

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 663 558**

51 Int. Cl.:

H04W 8/18 (2009.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **17.12.2014 PCT/EP2014/078270**

87 Fecha y número de publicación internacional: **02.07.2015 WO15097042**

96 Fecha de presentación y número de la solicitud europea: **17.12.2014 E 14824813 (1)**

97 Fecha y número de publicación de la concesión europea: **18.10.2017 EP 3087767**

54 Título: **Método para acceder a un servicio y dispositivo correspondiente**

30 Prioridad:

23.12.2013 EP 13306844

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

13.04.2018

73 Titular/es:

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

72 Inventor/es:

**ROUSSEL, NICOLAS;
JUBERT, NICOLAS;
LABOURIE, FLORENT;
DUPREZ, JÉRÔME y
FAURE, FRÉDÉRIC**

74 Agente/Representante:

CASANOVAS CASSA, Buenaventura

ES 2 663 558 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).

DESCRIPCION

Método para acceder a un servicio y dispositivo correspondiente.

5 **Campo de la invención:**

La invención se refiere en general a un método para acceder a un servicio.

10

Además, la invención se refiere a un primer dispositivo para acceder a un servicio.

El primer dispositivo puede ser un terminal, como particularmente un teléfono móvil.

15

La presente invención es especialmente aplicable a un campo de radio-comunicación móvil en el que un chip puede ser un chip integrado, como una Tarjeta Universal de Circuito Integrado incrustada (o eUICC) o un chip que está incluido dentro de una tarjeta inteligente denominada Módulo de Identidad de Subscriptor (o SIM) del tipo tarjeta o similares, como un elemento de seguro.

20

Dentro de la presente descripción, un elemento seguro (o SE) es un objeto inteligente que, por un lado, protege el acceso a los datos que almacena el objeto inteligente y, por otro lado, pretende comunicarse con el mundo exterior.

Estado de la técnica:

25

Como es conocido per se, un teléfono móvil, como un terminal de usuario, coopera con un SE, con el fin de identificar y autenticar un abonado a una red de radio-comunicación móvil. Para identificar y autenticar al abonado, la SE proporciona datos relativos a una suscripción de usuario a la red de radio-comunicación móvil.

WO2012/076461 y EP 2 461 613 A1 describe una técnica para la conmutación de una primera a una segunda suscripción (lógica) dentro de una y la misma UICC, como un elemento seguro.

30

Sin embargo, tal conmutación es transparente a un terminal receptor UICC. Puede ser que el terminal tenga una suscripción activa y la UICC tenga otra suscripción activa. Esto da como resultado que el terminal esté en un estado bloqueado cuando las dos suscripciones diferentes no están relacionadas con una única y misma red de radiocomunicación móvil. Dicho estado bloqueado implica una pérdida de conectividad de red que resulta molesta para el usuario del terminal. Para salir de ese estado bloqueado, se requiere un reinicio manual del equipo terminal, a fin de sincronizar el terminal y la UICC receptora.

35

Sumario de la invención:

40

La invención propone una solución para resolver el problema especificado en el párrafo anterior, proporcionando un método para acceder a un servicio, apareciendo definido dicho método en la reivindicación 1, y proporcionando un dispositivo correspondiente tal como se define en la reivindicación 8. Según la invención, un primer dispositivo accede a medios de almacenamiento de datos. Los medios de almacenamiento de datos almacenan al menos dos suscripciones. Una primera suscripción está activa. Al menos una segunda suscripción no está activa. El método incluye los siguientes pasos. Un segundo dispositivo envía a un gestor de suscripción una petición de conmutación a la segunda suscripción, como suscripción a ser activada. El gestor de suscripción incluye la primera variable relativa a la siguiente suscripción activa. El gestor de suscripción fija la primera variable a la segunda suscripción. El gestor de suscripción envía al sistema operativo del primer dispositivo un mensaje para solicitar al sistema operativo del primer dispositivo que relance una ejecución del gestor de suscripción y leer los datos. El sistema operativo del primer dispositivo envía al gestor de suscripción un mensaje que incluye un comando para relanzar una ejecución del gestor de suscripción. El gestor de suscripción desactiva, sobre la base del primer valor variable, la primera suscripción. El gestor de suscripción activa, sobre la base del primer valor variable, la segunda suscripción. Y el gestor de suscripción envía al sistema operativo del primer dispositivo los datos relativos a la segunda suscripción, como una suscripción activa actual.

55

El principio de la invención consiste en que, tan pronto como un gestor de suscripción recibe de un solicitante, como un segundo dispositivo, una petición de intercambio a una suscripción identificada, el gestor de suscripción:

60

- actualiza, mediante el uso de la suscripción identificada, una primera variable correspondiente a la siguiente suscripción activa;
- solicita el Sistema Operativo del primer dispositivo (u OS) para obtener los datos;
- activa, una vez lanzada, únicamente la suscripción identificada utilizando la variable inicial; y
- transmite al OS del primer dispositivo los datos relacionados con la suscripción identificada.

65

La solución de la invención permite sincronizar automáticamente una conmutación de una primera a una segunda suscripción entre el gestor de suscripción y el OS del primer dispositivo. En otras palabras, el OS del primer dispositivo y el gestor de suscripción comparten los datos relativos a la suscripción a la que el gestor de suscripción

se ha conmutado.

Contrariamente a la solución conocida, debido a la consistencia de la suscripción, no existe ningún problema referido al estado bloqueado ni a la pérdida de conectividad de red.

Contrariamente a la solución conocida, debido a un procesamiento automático de la conmutación a la suscripción identificada, la solución de la invención no requiere intervención humana para sincronizar la aplicación de tipo SIM y el primer dispositivo.

La solución de la invención no requiere ningún espacio de memoria adicional más que el que se utiliza para almacenar los datos relativos a las suscripciones, independientemente de su respectivo estado, ya sea activo o inactivo.

Es de notar que el gestor de suscripción es sostenido por la parte del cliente, es decir, ya sea el primer dispositivo en sí mismo o u otro dispositivo, como un tercer dispositivo. En otras palabras, el OS del primer dispositivo puede realizar intercambios con el gestor de suscripción del primer dispositivo o con un gestor de suscripción de un tercer dispositivo.

De acuerdo con un aspecto adicional, la invención es el primer dispositivo para acceder a un servicio.

Según la invención, el primer dispositivo comprende medios de almacenamiento de datos. Los medios de almacenamiento de datos almacenan un gestor de suscripción. Los medios de almacenamiento de datos almacenan al menos dos suscripciones. Una primera suscripción está activa. Al menos una segunda suscripción no está activa. El gestor de suscripción está configurado para recibir una petición de conmutación a la segunda suscripción, como una suscripción a ser activada. El gestor de suscripción incluye una primera variable relativa a la siguiente suscripción activa. El gestor de suscripción está configurado para fijar la primera variable a la segunda suscripción. El gestor de suscripción está configurado para enviar al sistema operativo del primer dispositivo un mensaje para solicitar al sistema operativo del primer dispositivo que relance una ejecución del gestor de suscripción y leer los datos. El gestor de suscripción está configurado para recibir un mensaje que incluye un comando para relanzar una ejecución del gestor de suscripción. El gestor de suscripción está configurado para desactivar, sobre la base del valor variable inicial, la primera suscripción, para activar, sobre la base del valor variable inicial, la segunda suscripción y enviar al sistema operativo del primer dispositivo los datos relativos a la segunda suscripción, como suscripción activa actual.

El primer dispositivo puede ser un terminal.

De acuerdo con todavía un aspecto adicional, la invención es un sistema para acceder a un servicio. Según la invención, el sistema comprende un primer dispositivo y un chip acoplado o conectado al primer dispositivo. El chip comprende medios de almacenamiento de datos. Los medios de almacenamiento de datos almacenan un gestor de suscripción. Los medios de almacenamiento de datos almacenan al menos dos suscripciones. Una primera suscripción está activa. Al menos una segunda suscripción no está activa. El gestor de suscripción está configurado para recibir una petición de conmutación a la segunda suscripción, como una suscripción a ser activada. El gestor de suscripción incluye una primera variable relativa a la siguiente suscripción activa. El gestor de suscripción está configurado para fijar la primera variable a la segunda suscripción. El gestor de suscripción está configurado para enviar al sistema operativo del primer dispositivo un mensaje para solicitar al sistema operativo del primer dispositivo que relance una ejecución del gestor de suscripción y leer los datos. El gestor de suscripción está configurado para recibir un mensaje que incluye un comando para relanzar una ejecución del gestor de suscripción. El gestor de suscripción está configurado para desactivar, sobre la base del valor variable inicial, la primera suscripción, para activar, sobre la base del valor variable inicial, la segunda suscripción y enviar al sistema operativo del primer dispositivo los datos relativos a la segunda suscripción, como suscripción activa actual.

El chip puede estar fijado o puede ser extraíble del primer dispositivo.

El chip puede ser incluido dentro de un elemento de seguro. La invención no impone ninguna restricción en cuanto a la clase de tipo de elemento seguro.

Como elemento de seguridad extraíble, puede ser una tarjeta de tipo SIM, un Módulo de Seguridad Extraíble (o SRM), un dongle inteligente de tipo USB (acrónimo de "Universal Serial Bus"), una (micro) tarjeta Digital Segura (o SD) o una tarjeta de tipo Multi-Media (o MMC) o cualquier formato de tarjeta para ser acoplado a un dispositivo huésped, como un primer dispositivo.

Breve descripción de los dibujos:

Las características adicionales y ventajas de la invención serán más claramente comprensibles después de la lectura detallada de la descripción de una realización preferida de la invención, dada como un ejemplo indicativo y no limitativo, en conjunción con los siguientes dibujos:

- La figura 1 ilustra un diagrama simplificado de un servidor remoto y una realización de un equipo terminal, el equipo terminal estando dispuesto internamente para sincronizar los datos relativos a una suscripción a la que el servidor solicita conmutarse, de acuerdo con la invención; y
- La figura 2 representa un ejemplo de un flujo de mensajes entre el servidor y las distintas entidades equipo terminal de la figura 1, de modo que un gestor de suscripción con el apoyo de un chip alojado en terminal controle un intercambio de datos con el terminal, con el fin de compartir los datos relativos a una suscripción que está activa después de una conmutación de suscripción.

Descripción detallada:

Más abajo se considera un caso en el que el método de la invención para acceder a un servicio es implementado por un teléfono móvil, como primer dispositivo y un dispositivo huésped de chip, un servidor remoto, como un segundo dispositivo, y un chip, como un tercer dispositivo, que es fijado al teléfono.

De acuerdo con otra realización, el método de la invención para acceder a un servicio es implementado por un teléfono móvil, como primer dispositivo y entidad independiente, y un servidor remoto, como un segundo dispositivo. En otras palabras, el teléfono, como terminal de usuario, no coopera con cualquier chip, con el fin de sincronizar, entre un gestor de suscripción admitido por el teléfono y el SO del teléfono, los datos relativos a una suscripción que es activa después de una conmutación de suscripción. De acuerdo con una realización de este tipo (no representada), el primer dispositivo está adaptado para realizar las funciones que realiza el chip y el primer dispositivo y que son descritos infra.

Naturalmente, la forma de realización que se describe a continuación es considerada sólo a título ejemplificador y no para reducir el alcance de la invención.

La Figura 1 muestra esquemáticamente un equipo terminal 10, como un sistema para acceder a un servicio, que está conectado a un servidor remoto 18.

Tal sistema para acceder a un servicio incluye un teléfono móvil 12, como un terminal de usuario, y una UICC 14.

En aras de la simplicidad, el teléfono móvil 12, la UICC 14 y el servidor remoto 18 se denominarán en adelante en el presente documento como el teléfono 12, el chip 14 y el servidor 18, respectivamente.

Por razones de claridad, sólo se representa un terminal. Sin embargo, el servidor 18 es capaz de proporcionar una flota de terminales/chips con una petición de conmutación a una suscripción para ser activado.

En lugar de un teléfono, puede ser cualquier otro dispositivo que incluye medios para procesar datos, que comprende o está conectado a medios de comunicación inalámbrica para intercambiar datos con el exterior, y que comprende o está conectado a medios para el almacenamiento de datos.

Dentro de la presente descripción, el adjetivo "inalámbrico" que se utiliza dentro de la expresión "medios de comunicación inalámbrica" indica en particular a que los medios de comunicación comunican a través de uno o varios enlaces de Radiofrecuencia (RF) de Largo Alcance (o LR).

Las RF LR pueden fijarse en varios cientos de MHz, por ejemplo, alrededor de 850, 900, 1800, 1900 y/o 2100 MHz.

En lugar de estar constituido por un teléfono, el dispositivo huésped de chip puede ser, por ejemplo, una caja de puesta a punto, un ordenador de sobremesa, un ordenador portátil, un reproductor media, una consola de juegos, una tableta, un netbook, un teléfono y/o una Asistente Digital Personal (o PDA) que incorpora preferentemente o coopera con un procesador de radio de banda base. El procesador de radio de banda de base gestiona funciones de radio en cooperación con una antena para la comunicación, Over-The-Air (o OTA), con otra entidad, como el servidor 18.

Dicho conjunto de dispositivo huésped de chip no es exhaustivo, sino que sólo tiene propósito ejemplificador.

El teléfono 12 se usa preferiblemente para acceder a una o varias redes móviles de radiocomunicación 16.

Las redes móviles de radiocomunicación 16 puede estar constituidas por un Servicio Global para Móviles (o GSM), un Servicio General de Paquetes vía Radio (o GPRS), un Sistema Universal de Telecomunicaciones Móviles (o UMTS), una UTRAN (acrónimo de "Red de Acceso Radio Terrestre UMTS"), un EDGE (acrónimo de "Tasas de Datos Mejoradas para la evolución de GSM"), un Código de División de Acceso Múltiple (o CDMA), una WLAN (acrónimo de "Red de Área Local Inalámbrica") y/o red(es) del tipo de Evolución a Largo Plazo (o LTE o).

Dicha conjunto de red de radiocomunicación móvil no es exhaustiva, sino que sólo tiene propósito ejemplificador.

El teléfono 12 incluye preferiblemente una pantalla de visualización 122 y un teclado 124, como Interfaz Hombre-

Máquina (o MMI).

Alternativamente, en lugar de un teclado físico separado de la pantalla de visualización, el teléfono 12 está equipado con una pantalla de visualización sensible al tacto, como un teclado virtual.

El MMI permite al usuario de un teléfono interactuar con el teléfono 12.

El teléfono 12 incluye una antena 126. La antena 126 permite la comunicación de datos, a través de un enlace(s) de RF LR 15, sobre varias redes móviles de radiocomunicación 16, con un Sistema de Aprovisionamiento Remoto (o RPS), como el servidor 18.

El teléfono 12 incluye medios de procesamiento de datos, como un microprocesador (no representado), medios de almacenamiento de datos (no representados), como la memoria del teléfono, y una o varias interfaces de entrada/salida (o I/O) que están vinculados todos juntos a través de un bus de control y datos (no representado).

El teléfono 12 juega, de manera preferente, un papel de un modulador-demodulador (o módem), para intercambiar datos con el servidor 18.

El teléfono 12 realiza las siguientes operaciones:

- una modulación de una señal portadora analógica para codificar la información digital a transmitir, a través de la antena 126, al servidor 18 (y/u otra entidad (no representada)), y
- una demodulación de una señal portadora analógica recibida para decodificar la información digital codificada que se recibe, a través de la antena 126, desde el servidor 18 (y/u otra entidad (no representada)).

La memoria del teléfono puede comprender una o varias memorias que incluyen una o varias memorias volátiles y una o varias memorias no volátiles.

Una memoria del teléfono, sea o no volátil, almacena, al menos de manera temporal, datos relativos a una suscripción que el teléfono 12 recibe del chip 14.

El teléfono 12 puede incluir, como memoria volátil, una memoria caché.

La memoria del teléfono almacena un Sistema Operativo (u OS) y una o varias aplicaciones.

El teléfono 12 está preferiblemente acoplado al chip 14.

Las interfaces I/O de teléfono incluyen una interfaz I/O para intercambiar datos con el chip 14.

El chip 14 está bajo control del microprocesador del teléfono.

Alternativamente, en lugar de estar acoplada al chip 14, la(s) memoria(s) del teléfono almacenan los datos almacenados en el chip 14 como se describe infra.

De acuerdo con una realización particular, el chip 14 se suelda a una Placa de Circuito Impreso (o PCB) del teléfono 12.

Según otra forma de realización, la interfaz I/O del teléfono con el chip 14 es una interfaz 7816 de la Organización Internacional de Normalización (o ISO), como interfaz de contacto, cuando se inserta el chip 14, de manera extraíble, en el teléfono 12.

Alternativamente, en lugar de una interfaz de contacto, la interfaz I/O de teléfono con el chip 14 está conectado a o incluye una interfaz sin contacto. El teléfono 12 está conectado a o incluye medios para la comunicación de datos durante el uso preferiblemente de un enlace de RF de Corto Alcance (o SR). El enlace de RF SR puede estar relacionado con cualquier tecnología que permite que el teléfono 12 intercambie datos con el chip 14. La RF SR puede fijarse en 13,56 MHz y relacionada con un tipo de tecnología de Comunicación de Campo Cercano (o NFC), como una tecnología sin contacto.

El chip 14 esta asociado preferentemente con o vinculado al servidor 18.

El chip 14 pertenece a un usuario, como abonado a un(os) servicio(s) inalámbrico(s).

El chip 14 está conectado, a través de un enlace bidireccional 13, al teléfono 12.

El chip 14 incluye un(os) microprocesador(es) 142, como medios de procesamiento de datos, una(s) memoria(s) 144, como medios de almacenamiento de datos, y una o varias interfaces I/O 146 que están internamente todas

conectadas, a través de un bus de datos bidireccional interno 143, una a las otras.

La(s) interfaz(ces) I/O 146 permite la comunicación de datos desde los componentes del chip interior al chip exterior y viceversa.

La memoria 144 preferiblemente almacena datos relativos a un Identificador de Recursos Uniforme (URI) o, un Localizador de Recursos Uniforme (URL) y/o una dirección de Protocolo de Internet (o IP) de una entidad externa a la que debe dirigirse, como el servidor 18.

La memoria 144 almacena un OS.

La memoria 144 almacena preferiblemente una o varias aplicaciones tipo Módulos de Identificación de Suscriptor (o SIM).

La aplicación(es) tipo SIM incluye, entre otros, una aplicación SIM para una red de tipo Servicio Global para Móviles (o GSM), una aplicación Módulo Universal de identificación de Abonado (o USIM) para una red del tipo Sistema Universal de Telecomunicaciones Móviles (o UMTS), una aplicación Acceso Múltiple por División de Código (o CDMA) Módulo de Identificación de Suscriptor (o CISM) y/o una aplicación Protocolo de Internet Subsistema Multimedia (o IMS) Módulo de Identificación de Suscriptor (o ISIM).

La(s) aplicación(es) de tipo de SIM permite(n) al teléfono 12 autenticarse a una o varias redes móviles de radiocomunicación 16.

Para autenticarse a la red de radiocomunicación móvil(es) 16, la(s) aplicación(es) de tipo SIM utiliza(n) preferentemente una clave de autenticación de red Ki relativa a una suscripción activa en curso. La(s) aplicación(es) de tipo SIM también utilizan preferiblemente datos, como una cuestión que es suministrada por una entidad externa que intenta autenticar al abonado, y un algoritmo de autenticación, como, por ejemplo, Milenage.

La memoria 144 almacena una o varias aplicaciones adicionales. Entre las aplicaciones soportadas, la memoria 144 almacena una aplicación de invención denominada gestor de suscripción.

El gestor de suscripción permite llevar a cabo una función de conmutación de suscripción a nivel del chip 14 y a nivel del teléfono 12, con el fin de almacenar datos en relación con una y la misma suscripción después de una conmutación de suscripción. El gestor de suscripción permite asegurar una conectividad de red de radiocomunicación móvil después de dicha conmutación de suscripción sin involucrar al usuario del terminal.

La memoria 144 almacena datos relativos a una pluralidad de suscripciones a una o varias redes de radiocomunicación móvil 16, como un(os) servicio(s) inalámbrico(s).

Cada conjunto de datos relativos a una suscripción a una o varias redes de radiocomunicación móvil 16 incluye:

- una Identidad Internacional del Suscriptor a un Móvil (o IMSI), como un suscriptor y un identificador de suscripción de servicio para acceder a una red de radiocomunicación móvil;
- una clave Ki, como una clave de autenticación de red, que permite autenticar el abonado correspondiente a la correspondiente red de radiocomunicación móvil;
- Milenage, como un algoritmo de autenticación, que permite autenticar el abonado correspondiente a la correspondiente red de radiocomunicación móvil;
- una o varias contraseñas, como un Número de identificación Personal (o PIN), y/o uno o varios algoritmo(s) criptográfico(s), como los datos relativos a secreto(s), que está(n) almacenado(s) de forma segura dentro del chip 14;
- un sistema de archivos que incluye al menos un Archivo Elemental (o EF);
- una o varias claves de seguridad, como una(s) clave(s) para el cifrado/descifrado de datos y/o una(s) clave(s) para los datos de firma de una(s) clave(s);
- una o varias claves aplicativas, como una clave para acceder a una cuenta bancaria del usuario a través de las redes de radiocomunicaciones móviles; y/o
- una o varias credenciales, como un nombre de usuario y/o un Identificador (o ID) del suscriptor, como datos relacionados con el usuario.

En aras de la simplicidad, la memoria 144 almacena, por ejemplo, sólo dos conjuntos de datos de suscripción, un conjunto de datos relativos a una primera suscripción, como "suscripción 1", y otro conjunto de datos relativos a una segunda suscripción, como "suscripción 2".

Sin embargo, la memoria 144 puede almacenar más de dos conjuntos de datos de suscripción y la invención continuaría siendo aplicable.

Dos suscripciones están disponibles, por el lado del cliente, dentro de un único y mismo chip 14.

La memoria 144 almacena dentro de un primer dominio de seguridad 145, como una primera área de memoria, el primer conjunto de datos relativos a una primera suscripción.

5 El primer conjunto de datos de suscripción permite acceder desde el teléfono 12 a una primera red de radiocomunicación móvil 161.

La suscripción primera "suscripción 1" está activa, es decir, está en un estado activado.

10 Los datos de la primera suscripción comprenden un identificador IMSI1, como un primer suscriptor, relativo a una primera suscripción.

15 Los datos de la primera suscripción incluyen preferiblemente una primera clave Ki1, como una primera clave Ki1 de autenticación de red, para autenticar al suscriptor de la primera red de radiocomunicación móvil 161. La primera clave Ki1 de autenticación de red está asociada con el primer suscriptor IMSI1. La primera clave Ki1 de autenticación de red permite la autenticación del primer suscriptor asociado a la primera red de radiocomunicación móvil 161.

20 El primer dominio de seguridad 145 puede almacenar adicionalmente una o varias aplicaciones que son accesibles con un Operador de Red Móvil (o MNO) que operan o permite operar la primera red de radiocomunicación móvil 161.

La memoria 144 almacena también, dentro de un segundo dominio de seguridad 147, como una segunda área de memoria, el segundo conjunto de datos relativos a una segunda suscripción.

25 El segundo conjunto de datos de suscripción permite acceder desde el teléfono 12 a la segunda red de radiocomunicación móvil 162.

La segunda suscripción "suscripción 2" no está activa, es decir, está en un estado desactivado.

30 Los datos de la segunda suscripción comprenden un identificador IMSI2, como un segundo suscriptor, relativo a una segunda suscripción.

35 Los datos de la segunda suscripción incluyen preferiblemente una segunda clave Ki2, como una segunda clave Ki2 de autenticación de red, para autenticar al abonado a una segunda red de radiocomunicación móvil 162. La segunda clave Ki2 de autenticación de red está asociada con el segundo suscriptor IMSI2. La segunda clave Ki2 de autenticación de red permite la autenticación del segundo abonado asociado a la segunda red de radiocomunicación móvil 162.

40 El segundo dominio de seguridad 147 puede almacenar adicionalmente una o varias aplicaciones que son accesibles con un MNO que opera o permite operar la segunda red de radiocomunicación móvil 162.

45 Una suscripción particular puede ser identificada por uno o varios identificadores, como un identificador de suscriptor IMSI, un identificador relativo a una aplicación, también denominado Identificador de Aplicación (o AID), un Emisor de Suscripción de Dominio de Seguridad (o SDSI) y/o un(os) identificador(es) en relación con cualquier entidad(es) de software o hardware que esté(n) involucrados en una vía de comunicación para acceder a la información de suscripción correspondiente.

El microprocesador 142 procesa, controla y comunica internamente datos con todos los otros componentes incorporados dentro del chip y, a través de la(s) interfaz(es) I/O 146, con el chip exterior.

50 El microprocesador 142 ejecuta o pone en marcha una o varias aplicaciones, incluyendo el gestor de suscripción.

55 El microprocesador 142 es preferiblemente capaz de iniciar acciones, con el fin de interactuar directamente con el mundo exterior, de una manera independiente del teléfono 12, como un dispositivo huésped de chip. Tal capacidad de interacción a iniciativa del chip 14 también se conoce como capacidad proactiva. Según una realización preferida, el chip 14 es capaz de utilizar comandos del tipo ToolKit SIM (o STK), como comandos proactivos.

60 El chip 14 es así capaz de enviar, por iniciativa propia, a través del teléfono 12, a cualquier dispositivo conectado al teléfono 12 un comando proactivo para enviar al servidor 18 un mensaje del tipo Servicio de Mensajes Cortos (o SMS), por ejemplo, un acuse de recibo de una petición de conmutación a una suscripción identificada, como una suscripción a ser activada.

El chip 14 es preferiblemente capaz de autenticar su interlocutor como el servidor 18 u otra entidad con la que el chip 14 está habilitado para comunicarse.

65 Según la invención, el gestor de suscripción está adaptado para recibir una petición de conmutación a la segunda suscripción, como una suscripción a ser activada.

El gestor de suscripción está preferiblemente preparado para analizar si todos los datos necesarios procedentes de una entidad externa son correctos.

Para llevar a cabo dicho análisis de datos, el gestor de suscripción verifica preferentemente:

- la longitud de los datos;
- si la suscripción (identificada) a ser activada, como un conjunto de datos de suscripción, se almacena eficazmente dentro del chip 14. Si la suscripción a ser activada no está incluida, entonces el gestor de suscripción puede solicitar a una entidad externa, como el servidor 18, que cargue el correspondiente conjunto de datos de suscripción que faltan. Entonces, una vez que el conjunto de datos de suscripción en cuestión se almacena de manera efectiva dentro del chip 14, el gestor de suscripción puede lanzar una conmutación a la suscripción a ser activada;
- si hay o faltan uno o varios parámetros para conmutar la suscripción a ser activada; y / o
- otra(s) característica(s) de datos que permite(n) llevar a cabo una conmutación adecuada a la suscripción a ser activada.

Si el análisis de datos falla, entonces el gestor de suscripción puede retornar al remitente de una petición de conmutación de suscripción un mensaje que incluye una alerta para informar de un fallo relativo a una ejecución de la petición de conmutación de suscripción.

Una vez que el análisis de los datos es satisfactorio, el gestor de suscripción utiliza una primera variable relativa a una siguiente suscripción activa.

Según una característica esencial invención, el gestor de suscripción está adaptado para establecer la primera variable a la segunda suscripción que se va a activar.

El gestor de suscripción está adaptado para enviar al OS del teléfono 12 un mensaje para solicitar al OS del teléfono 12 que lea los datos. Por lo tanto, el chip 14 obliga al teléfono 12 a obtener datos a actualizar y que incluyen los datos relativos a la segunda suscripción después de una conmutación de suscripción interna.

El gestor de suscripción está adaptado para, por una parte, desactivar, sobre la base del primer valor variable, la primera suscripción y, por otra parte, activar, sobre la base del primer valor variable, la segunda suscripción.

Por lo tanto, el gestor de suscripción cambia todos los datos relativos a una suscripción que se va a activar, a fin de activar la segunda suscripción. Dicho cambio se aplica a cada Archivo Elemental (o EF) que gestiona los datos relativos a una suscripción que ha de ser activada.

Una vez la conmutación de suscripción interna se lleva a cabo, el gestor de suscripción está adaptado además para suministrar, preferiblemente después de una petición del teléfono a través de un reinicio o restablecimiento del chip, al OS del teléfono 12 los datos relativos a la segunda suscripción, como una suscripción activa en curso.

De este modo, el teléfono 12 actualiza su memoria que almacena los datos relativos a la suscripción activa en curso, mientras que los sustituye por los datos proporcionados relativos a la segunda suscripción. Una memoria, como una memoria volátil, tal como una memoria caché, del teléfono 12 almacena los datos relativos a la segunda suscripción. El teléfono 12 y el chip 14 guardan tanto el primero como el mismo segundo conjunto de datos relativos a la segunda suscripción, como la suscripción activa en curso. No existe una posible discrepancia entre el teléfono 12 y el chip 14, en cuanto a la suscripción activa en curso. El teléfono 12 es informado de la última suscripción activada a fin de tener en cuenta un correspondiente contenido, concretamente todos los datos que permiten el acceso, en lugar de la primera red de radiocomunicación móvil 161, la segunda red de radiocomunicación móvil 162 en cuestión.

Una vez que se realiza la conmutación de suscripción, el gestor de suscripción puede fijar la primera variable, por ejemplo, a cero, como un valor predeterminado por defecto y un estado no definido.

Opcionalmente, una vez la conmutación de suscripción se lleva a cabo, el gestor de suscripción también utiliza una segunda variable en relación con una suscripción activa en curso. El gestor de suscripción fija la segunda variable a la segunda suscripción a activar.

El microprocesador 142 ejecuta, de manera preferida, una o varias funciones de seguridad.

Las funciones de seguridad incluyen, preferiblemente, un proceso de autenticación de usuario para ser utilizado antes de continuar para acceder a la memoria 144. Para autenticar al usuario, el usuario tiene que proporcionar un PIN o datos biométricos, como datos de referencia del usuario, que se almacenan de forma segura dentro de la memoria 144. Como datos biométricos, se pueden incluir una o varias huellas dactilares, una o varias copias del iris, una o varias impresiones de voz relativos a uno o varios usuarios autorizados.

Las redes de radiocomunicación móvil 16 está(n) conectada(s), a través de un enlace por cable bidireccional 17, al

servidor 18, como una plataforma OTA y servidor back-end.

El servidor 18 es identificado por un URI, como una URL o una dirección de IP, como identificador de servidor.

5 El identificador de servidor puede ser almacenado dentro de la memoria del chip 144 o una memoria del teléfono.

El servidor 18 puede ser operado por un operador de red de radiocomunicación móvil, como un MNO o un Operador de Red Móvil Virtual (o MVNO), un proveedor de servicios o en su nombre.

10 El servidor 18 está alojado en una computadora.

El servidor 18 está dedicado a la ejecución de una aplicación para la gestión de una base de datos y la comunicación de cierta información de la base de datos al exterior.

15 Alternativamente, otro servidor (no representado) que está conectado al servidor 18 gestiona la base de datos.

El servidor 18 incluye preferiblemente una memoria 182 que almacena la base de datos.

20 En lugar de una memoria interna, el servidor 18 está conectado a una memoria externa (no representada) que almacena la base de datos.

La base de datos contiene un conjunto de uno o varios identificadores relativos, cada uno, a un cliente individual, que está, cada uno, asociado a una conmutación de suscripción solicitada finalmente a una suscripción a ser activada.

25 En aras de la simplicidad, la base de datos representada registra los datos relativos a un solo cliente, el chip 14 (no representado), que está asociado con una conmutación solicitada finalmente a la segunda suscripción "conmutación a suscripción 2".

30 La Figura 2 representa una realización ejemplar de un flujo de mensaje 20 que involucra al teléfono 12, el chip 14 y el servidor 18. Un intercambio de mensajes entre el teléfono 12 y el chip 14 ocasiona una configuración del teléfono 12.

35 En el ejemplo explicado, se supone que el teléfono 12 está acoplado al chip 14, como un tercer dispositivo, que almacena un primer conjunto de datos relativos a una primera suscripción "suscripción 1" a ser desactivada y un segundo conjunto de datos relativos a un segundo suscripción "suscripción 2" a ser activada.

40 Se supone que sólo una suscripción se encuentra activa en un momento dado y que la primera suscripción "suscripción 1" está activa en el chip 14 y en el teléfono 12 antes de una conmutación de suscripción.

Se representa esquemáticamente el dominio seguro relativo a la suscripción que está activa en un momento dado durante un primer periodo de tiempo 21.

45 Ventajosamente, el servidor 18 u otra entidad conectada al teléfono 12 y referente a la primera red de radiocomunicación móvil 161 autentica correctamente el chip 14 mediante el uso de la primera clave Ki1 de autenticación y el primer suscriptor IMSI1 asociado.

50 El servidor 18 envía a un gestor de suscripción apoyado por el chip 14 un mensaje 22, como el llamado "SMS-punto a punto (o PP) tipo de sobre", incluyendo un comando de "SET Status", como una petición de conmutación a una suscripción (a ser identificada), que se acompaña de uno o varios identificadores relativos a la segunda suscripción a ser activada, como la AID 2 y/o IMSI 2.

El servidor 18 por lo tanto solicita al chip 14 conmutar internamente a la segunda suscripción.

55 El chip 14, más exactamente el gestor de suscripción, analiza preferiblemente los datos incluidos en el mensaje recibido y verifica que todos los datos originados desde el servidor 18, a saber, por ejemplo, la existencia de una suscripción a conmutarse internamente, son correctos.

60 Opcionalmente, el chip 14 envía de vuelta al servidor 18 un mensaje de tipo SMS 24 incluyendo un "Acuse de Recibo" (o POR), como un acuse de recibo de la petición de conmutación a una suscripción identificada, como una suscripción a ser activada. El acuse de recibo de la petición de conmutación a una suscripción identificada puede ir acompañado además del resultado de un análisis de datos, como un estado de ejecución referente al éxito o fracaso del análisis de datos.

65 En lugar del intercambio de datos mediante el uso de un mensaje de tipo SMS, el servidor 18 y el chip 14 pueden intercambiar datos utilizando un protocolo de tipo Protocolo de Transferencia de Hipertexto (o HTTP) o protocolo de

tipo Protocolo de Transferencia de Hipertexto Seguro (o HTTPS).

El gestor de suscripción incluye una primera variable 23 relativa a la siguiente suscripción activa.

5 Según la invención, el gestor de suscripción fija la primera variable 23 a la segunda suscripción "suscripción 2" que se identifica por su correspondiente SDSI, concretamente "SDSI2".

10 Una vez que la primera variable se actualiza después de recibir una petición de conmutación a la segunda suscripción a ser activada, el gestor de suscripción envía al OS del teléfono 12 los datos 26, como un "comando de tipo 91XX" y STK, como un mensaje para solicitar al OS del teléfono 12 que lea los datos. El comando tipo STK "91XX" significa que el chip 14 tiene parte de datos disponible para el teléfono 12 con una longitud igual a "XX" en hexadecimales.

15 Cuando el teléfono 12 ha recibido e interpretado los datos 26 enviados por el chip 14, el teléfono 12 envía al chip 14 un comando 28, como un "FETCH", como un comando de tipo STK, para recibir datos.

20 Una vez que el chip 14 recibe del teléfono 12 el comando para recibir datos, el gestor de suscripción envía (a través del OS del chip) al OS del teléfono 12 un comando de Actualización en un modo de restablecimiento UICC, como un comando tipo STK y un mensaje 210 para solicitar al OS del teléfono 12 que vuelva a poner en marcha una ejecución del gestor de suscripción y leer los datos.

Hasta que al chip 14 no se reinicie, la primera suscripción permanece activa a nivel del chip 14.

25 El teléfono 12 envía al gestor de suscripción un mensaje 212 que incluye una orden de reinicio. Dicha orden de reinicio permite el relanzamiento de una ejecución del gestor de suscripción y leer todos los archivos almacenados en la memoria del chip 144.

Opcionalmente, el gestor de suscripción solicita que el usuario del teléfono se autentifique.

30 Para autenticarse, el usuario tiene que proporcionar un PIN o datos biométricos, como datos de referencia del usuario, que están almacenados de forma segura dentro de la memoria 144. De lo contrario, el gestor de suscripción no se relanza.

35 Una vez que el teléfono 12 reinicia el chip 14 y después de una preferible autenticación de usuario exitosa, el gestor de suscripción es relanzado.

40 El gestor de suscripción lee el primer valor variable. Si el primer valor variable es definido como la siguiente suscripción activa, entonces el gestor de suscripción tiene una operación de conmutación de suscripción que llevar a cabo.

45 El gestor de suscripción desactiva, con base al primer valor variable, la primera suscripción. Para desactivar una(s) suscripción(es), el gestor de suscripción compara el primer valor variable con cada uno de la suscripción que está presente dentro del chip 14 y, si la suscripción no coincide con la segunda suscripción, entonces el gestor de suscripción deshabilita la suscripción en cuestión.

Hasta la desactivación de la primera suscripción, la primera suscripción se encuentra activa y el correspondiente primer dominio seguro "SDSI1" 145 está activo durante el primer periodo de tiempo 21.

50 Justo después de esta desactivación de la primera suscripción, no hay, de manera temporal, ninguna suscripción que está activa.

55 Entonces, el gestor de suscripción activa, basándose en el primer valor variable, la segunda suscripción. Para activar una suscripción, el gestor de suscripción compara el primer valor variable con cada uno de la suscripción que está presente dentro del chip 14 y, si la suscripción no coincide con la segunda de suscripción, entonces el gestor de suscripción habilita la suscripción en cuestión. Si la suscripción activa anterior no es la suscripción habilitada, entonces el gestor de la suscripción cambia la suscripción habilitada.

60 En el momento 213 de la activación de la segunda suscripción, la segunda suscripción se encuentra activa y el correspondiente segundo dominio seguro "SDSI2" 147 está activo durante un segundo periodo de tiempo 211. El segundo periodo de tiempo 211 es válido hasta la siguiente conmutación de suscripción.

Opcionalmente, el gestor de suscripción fija la primera variable a, por ejemplo, cero, como un estado no definido.

65 Una vez que la segunda suscripción está activa, el gestor de suscripción envía al OS del teléfono 12 una Respuesta a Reinicio acompañada de datos 214 relativos a la segunda suscripción, como una suscripción activa en curso.

Hasta la transmisión, al teléfono 12, de los datos 214 referentes a la segunda suscripción, el teléfono 12 no almacena en su memoria, al menos de manera temporal, como una memoria caché, la segunda suscripción.

5 Una vez recibida la segunda suscripción, el OS del teléfono 12 actualiza su memoria, al menos de manera temporal, mientras se duplica el segundo conjunto de datos relativos a la segunda suscripción.

10 Una vez suministrado por el gestor de suscripción, el teléfono 12 almacena los datos relativos a la segunda suscripción que constituye una copia de los datos relativos a la suscripción a la que el gestor de suscripción ha conmutado.

Así, la configuración del teléfono 12 permite acceder, después de una conmutación de suscripción dentro del chip 14, a un segundo conjunto de datos relativos a una segunda suscripción para estar también activa por la parte del teléfono 12.

15 El servidor 18 u otra entidad conectada al teléfono 12 y relativa a la segunda red de radiocomunicación móvil 162 autentifica satisfactoriamente el chip 14 mediante el uso de la segunda clave Ki2 de autenticación de red que está asociada con el segundo suscriptor IMSI2.

20 La solución de la invención permite cambiar a nivel de terminal, después de una conmutación de suscripción a nivel de gestor de suscripción, la suscripción activa sin necesidad de involucrar al usuario de teléfono, excepto para la aportación de los datos de autenticación de usuario, cuando sea aplicable.

25 La solución de la invención es transparente para el usuario, al margen de una posible operación de autenticación de usuario.

La solución de la invención puede ser segura mientras se autentica el equipo terminal del usuario y/o se intercambian datos de manera confidencial.

30 La forma de realización que se acaba de describir no pretende limitar el alcance de la invención en cuestión. Otras realizaciones pueden darse. Como otro ejemplo de realización, en lugar de intercambiar con un servidor remoto, el gestor de suscripción intercambia, en un enlace con contacto o sin contacto, con una entidad local, como otro terminal.

REIVINDICACIONES

1. Un método (20) para acceder a un servicio,
 5 incluyendo un primer dispositivo (12) que comprende un chip, comprendiendo el chip medios de almacenamiento de datos, los medios de almacenamiento de datos almacenando al menos dos suscripciones, encontrándose activa una primera de suscripción, al menos una segunda suscripción estando no activa, los medios de almacenamiento de datos almacenando un gestor de suscripción, comprendiendo el método los pasos siguientes:
 10 - el gestor de suscripción recibe una petición (22) de conmutación a la segunda suscripción, como una suscripción a ser activada;
 - el gestor de suscripción incluye una primera variable (23) relativa a la siguiente suscripción activa, el gestor de suscripción fija la primera variable a la segunda de suscripción;
 15 - el gestor de suscripción envía al sistema operativo del primer dispositivo un mensaje (210) para solicitar al sistema operativo del primer dispositivo que vuelva a poner en marcha una ejecución del gestor de suscripción y lea los datos;
 - el sistema operativo del primer dispositivo envía al gestor de suscripción un mensaje (212) que incluye un comando para relanzar una ejecución del gestor de suscripción;
 20 - el gestor de suscripción desactiva, con base al primer valor variable, la primera suscripción;
 - el gestor de suscripción activa, con base al primer valor variable, la segunda suscripción; y
 - el gestor de suscripción envía al sistema operativo del primer dispositivo (214) los datos relativos a la segunda suscripción, como suscripción activa en curso.
2. Método según la reivindicación 1, en el que, antes de enviar al sistema operativo del primer dispositivo los datos relativos a la segunda suscripción, el gestor de suscripción fija la primera variable a un estado no definido.
3. Método según la reivindicación 1 o 2, en el que el gestor de suscripción intercambia datos mediante el uso de un protocolo de tipo HTTP o HTTPS.
4. Método según la reivindicación 1 o 2, en el que la petición de conmutación a la segunda suscripción incluye un comando (22) "SET Status" acompañado de al menos un identificador relativo a la segunda suscripción a ser activada.
5. Método de acuerdo con cualquier reivindicación anterior, en el que el sistema operativo del primer dispositivo y el gestor de suscripción intercambian datos mediante el uso de comandos de tipo SIM Toolkit.
6. Método según la reivindicación 5, en donde el mensaje para solicitar al sistema operativo del primer dispositivo el relanzamiento de una ejecución del gestor de suscripción y la lectura de datos incluye un comando de Actualización (210) en un modo de reinicio UICC.
7. Método según la reivindicación 5 o 6, en el que el gestor de suscripción envía al sistema operativo del primer dispositivo una Respuesta a Reinicio (214) acompañada de los datos relativos a la segunda suscripción, como la suscripción activa en curso.
8. Un primer dispositivo (12) para acceder a un servicio,
 50 comprendiendo el primer dispositivo un chip (14), dicho chip comprende medios de almacenamiento de datos (114), almacenando los medios de almacenamiento de datos un gestor de suscripción, los medios de almacenamiento de datos almacenando al menos dos suscripciones, encontrándose activa una primera suscripción, al menos una segunda suscripción no estando activa, siendo capaz el gestor de suscripción de recibir una petición (22) para la conmutación a la segunda suscripción, como una suscripción a ser activada; incluyendo el gestor de suscripción una primera variable (23) relativa a la siguiente suscripción activa, estando configurado el gestor de suscripción para:
 55 - fijar la primera variable a la segunda suscripción;
 - enviar al sistema operativo del primer dispositivo un mensaje (210) para solicitar al sistema operativo del primer dispositivo que relance una ejecución del gestor de suscripción y lea los datos;
 - recibir un mensaje (212) que incluye un comando para el relanzamiento de una ejecución del gestor de suscripción;
 60 - desactivar, con base al primer valor variable, la primera suscripción;
 - activar, con base al primer valor variable, la segunda suscripción; y
 - enviar al sistema operativo del primer dispositivo (214) los datos relativos a la segunda suscripción, como una suscripción activa en curso.
9. Dispositivo primero según la reivindicación 8, en el que el chip está fijado al primer dispositivo.

10. Primer dispositivo según la reivindicación 8, en el que el chip es extraíble del primer dispositivo.
11. Primer dispositivo según cualquiera de las reivindicaciones 8 a 10, en el que el primer dispositivo incluye un terminal.
12. Primer dispositivo según cualquiera de las reivindicaciones 8 a 11, en el que el gestor de suscripción recibe de un segundo dispositivo la petición de conmutación a la segunda suscripción.
13. Primer dispositivo según la reivindicación 12, en el que el segundo dispositivo incluye un servidor remoto.
14. Primer dispositivo según la reivindicación 12, en el que el segundo dispositivo incluye un dispositivo local.
15. Primer dispositivo según la reivindicación 14, en el que el dispositivo local incluye un terminal.

5

10

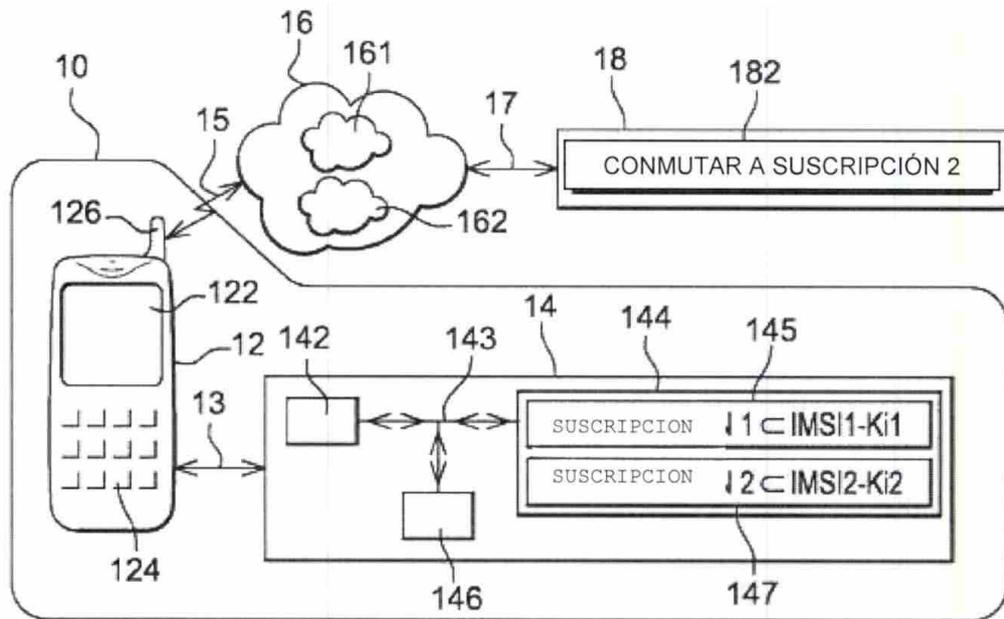


Fig. 1

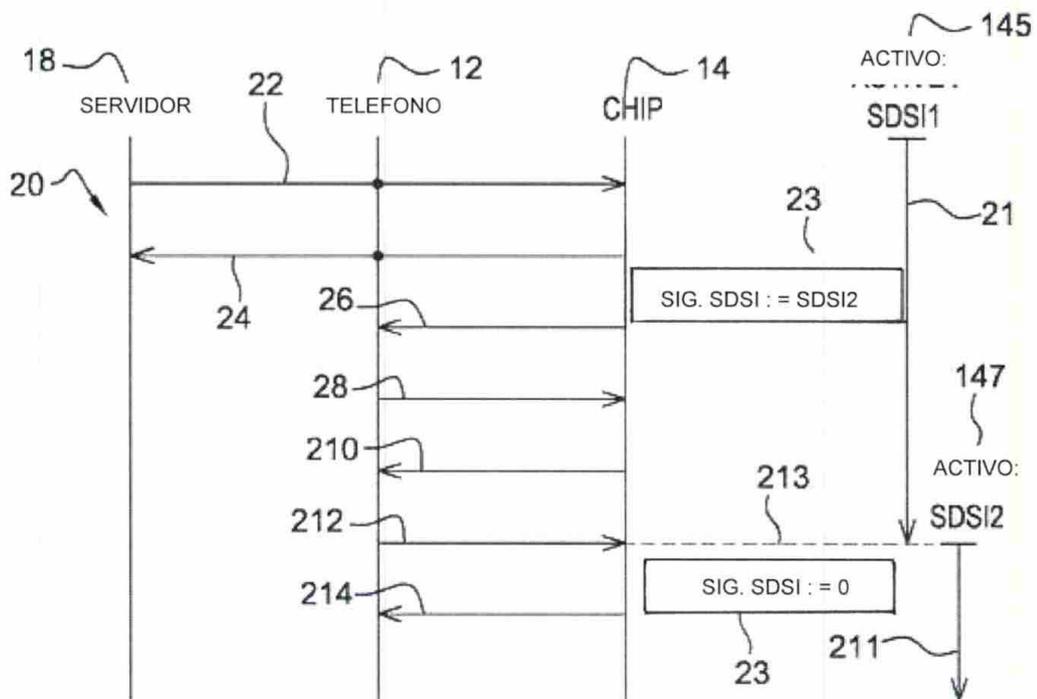


Fig. 2