

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 886 035**

51 Int. Cl.:

H04W 8/20 (2009.01)

H04W 4/60 (2008.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **24.06.2016** **PCT/EP2016/001084**

87 Fecha y número de publicación internacional: **29.12.2016** **WO16206813**

96 Fecha de presentación y número de la solicitud europea: **24.06.2016** **E 16732448 (2)**

97 Fecha y número de publicación de la concesión europea: **11.08.2021** **EP 3314933**

54 Título: **Comunicación de un módulo de identificación de abonado con un servidor, en particular, durante un cambio de perfil**

30 Prioridad:

25.06.2015 DE 102015008179

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

16.12.2021

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:

ISERN JARA, Jorge

ES 2 886 035 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

Comunicación de un módulo de identificación de abonado con un servidor, en particular, durante un cambio de perfil

5 Ámbito de la invención

La invención se refiere a un procedimiento para la comunicación con un servidor, de un módulo de identificación de abonado implementado o que se puede implementar en un dispositivo terminal, en el que, al menos, un perfil está configurado para el uso del dispositivo terminal móvil en una red de telefonía móvil, en particular, durante un cambio de perfil.

10 Estado de la técnica

Para el uso de un dispositivo terminal móvil como un teléfono inteligente o un teléfono móvil en una red de telefonía móvil de un operador de red, el dispositivo terminal contiene un módulo de identificación de abonado con un perfil de suscripción (perfil de suscripción = conjunto de datos de identificación de abonado), o también solo, brevemente, un perfil. El perfil de suscripción está formado por un conjunto de datos que permite el establecimiento, el funcionamiento y la finalización de una conexión del dispositivo terminal en la red de telefonía móvil. El conjunto de datos puede estar alojado en una estructura de archivos. El conjunto de datos comprende datos, que a su vez, comprenden datos generales y datos de autenticación ("credenciales"), y aplicaciones. En particular, el conjunto de datos comprende —como una credencial— una clave criptográfica de autenticación Ki, así como una Identidad Internacional del Abonado Móvil (IMSI). El módulo de identificación de abonado puede estar diseñado, por ejemplo, como tarjeta enchufable extraíble SIM (U,C) (SIM = Módulo de Identificación de Abonado) o UICC (Tarjeta de Circuito Integrado Universal), o como eUICC (UICC embebida) o SIM (U,C) unida fija por soldadura (o bien prevista para unión fija por soldadura) eUICC (UICC embebida) o SIM e(U,C).

SIM y USIM designan módulos de identificación de abonado con una tecnología de acuerdo con el estándar 3GPP mantenido por ETSI, que comprende GSM y UMTS. CSIM designa un módulo de identificación de abonado con una tecnología de acuerdo con el estándar 3GPP2, que comprende CDMA2000.

Entretanto, se proponen también módulos de identificación de abonado con varios perfiles, de los cuales por lo general respectivamente solo uno de ellos está en un estado activo o estado "habilitado", y otros perfiles están en un estado inactivo o estado "deshabilitado".

El documento [1] SGP02-Remote-Provisioning-Architecture-for-Embedded-UICC-Technical-Specification-v2.0, 13 de octubre de 2014, GSMA describe el mantenimiento remoto de perfiles en un módulo de identificación de abonado en forma de un eUICC por medio de un Ruteador Seguro de Gestión de Suscripción (SM-SR). Según [1] cap. 5.3.5, se puede activar un perfil en la eUICC por medio de una función «HabilitarPerfil» realizada en la eUICC, esto es, cambiar (conmutar) a un estado o status activo. Después de la ejecución, la función es capaz de emitir un estado de ejecución de función que indique si la activación fue exitosa. Este estado se puede enviar en un mensaje de estado al Ruteador Seguro de Gestión de Gestión de Suscripción (SM-SR).

El documento [2] DE 10 2012 018 540 A1 del estado de la técnica divulga un módulo de identificación de abonado con dos perfiles de suscripción, entre los cuales se puede conmutar.

El documento [3] WO 2013/075873 A1 del estado de la técnica divulga un módulo de identificación de abonado con dos perfiles de suscripción, entre los cuales se puede conmutar.

El documento [4] WO 2014/131785 A1 del estado de la técnica divulga un procedimiento para el cambio de estado en un módulo de identificación de abonado con varios perfiles de suscripción. Mediante un comando de estado «habilitar» o «deshabilitar» enviado desde un Servidor Gestor de Suscripción al módulo de identificación de abonado, se puede cambiar un estado de un perfil entre activo e inactivo. En el comando de estado que envía el servidor pueden estar añadidos parámetros de respuesta y un modo de respuesta, mediante los cuales el servidor establece la forma en la que el módulo de identificación de abonado deberá enviar una «respuesta» al servidor.

El documento [6] WO 2007/133139 A1 del estado de la técnica divulga un módulo de identificación de abonado con varios perfiles de suscripción, entre los cuales se puede conmutar, realizándose una selección por parte del usuario de una preferencia de perfil por medio de un control del lado de red.

El documento [7] US 2012/0106533 A1 del estado de la técnica divulga un módulo de identificación de abonado con varios perfiles de suscripción. El módulo recibe un mensaje de un sistema de programación con la orden de consultar inmediatamente actualizaciones del sistema de programación («*polling request*»). Para enviar la consulta, exploran estaciones base disponibles y, luego, sobre la base de los tipos hallados de estación base, se selecciona una tecnología para enviar la consulta.

Dependiendo de la tecnología empleada en el módulo de identificación de abonado (por ejemplo, 3GPP o 3GPP2) están codificados de manera diferente conexiones de datos y elementos de datos (por ejemplo, mensajes de Servicio de Mensajes Cortos, SMS) que el módulo de identificación de abonado intercambia con un servidor de la red de telefonía móvil. Si en un módulo de identificación de abonado tiene lugar un cambio de perfil entre perfiles, que están sujetos a diferentes tecnologías, por ello se puede perder o, al menos, se puede ver afectada la accesibilidad y/o la capacidad de emisión del dispositivo terminal por un cambio de perfil. A causa de ello, en particular, se puede dar la situación de que, tras un cambio de perfil, del cual va acompañado un cambio de tecnología, el módulo de identificación de abonado ya no está en condiciones de informar al Ruteador Seguro de Gestión de Suscripción (SM-SR) que ha tenido lugar el cambio de perfil.

En el documento [4] WO 2014/131785 A1 se asegura la accesibilidad y/o la capacidad de emisión del dispositivo terminal en el caso de un cambio de perfil, al añadirse al comando de estado, con el cual se realiza el cambio de perfil, parámetros de respuesta y un modo de respuesta que corresponden al perfil a activar. A causa de esto, la OTA se eleva hasta el volumen de datos a transmitir, como mínimo, en los datos para los parámetros de respuesta y el modo de respuesta. Además, en el caso de un cambio autónomo de perfil en el módulo de identificación de abonado, sin que el servidor solicite el cambio de perfil, el procedimiento del documento [4] WO 2014/131785 A1 no es aplicable y, no obstante, se pueden perder la accesibilidad y/o la capacidad de emisión del dispositivo terminal.

Resumen de la invención

La invención se basa en la tarea de crear un procedimiento eficiente para la comunicación de un módulo de identificación de abonado, en el que, al menos, un perfil está configurado para el uso del dispositivo terminal móvil en una red de telefonía móvil, con un servidor, en el que la accesibilidad y/o la capacidad de emisión del dispositivo terminal quedan garantizadas de la mejor manera posible. En particular, se debe detallar un procedimiento semejante para la comunicación, que se puede emplear en el caso de un cambio de perfil. El procedimiento, en particular, se debe poder emplear en el caso de un cambio autónomo de perfil que se realiza en el módulo de identificación de abonado, sin que el servidor solicite un cambio de perfil.

La tarea se cumple mediante un procedimiento de acuerdo con la reivindicación 1. En las reivindicaciones dependientes se detallan realizaciones ventajosas de la invención.

El procedimiento de acuerdo con la reivindicación 1 está configurado para la comunicación con un servidor de un módulo de identificación de abonado (eUICC) implementado o que se puede implementar en un dispositivo terminal, en el que, al menos, un perfil está configurado para el uso del dispositivo terminal móvil en una red de telefonía móvil. En el procedimiento se envía un mensaje desde el módulo de identificación de abonado al servidor. El procedimiento está caracterizado porque, antes de enviar el mensaje en el módulo de identificación de abonado, se ejecuta una etapa de la determinación de una tecnología, en la cual se determina a qué tecnología corresponde el perfil, y el envío se realiza de manera selectiva conforme a la tecnología.

Debido a que se determina la tecnología antes de enviar el mensaje y el envío se efectúa de manera selectiva conforme a la tecnología, se previene un fallo del envío, que en el estado de la técnica se puede producir por la incompatibilidad entre la tecnología presupuesta en el módulo de identificación de abonado y los ajustes tecnológicos empleados realmente durante el envío. En el estado de la técnica, un envío conforme a la tecnología se produce de manera sumamente ocasional, por ejemplo, en casos en los que no se produce un cambio de tecnología. Por lo tanto, la capacidad de emisión del módulo de identificación de abonado está asegurada. Asimismo, un participante de la comunicación que recibe un mensaje enviado como se describe más arriba puede reconocer la tecnología por medio del mensaje y enviar de vuelta al módulo de identificación de abonado un mensaje de respuesta conforme a la tecnología. Por lo tanto, también está asegurada la accesibilidad del módulo de identificación de abonado.

Por ello, en resumen, de acuerdo con la reivindicación 1, se ha creado un procedimiento en el que quedan garantizadas de la mejor manera posible la accesibilidad y/o la capacidad de emisión del dispositivo terminal.

Opcionalmente, como servidor está previsto un servidor de gestión de suscripción, en particular, un Ruteador Seguro de Gestión de Suscripción (SM-SR).

Opcionalmente, como tecnología está prevista 3GPP y/o 3GPP2. Aquí, opcionalmente se puede emplear en general una tecnología en un único perfil. En forma alternativa, en un único perfil están previstas varias tecnologías.

Opcionalmente, como mensaje está previsto un mensaje de estado, por medio del cual se indica un cambio de estado, en particular, de activación o desactivación, del perfil.

Opcionalmente, el perfil previsto en el módulo de identificación de abonado está primero en un estado activo. Allí, como mensaje está previsto un mensaje de estado, por medio del cual se indica un cambio de perfil, del perfil a un perfil distinto implementado en el módulo de identificación de abonado. Precisamente durante un cambio de perfil es importante que el dispositivo terminal siga teniendo capacidad de emisión. Mediante ello se garantiza que se pueda

comunicar el cambio de perfil al servidor, incluso cuando un cambio de tecnología va acompañado del cambio de perfil, por ejemplo, de CSIM a USIM o viceversa. En el estado de la técnica, por el contrario, puede quedar descubierto un cambio de perfil, puesto que el módulo de identificación de abonado, por el cambio de perfil, pierde la capacidad de emisión y el servidor, por lo tanto, supone falsamente que el perfil original sigue estando activo. En este supuesto, fallaría asimismo otra comunicación subsiguiente entre el servidor y el módulo de identificación de abonado.

Además, opcionalmente, el perfil (original) en el módulo de identificación de abonado está diseñado en primer lugar, en especial, como perfil activo, que por lo tanto tiene un estado activo. Adicionalmente al perfil, está implementado al menos otro perfil, que está planeado como perfil inactivo, que por lo tanto tiene un estado inactivo. Al menos la mayoría del tiempo solo un perfil a la vez tiene un estado activo. En el procedimiento se realiza un cambio de perfil al desactivarse primero el perfil activo, de modo que se lo pasa a un estado inactivo. Luego se activa uno de los otros perfiles, de modo que el otro perfil se pasa a un estado activo. Después del cambio de perfil, se envía el mensaje de estado al servidor. Si primero se desactiva el perfil activo y luego se activa el otro perfil, en general, solo está activo un perfil. Si, por el contrario, primero se activa uno de los otros perfiles e inmediatamente después se desactiva el perfil activo originalmente, al menos, la mayoría del tiempo solo está activo uno a la vez, excepto por el período breve entre la activación del nuevo perfil y la desactivación del viejo perfil. Sin embargo, con preferencia se realiza el cambio de perfil conmutando entre dos contenedores de perfil, de modo que la desactivación del antiguo perfil (al principio, activo) y la activación del nuevo perfil se realizan por medio de una única etapa. Opcionalmente, el cambio de perfil desde un perfil "antiguo" originalmente activo a un perfil nuevo se realiza al configurar, en el perfil antiguo primero activo, el contenedor de perfil del nuevo perfil como contenedor de perfil a activar, luego se envía un comando RESTABLECER al módulo de identificación de abonado, en reacción al RESTABLECER se conmuta el perfil activo del contenedor de perfil del perfil antiguo al contenedor de perfil del nuevo perfil y finalmente se inicia la comunicación normal, comenzando con una ATR (Respuesta a Reinicio) y eventualmente APDU subsiguientes. Aquí, la conmutación de perfil se realiza después del RESTABLECER y antes de la ATR. En lugar de RESTABLECER, eventualmente se podría emplear también un comando diferente con un efecto técnico equivalente.

Opcionalmente, durante la etapa de determinación de la tecnología, sobre la base de un resultado de la determinación, se establece una o varias vías de comunicación, las cuales luego se pueden emplear para la comunicación del módulo de identificación de abonado con el servidor. En particular, se pueden establecer varias de comunicación dispuestas según una instrucción de uso, en particular, de acuerdo con una priorización o selección. Opcionalmente, en cada caso se puede disponer una vía de comunicación de una tecnología, opcionalmente en cada caso una vía de comunicación diferente, pero opcionalmente también en algunos o en todos los casos la misma vía de comunicación.

Opcionalmente, las vías de comunicación comprenden una o varias de las siguientes: una conexión de datos, una conexión de Servicio de Mensajes Cortos (SMS), una conexión de mensaje de voz (término técnico, «voz»), una conexión de cadena SS, una conexión de cadena USSD.

Opcionalmente, en un perfil están previstas al menos dos porciones que corresponden a tecnologías diferentes (por ejemplo, USIM y CSIM), estableciéndose respectivamente una vía de comunicación diferente para las, como mínimo, dos tecnologías diferentes, por ejemplo, conexión de datos para USIM LTE y conexión de voz para CSIM, o viceversa.

Opcionalmente, el mensaje enviado o a enviar desde el módulo de identificación de abonado al servidor está embebido en un protocolo de establecimiento de conexión de 3 vías. Allí, el mensaje se envía como primer mensaje. De acuerdo con el protocolo de establecimiento de comunicación de 3 vías, después de enviar el primer mensaje, se debe enviar un segundo mensaje del servidor al módulo de identificación de abonado, y después de enviar el segundo mensaje, se debe enviar un tercer mensaje del módulo de identificación de abonado al servidor. En el protocolo de establecimiento de conexión de 3 vías realizado completamente, se envían todos, los tres, mensajes. En el estado de la técnica, se pueden llegar a producir terminaciones anormales en el protocolo debido a la pérdida de capacidad de emisión por el cambio no reconocido de tecnología. Con la invención se impiden dichas terminaciones anormales.

Opcionalmente, se comunican mensajes, con los que se informa un cambio de perfil, embebidos en un protocolo de establecimiento de conexión de 3 vías y otros mensajes se comunican embebidos en un protocolo de establecimiento de conexión de 2 vías. El mensaje particularmente crítico sobre el cambio de perfil se envía en el protocolo de establecimiento de conexión de 3 vías, que ofrece una seguridad mayor. Los mensajes generales menos críticos se transmiten en el protocolo de establecimiento de conexión de 2 vías, que ahorra datos.

Opcionalmente, la etapa de determinación de una tecnología se realiza al determinar un parámetro que tiene un valor de parámetro específico para una tecnología.

Opcionalmente, para la determinación de parámetros se lee un campo de parámetro (por ejemplo, ADF). Esto puede ocurrir opcionalmente mediante lectura directa y metódica. En forma alternativa, el campo de parámetro se puede leer procesando un comando, por ejemplo, un comando ISO/IEC 7816-4 como AUTENTICAR o un ETSI TS 102 223

PROPORCIONAR INFORMACIÓN DE LOCALIZACIÓN en el módulo de identificación de abonado, durante lo cual se usa el procesamiento del parámetro. Aquí, durante el procesamiento del comando, también se lee de paso el campo de parámetro.

- 5 Opcionalmente, a la tecnología se le asigna un canal lógico según ISO/IEC 7816-4, en particular, el canal básico Canal 0, o eventualmente, en caso de que existan varias tecnologías en el perfil, a cada tecnología se le asigna un canal lógico propio de acuerdo con ISO/IEC 7816-4.

Breve descripción de los dibujos

- 10 A continuación, se explica más en detalle la invención por medio de ejemplos de realización y con referencia a los dibujos en los que se muestra:

- Figura 1 un diagrama de un perfil para una suscripción a una red móvil;
- 15 Figura 2 un diagrama de detalle del campo de datos de aplicación mostrado en la figura 1;
- Figura 3 un diagrama para ilustrar la invención;
- 20 Figura 4 otro diagrama para ilustrar la invención;
- Figura 5 un diagrama para ilustrar la determinación de una tecnología mediante el procesamiento de un comando AUTENTICACIÓN INTERNA en el módulo de identificación de abonado.

Descripción detallada de ejemplos de realización

- La figura 1 muestra un diagrama de un perfil para una suscripción a una red móvil que, desde el punto de vista de la estructura básica, está desarrollado de acuerdo con el estado de la técnica ISO/IEC 7816-4, y que es adecuado para materializar la invención. En la figura 1, a modo de ejemplo, el perfil está alojado en un contenedor de perfil. En la
- 30 figura 1 y la figura 2 se emplean términos técnicos difundidos en inglés que se emplean en estándares técnicos relevantes y que, en parte, también se emplean en alemán sin traducirlos al alemán. El contenedor de perfil contiene un sistema de archivos que, a su vez, contiene un archivo maestro MF. Subordinados o secundarios al archivo maestro MF, el contenedor de perfil contiene archivos elementales EF, archivos dedicados DF y archivos de datos de aplicación ADF.

- 35 De especial importancia para la invención son los archivos de datos de aplicación ADF, como se expone en detalle por medio de la figura 2. El perfil contiene, al menos, un archivo de datos de aplicación ADF1, que, a su vez, está subordinado a los EF y los DF, como se muestra esquemáticamente en la figura 2. En el Archivo de Datos de aplicación ADF1 está indicada, en particular, una tecnología, en la cual se opera el perfil, para ADF1, por ejemplo, USIM.
- 40

- Con relación a la invención, es de importancia además el objeto «Ajustes SM-SR», en el cual se puede grabar, entre otros, qué vía de comunicación se debe emplear (por ejemplo, SMS, conexión de voz, conexión de datos) y allí, eventualmente, qué vía de comunicación, dependiendo de ciertas condiciones.

- 45 Opcionalmente, también se puede establecer una determinada vía de comunicación ya en la producción del módulo de identificación de abonado (tradicionalmente, en parte aún denominada «producción en tarjetas», incluso cuando el factor de forma ya no es necesariamente el de una tarjeta) como vía de comunicación estándar, que se usa en tanto no se imparta una orden expresa distinta para una vía de comunicación.

- 50 La figura 2 muestra, de acuerdo con una forma de realización de la invención, una zona de archivos de datos de aplicación ADF, en la cual están contenidos varios archivos de datos de aplicación ADF, ADF1, ADF2, ADF3, ... ADFn. Un primer archivo de datos de aplicación ADF1 está configurado para la tecnología USIM. Un segundo archivo de datos de aplicación ADF2 está configurado para la tecnología CSIM. Para el primer ADF1 operado con USIM está ocupado el canal básico «Canal lógico 0» de acuerdo con ISO/IEC 7816-4. Para el segundo ADF2 operado con CSIM, está ocupado un canal «Canal lógico 1» diferente al canal básico, según ISO/IEC 7816-4. Para otros ADF y tecnologías, pueden estar ocupados otros canales lógicos.
- 55

- La figura 3 muestra un diagrama, en el cual está ilustrado un procedimiento para la comunicación de un módulo de identificación de abonado eUICC con un servidor SM-SR durante un cambio de perfil, de acuerdo con una primera forma de realización de la invención. El servidor está realizado como Ruteador Seguro de Gestión de Suscripción SM-SR de acuerdo con [1] SGP02-Remote-Provisioning-Architecture-for-Embedded-UICC-Technical-Specification-v2.0, 13 de octubre de 2014, GSMA. En el ejemplo de la figura 3 está establecida en cada perfil P1, P2, en correspondencia con una forma básica de la invención, respectivamente, solo una única tecnología.
- 60

En el módulo de identificación de abonado eUICC están implementados un perfil inicialmente activo P1 y otro perfil P2. Cada uno de los dos perfiles P1, P2 está alojado, por ejemplo, en un contenedor propio de perfiles como el que se muestra en la figura 1, figura 2. En el campo de datos de la aplicación ADF está establecida la tecnología empleada para el perfil (o bien varias tecnologías, compárese con figura 2). Aquí, perfiles diferentes pueden estar sujetos a diferentes tecnologías. El módulo de identificación de abonado eUICC realiza internamente un cambio de perfil del perfil inicialmente activo P1 a otro perfil P2, es decir, activa el otro perfil P2 y desactiva el perfil inicialmente activo P1 (cómo y, eventualmente, siempre también en qué orden). El cambio de perfil se puede efectuar, con preferencia, de manera completamente autónoma en el módulo de identificación de abonado eUICC, pero de manera alternativa también puede ser iniciada desde el exterior por el servidor SM-SR. Después del cambio de perfil, el módulo de identificación de abonado eUICC verifica (pseudocomando «verificar») a qué tecnología corresponde el nuevo perfil activo P2 y determina como tecnología T2 de P2 la tecnología CSIM. A continuación, el módulo de identificación de abonado eUICC comunica al servidor SM-SR en un establecimiento de conexión de 3 vías que el otro perfil P2 es el perfil activo. Para ello, el módulo de identificación de abonado eUICC envía un primer mensaje de estado m1 al servidor SM-SR. El servidor SM-SR recibe el primer mensaje m1 y ahora sabe que la vía de comunicación funciona del módulo de identificación de abonado eUICC al servidor SM-SR. El servidor SM-SR envía al módulo de identificación de abonado eUICC un segundo mensaje m2 como confirmación de la recepción del primer mensaje m1. El módulo de identificación de abonado eUICC recibe el segundo mensaje m2 y ahora sabe que ambas vías de comunicación entre el módulo de identificación de abonado eUICC y el servidor SM-SR funcionan. El módulo de identificación de abonado eUICC envía al servidor SM-SR en respuesta al segundo mensaje m2 un tercer mensaje m3, como confirmación de la recepción de la primera confirmación. El servidor SM-SR recibe el tercer mensaje m3 y ahora sabe que ambas vías de comunicación entre el módulo de identificación de abonado eUICC y el servidor SM-SR funcionan.

La figura 4 muestra un diagrama, en el cual se ilustra un procedimiento para la comunicación de un módulo de identificación de abonado eUICC con un servidor SM-SR durante un cambio de perfil, de acuerdo con una segunda forma de realización de la invención. En principio, el procedimiento es análogo al desarrollado en la figura 3. Adicionalmente, en el procedimiento según la figura 4, después de determinar la tecnología aplicable al otro perfil P2, aquí asimismo CSIM, se fija (pseudocomando «informar») que para el otro perfil P2 ahora activo, con tecnología CSIM, se debe emplear la vía de comunicación de los Mensajes de Servicio de Mensajes Cortos SMS. En consecuencia, se envían el primer, el segundo y el tercer mensaje m1, m2, m3 en forma de mensajes de Servicio de Mensajes Cortos SMS. En lugar de SMS, de manera alternativa, se puede fijar conexión de datos como vía de comunicación.

El comando «informar», con el que se fija la vía de comunicación, puede ser parte, por ejemplo, del comando GSMA ENABLE, con el cual se activa un perfil.

En desarrollos ulteriores de la segunda forma de realización de acuerdo con la Fig. 4 se fija por medio de «instrucción» una lista de vías de comunicación priorizadas. Por ejemplo, se fija que se intenta primero el envío SMS del primer mensaje m1. En caso de que falle el envío mediante SMS, se intenta luego un envío por medio de una conexión de datos. De modo opcional, se intenta primero con conexión de datos y luego por medio de SMS.

La figura 5 muestra un diagrama para ilustrar la determinación de una tecnología T, aquí CSIM, mediante el procesamiento de un comando AUTENTICACIÓN INTERNA en el módulo de identificación de abonado eUICC. El Registro de Ubicación Base ETSI HLR envía al módulo de identificación de abonado eUICC una consulta de autenticación. Como reacción, el módulo de identificación de abonado eUICC formula una AUTENTICACIÓN APDU de acuerdo con [5] ISO/IEC 7816-4. De todos modos, para formular la AUTENTICACIÓN APDU, el módulo de identificación de abonado eUICC debe determinar internamente la tecnología utilizada. La información así determinada sobre la tecnología utilizada se emplea para la selección de la vía de comunicación.

Una especificación de una tecnología, la cual se debe emplear en el eUICC, se realiza preferentemente de una manera conocida en sí misma durante el arranque del módulo de identificación de abonado eUICC en el dispositivo terminal móvil y comprende, habitualmente, la realización de las siguientes funciones.

SELECCIONAR MF: Selección de un MF y, con ello, la detección de que existen ADF.

SELECCIONAR EF_Dir: EF_Dir contiene la identificación de aplicación AID de todos los ADF existentes en el eUICC.

SELECCIONAR ADF: Selección de un ADF especial de la lista en EF_Dir y, con ello, especificación del ADF especial y, por lo tanto, de la tecnología de acuerdo con el ADF especial.

Por lo general, el arranque del eUICC se realiza en el canal básico «Canal lógico 0». Con ello, después del arranque, se ha especificado la tecnología correspondiente al canal básico «Canal lógico 0» (y el correspondiente ADF).

Estado de la técnica citado

- [1] SGP02-Remote-Provisioning-Architecture-for-Embedded-UICC-Technical-Specification-v2.0, 13 de octubre de 2014, GSMA
- [2] DE 10 2012 018 540 A1
- 5 [3] WO 2013/075873 A1
- [4] WO 2014/131785 A1
- [5] ISO / IEC 7816-4, "Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 4: Interindustry commands for interchange", 1995
- [6] WO 2007/133139 A1
- 10 [7] US 2012/0106533 A1

REIVINDICACIONES

1. Procedimiento para la comunicación con un servidor de un módulo de identificación de abonado (eUICC) implementado o que se puede implementar en un dispositivo terminal, en el que, al menos, un perfil está configurado para la utilización del dispositivo terminal móvil en una red de telefonía móvil, en el que en dicho procedimiento se envía un mensaje de estado (m1), mediante el cual se indica un cambio de estado del perfil, del módulo de identificación de abonado (eUICC) al servidor, en el que antes de enviar el mensaje de estado (m1), se ejecuta en el módulo de identificación de abonado (eUICC) una etapa de la determinación de una tecnología, en la cual se determina a qué tecnología corresponde el perfil, y el envío se realiza conforme a la tecnología, y estando especificada la tecnología en un campo de datos de la aplicación (ADF) del perfil.
2. Procedimiento de acuerdo con la reivindicación 1, en el que como servidor está previsto un servidor de gestión de suscripción, en particular, un Ruteador Seguro de Gestión de Suscripción (SM-SR).
3. Procedimiento de acuerdo con la reivindicación 1 o 2, en el que como tecnología está prevista 3GPP y/o 3GPP2.
4. Procedimiento de acuerdo con una de las reivindicaciones 1 a 3, en el que el cambio de estado es una activación o una desactivación del perfil.
5. Procedimiento de acuerdo con una de las reivindicaciones 1 a 4, en el que el perfil (P1) está primero en un estado activo, y en el que mediante el mensaje de estado (m1) se indica un cambio de perfil del perfil (P1) a un perfil distinto (P2) implementado en el módulo de identificación de abonado.
6. Procedimiento de acuerdo con la reivindicación 5, en el que:
 - el perfil en el módulo de identificación de abonado está creado inicialmente como perfil activo (P1) que tiene un estado activo;
 - adicionalmente al perfil, está implementado, al menos, un perfil distinto, que está creado como perfil inactivo (P2), que tiene un estado inactivo, en el que preferentemente —al menos la mayor parte del tiempo— en cada caso solo un perfil está en un estado activo a la vez;
 - en el procedimiento se realiza un cambio de perfil al desactivar el perfil activo inicialmente (P1) de modo que se pasa a un estado inactivo, y se activa uno de los otros perfiles (P2) de modo que el otro perfil (P2) se pasa a un estado activo; y
 - después del cambio de perfil, se envía el mensaje de estado (m1) de acuerdo con la reivindicación 5 al servidor.
7. Procedimiento de acuerdo con una de las reivindicaciones 1 a 6, en el que durante la etapa de determinación de la tecnología, sobre la base de un resultado de la determinación, se especifican una o varias vías de comunicación, las cuales a continuación se emplean para la comunicación del módulo de identificación de abonado (eUICC) con el servidor, en particular, varias vías de comunicación ordenadas de acuerdo con una instrucción de uso, en particular, priorización o selección, en el que a una tecnología se ha asignado una vía de comunicación más particular.
8. Procedimiento de acuerdo con la reivindicación 7, en el que las vías de comunicación comprenden una o varias de las siguientes: una conexión de datos, conexión de Servicio de Mensajes Cortos (SMS), una conexión de mensaje de voz, una conexión de cadena SS, una conexión de cadena USSD.
9. Procedimiento de acuerdo con la reivindicación 7 o 8, en un perfil individual están previstos, como mínimo, dos porciones que corresponden a tecnologías diferentes (USIM; CSIM), y en el que para las, al menos, dos tecnologías diferentes (USIM; CSIM) se especifica respectivamente una vía diferente de comunicación (USIM: LTE conexión de datos; CSIM: conexión de voz).
10. Procedimiento de acuerdo con una de las reivindicaciones 1 a 9, en el que el mensaje de estado (m1) del módulo de identificación de abonado (eUICC) al servidor (SM-SR) está embebido en un protocolo de establecimiento de conexión de 3 vías, en el que el mensaje de estado se envía como primer mensaje (m1), en el que de acuerdo con el protocolo de establecimiento de la conexión de 3 vías, después de enviar el primer mensaje (m1), se debe enviar un segundo mensaje (m2) de servidor (SM-SR) al módulo de identificación de abonado (eUICC) y, después de enviar el segundo mensaje (m2), se debe enviar un tercer mensaje (m3) del módulo de identificación de abonado (eUICC) al servidor (SM-SR).
11. Procedimiento de acuerdo con la reivindicación 10, en el que se comunican mensajes, con los que se informa un cambio de perfil, embebidos en un protocolo de establecimiento de comunicación de 3 vías, y se comunican otros mensajes embebidos en un protocolo de establecimiento de conexión de 2 vías.

12. Procedimiento de acuerdo con una de las reivindicaciones 1 a 11, en el que se ejecuta la etapa de determinación de una tecnología al determinar un parámetro que tiene un valor específico de parámetro para una tecnología.
- 5 13. Procedimiento de acuerdo con la reivindicación 12, en el que se determina el parámetro al leer campo de parámetro (ADF), en particular, al procesar un comando (AUTENTICAR; PROPORCIONAR INFORMACIÓN DE LOCALIZACIÓN) en el módulo de identificación de abonado, durante cuyo procesamiento se usa el parámetro, y en el que, durante el procesamiento, se lee el campo de parámetro.
- 10 14. Procedimiento de acuerdo con una de las reivindicaciones 1 a 13, en el que se le asigna a la tecnología un canal lógico de acuerdo con ISO/IEC 7816-4, en particular, el canal básico canal 0 o eventualmente a cada tecnología se le asigna un canal lógico propio de acuerdo con ISO/IEC 7816-4.

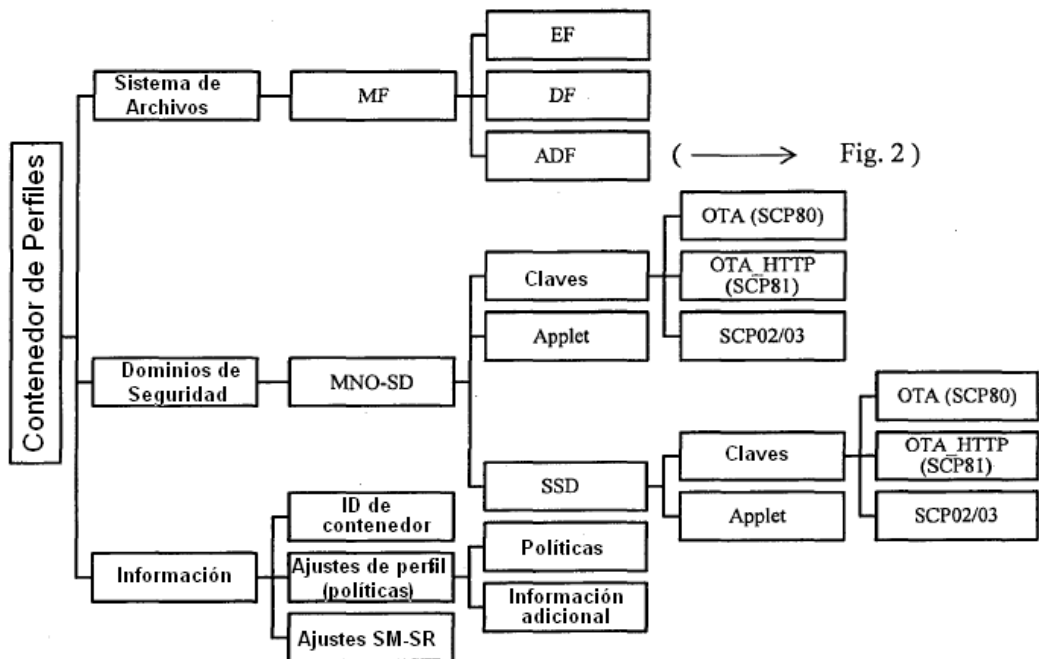


Fig. 1

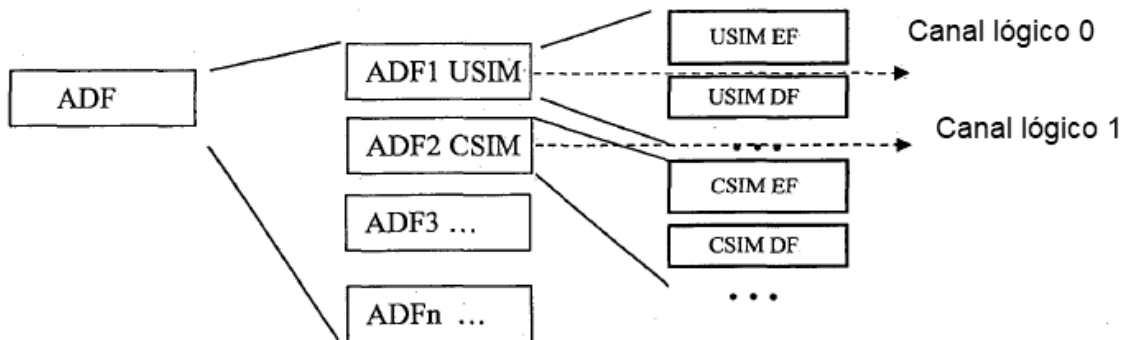


Fig. 2

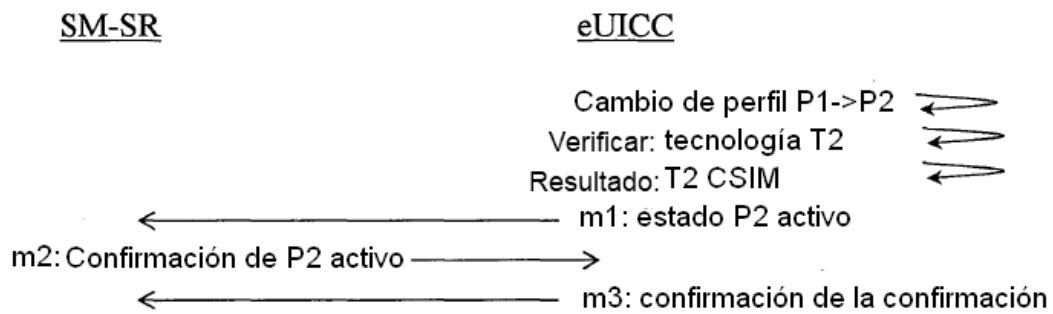


Fig. 3

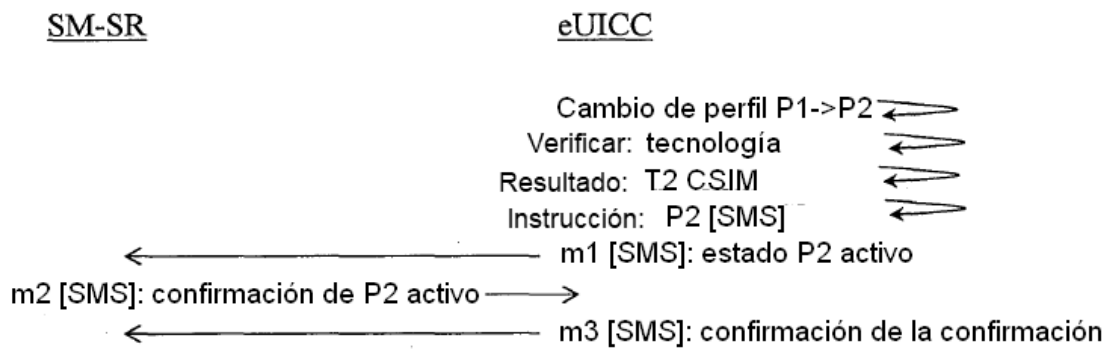


Fig. 4



* b2 b1 = 0 0 => canal lógico 0, ISO/IEC 7816-4, 5.4.1

Fig. 5