
420, rue d'Estienne d'Orves
92700 Colombes, FR

(72) Inventor/es:

MAZALI, KAOUTAR;
LARIGNON, GUILLAUME y
DANREE, ARNAUD

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Procedimiento de personalización de un elemento de seguridad

Antecedentes de la invención

La presente invención se sitúa en el campo de la personalización de elementos de seguridad, por ejemplo tarjetas de chips, y en particular tarjetas de chips integradas de tipo eUICC (embedded Universal Integrated Circuit Cards).

De manera conocida, las tarjetas SIM permiten a un operador, por ejemplo a un operador de telefonía móvil, definir los servicios que desea ofrecer a un cliente mediante un mecanismo denominado de "personalización".

La personalización, se efectúa generalmente ya sea por el operador, ya sea por un tercero por cuenta del operador, típicamente un fabricante de la tarjeta consiste de una manera general en configurar la tarjeta SIM con un perfil personalizado que incluye datos de personalización y eventualmente programas, por ejemplo unas applets. Las tarjetas SIM pueden memorizar hoy en día varios perfiles, lo que no era el caso en su origen.

Las dimensiones de las tarjetas SIM extraíbles hacen difícil su utilización en unos aparatos de pequeño tamaño. Para paliar este problema, el ETSI (European Telecommunications Standards Institute) ha definido un formato unido de las tarjetas SIM (MFF2: M2M Form Factor 2) y la GSMA ha definido la arquitectura de software de los elementos de seguridad eUICC a saber "de pequeños elementos de hardware de confianza, que pueden integrarse en los aparatos móviles, para ejecutar unas aplicaciones SIM y permitir el cambio con seguridad de la identidad de suscripción o de datos de suscripción" así como la solución para administrar estos elementos de seguridad eUICC.

La solución adoptada por la GSMA es diferir la personalización de las eUICC hasta que el terminal esté en las manos del usuario final.

La figura 1 representa la arquitectura propuesta por la GSMA para la personalización OTA (Over the Air). Se basa en particular en unos servidores SM-DP (Subscription Management-Data Preparation) adecuados para preparar unos scripts de personalización ejecutables por el elemento de seguridad eUICC por sí mismo. Estos scripts de personalización incluyen una secuencia de comandos, generalmente unos comandos APDU de acuerdo con la norma ISO 7816-4 APDUs.

El documento "Reprogrammable SiMs: Technology, Evolution and Implications Final Report" del 25 de septiembre de 2012, págs. 1-95, trata de la personalización de los elementos SIM reprogramables.

Siempre en el estado actual de la técnica, los scripts de personalización preparados por los servidores SM-DP son entregados al elemento de seguridad eUICC a través de un servidor de transporte SM-SR "Subscription Management-Secure Routing" en una sesión OTA (Over The Air).

Es necesario observar que los scripts de personalización son unos scripts propietarios aunque el operador de la red MNO debe en la práctica comunicar con un servidor SM-DP diferente para cada fabricante de la tarjeta.

La invención se dirige a un método de personalización que no presente dichos inconvenientes.

Objeto y sumario de la invención

De ese modo, y según un primer aspecto, la invención se refiere a un procedimiento de personalización de un elemento de seguridad de acuerdo con la reivindicación 1.

Correlativamente, la invención se refiere también a un servidor de personalización de un elemento de seguridad de acuerdo con la reivindicación 10.

De ese modo, y de manera muy ventajosa, la invención permite al operador no interrelacionarse más que con el servidor de personalización de acuerdo con la invención, siendo adecuado este servidor para comunicar con unos servidores de scripts de pre-personalización para construir unos scripts de personalización propietarios, dicho de otra manera, propios de los diferentes tipos de tarjetas.

En efecto, la invención propone construir unos scripts de personalización a partir:

- de un script de pre-personalización que contiene todos los elementos específicos o propietarios, siendo delegados estos scripts a los servidores de scripts de pre-personalización; y
- de datos de personalización que no hacen referencia a estos formatos propietarios.

De este modo, en el sentido de la invención, la personalización permite transformar un perfil de pre-personalización genérico en un perfil personalizado vinculado a un contrato de servicio específico.

Dicho de otra manera la pre-personalización crea sobre la tarjeta una interfaz de personalización que comprende principalmente un sistema de archivos tal como se define por la norma ISO 7816-4§5, esta interfaz permite modificar el sistema de archivos mediante la utilización de comandos normalizados tales como los definidos por la norma ISO 7816-4§6.

La personalización, que se efectúa a través de esta interfaz, permite transformar una tarjeta genérica en una tarjeta específica para el titular de la tarjeta y para el contrato que vincula a este titular con un suministrador de servicio. Los datos de personalización, tales como el nombre del titular, las claves que permiten el acceso a un servicio de telefonía, un número de cuenta bancaria, por ejemplo, se escribirán mediante la utilización de comandos ISO 7818-4§6.

De manera preferente pero no limitativa, los servidores de scripts de pre-personalización utilizados en la invención pueden estar integrados o conectados a unos servidores SM-DP (Subscription Manager - Data Preparation) del estado actual de la técnica definidos en el documento: "Remote Provisioning Architecture for Embedded UICC" - Versión 1.43 - 1 de julio de 2013, de la GSMA así como el documento "Remote Provisioning Architecture for Embedded UICC - Technical Specification - Draft 1.8" - 20 de septiembre de 2013 de la GSMA.

El servidor de scripts de pre-personalización puede ser un nuevo proceso del servidor SMDP de la técnica anterior.

Se observará que estos servidores SMDP de la técnica anterior son también adecuados para procesar la solicitud emitida por el operador. Estos servidores son:

- conectados a al menos un servidor de operador;
- adecuados para recibir unos modelos o unas especificaciones de perfil de un operador;
- adecuados para generar unos scripts de personalización a partir de reglas internas y para enviar estos scripts a unos servidores de transporte SM-SR.

Por consiguiente, en este modo de realización la invención no modifica ni la interfaz entre el servidor del operador y el servidor de personalización, ni la interfaz entre el servidor de personalización y el servidor de transporte SM-SR, estando definidas estas interfaces en el documento "Remote Provisioning Architecture for Embedded UICC - Technical Specification - Draft 1.8" - 20 de septiembre de 2013 de la GSMA.

En un modo particular de realización de la invención en el que el servidor de personalización es adecuado para analizar y para modificar el script de pre-personalización, el script de personalización se genera integrando los datos de personalización en el script de pre-personalización.

En otro modo de realización, el script de personalización se genera concatenando dichos datos de personalización al script de pre-personalización recibido del servidor de scripts de pre-personalización sin modificación del script de pre-personalización. Este modo de realización es ventajoso principalmente cuando el servidor de personalización no sabe interpretar o no puede modificar el script de pre-personalización.

En un modo particular de realización, el script de pre-personalización y los datos de personalización del script de personalización se envían al elemento de seguridad en un mismo mensaje.

Como variante, el script de pre-personalización y los datos de personalización del script de personalización pueden enviarse al elemento de seguridad por separado, siendo enviados los datos de personalización después de la recepción del mensaje que confirma la buena ejecución del script de pre-personalización en el elemento de seguridad.

En un modo particular de realización, el procedimiento de personalización según la invención incluye una etapa de envío, a un servidor de transporte, de una solicitud para generar un campo de seguridad para el elemento de seguridad en el que deberá instalarse el perfil personalizado.

En un modo particular de realización, el procedimiento de personalización según la invención incluye:

- una etapa de obtención de claves de cifrado generadas por el elemento de seguridad; y
- una etapa de cifrado del script de personalización con las claves.

En un modo particular de realización del procedimiento de personalización según la invención, el script de personalización se envía a un servidor de transporte adecuado para transmitir este script al elemento de seguridad a través de un canal OTA (Over the Air) u OTI (Over the Internet).

En un modo particular de realización, las diferentes etapas del procedimiento de personalización se determinan mediante unas instrucciones de programas informáticos.

En consecuencia, la invención se dirige también a un programa informático sobre un soporte de informaciones, siendo susceptible este programa de ser implementado por un ordenador, incluyendo este programa unas instrucciones adaptadas para la implementación del procedimiento de personalización tal como se ha mencionado anteriormente.

Este programa puede utilizar no importa qué lenguaje de programación, y estar en la forma de código fuente, código objeto, o de un código intermedio entre el código fuente y el código objeto, tal como en una forma parcialmente compilada, o en no importa qué otra forma deseable.

La invención se dirige también a un soporte de informaciones legible por un ordenador, y que incluye unas instrucciones de un programa de ordenador tal como se ha mencionado anteriormente.

El soporte de informaciones puede ser no importa qué entidad o dispositivo capaz de almacenar el programa. Por ejemplo, el soporte puede incluir un medio de almacenamiento, tal como una ROM, por ejemplo un CD-ROM o una ROM de circuito microelectrónico, o también un medio de registro magnético, por ejemplo un disquete (floppy disc) o un disco duro.

Por otra parte, el soporte de informaciones puede ser un soporte transmisible tal como una señal eléctrica u óptica, que puede encaminarse a través de un cable eléctrico u óptico, por radio o por otros medios. El programa según la invención puede descargarse en particular desde una red de tipo Internet.

Alternativamente, el soporte de informaciones puede ser un circuito integrado en el que se incorpora el programa, estando adaptado el circuito para ejecutar o para ser utilizado en la ejecución del procedimiento en cuestión.

Breve descripción de los dibujos

Surgirán otras características y ventajas de la invención a la luz de la descripción que sigue, realizada con referencia los dibujos y a los anexos en los que:

- la figura 1 ya descrita representa la arquitectura propuesta por la GSMA para la personalización OTA;
- la figura 2 representa un servidor de personalización de acuerdo con un modo particular de realización de la invención;
- la figura 3 representa en la forma de organigrama las principales etapas del procedimiento de personalización de acuerdo con un modo particular de realización de la invención;
- el anexo 1 proporciona un ejemplo de datos de personalización;
- el anexo 2 proporciona un ejemplo de modelo de perfil;
- el anexo 3 proporciona un ejemplo de script de pre-personalización; y
- los anexos 4 y 5 proporcionan dos ejemplos de script de personalización.

Descripción detallada de un primer modo de realización

La figura 2 representa un servidor de personalización OTPM de acuerdo con un modo particular de realización de la invención. Este servidor OTPM se conecta al servidor MNO del operador de telefonía, a un servidor SMSR de transporte del perfil y a dos servidores SMDP1, SMDP2 de pre-personalización a través de una red de comunicación NTW. Cada uno de los servidores SMDP1, SMDP2 se distingue de los servidores SM-DP del estado de la técnica en que incorpora un servidor de script de pre-personalización SSPP1, SSPP2. El servidor SMSR de transporte es adecuado para comunicar con un elemento de seguridad eUICC1, eUICC2 a través de un canal OTA (Over The Air) u OTI (Over The Internet).

El servidor de personalización OTPM tiene la arquitectura de hardware de un ordenador. Incluye principalmente un procesador 10, una memoria no volátil de tipo ROM 11, una memoria volátil de tipo RAM 12, unos medios de comunicación 13 y una base de datos 14.

Esta base de datos 14 incluye:

- unos modelos de perfiles Temp1, Temp2 definidos con el operador MNO y descritos en un lenguaje estructurado;
- una tabla que asocia unos servidores de pre-personalización SMDP1, SMDP2 y unos servidores de script de pre-personalización SSDP1, SSDP2 a los identificadores eUID1, eUID2 de elementos de seguridad eUICC1, eUICC2.

La memoria no volátil de tipo ROM 11 constituye un soporte de acuerdo con la invención, incluyendo este soporte un programa informático PG adecuado para implementar un procedimiento de personalización de acuerdo con un primer modo de realización de la invención y cuyas esencias se representan en forma de organigrama en la figura 3.

En el curso de una etapa E10, el servidor de personalización OT-PM recibe una solicitud de personalización RQ1 emitida por un operador MNO para descargar un perfil personalizado de acuerdo con el modelo Temp1 en un

elemento de seguridad eUICC1. Esta solicitud RQ1 incluye unos datos DP de personalización del perfil suministrados en el Anexo 1, un identificador eUID1 del elemento de seguridad eUICC1 y o bien el modelo de perfil Temp1 o bien un identificador Temp1Ref de este modelo de perfil.

Cuando la solicitud RQ1 incluye el modelo de perfil en sí mismo, este se almacena en la base de datos 14.

Se da un ejemplo de modelo de perfil Temp1 en el Anexo 2. Se trata en este ejemplo de un esquema XML que define un archivo a escribir en el elemento de seguridad.

El servidor de personalización OT-PM memoriza los datos de personalización DP en su base de datos 14 en el curso de la etapa E10.

En el curso de una etapa E20, el servidor de personalización OTPM identifica, en la base de datos 14, el servidor de script de pre-personalización SSPP1 capaz de generar un script de pre-personalización del elemento de seguridad eUICC1, a partir del identificador eUID1 de este elemento de seguridad. En el caso en el que el servidor de personalización OTPM es capaz de generar un script de personalización para una tarjeta dada sin necesidad de referirse a un SMDP, el registro para esta tarjeta contendrá, en el campo SMDP, un valor distinto que la dirección del servidor SMDP, un nulo, por ejemplo.

En el modo de realización aquí descrito, el servidor de script de pre-personalización SSPP1 es un proceso del servidor de pre-personalización SMDP1.

En el curso de una etapa E30, el servidor de personalización OT-PM envía al servidor de pre-personalización SMDP1, a través de un enlace de seguridad, una solicitud RQ2 con el fin de obtener un script de pre-personalización SPP1 para el elemento de seguridad eUICC1. Esta solicitud RQ2 incluye el modelo de perfil Temp1 que corresponde al identificador Temp1Ref, al identificador eUID1 del elemento de seguridad eUICC1, y, en este modo de realización, a una referencia RQ1ID de la solicitud RQ1 recibida del operador en la etapa E10.

El servidor de script de pre-personalización SSPP1, genera, en el curso de una etapa F10, un script de pre-personalización ScrPP1 bajo la forma de un bloque de datos estructurado. Este script de pre-personalización ScrPP1, basado en la descripción del modelo de perfil Temp1 incluye unos comandos necesarios para la creación del perfil solicitado por el operador MNO. Se suministra en este ejemplo en el Anexo 3.

En el curso de una etapa E40, el servidor de personalización OTPM recibe del servidor de pre-personalización SPP1, en un enlace de seguridad, un mensaje que incluye el script de pre-personalización ScrPP1, el identificador RQ2ID de la solicitud RQ2 y una dirección de servicio en la que el script de pre-personalización debe enviarse en el elemento de seguridad eUICC1. Esta dirección de servicio puede estar constituida por ejemplo por la Toolkit Application Reference TAR definida en la especificación ETSI SCP 101. 220. En el modo de realización aquí descrito, si no se especifica esta dirección de servicio, el servidor de personalización OTPM utiliza la definida por la norma.

En este primer modo de realización, el servidor de personalización OTPM es adecuado para interpretar el script de pre-personalización ScrPP1. En el curso de una etapa E50, el servidor de personalización OTPM genera un script de personalización ScrP1 integrando los datos de personalización DP en el script de pre-personalización ScrPP1. Este script de personalización ScrP1 se suministra en el Anexo 4 en este ejemplo.

En el curso de una etapa E60, el servidor de personalización OTPM envía al servidor SMSR de transporte de perfil una solicitud RQ3 para que este genere un campo de seguridad en el elemento de seguridad eUICC1, Estando destinado este campo de seguridad, como es conocido, a asegurar la seguridad y la confidencialidad de un perfil personalizado cargado en este elemento de seguridad. En el modo de realización aquí descrito, la solicitud RQ3 incluye un identificador RQ3ID de esta solicitud RQ3, el identificador eUID1 del elemento de seguridad eUICC1 y una descripción DESC1 del perfil personalizado a cargar en el campo de seguridad, una dirección (por ejemplo TAR) de destino del servicio en el elemento de seguridad y el identificador del servidor de pre-personalización SMDP1.

Con la recepción de esta solicitud RQ3, el servidor SMSR de transporte verifica, en el curso de una etapa G10 denominada de elegibilidad, que el perfil solicitado puede ser cargado efectivamente en el elemento de seguridad eUICC1. Esta etapa de elegibilidad puede consistir principalmente en verificar que el tamaño de memoria disponible en el elemento de seguridad eUICC1 es suficiente para memorizar el perfil.

Si se confirma esta elegibilidad, el servidor de transporte SMSR y el elemento de seguridad eUICC1 comunican en el curso de una etapa general G20, a través del canal OTA para crear un campo de seguridad en el seno del elemento de seguridad eUICC1 de acuerdo con las especificaciones GlobalPlatform.

En el curso de una etapa H20 denominada de "Key Generation", una entidad de confianza del elemento de seguridad eUICC1 crea unas claves y asegura la confidencialidad, estando destinadas esas claves a ser proporcionadas como se describe posteriormente al servidor de personalización OTPM.

En el curso de una etapa H30, el elemento de seguridad eUICC1 confirma al servidor de transporte SMSR la creación del campo de seguridad y la generación de las claves. El servidor SMSR informa su vez al servidor de personalización OTPM sobre el buen desarrollo del procedimiento. Este mensaje de confirmación es recibido por el servidor de personalización OTPM en el curso de una etapa E70.

En el curso de una etapa E80, el servidor de personalización OTPM ejecuta un procedimiento para recuperar de manera confidencial las claves generadas en el seno del elemento de seguridad eUICC1 en la etapa H20. Almacena estas claves en su base de datos 14.

En el curso de una etapa E90, el servidor de personalización OTPM cifra el script de personalización ScrP1 utilizando el juego de claves recuperado en la etapa E80. Este cifrado denominado también "Secure Channel" en la norma GlobalPlatform está por ejemplo de acuerdo con el SCP02 de esta norma. A continuación de este cifrado, el perfil personalizado cifrado es un script que contiene una serie de comandos APDU que se descifrarán y ejecutarán por el campo de seguridad del elemento de seguridad eUICC1 creado en la etapa G20.

En el curso de una etapa E100, el servidor de personalización OTPM envía una solicitud RQ4 al servidor de transporte SMSR, incluyendo esta solicitud un identificador de solicitud RQ4ID, la dirección de servicio TAR del elemento de seguridad eUICC1 y un comando CC de carga del perfil personalizado cifrado ScrP1.

El servidor de transporte SMSR autentifica el servidor de personalización OTPM emisor de la solicitud en el curso de la etapa G50, y cifra esta solicitud RQ4 para el transporte de manera que abra un "secure channel" en el seno de la norma GlobalPlatform con el elemento de seguridad eUICC1, por ejemplo siguiendo el método SCP80 o SCP81 de la especificación GP2.2 de esta norma.

El servidor de transporte envía el script de personalización cifrado ScrP1 al campo de seguridad del elemento de seguridad eUICC1 identificado por su dirección de servicio TAR a través del canal OTA u OTI en el curso de una etapa G60.

Este script es recibido por el elemento de seguridad en el curso de una etapa H40. En el curso de una etapa H50, el elemento de seguridad retira el cifrado de transporte efectuado en la etapa G50 y posteriormente transmite este script al campo de seguridad. El campo de seguridad retira entonces el cifrado efectuado por el servidor de personalización OTPM en la etapa E90.

El servicio identificado por su dirección TAR en el elemento de seguridad eUICC1 instala el perfil personalizado ejecutando el script ScrP1 en el curso de una etapa H60. El perfil instalado pero no activo aún pasa entonces al estado DISABLED.

En el curso de una etapa H70, el elemento de seguridad eUICC1 devuelve un acuse de recibo al servidor de transporte SMSR. El servidor SMSR informa su vez al servidor de personalización OTPM sobre el buen desarrollo del procedimiento. Este mensaje de confirmación es recibido por el servidor de personalización OTPM en el curso de una etapa E110.

El servidor de personalización OTPM actualiza su base de datos 14 para reflejar los cambios producidos durante la descarga del perfil del servidor MNO. Genera a continuación un archivo "datos salida" que incluye informaciones útiles para el servidor MNO para activar el perfil en su red, principalmente las claves OTA que le permitirán activar el perfil cuando se active este en el seno del elemento de seguridad eUICC1.

El servidor de personalización OTPM confirma a continuación el buen desarrollo del procedimiento de descarga al servidor MNO.

Primera variante

En el primer modo de realización descrito anteriormente, el servidor de personalización OTPM era adecuado para interpretar el script de pre-personalización ScrPP1 recibido en la etapa E40 y para generar, en la etapa E50, el script de personalización ScrP1 integrando los datos de personalización en el script de pre-personalización ScrPP1.

En una variante de realización de la invención, el servidor de personalización OTPM no sabe interpretar el script de pre-personalización recibido del servidor SMDP1. En ese caso, puede crear, en el curso de una etapa E50', un script de personalización ScrP1' obtenido concatenando el script de pre-personalización ScrPP1, sin modificarlo, con los datos de personalización DP. Se puede utilizar para ello la técnica conocida para el experto en la materia bajo el nombre de "chained scripts" de la que se suministra una representación en el Anexo 5.

Se observará que en el ejemplo del Anexo 5, el script de personalización ScrP1' utiliza dos direcciones de servicio TAR1, TAR2.

Por consiguiente, en este modo de realización, después de la etapa de descifrado H50, el elemento de seguridad eUICC1 separa los dos bloques en el curso de una etapa H60', transmite el script de pre-personalización ScrPP1 a la primera dirección de servicio TAR1 que está encargada de instalarlo. El estado del perfil pasa a PRE-PERSONNALIZED.

Después, el elemento de seguridad transmite el segundo bloque correspondiente a los datos de personalización al servicio de dirección TAR2 encargado de provisionar los datos.

Las direcciones de servicio TAR1 y TAR2 pueden ser diferentes o idénticas.

Segunda variante

En el primer modo de realización, y en la primera variante anterior, el script de pre-personalización ScrPP1 y los datos de personalización DP eran transmitidas por el servidor de personalización OTPM al elemento de seguridad eUICC1, a través del servidor de transporte SMSR, en una única solicitud RQ4 (etapas E100 y G60).

Como variante, es posible efectuar esta descarga en dos veces. Se obtiene entonces el escenario siguiente, después de la etapa E80 de recuperación de las claves por el servidor de personalización OTPM:

- el servidor OTPM cifra únicamente el script de pre-personalización y lo transmite al servidor de transporte SMSR;
- el servidor de transporte SMSR añade un cifrado de transporte y transmite el script de pre-personalización al elemento de seguridad eUICC1;
- el script de pre-personalización es recibido por el elemento de seguridad a través del canal OTA/OTI, descifrado, e instalado en el campo de seguridad;
- un vez recibida la confirmación por el servidor de personalización OTPM, este cifra el script de personalización y reitera el proceso anterior (transmisión al servidor de transporte SMSR, cifrado, trasmisión al elemento de seguridad por el canal OTA/OTI, descifrado por el elemento de seguridad eUICC1 para instalación en el campo de seguridad, confirmación, envío del archivo "datos salida" al servidor MNO.

ANEXO 1

EF 2F00:
contenido: 611E4F07A00000000101015013

ANEXO 2

```
<scdp: EstructuraDatos>
    <scdp: EstructuraArchivo ElementoMatriz="EF" IndiceMatriz="#">
      <scdp: EF fid="2F00" sfi="30" tipo="LV" formato="asnl.efdir" nombre="EF_DIR" contenido=""/>
</scdp:EstructuraArchivo>
</scdp:EstructuraDatos>
```

ANEXO 3

ISO 7816-4 comando para crear EF DIR

ANEXO 4

ISO 7816-4 comando para crear EF_DIR
ISO 7816-4 comando para escribir 611E4F07A00000000101015013 en EF_DIR

ANEXO 5

comienzo del script encadenado
TAR1
abrir sesión
ScrPP1 encriptado
cerrar sesión

TAR2
abrir sesión
encriptado (ISO 7816-4 comando para escribir 611E4F07A00000000101015013 en EF_DIR)
cerrar sesión
fin del script encadenado

REIVINDICACIONES

1. Procedimiento de personalización de un elemento de seguridad (eUICC) que incluye:

- una etapa (E10) de recepción de una solicitud de personalización (RQ1) emitida por un operador (MNO) para descargar un perfil personalizado en un elemento de seguridad (eUICC1), incluyendo dicha solicitud unos datos de personalización (DP) y un identificador del elemento de seguridad (eUID1);
- una etapa (E50) de generación de un script (ScrP1) de personalización de dicho elemento de seguridad (eUICC1);
- una etapa (E100) de envío del script de personalización con destino en dicho elemento de seguridad (eUICC), siendo adecuado dicho elemento de seguridad (eUICC) para ejecutar dicho script de personalización (ScrP1) para instalar dicho perfil personalizado en dicho elemento de seguridad (eUICC1),

estando dicho procedimiento caracterizado por que:

- en dicha solicitud de personalización, el perfil personalizado está de acuerdo con un modelo de perfil (Temp1), emitiendo el operador o bien este modelo de perfil, o bien un identificador (Temp1Ref) de dicho modelo en dicha solicitud y por que incluye:

- una etapa (E20) de identificación, a partir del identificador del elemento de seguridad, de un servidor de pre-personalización (SSPP) adecuado para comunicar un script de pre-personalización, siendo adecuado dicho script para pre-personalizar dicho elemento de seguridad (eUICC1);
- una etapa (E40) de recepción del mensaje de dicho servidor de pre-personalización (SMDP1) que incluye un script (ScrPP1) de pre-personalización del elemento de seguridad (eUICC1) basado en la descripción de dicho modelo de perfil, siendo generado dicho script de personalización utilizando dicho script (ScrPP1) de pre-personalización y los datos (DP) de personalización.

2. Procedimiento de personalización según la reivindicación 1, caracterizado por que dicho servidor de pre-personalización (SSPP) se conecta a un servidor de personalización (SMDP).

3. Procedimiento de personalización según la reivindicación 1 o 2, caracterizado por que dicho script de personalización (ScrP1) se genera (E50) integrando dichos datos de personalización (DP) en dicho script de pre-personalización (ScrPP1).

4. Procedimiento de personalización según la reivindicación 1 o 2, caracterizado por que dicho script de personalización (ScrP1') se genera (E50') concatenando dichos datos de personalización (DP) al script de pre-personalización (ScrPP1) recibido en dicho servidor de pre-personalización (SMDP1) sin modificación de dicho script de pre-personalización (ScrPP1).

5. Procedimiento de personalización según una cualquiera de las reivindicaciones 1 a 4, caracterizado por que dicho script de pre-personalización y dichos datos de personalización de dicho script de personalización se envían al elemento de seguridad (eUICC1) en un mismo mensaje.

6. Procedimiento de personalización según una cualquiera de las reivindicaciones 1 a 4, caracterizado por que dicho script de pre-personalización y dichos datos de personalización de dicho script de personalización se envían al elemento de seguridad (eUICC1) por separado, siendo enviados dichos datos de personalización después de la recepción del mensaje que confirma la buena ejecución del script de pre-personalización en el elemento de seguridad.

7. Procedimiento de personalización según una cualquiera de las reivindicaciones 1 a 6, caracterizado por que incluye una etapa (E60) de envío a un servidor (SMSR) de transporte, de una solicitud (RQ3) para generar un campo de seguridad en dicho elemento de seguridad (eUICC1) en el que deberá instalarse dicho perfil personalizado.

8. Procedimiento de personalización según una cualquiera de las reivindicaciones 1 a 7, caracterizado por que incluye:

- una etapa (E80) de obtención de claves de cifrado generadas por el elemento de seguridad (eUICC1); y
- una etapa (E90) de cifrado de dicho script de personalización (ScrP1) con dichas claves.

9. Procedimiento de personalización según una cualquiera de las reivindicaciones 1 a 8, caracterizado por que dicho script de personalización (ScrP1) se envía (E100) a un servidor de transporte (SMSR) adecuado para transmitir dicho script al elemento de seguridad a través de un canal OTA (Over the Air) u OTI (Over the Internet).

10. Servidor (OTPM) de personalización de un elemento de seguridad (eUICC) que incluye:

- unos medios (13) de recepción de una solicitud de personalización (RQ1) emitida por un operador (MNO) para descargar un perfil personalizado en un elemento de seguridad (eUICC1), incluyendo dicha solicitud unos datos de personalización (DP) y un identificador del elemento de seguridad (eUID1);
- unos medios (10) de generación de un script (ScrP1) de personalización de dicho elemento de seguridad (eUICC1);
- unos medios (13) de envío del script de personalización (ScrPI) con destino en dicho elemento de seguridad (eUICC), siendo adecuado dicho elemento de seguridad (eUICC) para ejecutar dicho script de personalización (ScrPI) para instalar dicho perfil personalizado en dicho elemento de seguridad (eUICCI),

estando dicho servidor caracterizado por que incluye:

- unos medios (14) de identificación, a partir del identificador del elemento de seguridad, de un servidor de pre-personalización (SMDP1) adecuado para pre-personalizar dicho elemento de seguridad (eUICC1);
- unos medios (13) de interrogación de dicho servidor de pre-personalización (SMDP1) para obtener un mensaje que incluye un script (ScrPP1) de pre-personalización del elemento de seguridad (eUICC1) basado en la descripción de dicho modelo de perfil, siendo generado dicho script de personalización utilizando dicho script (ScrP1) de pre-personalización y los datos (DP) de personalización.

11. Programa informático (PG) que incluye instrucciones para la ejecución de las etapas del procedimiento de personalización según una cualquiera de las reivindicaciones 1 a 9, cuando dicho programa se ejecuta por un ordenador (OTPM).

12. Soporte de registro (11) legible por un ordenador (OTPM) en el que se registra un programa informático (PG) que comprende unas instrucciones para la ejecución de las etapas del procedimiento de personalización según una cualquiera de las reivindicaciones 1 a 9.

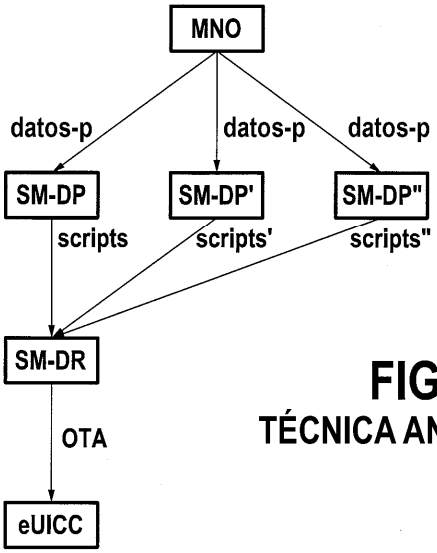

FIG.1
TÉCNICA ANTERIOR

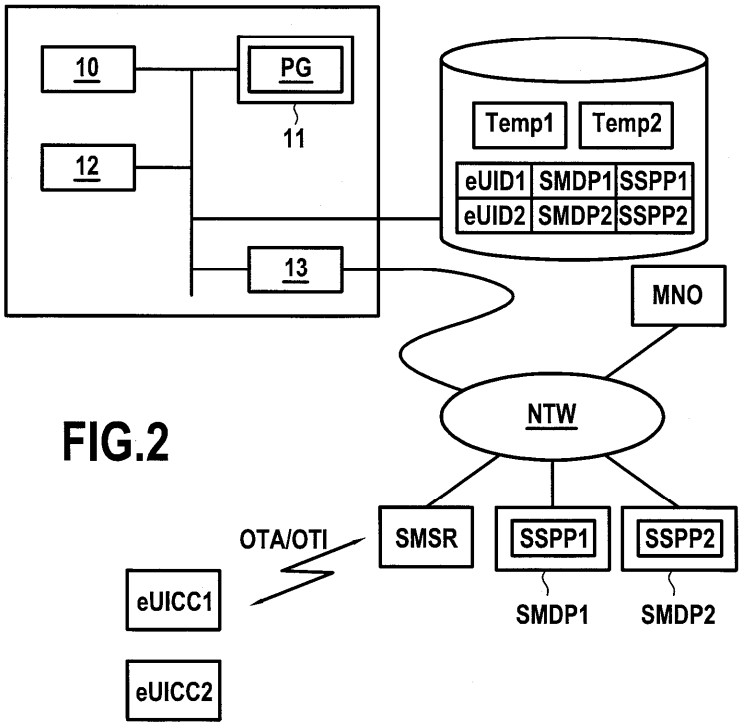

FIG.2

FIG.3a
FIG.3b
FIG.3

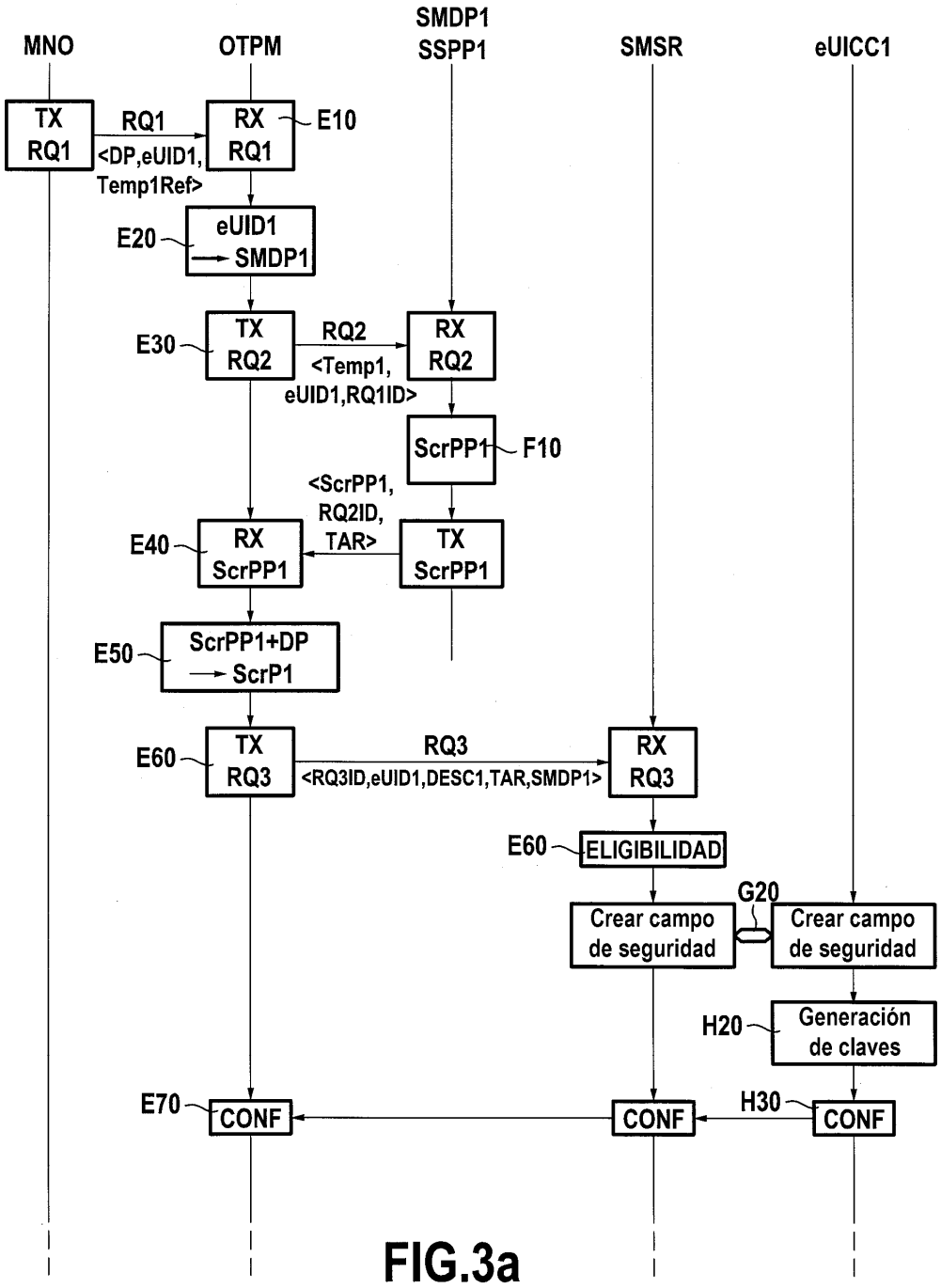

FIG.3a

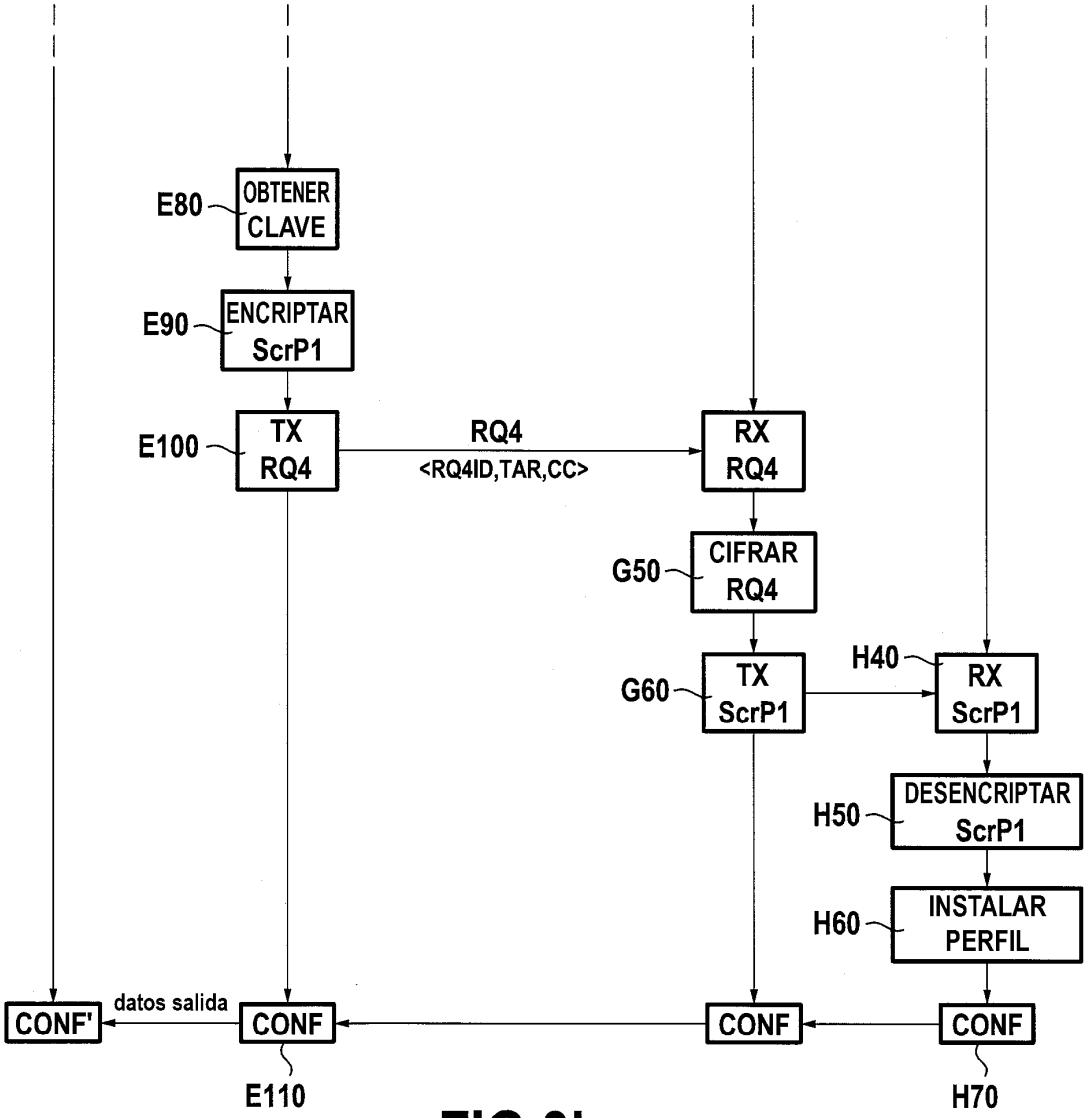
E80
OBTENER CLAVE
E90
ENCRIPTAR ScrP1
E100
TX RQ4
RQ4
<RQ4ID,TAR,CC>
RX RQ4
G50
CIFRAR RQ4
G60
TX ScrP1
H40
RX ScrP1
H50
DESENCRIPTAR ScrP1
H60
INSTALAR PERFIL
CONF'
datos salida
CONF
CONF
CONF
E110
H70

FIG.3b