

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 802 548**

51 Int. Cl.:

H04W 8/18 (2009.01)

H04W 8/20 (2009.01)

H04W 88/06 (2009.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **20.12.2016 PCT/FR2016/053576**

87 Fecha y número de publicación internacional: **29.06.2017 WO17109384**

96 Fecha de presentación y número de la solicitud europea: **20.12.2016 E 16826412 (5)**

97 Fecha y número de publicación de la concesión europea: **13.05.2020 EP 3395090**

54 Título: **Método de control de un módulo de identidad de abonado integrado**

30 Prioridad:

22.12.2015 FR 1563135

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

20.01.2021

73 Titular/es:

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

72 Inventor/es:

**JOLIBOIS, ROMUALD;
DUMOULIN, JÉRÔME y
WOZNIAK, TOMASZ**

74 Agente/Representante:

LEHMANN NOVO, María Isabel

ES 2 802 548 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

Método de control de un módulo de identidad de abonado integrado

5 ANTECEDENTES DE LA INVENCION

La presente invención se refiere al dominio de los módulos de identidad de abonado integrados, también denominados módulos eUICC (por "módulo de circuito integrado universal incorporado"), y se refiere más en particular a dichos módulos eUICC capaces de gestionar de manera adecuada una pluralidad de perfiles de comunicación.

10 De manera conocida, una tarjeta SIM convencional está configurada para permitir a un terminal de comunicación (tal como un teléfono móvil, por ejemplo), con el que coopera, utilizar la red de comunicación de un único operador telefónico. Para hacer esto, la tarjeta SIM incluye datos de suscripción, tal como un identificador IMSI (por "Identidad de Abonado Móvil Internacional"), claves criptográficas y algoritmos específicos del operador asociado. Estos datos
15 de suscripción se almacenan permanentemente en una memoria de solamente lectura.

Cuando un teléfono móvil intenta utilizar los servicios de una red móvil, envía todos los datos de suscripción, almacenados en la tarjeta SIM, necesarios para que el operador de la red obtenga acceso a los servicios requeridos. De este modo, el operador puede autenticar al usuario y verificar utilizando una base de datos HLR (por "Registro de Localización Inicial") que se ha abonado al servicio solicitado. Si es así, el operador autoriza el acceso al teléfono móvil que lleva la tarjeta SIM, cuyos datos se han utilizado para la autenticación y el registro en la red del operador.

Además, actualmente se conocen tarjetas SIM reprogramables, y más en particular módulos de identidad de abonado integrado o módulo eUICC. Estos módulos reprogramables permiten al usuario cambiar de operador sin tener que
25 sustituir físicamente la tarjeta SIM en el teléfono móvil. Las especificaciones principales de un módulo eUICC están definidas por el grupo GSMA (por "Global System for Mobile Communications Association - Sistema Global para la Asociación de Comunicaciones Móviles") en la norma GSMA SGP.02 v3.0 titulada "Arquitectura de Aprovisionamiento Distante para UICC Integrado - Especificaciones técnicas - Versión 3.0" de fecha 30 de junio de 2015. Un módulo eUICC es un elemento de hardware seguro, generalmente pequeño, que puede integrarse en un terminal móvil para
30 poner en práctica las funciones de una tarjeta SIM tradicional.

En particular, un módulo eUICC es capaz de contener varios perfiles de comunicación (en adelante, también denominados "perfiles"). Cada perfil está contenido en un dominio seguro dedicado denominado ISD-P de conformidad con dicha norma GSMA. Cuando un perfil de comunicación está activo, permite que el teléfono móvil acceda de
35 manera segura a la red de comunicación de un operador asociado, así como a los servicios definidos por el perfil en cuestión. Al cambiar el perfil de comunicación activa en el módulo eUICC, es posible cambiar de operador o modificar el acceso a los servicios asociados (servicios de voz y/o datos, por ejemplo).

Sin embargo, cuando un módulo eUICC comprende varios perfiles de comunicación, es necesario desactivar un perfil cuando se desea activar otro. Para hacer lo que antecede, el servidor SM-SR a cargo del ciclo de vida de los perfiles cargados dentro de un módulo eUICC envía demandas a través de la red móvil para, por ejemplo, activar o desactivar el perfil en cuestión en el módulo eUICC.

45 Sin embargo, el envío de estas demandas de activación y desactivación, a través de la red móvil, genera tráfico de datos en la red y solicita recursos de red, lo que no siempre es deseable. De manera más general, no siempre es deseable implicar a un operador para activar o desactivar un perfil en un terminal de comunicación.

En la actualidad existe la necesidad de mejorar la gestión del estado de un perfil de comunicación en un módulo eUICC que coopera con un terminal de comunicación.

50 Los documentos EP2773077 A1, US2015350878 A1 y EP2884712 A1 proporcionan datos relacionados con el contexto de la presente solicitud y de las reivindicaciones que definen la invención.

55 SUMARIO DE LA INVENCION

La invención está definida por las reivindicaciones.

Para este fin, una forma de realización se refiere a un módulo de identidad de abonado integrado (también denominado eUICC) capaz de cooperar con un terminal de comunicación, en donde el módulo eUICC es capaz de mantener, de
60 manera simultánea, en el estado activo una pluralidad de perfiles de comunicación, autorizando cada perfil de comunicación activo al terminal de comunicación a comunicarse con una red de telefonía móvil asociada con dicho perfil de comunicación.

Esta forma de realización permite, de manera ventajosa, mejorar la gestión del estado (activo/inactivo) de los perfiles en un módulo eUICC y, en particular, hace posible mantener varios perfiles activos de manera simultánea para que ya
65 no sea necesario enviar demandas de activación y/o desactivación al módulo eUICC siempre que sea necesario utilizar

un perfil diferente. Por lo tanto, es posible limitar el tráfico de red y los recursos normalmente necesarios para enviar y gestionar demandas de activación y desactivación de perfiles.

5 De conformidad con una forma de realización particular, el terminal de comunicación comprende al menos una interfaz de radio, pudiendo cada perfil de comunicación activo, cuando tiene acceso a dicha al menos una interfaz de radio, establecer comunicación entre el terminal de comunicación y la red de telefonía móvil asociada con dicho perfil de comunicación activa.

10 De conformidad con una forma de realización particular, el módulo eUICC está configurado, al recibir una demanda de activación de un perfil de comunicación o al recibir una demanda para desactivar un perfil de comunicación, para mantener el estado activo de cualquier otro perfil de comunicación ya activo en dicho módulo de identidad de abonado integrado.

15 Según una forma de realización particular, el módulo eUICC comprende:

- un módulo de recepción capaz de recibir una demanda de activación de un primer perfil de comunicación que se encuentra en estado inactivo en el módulo de identidad de abonado integrado;
- un módulo de configuración capaz de configurar el módulo de identidad de abonado integrado en un primer modo o en un segundo modo según el estado de un primer parámetro incluido en dicha demanda de activación,

en donde, cuando cualquier segundo perfil de comunicación distinto de dicho primer perfil ya está activo al recibir dicha demanda de activación, se configura el módulo de identidad de abonado integrado:

- 25 o en el primer modo, para activar el primer perfil de comunicación mientras se mantiene activo dicho segundo perfil de comunicación;
- o en el segundo modo, para activar el primer perfil de comunicación y desactivar cada perfil de comunicación que no sea el primer perfil de comunicación.

30 Según una forma de realización particular, el módulo eUICC comprende:

- un módulo de recepción capaz de recibir una demanda de desactivación de un primer perfil de comunicación que se encuentra ya en el estado activo en el módulo de identidad de abonado integrado;
- 35 - un módulo de configuración capaz de configurar el módulo de identidad de abonado integrado en un tercer modo o en un cuarto modo según el estado de un segundo parámetro incluido en dicha demanda de desactivación,

40 en donde, cuando cualquier segundo perfil de comunicación distinto de dicho primer perfil ya está activo al recibir dicha demanda de desactivación, se configura el módulo de identidad de abonado integrado:

- o en el tercer modo, para desactivar el primer perfil de comunicación mientras se mantiene activo dicho segundo perfil de comunicación;
- 45 o en el cuarto modo, para activar un perfil de comunicación predefinido tal como el perfil predeterminado y para desactivar cada perfil de comunicación que no sea dicho perfil predeterminado.

50 Según una forma de realización particular, en el tercer modo, el módulo de identidad de abonado integrado está configurado, en respuesta a la demanda de desactivación, para mantener activo el segundo perfil de comunicación, incluso si dicho segundo perfil de comunicación no es un perfil de comunicación predefinido por defecto en el módulo eUICC.

55 De conformidad con una forma de realización particular, dicha orden de activación y/o dicha orden de desactivación son órdenes APDU de conformidad con la norma ISO 7816-4.

De conformidad con una forma de realización particular, el módulo eUICC es capaz, de conformidad con un quinto modo, de recibir una segunda demanda que identifica al menos dos perfiles de comunicación, cada uno de los cuales debe activarse o desactivarse en dicho módulo eUICC, siendo dicho módulo eUICC capaz, según dicho quinto modo de:

- 60 - configurar, en el estado activo, cada perfil de comunicación identificado como un perfil para ser activado en dicha segunda demanda; y
- configurar, en el estado inactivo, cada perfil de comunicación identificado como un perfil para ser desactivado en dicha segunda demanda.

Según una forma de realización particular, la segunda demanda identifica al menos un primer perfil de comunicación que se activará en el módulo de identidad de abonado integrado y al menos un segundo perfil de comunicación que se desactivará en el módulo de identidad de abonado integrado.

5 Según una forma de realización particular, la segunda demanda identifica solamente al menos dos primeros perfiles de comunicación para activar o solamente al menos dos perfiles de comunicación para desactivar en el módulo de identidad de abonado integrado.

10 Según una forma de realización particular, la segunda demanda comprende un tercer parámetro que puede tomar un primer estado o un segundo estado y un cuarto parámetro que puede tomar un primer estado, un segundo estado o un tercer estado,

en donde el módulo de identidad de abonado integrado está configurado para:

15 ○ procesar la segunda demanda como una orden de activación cuando el tercer parámetro está en el primer estado y el cuarto parámetro está en el primer o segundo estado;

○ procesar la segunda demanda como una orden de desactivación cuando el tercer parámetro está en el segundo estado y el cuarto parámetro está en el primer o segundo estado; y

20 ○ procesar la segunda demanda como una orden híbrida de activación y desactivación cuando el tercer parámetro está en el primer o segundo estado, y el cuarto parámetro está en el tercer estado.

Según una forma de realización particular, el módulo eUICC está configurado para procesar la segunda demanda:

25 ○ según el primer modo si el tercer parámetro está en el primer estado y el cuarto parámetro está en el primer estado;

30 ○ según el segundo modo si el tercer parámetro está en el primer estado y el cuarto parámetro está en el segundo estado;

○ según el tercer modo si el tercer parámetro está en el segundo estado y el cuarto parámetro está en el primer estado;

35 ○ de conformidad con el cuarto modo si el tercer parámetro está en el segundo estado y el cuarto parámetro está en el segundo estado; y

40 ○ según el quinto modo si el tercer parámetro está en el primer estado y el cuarto parámetro está en el tercer estado, o si el tercer parámetro está en el segundo estado y el cuarto parámetro está en el tercer estado.

Según una forma de realización, la invención se pone en práctica por medio de componentes de software y/o hardware. En esta perspectiva, el término "módulo" puede corresponder, en este documento, tanto a un componente de software, como a un componente de hardware o a un conjunto de componentes de hardware y software.

45 Una forma de realización también se refiere a un dispositivo (por ejemplo, un servidor de gestión de perfiles, del tipo SM-SR, por ejemplo) capaz de comunicarse con un terminal de comunicación que coopera con un módulo eUICC, comprendiendo dicho dispositivo:

50 - un módulo de envío capaz de enviar al módulo de identidad de abonado integrado una demanda de activación de un primer perfil de comunicación que se encuentra en el estado inactivo en el módulo de identidad de abonado integrado o para enviar una demanda para desactivación de un primer perfil de comunicación que se encuentra ya en el estado activo en el módulo de identidad de abonado integrado;

55 - un módulo de inserción capaz de incluir, antes de enviar al módulo de identidad de abonado integrado, uno de entre:

○ un primer parámetro en la demanda de activación; y

60 ○ un segundo parámetro en la demanda de desactivación,

en donde:

65 el primer parámetro está en un estado que define si el módulo de identidad de abonado integrado debe configurarse en un primer modo o en un segundo modo cuando cualquier segundo perfil de comunicación distinto de dicho primer perfil ya está activo en el módulo de identidad abonado integrado al recibir dicha demanda de activación, controlando el estado del primer parámetro al módulo de identidad de abonado integrado:

- o en el primer modo, para activar el primer perfil de comunicación mientras se mantiene activo dicho segundo perfil de comunicación;
- 5 o en el segundo modo, para activar el primer perfil de comunicación y desactivando cada perfil de comunicación que no sea el primer perfil de comunicación.
 - el segundo parámetro está en un estado que define si el módulo de identidad de abonado integrado debe configurarse en un tercer modo o en un cuarto modo cuando cualquier segundo perfil de comunicación distinto de
- 10 dicho primer perfil ya está activo al recibir dicha demanda de desactivación, controlando el estado del segundo parámetro al módulo de identidad de abonado integrado:
 - o en el tercer modo, para desactivar el primer perfil de comunicación mientras se mantiene activo dicho segundo perfil de comunicación;
 - 15 o en el cuarto modo, para activar un perfil de comunicación predefinido tal como el perfil predeterminado y para desactivar cada perfil de comunicación que no sea dicho perfil predeterminado.

20 Las diversas formas de realización definidas con anterioridad con referencia al módulo eUICC se aplican por analogía al dispositivo de la invención.

Una forma de realización también se refiere a un sistema que comprende:

- 25 - un módulo eUICC tal como se definió con anterioridad;
- un terminal de comunicación que coopera con el módulo eUICC; y
- al menos un dispositivo tal como se definió con anterioridad.

30 De manera correlativa, una forma de realización se refiere a un método de control puesto en práctica por un módulo de identidad de abonado integrado (eUICC) capaz de cooperar con un terminal de comunicación, comprendiendo dicho método una etapa de mantener el estado activo, de manera simultánea, de una pluralidad de perfiles de comunicación, autorizando cada perfil de comunicación activo al terminal de comunicación a comunicarse con una red de telefonía móvil asociada con dicho perfil de comunicación.

35 Una forma de realización también se refiere a un método de envío puesto en práctica por un dispositivo tal como se definió con anterioridad para enviar una orden a un módulo eUICC.

40 En una forma de realización particular, las diferentes etapas del método de control y del método de envío se determinan mediante instrucciones de programas informáticos.

45 En consecuencia, una forma de realización también se refiere a un programa informático en un soporte de información (o medio de registro), siendo este programa susceptible de ponerse en práctica en un módulo de identidad de abonado integrado, en un dispositivo, o más en general, en un ordenador, incluyendo este programa instrucciones adaptadas a la puesta en práctica de las etapas de un método de control o de un método de envío tal como se definió con anterioridad.

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

Una forma de realización también se refiere a un soporte de información (o medio de registro) legible por un ordenador, y que comprende instrucciones de un programa informático tal como se describió con anterioridad.

55 El portador de información puede ser cualquier entidad o dispositivo capaz de almacenar el programa. Por ejemplo, el soporte puede incluir un medio de almacenamiento, tal como una memoria ROM, por ejemplo, un CD-ROM o una memoria ROM de circuito microelectrónico, memoria de tipo instantáneo o también un medio de registro magnético, por ejemplo, un disquete (floppy disc) o un disco duro.

60 Por otro lado, el soporte de información puede ser un medio transmisible, tal como una señal eléctrica u óptica, que puede enrutarse a través de un cable eléctrico u óptico, por radio o por otros medios. El programa, según la invención, se puede descargar en particular en una red del tipo Internet.

65 De manera alternativa, el soporte de información puede ser un circuito integrado en donde se incorpora el programa, estando el circuito adaptado para ejecutarse o para ser utilizado en la ejecución del proceso en cuestión.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

- 5 Otras características y ventajas de la presente invención surgirán de la descripción que se proporciona a continuación, con referencia a los dibujos adjuntos que ilustran ejemplos de formas de realización desprovistas de cualquier carácter limitante. En las figuras:
- La Figura 1 representa, de manera esquemática, un sistema que comprende un módulo de identidad de abonado integrado y un servidor de gestión de perfiles, de conformidad con una forma de realización particular de la invención;
- 10 Las Figuras 2A y 2B representan, de manera esquemática, dos formas de realización del terminal;
- La Figura 3 representa, de manera esquemática, módulos puestos en práctica en el módulo de identidad de abonado integrado de la Figura 1, de conformidad con una forma de realización particular de la invención;
- 15 La Figura 4 representa, en forma de diagrama, las etapas de un método de control y de un método de envío, de conformidad con una forma de realización particular de la invención;
- La Figura 5 representa, en forma de diagrama, las etapas de un método de control y de un método de envío, de conformidad con una forma de realización particular de la invención;
- 20 La Figura 6 representa, de manera esquemática, una orden capaz de ser enviada por un servidor de gestión de perfiles a un módulo de identidad de abonado integrado, de conformidad con una forma de realización particular de la invención;
- 25 La Figura 7 representa, en forma de diagrama, las etapas de un método de control y de un método de envío, de conformidad con una forma de realización particular de la invención; y
- Las Figuras 8 y 9 representan, de manera esquemática, órdenes susceptibles de enviarse por un servidor de gestión de perfiles a un módulo de identidad de abonado integrado, de conformidad con una forma de realización particular de la invención.
- 30

DESCRIPCIÓN DETALLADA DE LAS FORMAS DE REALIZACIÓN

- 35 Tal como ya se indicó con anterioridad, la invención se refiere a módulos de identidad de abonado integrados (también denominados "módulos eUICC") y más en particular se refiere al uso de dichos módulos para gestionar, de manera simultánea, varios perfiles de comunicación en cooperación con un terminal de comunicación.
- En la actualidad, la norma GSMA SGP.02 v3.0 (en adelante denominada "norma GSMA") impone una restricción en el sentido de que solamente un perfil a la vez puede estar en estado activo en un módulo eUICC. Dicho de otro modo, 40 la norma GSMA prohíbe el caso en donde varios perfiles de comunicación estén activos al mismo tiempo en un módulo eUICC.
- En los módulos eUICC convencionales, el hecho de que solamente un perfil pueda estar activo en un momento dado tiene la consecuencia de que no es posible utilizar varias suscripciones de telefonía móvil de manera simultánea, como 45 ello es posible, por ejemplo, en un teléfono DUAL SIM que utiliza dos tarjetas SIM distintas al mismo tiempo.
- Para utilizar varias suscripciones de manera simultánea en el mismo terminal de comunicación, una solución podría consistir en integrar varios módulos eUICC en un mismo terminal de comunicación. Dicho método, sin embargo, 50 presenta limitaciones significativas en términos de coste y fabricación en particular.
- En particular, para resolver los problemas mencionados con anterioridad y mejorar la gestión de los perfiles de comunicación en un módulo eUICC, la presente invención propone configurar un módulo eUICC para que pueda mantener en el estado activo una pluralidad de perfiles de comunicación al mismo tiempo.
- 55 En este caso entendemos por perfil "activo", o perfil en el estado "activo", el hecho de que un perfil de comunicación se activa en el módulo eUICC para autorizar al terminal de comunicación (con el cual el módulo eUICC coopera) para comunicarse con la red telefónica asociada con el perfil en cuestión. De conformidad con la norma GSMA, se dice que un perfil (o el dominio seguro ISD-P en donde está contenido) está "activo" (ENABLE) cuando su parámetro de estado, denominado "ciclo de vida", se establece en el estado '3F'. De conformidad con la norma GSMA, se dice que un perfil 60 está "inactivo" (DISABLE) cuando su parámetro de estado "ciclo de vida" se establece en el estado '1F'.
- Tal como se describe con más detalle a continuación, un perfil de comunicación puede estar activo sin tener acceso a la interfaz de radio del terminal de comunicación. En ciertos casos, el acceso a esta interfaz de radio puede ser limitado, en particular cuando no hay tantas interfaces de radio en el terminal de comunicación como perfiles activos al mismo 65 tiempo en el módulo eUICC. Un perfil activo solamente permite el establecimiento de una comunicación entre el

terminal de comunicación y la red de telefonía móvil asociada con el perfil cuando este último tiene acceso al recurso de radio del terminal de comunicación.

5 A menos que se indique lo contrario, los elementos comunes o análogos a varias figuras que llevan los mismos signos de referencia y tienen características idénticas o similares, de modo que estos elementos comunes generalmente no se describen nuevamente por razones de simplicidad.

10 La Figura 1 muestra, de manera esquemática, la estructura de un módulo eUICC (mencionado aquí como eUICC1) capaz de cooperar con un terminal de comunicación T para permitir el acceso a una red de telefonía móvil R. El módulo eUICC1 está, por ejemplo, soldado o integrado en el terminal T.

En la forma de realización aquí descrita, el terminal T es un terminal móvil tal como un teléfono portátil, por ejemplo, siendo posibles otras puestas en práctica dentro del marco de la invención.

15 En la forma de realización aquí descrita, el terminal móvil T puede utilizar el módulo eUICC1 para acceder de forma segura a las redes R1, R2 y R3 (denominadas colectivamente R), así como a los servicios proporcionados por el operador respectivo de telefonía MNO1, MNO2 y MNO3 (denominados colectivamente MNO por "Operador de Red Móvil").

20 En esta forma de realización particular, el terminal móvil T incluye un sistema operativo OS2 capaz de controlar en particular una interfaz de radio INT. La interfaz de radio INT del terminal T es capaz de transmitir y recibir comunicaciones de radio con el exterior a través de, por ejemplo, una antena (no ilustrada).

25 Tal como se muestra en la Figura 2A, esta interfaz de radio INT incluye, por ejemplo, de manera conocida, una unidad transmisora/receptora de radio 30 acoplada a una antena 32. Tal como se describe a continuación con referencia a la Figura 2B, también se puede considerar la presencia en el terminal T de una pluralidad de interfaces de radio.

30 En la forma de realización aquí descrita, el módulo eUICC1 comprende un sistema operativo OS1 (almacenado en una memoria no volátil, una memoria de solamente lectura o memoria instantánea, por ejemplo) acoplado a una memoria MR no volátil regrabable.

El sistema operativo OS1 comprende un cierto número de módulos que se describirán con más detalle a continuación con referencia a la Figura 3.

35 El sistema operativo OS1 constituye un ejemplo de un programa informático en el sentido de la invención, incluyendo este programa instrucciones para la ejecución de las etapas de un método de control de conformidad con una forma de realización particular de la invención. La memoria en donde se encuentra el sistema operativo OS1 constituye así un ejemplo de soporte de registro en el sentido de la invención, legible por un procesador (no ilustrado) del módulo eUICC1.

40 Tal como se muestra en la Figura 1, la memoria MR no volátil del módulo eUICC1 también incluye un dominio de seguridad privilegiado ISD-R, así como una pluralidad de dominios de seguridad secundarios ISD-P indicados en este ejemplo ISD-P1, ISD-P2 e ISD-P3. Cada dominio de seguridad ISD-P (o dominio seguro) constituye un compartimento seguro del módulo eUICC1. Se entenderá que la forma de realización particular aquí prevista constituye solamente un ejemplo no limitativo de puesta en práctica de la invención, pudiendo adaptarse el número de dominios ISD-P en particular según el caso de uso.

45 El dominio de seguridad ISD-R tiene el privilegio de que es particularmente capaz de crear, eliminar, activar o desactivar dominios de seguridad secundarios ISD-P en la memoria no volátil MR. En las formas de realización que se describen a continuación, es el dominio de seguridad ISD-R el que gestiona el estado activo o inactivo de los perfiles de comunicación del módulo eUICC1.

50 Cada dominio de seguridad secundario ISD-P es capaz de contener un único perfil de comunicación P (o perfil operativo) asociado con un operador MNO particular para telefonía. Por lo tanto, cada perfil P está contenido en un dominio de seguridad ISD-P dedicado. De manera conocida, un perfil de comunicación P comprende datos de abonado (por ejemplo, identificadores (IMSI, etc.), claves criptográficas, algoritmos (por ejemplo, autenticación), etc.) y también puede incluir un sistema de archivos, aplicaciones, y/o reglas de ejecución predeterminadas. En el ejemplo aquí considerado, los perfiles P se ajustan a la norma GSMA.

60 En el ejemplo aquí descrito, tal como se ilustra en la Figura 1, se supone que la memoria MR del módulo eUICC1 comprende tres dominios de seguridad secundarios denominados ISD-P1, ISD-P2 e ISD-P3, conteniendo estos dominios de seguridad secundarios, respectivamente, un único perfil P1, P2 y P3 que puede estar cada uno en estado activo o inactivo.

65 El perfil P1 (respectivamente P2) autoriza, cuando está activo, al terminal T para comunicarse con una red móvil R1 (respectivamente R2) asociada con el operador telefónico MNO1 (respectivamente MNO2). El dominio de seguridad

ISD-P1 (respectivamente ISD-P2) también puede incluir aplicaciones APP1 (respectivamente APP2) específicas para el operador MNO1 (respectivamente MNO2) al que se ha abonado el usuario. De manera alternativa, las aplicaciones APP1 (respectivamente APP2) definidas para el perfil P1 (respectivamente P2) pueden estar contenidas en el perfil P1 (respectivamente P2).

En este ejemplo, en ciertos casos (que se describirá con más detalle a continuación), el perfil P3 contenido en el dominio de seguridad secundario ISD-P3 es procesado por el módulo eUICC1 como un perfil predefinido por defecto en el sentido de que este perfil se activa de manera automática por defecto a la recepción de una demanda para desactivar otro perfil activo en el módulo eUICC.

Al igual que los perfiles P1 y P2, el perfil P3 autoriza, cuando está activo, al terminal T para comunicarse con una red móvil R3 asociada con un operador telefónico MNO3. El dominio de seguridad ISD-P3 también puede incluir aplicaciones APP3 específicas para el operador MNO3 al que se ha abonado el usuario. De manera alternativa, las aplicaciones APP3 definidas para el perfil P3 pueden estar contenidas en el perfil P3 mismo.

De conformidad con la invención, el módulo eUICC1 es capaz de mantener una pluralidad de perfiles de comunicación P en el estado activo al mismo tiempo.

El módulo eUICC1 también puede comunicarse, a través del terminal T (y en particular su interfaz de radio INT), de manera segura con un servidor de gestión de perfiles que, en este ejemplo, es un servidor SM-SR (por "Gestor de Suscripción-Enrutamiento Seguro"). En este ejemplo, el servidor de gestión de perfiles SM-SR pertenece a cada una de las redes R1, R2 y R3.

La comunicación entre el módulo eUICC1 y el terminal T se realiza, por ejemplo, a través de un enlace L conforme a la norma ISO 7816 (más en particular de conformidad con las normas ISO 7816-3 e ISO 7816-4).

En esta forma de realización particular, el servidor SM-SR permite a cada operador MNO controlar el estado (activo o inactivo) del perfil P del que es responsable en el módulo eUICC1. En este caso se supone que los operadores MNO1, MNO2 y MNO3 pueden controlar el servidor SM-SR para que este último active o desactive los perfiles P1, P2 y P3, respectivamente. Para realizar lo que antecede, el servidor SM-SR puede enviar una orden de activación o desactivación CMD al terminal T al módulo eUICC1. Estas órdenes son, por ejemplo, del tipo APDU de conformidad con la norma ISO 7816-4.

En el ejemplo aquí considerado, el servidor SM-SR pone en práctica un sistema operativo OS3 registrado en un soporte de información (no ilustrado).

El módulo eUICC1 es capaz de recibir los órdenes de activación o desactivación CMD del servidor distante SM-SR y dirigirlas hacia el dominio de seguridad privilegiado ISD-R. En respuesta a una orden CMD, el dominio de seguridad privilegiado ISD-R está configurado para activar o desactivar al menos un perfil P en el módulo eUICC1.

El módulo eUICC1, el terminal T y el servidor de gestión de perfiles SM-SR forman conjuntamente un sistema SY.

Se entenderá que ciertos elementos generalmente presentes en un módulo eUICC, en un terminal de comunicación T o incluso en un servidor SM-SR se han omitido de forma deliberada porque no son necesarios para comprender la presente invención. Además, los expertos en esta técnica entenderán que aquí se describen ciertos elementos para facilitar la comprensión de la invención, aunque no son obligatorios ni están directamente implicados en la puesta en práctica de la invención.

Tal como se indicó con anterioridad, con referencia a la Figura 2A, el terminal T puede incluir una única interfaz de radio INT. En este caso, solamente uno de los perfiles P activos en el módulo eUICC1 puede permitir, en un instante dado, el establecimiento de una comunicación entre el terminal T y la red móvil R. En este caso, cuando al menos dos de entre los perfiles P1, P2 y P3 están activos al mismo tiempo, solamente uno de los dos perfiles P es capaz de establecer comunicación con la red del operador MNO asociado.

Sin embargo, se puede considerar la inclusión en el terminal T de una pluralidad de interfaces de radio INT. La Figura 2B representa, por ejemplo, una forma de realización según la cual el terminal T comprende un conmutador 34 capaz de guiar las comunicaciones entre el módulo eUICC1 y dos interfaces de radio INTA e INTB del terminal T. La interfaz de radio INTA (respectivamente INTB) comprende en este caso una unidad transmisora/receptora de radio 36A (respectivamente 36B) acoplada a una antena 38A (respectivamente 38B). Según esta forma de realización, el conmutador 34 puede dirigir cada orden CMD recibida por una de las interfaces de radio INTA, INTB hacia el módulo eUICC1. Cuando se utiliza un canal entre el módulo eUICC1 y una interfaz de radio INTA, INTB, el otro canal entre el módulo eUICC1 y la otra interfaz de radio no está disponible. Sin embargo, otras puestas en práctica de la invención son concebibles.

Tal como ya se indicó con anterioridad, un perfil de comunicación P que está activo en el módulo eUICC1 solamente es capaz de establecer comunicación entre el terminal T y una red móvil asociada R solamente cuando este perfil P tiene acceso a los recursos de radio del terminal T (es decir, en la interfaz de radio).

5 Según una forma de realización particular, el terminal T puede multiplexar en el tiempo los datos enviados o recibidos por diferentes perfiles P en el módulo eUICC1.

10 En la forma de realización aquí descrita, el terminal de comunicación T comprende al menos una interfaz de radio INT, siendo capaz cada perfil de comunicación P activo en el módulo eUICC1, cuando tiene acceso a dicha al menos una interfaz de radio INT, de establecer una comunicación entre el terminal T y la red de telefonía móvil R asociada con el perfil de comunicación activo P.

15 De conformidad con la invención, el módulo eUICC1 es capaz de mantener, de manera simultánea, en el estado activo, una pluralidad de perfiles de comunicación P, entre los perfiles P1, P2 y P3 en este ejemplo. Tal como aparecerá en el resto de esta descripción, se pueden prever varias configuraciones del módulo eUICC1 en el marco de la invención.

20 En la forma de realización aquí descrita, el módulo eUICC1 se configura, al recibir una demanda CMD para activar un perfil P o al recibir una demanda CMD para desactivar un perfil P, para mantener en estado activo, cualquier otro perfil P que ya esté activo en el módulo eUICC1. Si, por ejemplo, un primer perfil P está activo en el módulo eUICC1 al recibir una demanda CMD para activar un segundo perfil P (distinto del primer perfil), el módulo eUICC1 está configurado para activar el segundo perfil y para mantener activo el primer perfil, cualquiera que sea el caso.

25 De manera similar, si, por ejemplo, un primer y un segundo perfil P están activos al recibir una demanda CMD para la desactivación del primer perfil P, el módulo eUICC1 está configurado para desactivar el primer perfil P y para mantener el estado activo del segundo perfil P, cualquiera que sea (es decir, incluso si el segundo perfil P no es el perfil P3 predeterminado por defecto).

30 Tal como se muestra en la Figura 3, el sistema operativo OS1 del módulo eUICC1 pone en práctica, en este ejemplo, un determinado número de módulos, a saber: un módulo de recepción M2, un módulo de configuración M4 y un módulo de procesamiento M6. En las formas de realización aquí consideradas, estos módulos M2, M4 y M6 son ejecutados por el dominio de seguridad ISD-R del módulo eUICC1. Más concretamente, tal como se describe a continuación, el dominio de seguridad ISD-R está configurado para controlar el estado (activo o inactivo) de los perfiles P del módulo eUICC1. La gestión del estado de los perfiles P1-P3 se lleva a cabo por el dominio de seguridad ISD-R en respuesta a una o más órdenes que recibe del terminal T.

35 El módulo de recepción M2 puede recibir una demanda de gestión de perfil CMD del servidor SM-SR. Tal como ya se indicó, puede ser una demanda de activación o una demanda de desactivación para un perfil P dado en el módulo eUICC1. Tal como se explica a continuación, se pueden prever otros tipos de órdenes CMD en el contexto de la invención.

40 El módulo de configuración M4 es capaz de configurar el módulo eUICC1 de conformidad con varios modos operativos, dependiendo del caso de uso considerado.

45 El módulo de procesamiento M6 puede, en respuesta a una orden de activación o desactivación de CMD, gestionar el estado (activo o inactivo) de los perfiles P en el módulo eUICC1, y esta conformidad con el modo operativo en que el módulo de configuración M4 ha configurado el módulo eUICC1.

50 Se entenderá que la definición anterior de módulos M2 a M6 es solamente una forma de realización no limitativa de la invención. Al menos dos de estos módulos pueden en particular formar un único módulo puesto en práctica en el módulo eUICC1.

55 Una forma de realización particular de la invención, puesta en práctica por el módulo eUICC1 y por el servidor de gestión de perfiles SM-SR, se describe a continuación con referencia al diagrama de la Figura 4. Para hacerlo, el módulo eUICC1 ejecuta el sistema operativo OS1 para poner en práctica un método de control según una forma de realización particular, y el servidor de gestión de perfiles SM-SR ejecuta el sistema operativo OS3 para poner en práctica un método de envío según una forma de realización particular.

60 En este caso se supone que el perfil P2 está activo y que los perfiles P1 y P3 están inactivos en el módulo eUICC1 (A2).

Durante una etapa de inclusión C3, el servidor SM-SR genera una orden (o demanda) CMD1 para activar el perfil P1 e incluye en la orden CMD1 un parámetro PR1 que indica según qué modo operativo dicha orden CMD1 debe ser procesada por el módulo eUICC1.

65 Durante una etapa de envío C4, el servidor de gestión de perfiles SM-SR envía la orden CMD1 al terminal T.

Una vez recibida (B4), el terminal T envía (B6) la orden CMD1 al módulo eUICC1.

El módulo eUICC1 recibe la orden CMD1 durante una etapa de recepción A6.

5 El módulo eUICC1 se configura (A8) a continuación en un modo operativo, dicho modo es una función del parámetro PR1 incluido en la orden CMD1 recibida. Más en particular, el módulo de configuración M4 configura el módulo eUICC1 en un primer modo MD1 o en un segundo modo MD2 según el estado del parámetro PR1. Según una variante, el parámetro PR1 se recibe por separado de la orden CMD1.

10 Si el módulo eUICC1 está configurado en A8 de conformidad con el primer modo MD1 para procesar la orden CMD1 para activar el perfil P1, el proceso continúa con las etapas A10 y A14. Más en particular, de conformidad con este modo MD1, en respuesta a la orden de activación CMD1, el módulo eUICC1 (y más en particular el módulo de procesamiento M6) mantiene (A10) activo el perfil P2, que ya estaba activo en la recepción de la orden CMD1, y activa (A14) el perfil P1.

15 Si, por el contrario, el módulo eUICC1 está configurado en A8 de conformidad con el segundo modo MD2 para procesar la orden CMD1 para activar el perfil P1, el proceso continúa con las etapas A12 y A14. Más en particular, de conformidad con este segundo modo MD2, en respuesta a la orden CMD1, el módulo eUICC1 (y más en particular el módulo de procesamiento M6) desactiva (A12) el perfil P2 y activa (A14) el perfil P1. Dicho de otro modo, en el segundo modo MD2, en respuesta a una demanda de activación de un primer perfil P, el módulo eUICC1 activa dicho primer perfil P y desactiva cada perfil que no sea dicho primer perfil P.

20 En este ejemplo, después de procesar la orden CMD1 de conformidad con el primer modo MD1, los perfiles P1 y P2 autorizan al terminal T a comunicarse con la red móvil R1 y R2, respectivamente.

25 Como resultado del procesamiento de la orden CMD1 de conformidad con el segundo modo MD2, solamente el perfil P1 autoriza al terminal T a comunicarse con la red móvil R1.

30 Dicho de otro modo, en el segundo modo MD2, el módulo eUICC1 procesa de manera convencional la orden de activación CMD1 del perfil P1, pudiendo un solo perfil estar activo a la vez en el módulo eUICC. Por otro lado, en el primer modo MD1, el módulo eUICC1 procesa la orden de activación CMD1 de conformidad con el principio de la invención para que varios perfiles P puedan estar activos de manera simultánea en el módulo eUICC1.

35 El uso del parámetro PR1 permite, de manera ventajosa, controlar la forma en que se gestiona el estado de los perfiles en un módulo eUICC en respuesta a una demanda de activación de uno de los perfiles del módulo eUICC.

40 Una forma de realización particular de la invención, puesta en práctica por el módulo eUICC1 y por el servidor de gestión de perfiles SM-SR, se describe a continuación con referencia al diagrama de la Figura 5. Para hacer lo que antecede, el módulo eUICC1 ejecuta el sistema operativo OS1 para poner en práctica un método de control de conformidad con una forma de realización particular, y el servidor de gestión de perfiles SM-SR ejecuta el sistema operativo OS3 para poner en práctica un método de envío de conformidad con una forma de realización particular.

45 En este caso se supone que los perfiles P1 y P2 están activos y que el perfil P3 está inactivo en el módulo eUICC1 (A20).

Durante una etapa de inclusión C21, el servidor SM-SR genera una orden (demanda) CMD2 para desactivar el perfil P1 e incluye en la orden CMD2 un parámetro PR2 que indica según qué modo operativo dicha orden CMD2 debe procesarse por el módulo eUICC1.

50 Durante una etapa de envío C22, el servidor de gestión de perfiles SM-SR envía la orden CMD2 al terminal T.

Una vez recibida (B22), el terminal T envía (B24) la orden CMD2 al módulo eUICC1.

El módulo eUICC1 recibe la orden CMD2 durante una etapa de recepción A24.

55 El módulo eUICC1 se configura (A26) a continuación en un modo operativo, dicho modo es una función del parámetro PR2 incluido en la orden CMD2 recibida. Más en particular, el módulo de configuración M4 configura el módulo eUICC1 en un tercer modo MD3 o en un cuarto modo MD4 según el estado del parámetro PR2. Según una variante, el parámetro PR2 se recibe por separado de la orden CMD2.

60 Si el módulo eUICC1 está configurado en A26 de conformidad con el tercer modo MD3 para procesar la orden CMD2 para desactivar el perfil P1, el método de control continúa con las etapas A28 y A30. Más en particular, de conformidad con este tercer modo MD3, en respuesta a la orden de desactivación CMD2, el módulo eUICC1 (y más en particular el módulo de procesamiento M6) mantiene (A28) activo el perfil P2, cualquiera que sea el perfil P2 en cuestión (incluso si el perfil P2 no es un perfil predefinido como el perfil por defecto en el módulo eUICC1) y desactiva (A30) el perfil P1.

65

En un ejemplo particular, de conformidad con el tercer modo MD3, en respuesta a la orden de desactivación CMD2, el módulo eUICC1 mantiene, además, inactivo el perfil P3 predefinido por defecto.

5 Si, por otro lado, el módulo eUICC1 está configurado en A26 de conformidad con el cuarto modo MD4 para procesar la orden CMD2 para desactivar el perfil P1, el método de control continúa con las etapas A32, A34 y A36. Más en particular, de conformidad con este cuarto modo MD4, en respuesta a la orden de desactivación CMD2, el módulo eUICC1 (y más en particular el módulo de procesamiento M6) desactiva (A32) el perfil P2, desactiva (A34) el perfil P1 y activa (A36) el perfil P3 como un perfil predefinido por defecto. Dicho de otro modo, en este cuarto modo MD4, en respuesta a una demanda para desactivar un primer perfil P, el módulo eUICC1 activa el perfil predefinido como el perfil predeterminado en el módulo eUICC1 y desactiva cada perfil además de dicho perfil predefinido por defecto.

En este ejemplo, como resultado del procesamiento de la orden de desactivación de CMD2 de conformidad con el tercer modo MD3, solamente el perfil P2 autoriza al terminal T a comunicarse con la red móvil R2.

15 Al final del procesamiento de la orden de desactivación CMD2, según el cuarto modo MD4, solamente el perfil P3 autoriza al terminal T a comunicarse con la red móvil R3.

Dicho de otro modo, en el cuarto modo MD4, el módulo eUICC1 procesa, de manera convencional, la orden de desactivación CMD2 del perfil P1. Por otro lado, en el tercer modo MD3, el módulo eUICC1 procesa la orden de desactivación CMD2 de conformidad con el principio de la invención para que varios perfiles P puedan estar activos de manera simultánea en el módulo eUICC1. Según el modo MD3, la desactivación de un perfil no causa sistemáticamente la activación de un perfil predefinido por defecto en el módulo eUICC, como es el caso de los módulos eUICC convencionales.

25 El uso del parámetro PR2 permite, de manera ventajosa, controlar la forma en que se gestiona el estado de los perfiles en un módulo eUICC en respuesta a una demanda de desactivación de uno de los perfiles del módulo eUICC.

Las órdenes CMD1 y CMD2 mencionadas con anterioridad son, por ejemplo, órdenes APDU de conformidad con la norma ISO 7816-4.

30 Tal como se indicó con anterioridad, son posibles diversas formas de realización dentro del alcance de la invención.

En las formas de realización descritas con anterioridad con referencia a las Figuras 4 y 5, el servidor de gestión de perfiles SM-SR (ilustrado en la Figura 1), controlado por un programa informático almacenado en una memoria no volátil de dicho servidor SM-SR, por ejemplo, pone en práctica los siguientes módulos:

- un módulo de envío capaz de enviar al módulo eUICC1 la demanda de activación de CMD1 y/o para enviar la demanda de desactivación de CMD2;
- 40 - un módulo de inserción capaz de incluir, antes de enviar al módulo eUICC1, al menos uno de entre:
 - el primer parámetro PR1 en la demanda de activación CMD1; y
 - el segundo parámetro PR2 en la demanda de desactivación;

45 en donde el parámetro PR1 está en un estado que define si el módulo eUICC1 debe configurarse en el primer modo MD1 o en el segundo modo MD2 para procesar la orden de activación CMD1; y

50 en donde el parámetro PR2 está en un estado que define si el módulo eUICC1 debe configurarse en el tercer modo MD1 o en un cuarto modo MD4 para procesar la orden de desactivación CMD2.

A continuación, se describe una forma de realización particular con referencia a las Figuras 6 y 7. En esta forma de realización, el módulo eUICC1 también puede mantener, de manera simultánea, en el estado activo, una pluralidad de perfiles de comunicación P, autorizando cada perfil P activo al terminal de comunicación T para comunicarse con una red de telefonía móvil R asociada con dicho perfil de comunicación. Por otro lado, el módulo eUICC1 está configurado para gestionar el estado de los perfiles P en el módulo eUICC1 de manera diferente de lo que se ha descrito previamente con referencia a las formas de realización ilustradas en las Figuras 4 y 5.

60 En la forma de realización ilustrada en las Figuras 6 y 7, el servidor de gestión de perfiles SM-SR está configurado para enviar al módulo eUICC1, a través del terminal T, una orden (o demanda) CMD3, denominado orden híbrida. La orden híbrida CMD3 identifica al menos dos perfiles P, cada uno de los cuales debe activarse o desactivarse en el módulo eUICC correspondiente. Dicho de otro modo, la orden híbrida CMD3 ordena, para cada uno de al menos dos perfiles de comunicación P, la activación o desactivación en el módulo eUICC de destino.

65 En esta forma de realización, se supone que el módulo eUICC1 funciona de conformidad con un quinto modo MD5. De conformidad con este modo MD5, el módulo eUICC1 es adecuado para:

- configurar en el estado activo cada perfil de comunicación P identificado como un perfil para ser activado en la orden híbrida CMD3; y

5 - configurar en el estado inactivo cada perfil de comunicación P identificado como un perfil para desactivar en orden híbrida CMD3.

Tal como se ilustra en la Figura 6, la orden CMD3 contiene, por ejemplo, una primera lista LT1 que identifica al menos un perfil P para activar, y una segunda lista LT2 que identifica al menos un perfil P para desactivar. Una de estas listas LT1, LT2 puede, si fuere necesario, estar vacía.

En el ejemplo ilustrado en la Figura 6, la lista LT1 incluye los identificadores IDP1 e IDP2 de los respectivos perfiles P1 y P2. Además, la lista LT2 incluye el identificador IDP3 del perfil P3. Además, en este ejemplo particular, en respuesta a la orden híbrida CMD3, el módulo eUICC1 activa los perfiles P1 y P2, y desactiva el perfil P3.

Esta forma de realización permite, de manera ventajosa, controlar de manera simultánea, para cada uno de entre una pluralidad de perfiles P, la activación o desactivación en un módulo eUICC. Por lo tanto, es posible requerir, en una sola orden, una configuración más o menos compleja de estados de perfil en un módulo eUICC.

20 En un ejemplo particular, la orden híbrida CMD3 identifica al menos un primer perfil P para activar en el módulo eUICC1 y al menos un segundo perfil P para desactivar en el módulo eUICC1. Dicho de otro modo, la orden CMD3 aquí es tanto una orden de activación como de desactivación, lo que permite, de manera ventajosa, controlar de manera precisa y simultánea una configuración del estado de los perfiles que se ponen en práctica en un módulo eUICC.

25 Según un ejemplo particular, la orden híbrida CMD3 identifica solamente al menos dos perfiles P para activar (es decir, al menos dos perfiles P para activar, y ningún perfil P para desactivar). En este caso, la orden CMD3 es exclusivamente una orden de activación en el sentido de que no ordena la desactivación del perfil.

30 Según un ejemplo particular, la orden híbrida CMD3 solamente identifica al menos dos perfiles P para desactivar (es decir, al menos dos perfiles P para desactivar y ningún perfil P para activar). En este caso, la orden CMD3 es exclusivamente una orden de desactivación en el sentido de que no ordena la activación del perfil.

A continuación, se da a conocer, con referencia a las Figuras 6 y 7, un método de control puesto en práctica por el módulo eUICC1 y un método de envío puesto en práctica por el servidor de gestión de perfiles SM-SR, según un ejemplo particular de realización.

En una etapa C50, el servidor SM-SR envía al terminal T una orden híbrida CMD3 destinada al módulo eUICC1, esta orden CMD3 comprende los identificadores IDP1 e IDP2 de los respectivos perfiles P1 y P2 en la lista LT1, y el identificador IDP3 del perfil P3 en la lista LT2.

Una vez recibida (B50), el terminal T envía (B52) la orden CMD3 que comprende las listas LT1 y LT2 al módulo eUICC1.

El módulo eUICC1 recibe la orden CMD3 durante una etapa de recepción A52.

El módulo eUICC1 configura (A54) el estado de los perfiles de comunicación P a partir de la orden CMD3, y más concretamente, a partir de los perfiles P identificados en la orden CMD3 como perfiles para activar y/o como perfiles para desactivar. Tal como ya se indicó con anterioridad, se supone que el módulo eUICC1 funciona en este caso en un quinto modo MD5. En el presente ejemplo, de conformidad con el modo MD5, el módulo eUICC1:

50 - configura, en el estado activo, cada perfil de comunicación P (concretamente P1 y P2) identificado como un perfil para ser activado en la orden híbrida CMD3; y

55 - configura, en el estado inactivo, cada perfil de comunicación P (es decir, P3) identificado como un perfil para ser desactivado en la orden híbrida CMD3.

Asimismo, podemos considerar poner en práctica la invención de conformidad con cualquier combinación de las formas de realización y variantes descritas con anterioridad.

60 A continuación, se describe una forma de realización particular con referencia a las Figuras 8 y 9. En esta forma de realización, el servidor de gestión de perfiles SM-SR puede enviar al terminal, con destino al módulo eUICC1, una orden CMD4 y/o CMD5 que comprende:

65 - un primer parámetro DGI que puede tomar un primer estado (o valor) "ENABLE PROFILE" (por ejemplo, 3A03) o un segundo estado "DISABLE PROFILE" (por ejemplo, 3A04); y

- un segundo parámetro TAG1 (que puede representarse, por ejemplo, por el valor "55" o "58") que identifica un modo que puede tomar, por ejemplo y sin limitación, un primer estado (o valor), a saber, "00", un segundo estado "01" o un tercer estado "02".

5 En estas formas de realización a modo de ejemplo, las órdenes CMD4 y CMD5 son del tipo TLV, otros formatos de orden que se pueden prever en el contexto de la invención.

Más en particular, las Figuras 8 y 9 representan, respectivamente, una orden CMD4 y CMD5 que el servidor SM-SR puede enviar al terminal T, pudiendo cada una de estas órdenes controlar la configuración (activa o inactiva) del estado de al menos un perfil P en el módulo eUICC1 de conformidad con un modo operativo dado.

En esta forma de realización, el módulo eUICC1 está configurado para:

- 15 o procesar la orden (CMD4) como orden de activación si el parámetro DGI está en el primer estado ENABLE PROFILE y el parámetro TAG1 está en el primer o segundo estado (00, 01);
- o procesar la orden (CMD5) como una orden de desactivación si el parámetro DGI está en el segundo estado DISABLE PROFILE y el parámetro TAG1 está en el primer o segundo estado (00, 01); y
- 20 o procesar las órdenes (CMD4 y CMD5) tal como una orden híbrida de activación y desactivación si:
 - el parámetro DGI está en el primer estado "ENABLE VALUE" y el parámetro TAG1 está en el tercer estado 02; y si
 - 25 ▪ el parámetro DGI está en el segundo estado "DISABLE VALUE" y el parámetro TAG1 está en el tercer estado 02.

Tal como se ilustra en la Figura 8, la orden CMD4 incluye el parámetro DGI en el estado ENABLE PROFILE que indica que la orden CMD4 debe tratarse como una orden de activación (o híbrida) y el parámetro TAG1 que indica el modo operativo según el cual esta orden CMD4 debe ser procesada por el módulo eUICC1.

En respuesta a la orden CMD4, el módulo eUICC1 está configurado para:

- 35 - procesar la orden CMD4 como una orden de activación de conformidad con el primer modo MD1 descrito con anterioridad con referencia a la Figura 4 si el parámetro TAG1 está en el valor 00;
- procesar la orden CMD4 como una orden de activación según el segundo modo MD2 descrito con anterioridad con referencia a la Figura 4 si el parámetro TAG1 está en el valor 01; y
- 40 - procesar la orden CMD4 como una orden híbrida de conformidad con el quinto modo MD5 descrito con anterioridad con referencia a las Figuras 6 y 7 si el parámetro TAG1 está en el valor 02.

Para realizar lo que antecede, la orden CMD4 incluye, bajo la referencia de un parámetro TAG6 (que puede representarse, por ejemplo, por el valor "4F"), el identificador AID ("Application Identifier" en terminología inglesa) de Perfil P (o el dominio ISD-P correspondiente) para activar cuando el parámetro TAG1 está en el valor 00 o 01.

Además, la orden CMD4 incluye:

- 50 - bajo la referencia de un parámetro TAG2 (que puede representarse, por ejemplo, por el valor "56"), la lista LT1 de al menos un identificador AID de un perfil P (o del dominio ISD-P correspondiente) que se activará cuando el parámetro TAG1 está en el valor 02. Por ejemplo, cada identificador de AID enumerado se referencia bajo un parámetro TAG8 (que puede representarse, por ejemplo, por el valor "4F") y cuyo valor representa el valor del identificador de AID del Perfil P (o del dominio ISD-P correspondiente);
- 55 - bajo la referencia de un parámetro TAG4 (que puede representarse, por ejemplo, por el valor "57"), la lista LT2 de al menos un identificador AID de un perfil P (o del dominio ISD-P correspondiente) para desactivar cuando el parámetro TAG1 está en el valor 02. Por ejemplo, cada identificador de AID enumerado se referencia bajo un parámetro TAG10 (que puede representarse, por ejemplo, por el valor "4F") y cuyo valor representa el valor del identificador de AID del Perfil P (o del dominio ISD-P correspondiente).

60 En un caso particular, una de las listas LT1 y LT2 está vacía, y la lista no vacía entre LT1 y LT2 incluye al menos dos identificadores de perfil P.

65 Tal como se ilustra en la Figura 9, la orden CMD5 comprende el parámetro DGI en el estado DISABLE PROFILE que indica que la orden CMD5 debe tratarse como una orden de desactivación (o híbrida) y el parámetro TAG1 que indica el modo operativo de conformidad con que debe procesar esta orden CMD5 por el módulo eUICC1.

En respuesta a la orden CMD5, el módulo eUICC1 está configurado para:

- 5 - procesar la orden CMD5 como una orden de desactivación de conformidad con el tercer modo MD3 descrito con anterioridad con referencia a la Figura 5 si el parámetro TAG1 está en el valor 00;
- procesar la orden CMD5 como una orden de desactivación de conformidad con el cuarto modo MD4 descrito con anterioridad con referencia a la Figura 5 si el parámetro TAG1 está en el valor 01; y
- 10 - procesar la orden CMD5 como una orden híbrida de conformidad con el quinto modo MD5 descrito con anterioridad con referencia a las Figuras 6 y 7 si el parámetro TAG1 está en el valor 02.

15 Para hacer lo que antecede, la orden CMD5 incluye, bajo la referencia a un parámetro TAG7 (que puede representarse, por ejemplo, por el valor "4F"), el identificador AID del perfil P (o del dominio ISD-P correspondiente) para desactivar cuando el parámetro TAG1 está en el valor 00 o 01.

Además, la orden CMD5 comprende:

- 20 - bajo la referencia del parámetro TAG2 (que puede representarse, por ejemplo, con el valor "59"), la lista LT1 de al menos un identificador AID de un perfil P (o del dominio ISD-P correspondiente) que se activará cuando el parámetro TAG1 esté en el valor 02. Por ejemplo, cada identificador de AID enumerado se referencia bajo un parámetro TAG8 (que puede representarse, por ejemplo, por el valor "4F") y cuyo valor representa el valor del identificador de AID del perfil P (o del dominio ISD-P correspondiente).
- 25 - bajo la referencia del parámetro TAG4 (que puede representarse, por ejemplo, con el valor "5A"), la lista LT2 de al menos un identificador AID de un perfil P (o del dominio ISD-P correspondiente) para desactivar cuando el parámetro TAG1 esté en el valor 02. Por ejemplo, cada identificador de AID enumerado se referencia bajo un parámetro TAG10 (que puede representarse, por ejemplo, por el valor "4F") y cuyo valor representa el valor del identificador de AID del perfil P (o del dominio ISD-P correspondiente).

30 En un caso particular, una de las listas LT1 y LT2 está vacía, y la lista no vacía entre LT1 y LT2 incluye al menos dos identificadores de perfil P.

35 Se entenderá que la forma de realización descrita con anterioridad con referencia a las Figuras 8 y 9 constituye un ejemplo de puesta en práctica no limitativa de la invención. Según una variante, el parámetro TAG1 de las órdenes CMD4 y CMD5 solamente puede tomar dos de los valores 00, 01 y 02 (por ejemplo, los valores 00 y 02).

40 La invención permite, de manera ventajosa, mejorar la gestión del estado de los perfiles en un módulo eUICC y, en particular, permite mantener varios perfiles activos de manera simultánea para que ya no sea necesario enviar demandas de activación y/o desactivación al módulo eUICC siempre que sea necesario utilizar un perfil diferente. Por lo tanto, es posible limitar el tráfico de red y los recursos normalmente necesarios para enviar y gestionar demandas para activar y desactivar perfiles.

45 Un experto en esta técnica entenderá que las formas de realización y variantes descritas con anterioridad solamente constituyen ejemplos no limitativos de puesta en práctica de la invención. En particular, un experto en esta técnica puede prever cualquier adaptación o combinación de las formas de realización y variantes descritas con anterioridad para satisfacer una necesidad muy específica.

50

REIVINDICACIONES

1. Módulo de identidad de abonado integrado (eUICC1) capaz de cooperar con un terminal de comunicación (T), en donde el módulo de identidad de abonado integrado comprende:
- 5 una pluralidad de dominios de seguridad secundarios (ISD-P), cada uno capaz de contener un perfil de comunicación, con cada perfil de comunicación activo autorizando al terminal de comunicación a comunicarse con una red de telefonía móvil (R) asociada con dicho perfil de comunicación;
- 10 un dominio de seguridad privilegiado (ISD-R) configurado para controlar un estado, activo o inactivo, de cada perfil de comunicación, siendo el dominio de seguridad privilegiado capaz de mantener, de manera simultánea, en el estado activo una pluralidad de perfiles de comunicación (P),
- 15 en donde dicho dominio de seguridad privilegiado (ISD-R) se configura al recibir una demanda de activación (CMD1) de un perfil de comunicación o al recibir una demanda de desactivación (CMD2) de un perfil de comunicación, para mantener, en el estado activo, cualquier otro perfil de comunicación ya activo en dicho módulo de identidad de abonado integrado.
2. Módulo de identidad de abonado integrado según la reivindicación 1, en donde el terminal de comunicación (T) comprende al menos una interfaz de radio (INT), siendo capaz cada perfil de comunicación activo (P), cuando tiene acceso a dicha al menos una interfaz de radio, para establecer una comunicación entre el terminal de comunicación y la red de telefonía móvil asociada con dicho perfil de comunicación activo.
3. Módulo de identidad de abonado integrado según la reivindicación 1 o 2, que comprende:
- 25 - un módulo de recepción (M2) capaz de recibir una demanda de activación (CMD1) de un primer perfil de comunicación (P1) que se encuentra en estado inactivo en el módulo de identidad de abonado integrado;
- 30 - un módulo de configuración (M4) capaz de configurar el módulo de identidad de abonado integrado en un primer modo (MD1) o en un segundo modo (MD2) según el estado de un primer parámetro (PR1) incluido en dicha demanda de activación,
- 35 - en donde, cuando cualquier segundo perfil de comunicación (P2) distinto de dicho primer perfil (P1) ya está activo al recibir dicha demanda de activación, se configura el módulo de identidad de abonado integrado:
- 40 - en el primer modo, para activar el primer perfil de comunicación (P1) mientras se mantiene activo dicho segundo perfil de comunicación (P2);
- 40 - en el segundo modo, para activar el primer perfil de comunicación (P1) y desactivar cada perfil de comunicación (P2, P3) que no sea el primer perfil de comunicación.
4. Módulo de identidad de abonado integrado según cualquiera de las reivindicaciones 1 a 3, que comprende:
- 45 - un módulo de recepción (M2) capaz de recibir una demanda de desactivación (CMD2) de un primer perfil de comunicación (P1) que se encuentra ya en el estado activo en el módulo de identidad de abonado integrado;
- 50 - un módulo de configuración (M4) capaz de configurar el módulo de identidad de abonado integrado en un tercer modo (MD3) o en un cuarto modo (MD4) según el estado de un segundo parámetro (PR2) incluido en dicha demanda de desactivación,
- 50 - en donde, cuando cualquier segundo perfil de comunicación (P2) distinto de dicho primer perfil (P1) ya está activo al recibir dicha demanda de desactivación, se configura el módulo de identidad de abonado integrado:
- 55 - en el tercer modo, para desactivar el primer perfil de comunicación (P1) mientras se mantiene activo dicho segundo perfil de comunicación (P2);
- 55 - en el cuarto modo, para activar un perfil de comunicación predefinido (P3) como el perfil predeterminado y para desactivar cada perfil de comunicación (P1, P2) que no sea dicho perfil predeterminado.
- 60 5. Módulo de identidad de abonado integrado según la reivindicación 4, en donde, en el tercer modo, el módulo de identidad de abonado integrado está configurado, en respuesta a la demanda de desactivación (CMD2), para mantener activo el segundo perfil (P2) de comunicación, incluso si dicho segundo perfil de comunicación no es un perfil de comunicación (P3) predefinido por defecto en el módulo de identidad de abonado integrado (eUICC1).
- 65 6. Módulo de identidad de abonado integrado según una cualquiera de las reivindicaciones 1 a 5, en donde dicha orden de activación y/o dicha orden de desactivación son órdenes APDU de conformidad con la norma ISO 7816-4.

- 5 7. Módulo de identidad de abonado integrado según cualquiera de las reivindicaciones 1 a 6, en donde el módulo de identidad de abonado integrado es capaz, según un quinto modo (MD5), de recibir una primera demanda (CMD3) que identifica al menos dos perfiles de comunicación (P1, P2, P3), cada uno de los cuales se activará o desactivará en dicho módulo de identidad de abonado integrado,
- siendo dicho módulo de identidad de abonado integrado capaz, según dicho quinto modo de:
- 10 - configurar en el estado activo cada perfil de comunicación (P1, P2) identificado como un perfil para ser activado en dicha primera demanda; y
- configurar en el estado inactivo cada perfil de comunicación (P3) identificado como un perfil para ser desactivado en dicha primera demanda.
- 15 8. Módulo de identidad de abonado integrado según la reivindicación 7, en donde la primera demanda identifica al menos un primer perfil de comunicación que se activará en el módulo de identidad de abonado integrado y al menos un segundo perfil de comunicación que se desactivará en el módulo de identidad de abonado integrado.
- 20 9. Módulo de identidad de abonado integrado según la reivindicación 7 u 8, en donde la primera demanda identifica solamente al menos dos primeros perfiles de comunicación para activar o solamente al menos dos perfiles de comunicación para desactivar en el módulo de identidad de abonado integrado.
- 25 10. Módulo de identidad de abonado integrado según la combinación de al menos las reivindicaciones 3, 4 y 7, en donde la primera demanda (CMD3) comprende un tercer parámetro (DGI) que puede tomar un primer estado (ENABLE PROFILE) o un segundo estado (DISABLE PROFILE) y un cuarto parámetro (TAG1) que puede tomar un primer estado (00), un segundo estado (01) o un tercer estado (02),
- en donde el módulo de identidad de abonado integrado está configurado para:
- 30 ○ procesar la primera demanda como orden de activación cuando el tercer parámetro (DGI) está en el primer estado y el cuarto parámetro (TAG1) está en el primer o segundo estado (00, 01);
- procesar la primera demanda como una orden de desactivación cuando el tercer parámetro (DGI) está en el segundo estado y el cuarto parámetro (TAG1) está en el primer o segundo estado (00, 01); y
- 35 ○ procesar la primera demanda como una orden híbrida de activación y de desactivación cuando el tercer parámetro (DGI) está en el primer o segundo estado, y el cuarto parámetro (TAG1) está en el tercer estado (02).
- 40 11. Módulo de identidad de abonado integrado según la reivindicación 10, en donde el módulo de identidad de abonado integrado está configurado para procesar la primera demanda (CMD3):
- 45 ○ según el primer modo (MD1) si el tercer parámetro (DGI) está en el primer estado y el cuarto parámetro (TAG1) está en el primer estado;
- según el segundo modo (MD2) si el tercer parámetro (DGI) está en el primer estado y el cuarto parámetro (TAG1) está en el segundo estado;
- 50 ○ según el tercer modo (MD3) si el tercer parámetro (DGI) está en el segundo estado y el cuarto parámetro (TAG1) está en el primer estado;
- según el cuarto modo (MD4) si el tercer parámetro (DGI) está en el segundo estado y el cuarto parámetro (TAG1) está en el segundo estado; y
- 55 ○ según el quinto modo (MD5) si el tercer parámetro (DGI) está en el primer estado y el cuarto parámetro (TAG1) está en el tercer estado, o si el tercer parámetro (DGI) está en el segundo estado y el cuarto parámetro (TAG1) está en el tercer estado.
- 60 12. Dispositivo (SM-SR) capaz de comunicarse con un terminal de comunicación (T) que coopera con un módulo de identidad de abonado integrado (eUICC1), comprendiendo dicho dispositivo:
- un módulo de envío capaz de enviar al módulo de identidad de abonado integrado una demanda de activación de un primer perfil de comunicación que se encuentra en el estado inactivo en el módulo de identidad de abonado integrado o para enviar una demanda de desactivación de un primer perfil de comunicación que se encuentra ya en el estado activo en el módulo de identidad de abonado integrado;
- 65

- un módulo de inserción capaz de incluir, antes de enviar al módulo de identidad de abonado integrado, uno de entre:
 - 5 o un primer parámetro en la demanda de activación; y
 - o un segundo parámetro en la demanda de desactivación,
- en donde:
- 10 - el primer parámetro está en un estado que define si el módulo de identidad de abonado integrado debe configurarse en un primer modo o en un segundo modo cuando cualquier segundo perfil de comunicación distinto de dicho primer perfil ya está activo en el módulo de identidad de abonado integrado al recibir dicha demanda de activación, controlando el estado del primer parámetro al módulo de identidad de abonado integrado:
 - 15 o en el primer modo, activando el primer perfil de comunicación mientras se mantiene activo dicho segundo perfil de comunicación;
 - o en el segundo modo, activando el primer perfil de comunicación y desactivando cada perfil de comunicación que no sea el primer perfil de comunicación.
 - 20 - el segundo parámetro está en un estado que define si el módulo de identidad de abonado integrado debe configurarse en un tercer modo o en un cuarto modo cuando cualquier segundo perfil de comunicación distinto de dicho primer perfil ya está activo al recibir dicha demanda de desactivación, controlando el estado del segundo parámetro al módulo de identidad de abonado integrado:
 - 25 o en el tercer modo, desactivando el primer perfil de comunicación mientras se mantiene activo dicho segundo perfil de comunicación;
 - 30 o en el cuarto modo, activando un perfil de comunicación predefinido como el perfil predeterminado y desactivando cada perfil de comunicación que no sea dicho perfil predeterminado.
13. Sistema (SY) que comprende:
- 35 - un módulo de identidad de abonado integrado (eUICC1) según cualquiera de las reivindicaciones 1 a 11;
 - un terminal de comunicación (T) que coopera con el módulo de identidad de abonado integrado; y
 - al menos un dispositivo (SM-SR) según la reivindicación 12.
- 40 14. Método de control puesto en práctica por un módulo de identidad de abonado integrado (eUICC1) capaz de cooperar con un terminal de comunicación (T),
- comprendiendo dicho módulo de identidad de abonado integrado:
- 45 - una pluralidad de dominios de seguridad secundarios (ISD-P), cada uno capaz de contener un perfil de comunicación; y
 - un dominio de seguridad privilegiado (ISD-R) configurado para controlar un estado activo o inactivo de cada perfil de comunicación;
- 50 comprendiendo dicho método una etapa de mantenimiento en el estado activo, de manera simultánea, de una pluralidad de perfiles de comunicación (P), autorizando cada perfil de comunicación activo al terminal de comunicación a comunicarse con una red de telefonía móvil (R) asociada con dicho perfil de comunicación,
- 55 comprendiendo dicho método, al recibir una demanda de activación (CMD1) de un perfil de comunicación o al recibir una demanda de desactivación (CMD2) de un perfil de comunicación, el mantenimiento en el estado activo, por dicho dominio de seguridad privilegiado (ISD-R), de cualquier otro perfil de comunicación ya activo en dicho módulo de identidad de abonado integrado.

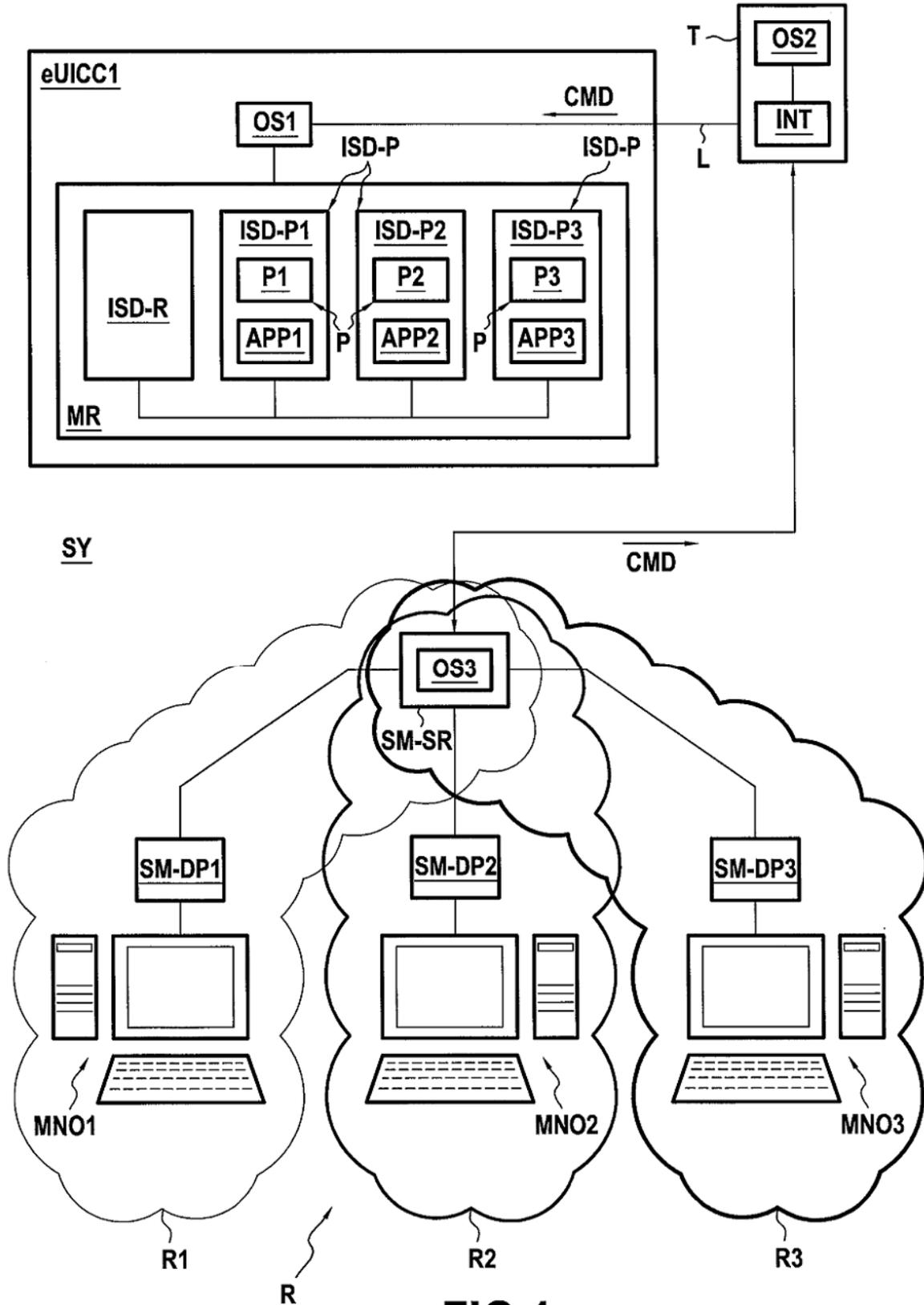


FIG.1

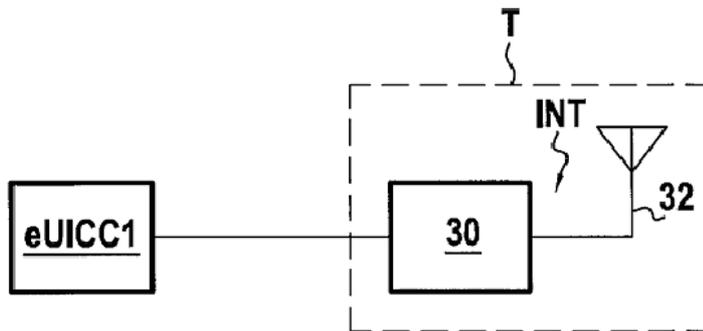


FIG. 2A

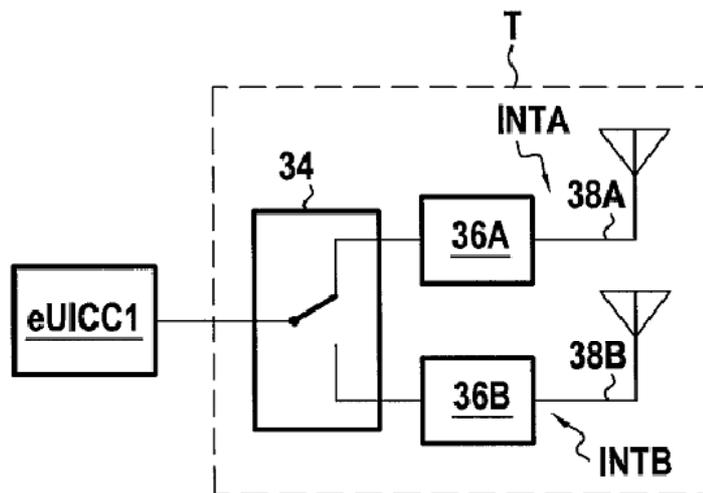


FIG. 2B

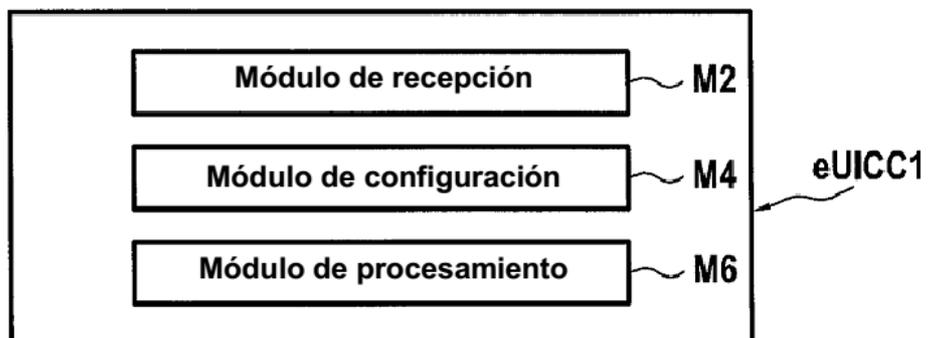


FIG. 3

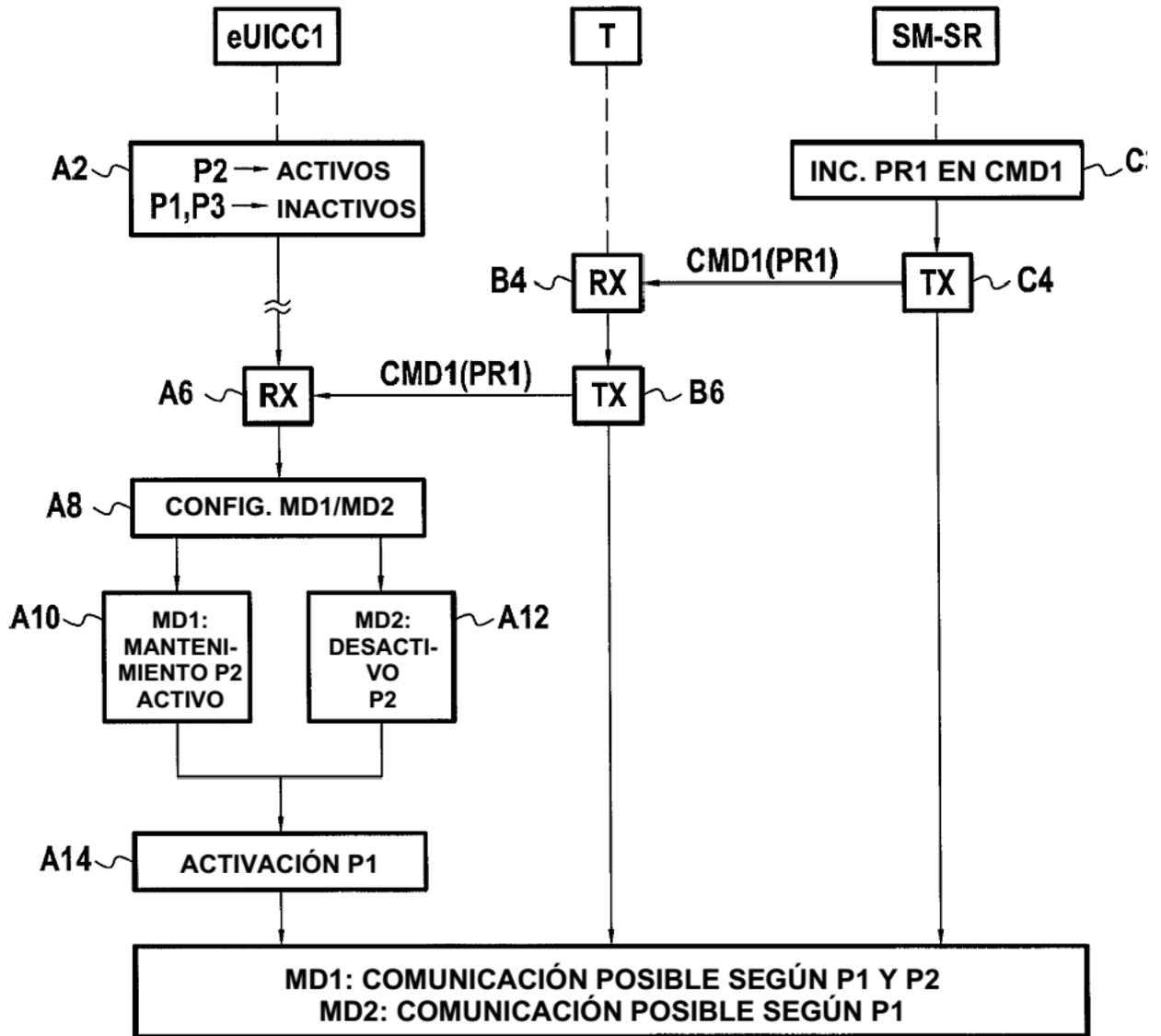


FIG.4

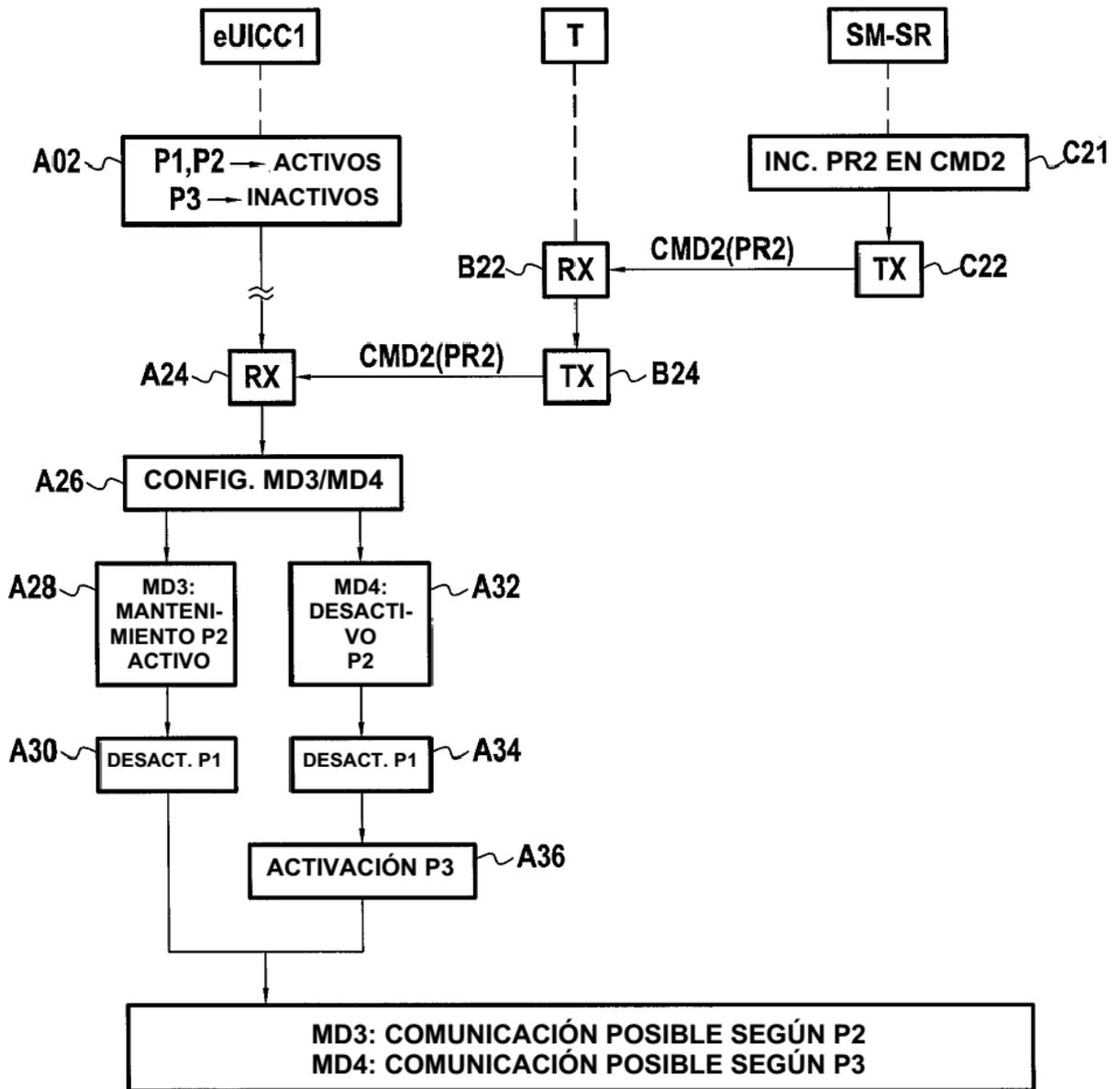


FIG.5

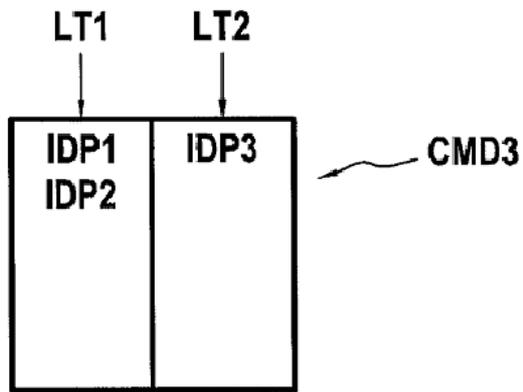


FIG.6

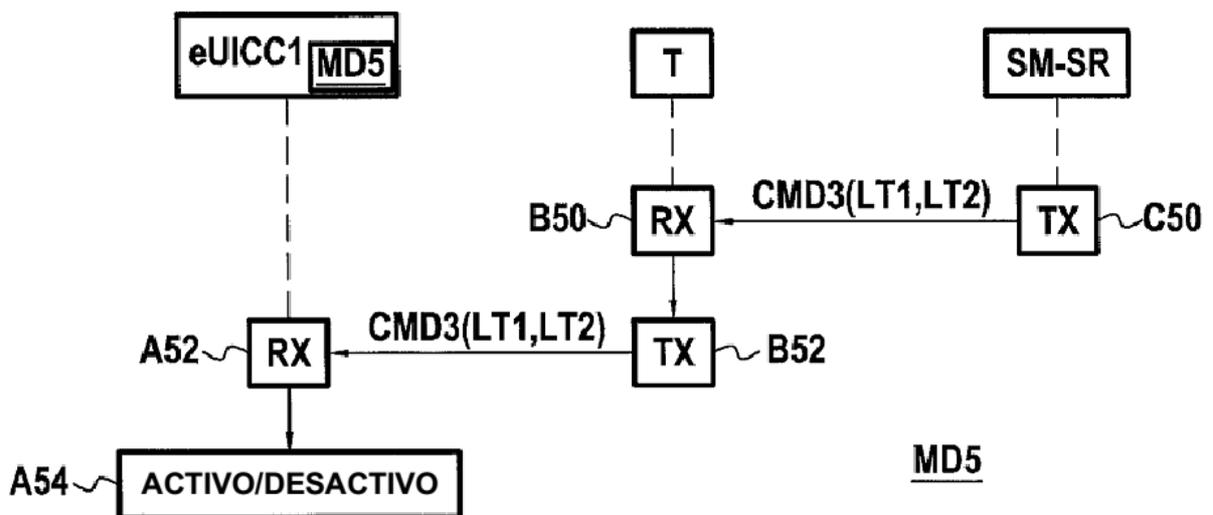


FIG.7

DGI	LONGITUD	VALOR			
	3A03	VAR	HABILITAR PERFIL		
CMD4	TAG1	TAG	LONGITUD	VALOR	
		55	LONGITUD	MODO	
			01	00: 00: HABILITAR NUEVO ISD-P + PERMANECER ACTIVADO ISD-P YA ACTIVADO	
			01	01: 01: HABILITAR ISD-P REFERENCIADO + INHABILITAR TODOS LOS DEMÁS	
	TAG6	4F	01	02 02: HABILITAR LISTA LT1 DE ISD-P + INHABILITAR LISTA LT2 DE ISD-P	
			01	...	
	TAG2	56	LISTA LT1		
			5-16	ISD-P AID	
	TAG4	57	LISTA LT2		
			TAG8	LONGITUD	VALOR
4F			5-16	ISD-P AID	
...			
		4F	5-16	ISD-P AID	
		TAG10	LONGITUD	VALOR	
		4F	5-16	ISD-P AID	
		
		4F	5-16	ISD-P AID	

FIG.8

DGI	LONGITUD	VALOR		
DGI 3A04	VAR	INHABILITAR PERFIL		
	TAG1	TAG	LONGITUD VALOR	
		58	LONGITUD MODO	
	TAG7	01	00: INHABILITAR ISD-P REFERENCIADO + PERMANECER ACTIVADO ISD-P YA ACTIVADO	
		01	01: INHABILITAR TODOS LOS ISD-P ACTIVADOS + ACTIVACIÓN DE PERFIL DE RETROCESO	
		01	02: HABILITAR LISTA LT1 DE ISD-P + INHABILITAR LISTA LT2 DE ISD-P	
	TAG2	01	...	
		4F	5-16	ISD-P AID
	TAG4	56	LISTA LT1	
		TAG8	TAG	LONGITUD VALOR
4F			5-16	ISD-P AID
...		
4F	5-16	ISD-P AID		
TAG4	57	LISTA LT2		
	TAG1	TAG	LONGITUD VALOR	
		4F	5-16	ISD-P AID
	
4F	5-16	ISD-P AID		

CMD5 →

FIG.9