(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 297 917**

(51) Int. Cl.:
H04Q 7/22 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **99460062 .5**
(86) Fecha de presentación : **19.10.1999**
(87) Número de publicación de la solicitud: **0996300**
(87) Fecha de publicación de la solicitud: **26.04.2000**

(54) Título: **Procedimiento de acceso a un módulo de servicios a partir de una estación móvil, módulo de identificación de abonado y terminal correspondientes.**

(30) Prioridad: **22.10.1998 FR 98 13455**
04.11.1998 FR 98 14044

(45) Fecha de publicación de la mención BOPI:
01.05.2008

(45) Fecha de la publicación del folleto de la patente:
01.05.2008

(73) Titular/es:
Société Française du Radiotéléphone-SFR
42, avenue de Friedland
75008 Paris, FR

(72) Inventor/es: **Beaudou, Patrice**

(74) Agente: **Elzaburu Márquez, Alberto**

DESCRIPCIÓN

Procedimiento de acceso a un módulo de servicios a partir de una estación móvil, módulo de identificación de abonado y terminal correspondientes.

El ámbito de la invención es el de los sistemas de radiocomunicación con los móviles.

Más precisamente, la invención se refiere al acceso a un módulo de servicios a partir de una estación móvil de un sistema de radiocomunicación.

La estación móvil que permite la puesta en práctica de la presente invención puede estar comprendida, especial pero no exclusivamente, en un sistema de radiocomunicación de tipo GSM (de *"Global System for Mobile Communications"* "Sistema Global para Comunicaciones Móviles", en inglés), DCS 1800 (de *"Digital Cellular System 1800"*, "Sistema Celular Digital", en inglés), PCS 1900 (de *"Personal Communication System"*, "Sistema Personal de Comunicación", en inglés), DECT (de *"Digital European Cordless Telecommunications"*, "Sistema Digital Inalámbrico Europeo", en inglés), o incluso UMTS (de *"Universal Móvil Telecommunication System"*, "Sistema Universal de Telecomunicación Móvil", en inglés).

De manera clásica, una estación móvil incluye un terminal (o ME, de *"Mobile Equipment"*, "Equipo Móvil", en inglés, según la terminología de GSM) que coopera con un módulo de identificación de abonado (o SIM, de *"Subscriber Identity Module"*, en inglés, según la terminología GSM, o incluso DAM, de *"DECT Authentication Mobile"*, "Móvil de autentificación de DECT" según la terminología DECT). Se tendrá en cuenta que, según los sistemas, la estación móvil a veces se llama también radioteléfono móvil o teléfono portátil.

Por otra parte, la presente invención se aplica a todo tipo de estación móvil, y, en particular, que emita y/o reciba voz y/o datos. En el caso de una emisión/recepción de datos, se puede conectar el terminal a un microordenador (preferiblemente portátil), que procesa los datos emitidos/recibidos.

La invención no se limita al acceso a un tipo de módulo de servicios particular. Se aplica por tanto, en particular, a los dos tipos de módulos de servicios, conocidos en sí mismos, cuyas características se recuerdan aquí brevemente a continuación.

Un primer tipo de módulo de servicios ofrece al menos un servicio de acceso a una red informática de tipo Internet. Este primer tipo de módulo de servicios, generalmente llamado "plataforma de acceso", permite al usuario navegar en el seno de la red informática de tipo Internet, es decir, acceder a otros servidores presentes en esta red informática de tipo Internet. Estos otros servidores, generalmente llamados "servidores de Internet", dan soporte a unos "sitios Web" y ofrecen cada uno al menos un servicio de pago (gestión de una cuenta bancaria, transacciones, ...) y/o de reserva (billetes de tren, avión, entradas de espectáculos, ...) y/o de consulta (meteorología, horarios, ...).

Un segundo tipo de módulo de servicios ofrece al menos un servicio de pago y/o de reserva y/o de consulta. Este segundo tipo de módulo de servicios presenta una oferta de servicios de la misma naturaleza que los servidores de Internet antes citados, pero se distingue de estos últimos en que es accesible directamente y no mediante una plataforma de acceso. En otros términos, el segundo tipo de módulo de servicios no es un servidor de Internet, y no es por tanto accesible a través de la red informática de tipo Internet.

En la presente descripción, se entiende por red informática de tipo Internet no sólo la red mundial bautizada como "Internet" (que es una red que interconecta numerosísimas máquinas y actualmente se encuentra en muy fuerte expansión), sino también todo tipo de red informática y/o de telecomunicación que aplica la tecnología Internet. Se recuerda, en efecto, que la red de Internet (la red mundial), no es el único tipo de red de telecomunicación que aplica la tecnología Internet. En particular, una organización puede perfectamente desplegar su propia red, generalmente llamada "red Intranet", en base a la tecnología Internet sin por ello estar conectada a la red de Internet (la red mundial). Por supuesto, si esta organización desea a continuación conectarse a la misma, se le facilitará la tarea, puesto que utiliza la misma tecnología. La tecnología de Internet, también llamada tecnología TCP/IP, se basa en la utilización de los protocolos TCP/IP que se definen como una serie de protocolos destinados no sólo a interconectar ordenadores unidos por una misma red física, sino también a interconectar estas distintas redes físicas entre sí para constituir una única red lógica.

De manera conocida, después de que se haya establecido una comunicación con un módulo de servicios, el terminal de una estación móvil ejecuta una aplicación específica que le permite beneficiarse del (de los) servicio(s) ofrecido(s) por este módulo de servicios. En la continuación de la descripción, esta aplicación específica, realizada por el terminal, se denomina "aplicación de servicios".

El documento WO 97/04609 A divulga un procedimiento de acceso a un módulo de servicios de pago a partir de una estación móvil comprendida en un sistema de radiocomunicación. La estación móvil comprende un terminal que coopera con un módulo de identificación de abonado. El terminal puede ejecutar una aplicación de servicios de manera que se beneficie de los servicios de pago ofrecidos por el servidor después de que se haya establecido una comunicación entre el terminal y el módulo de servicios.

El mecanismo de lanzamiento de esta aplicación específica por el terminal presenta varios inconvenientes. Estos inconvenientes se presentan a continuación en el caso del primer tipo de módulo de servicios antes citado (y denominado "plataforma de acceso"). Sin embargo, está claro que estos inconvenientes existen también en el caso del segundo tipo de módulo de servicios antes citado.

Así pues, ya es posible hoy, con algunas estaciones móviles, acceder a una red informática de tipo Internet. Para eso, el terminal debe incluir una tecla específica ("tecla de acceso a Internet") y la aplicación de servicios específica en este caso se denomina "navegador" (o "*browser*" en inglés). El navegador, que utiliza un lenguaje específico, permite al terminal navegar en la red informática de tipo Internet, en cuanto se haya establecido una comunicación entre el terminal y una plataforma de acceso a la red informática de tipo Internet.

Con este tipo de terminal, el procedimiento de acceso, por ejemplo a la red mundial Internet, es el siguiente: después de que el usuario haya apretado la "tecla de acceso a Internet", el terminal intenta establecer una comunicación con una plataforma de acceso; si esta comunicación se establece efectivamente, el terminal lanza el navegador, de modo que el terminal pueda navegar en el seno de la red de Internet.

Sin embargo, resulta que esta solución actual no es satisfactoria, debido a que, en la estación móvil, solamente se implica el terminal (es él el que está provisto de la "tecla de acceso a Internet", el que intenta establecer la comunicación con la plataforma de acceso, y el que lanza el navegador).

Esto implica, en efecto, que el usuario no es enteramente libre en la elección de su terminal puesto que debe imperativamente elegir un terminal provisto de la "tecla de acceso a Internet".

Esto implica por otra parte que, cualquiera que sea el operador al cual se abonó, el usuario se ve obligado acceder a la red informática de tipo de Internet según elecciones técnicas efectuadas por el fabricante de su terminal. Especialmente, el usuario no elige el número de la plataforma de acceso, ni las informaciones útiles para el navegador una vez que haya sido lanzado, como por ejemplo números de tipo IP (de *"Internet Protocol",* "Protocolo de Internet", en inglés), claves secretas de autentificación del navegador y/o de encriptación de datos, números de centro de servicio de mensajes cortos (o "*SMS Center*", Centro de SMS, en inglés),....

La invención tiene por objetivo, en particular, paliar estos distintos inconvenientes del estado de la técnica.

Más precisamente, uno de los objetivos de la presente invención es proporcionar un procedimiento que permita a un usuario acceder a un módulo de servicios a partir de una estación móvil cualquiera (en el sentido que esta última no esté provista necesariamente de una "tecla de acceso a Internet" como la antes citada).

La invención tiene igualmente por objetivo ofrecer una funcionalidad suplementaria (es decir, el acceso a un módulo de servicios) en el seno de una "aplicación de operador" (o "aplicación de SIM", o incluso "menú de operador") almacenada por el módulo de identificación de abonado y ejecutada por éste.

Se sabe, en efecto, que mediante el módulo de identificación de abonado que distribuyen y que les son específicos, los distintos operadores proponen a sus abonados unos "menús de operador" distintos. Cada operador intenta, por supuesto, incorporar un máximo de funcionalidades en el seno de su menú de operador, y para eso pretende elaborar nuevas funcionalidades. Según el conocimiento del inventor, ninguno de los "menús de operador" existentes ofrece la funcionalidad de "acceso a un módulo de servicios" (como por ejemplo "acceso a Internet"), que es precisamente el objeto de la presente invención.

Otro objetivo de la invención consiste en proporcionar un procedimiento tal que permita al usuario acceder al módulo de servicios según unas elecciones técnicas efectuadas por su operador (y no por el fabricante de su terminal).

Un objetivo complementario de la invención consiste en proporcionar un procedimiento de este tipo que sea simple de poner en práctica y poco costoso.

Estos diferentes objetivos, así como otros que aparecerán más adelante, se alcanzan según la invención con ayuda de un procedimiento de acceso a un módulo de servicios a partir de una estación móvil comprendida en un sistema de radiocomunicación, comprendiendo dicha estación móvil un terminal que coopera con un módulo de identificación de abonado, pudiendo ejecutar dicho terminal una aplicación de servicios de manera que se beneficie del (de los) servicio(s) ofrecido(s) por dicho módulo de servicios después de que se haya establecido una comunicación entre dicho terminal y dicho módulo de servicios,

comprendiendo dicho procedimiento las etapas siguientes:

- el módulo de identificación de abonado envía al terminal, para que el terminal la ejecute, una orden de establecimiento de una comunicación entre el terminal y un primer módulo de servicios, estando dicha orden referida a unos parámetros correspondientes a un primer juego de parámetro(s) que comprende un primer número de teléfono de dicho primer módulo de servicios y, eventualmente, al menos un primer parámetro de llamada;

- el terminal compara dicho primer juego de parámetro(s) con una lista predeterminada de juego(s) de parámetro(s), que comprende al menos un juego de parámetro(s);

- si dicho primer juego de parámetro(s) forma parte de dicha lista, el terminal ejecuta dicha orden e intenta establecer una comunicación con dicho primer módulo de servicios, según dicho primer juego de parámetro(s);

- si se establece efectivamente dicha comunicación con dicho primer servidor, el terminal lanza la ejecución de dicha aplicación de servicios, de modo que dicho terminal pueda beneficiarse del (de los) servicio(s) ofrecido(s) por dicho primer módulo de servicios.

Es pues el módulo de identificación de abonado (y no el terminal) el que "lanza" el procedimiento de acceso al módulo de servicios, gracias al envío por este módulo de identificación de abonado de la orden que solicita al terminal establecer una comunicación con el primer módulo de servicios. Por consiguiente, para poder ser aplicado, el procedimiento de la invención no impone de ninguna manera que el terminal esté provisto de una "tecla de acceso a un módulo de servicios". Se recuerda que, por el contrario, con la solución conocida antes citada, el terminal debe estar provisto imperativamente de tal tecla, puesto que en este caso, es el terminal el que "lanza" el procedimiento de acceso.

Está claro que la invención no contempla proteger una orden que permita al módulo de identificación de abonado pedir al terminal que establezca una comunicación. En efecto, ya resulta conocida en sí misma una orden de este tipo. En cambio, la presente invención tiene por objeto proteger el concepto general de utilizar tal orden "para lanzar" a partir de un módulo de identificación de abonado un procedimiento de acceso a un módulo de servicios. Para eso, la orden es referida a unos parámetros como el número de teléfono de un módulo de servicios y, eventualmente, a uno o más parámetros de llamada. Esto no se había contemplado nunca anteriormente. En efecto, los prejuicios del experto en la técnica oficio le han incitado siempre a pensar que es el terminal el que debe "lanzar" el acceso a Internet, debido a que la aplicación de servicios se encuentra en el terminal y es ejecutada por éste.

En combinación con esta orden "de lanzamiento", la invención prevé un mecanismo que permite al terminal saber cuándo debe "tomar la iniciativa" y lanzar su aplicación de servicios. Este mecanismo consiste en que el terminal verifique, por una parte (por comparación), que el número de teléfono correspondiente al parámetro de la orden es efectivamente un número de módulo de servicios y, por otra parte, que se ha establecido bien la comunicación con el módulo de servicios.

Desde el momento en que lanzó su aplicación de servicios, el terminal puede comunicar con el módulo de servicios y beneficiarse del o de los servicios ofrecidos por éste último, según un funcionamiento totalmente clásico que por tanto no se describirá aquí con más detalle.

Preferentemente, cada juego de parámetro(s) distinto que permite adaptar dicha orden de establecimiento de una comunicación comprende al menos:

- un número de teléfono de un módulo de servicios;

- un parámetro de llamada que define un modo de comunicación.

En un primer modo de realización preferente de la invención, dicho módulo de servicios, denominado plataforma de acceso, ofrece al menos un servicio de acceso a una red informática de tipo Internet,

siendo dicha aplicación de servicios ejecutada por el terminal un navegador que permite navegar al terminal en el seno de dicha red informática de tipo Internet, después de que se estableció efectivamente dicha comunicación entre el terminal y dicha plataforma de acceso.

Así pues, la presente invención se aplica al primer tipo de módulo de servicios anteriormente citado, llamado generalmente "plataforma de acceso".

Ventajosamente, dicho navegador utiliza un lenguaje específico del tipo "WAP/HDML".

Preferiblemente, al menos una información, útil al navegador después de que haya sido lanzado, está igualmente almacenada en dicho módulo de identificación de abonado.

De esta forma, el usuario accede a la red informática de tipo Internet según unas elecciones técnicas efectuadas por su operador (y no por el fabricante de su terminal). En otros términos, la forma en que el usuario accede a la red informática de tipo Internet ya no es (o casi ya no es) dependiente del terminal con el cual coopera su módulo de identificación de abonado.

De manera ventajosa, dicha al menos una información, útil para el navegador después de que haya sido lanzado, pertenece al grupo que comprende: números de tipo IP, claves secretas de autentificación del navegador y/o de encriptación de datos, identificadores de usuarios ante las plataformas de acceso y números de centro de servicio de mensajes cortos.

Se tiene por ejemplo dos números de tipo IP, que son las "direcciones de Internet" de máquinas cuya utilización se reserva al operador (siendo una de las dos máquinas una máquina de emergencia).

En un segundo modo de realización preferente de la invención, dicho módulo de servicios ofrece al menos un servicio de pago y/o de reserva y/o de consulta,

siendo dicha aplicación de servicios ejecutada por el terminal una aplicación de pago y/o de reserva y/o de consulta, que permite al terminal beneficiarse de dicho al menos un servicio de pago y/o de reserva y/o de consulta (por ejemplo de servidores) ofrecido por dicho módulo de servicios, después de que se haya establecido efectivamente dicha comunicación entre el terminal y dicho módulo de servicios.

Así pues, la presente invención se aplica al segundo tipo de módulo de servicios anteriormente citado.

De manera ventajosa, dicho módulo de identificación de abonado almacena al menos una "aplicación de operador" cuya ejecución permite ofrecer al menos una funcionalidad a un usuario de dicha estación móvil,

correspondiendo dicha etapa de envío por el módulo de identificación de abonado, al terminal, de una orden de establecimiento de una comunicación entre el terminal y el primer módulo de servicios a una funcionalidad suplementaria, cuya elección se ofrece al usuario durante la ejecución por el módulo de identificación de abonado de dicha aplicación de operador.

En otros términos, gracias al procedimiento según la invención, el "menú de operador" puede ofrecer la funcionalidad "acceso a un módulo de servicios". Se recuerda que hasta ahora, esta funcionalidad era accesible solamente mediante una "tecla de acceso a un módulo de servicios" de la cual debía estar provisto el terminal.

Preferentemente, dicho sistema de radiocomunicación al cual pertenece dicha estación móvil corresponde al grupo que comprende: los sistemas de radiocomunicación de tipo GSM, los sistemas de radiocomunicación de tipo DCS 1800, los sistemas de radiocomunicación de tipo PCS 1900, los sistemas de radiocomunicación de tipo UMTS y los sistemas de radiocomunicación de tipo DECT. Está claro que esta lista no es de ninguna manera exhaustiva.

En un modo ventajoso de realización de la invención, dicha orden de establecimiento de una comunicación, enviada por el módulo de identificación de abonado al terminal, es la orden "SET UP CALL" (ESTABLECER LLAMADA) del juego de órdenes del *"SIM Application Toolkit"* (Herramientas de Aplicación del SIM).

Para más precisiones relativas a esta orden "SET UP CALL", se puede hacer referencia a la norma "GSM 11.14 (Fase 2+)" de la ETSI.

De manera preferente, dicha lista predeterminada de juego de parámetro(s) se almacena en dicho módulo de identificación de abonado, comprendiendo cada juego de parámetro(s) un número de teléfono de módulo de servicios y, eventualmente, al menos un parámetro de llamada,

y comprendiendo además dicho procedimiento la etapa siguiente, previa a dicha etapa de comparación:

- el terminal lee dicha lista predeterminada de juego de parámetro(s), almacenada en dicho módulo de identificación de abonado.

De esta forma, el usuario accede a un módulo de servicios (plataforma de acceso u otro) escogido por su operador (y no por el fabricante de su terminal). Además la lista de números de módulo de servicios puede ser modificada o completada a discreción por el operador. En efecto, hoy en día se puede modificar perfectamente a distancia el contenido de un módulo de identificación, por carga a distancia de datos (y esto de manera generalmente transparente para el usuario).

Ventajosamente, dicha etapa de lectura, por el terminal, de dicha lista predeterminada de juego de parámetro(s) se ejecuta durante al menos alguna(s) inicialización(es) de dicho terminal.

En un modo de realización particular de la invención, si las condiciones para que el terminal lance la ejecución de dicha aplicación de servicios no se satisfacen, dicho procedimiento comprende además las etapas complementarias siguientes, que pueden ser eventualmente reiteradas:

- el módulo de identificación de abonado envía al terminal, para que el terminal la ejecute, una nueva orden de establecimiento de una comunicación entre el terminal y dicho primer módulo de servicios o entre el terminal y un segundo módulo de servicios, distinto del primer módulo de servicios, estando referida dicha nueva orden a unos parámetros con un nuevo juego de parámetro(s) distinto de dicho primer juego de parámetro(s);

- el terminal compara dicho nuevo juego de parámetro(s) con dicha lista predeterminada de juego(s) de parámetro(s);

- si el resultado de dicha comparación es positivo, el terminal ejecuta dicha orden e intenta establecer una comunicación con dicho primer o segundo módulo de servicios, según dicho nuevo juego de parámetro(s);

- si se establece efectivamente dicha comunicación con dicho primer o segundo módulo de servicios, el terminal lanza la ejecución de dicha aplicación de servicios, de modo que dicho terminal pueda beneficiarse del (de los) servicio(s) ofrecido(s) por dicho primer o segundo módulo de servicios.

Así pues, se puede efectuar sucesivamente varias tentativas de acceso, con números de módulo de servicios distintos. Se tendrá en cuenta que cada nueva tentativa puede efectuarse:

- bien con el mismo módulo de servicios, pero utilizando un nuevo juego de parámetro. Se supone en este caso que un mismo módulo de servicios se puede llamar de distintas maneras, es decir, con distintos juegos de parámetros. Dos juegos de parámetros son diferentes si comprenden números de teléfono distintos y/o parámetros de llamada distintos (un parámetro de llamada distinto es por ejemplo el modo de transmisión: en uno de los juegos de parámetros puede tratarse de un procedimiento digital y en el otro de un procedimiento analógico);

- o bien con otro módulo de servicios.

Ventajosamente, dicha etapa de envío por el módulo de identificación de abonado, al terminal, de una nueva orden de establecimiento de una comunicación se efectúa automáticamente si, después de una tentativa precedente, no se cumplen las condiciones para que el terminal lance la ejecución de dicha aplicación de servicios.

En este caso, el usuario no tiene que actuar puesto que se efectúa automáticamente cada nueva tentativa de acceso por el módulo de identificación de abonado.

Según una alternativa ventajosa, dicha etapa de envío por el módulo de identificación de abonado, al terminal, de una nueva orden de establecimiento de una comunicación corresponde a una funcionalidad suplementaria, cuya elección se ofrece al usuario en la ejecución por el módulo de identificación de abonado de dicha aplicación de operador.

En otros términos, el usuario puede decidir, para cada tentativa de acceso (e incluso para la primera tentativa), a qué módulo de servicios desea acceder y/o con que juego de parámetro desea que se efectúe esta tentativa de acceso.

Preferentemente, dicha etapa de lanzamiento por el terminal de la ejecución de dicha aplicación de servicios va seguida de una etapa de autentificación de dicho módulo de identificación de abonado por dicho módulo de servicios, que comprende a su vez las siguientes etapas:

- el servidor de servicios envía un número aleatorio, denominado de desafío, al módulo de identificación de abonado, a través del terminal;

- en función de dicho desafío y con ayuda de un algoritmo de autentificación y/o al menos una clave de autentificación contenido(s) en unas zonas protegidas del módulo de identificación de abonado, el módulo de identificación de abonado calcula una primera firma electrónica;

- mediante el terminal, el módulo de identificación de abonado envía dicha primera firma electrónica al módulo de servicios;

- en función de dicho desafío y con la ayuda de dicho algoritmo de autentificación y/o de dicha al menos una clave de autentificación, que conoce también, dicho módulo de servicios calcula una segunda firma electrónica;

- dicho módulo de servicios compara dichas primera y segunda firmas electrónicas, y si son idénticas, autentifica dicho módulo de identificación de abonado.

Esta etapa de autentificación puede calificarse de dinámica debido a que es el módulo de identificación de abonado, y no el terminal, el que calcula la firma electrónica. Es importante tener en cuenta que, de esta forma, es el módulo de identificación de abonado el que es autentificado por el módulo de servicios, y no el terminal. Además esta solución ofrece una buena seguridad ya que, por una parte, la firma electrónica varía en cada nueva autentificación y, por otra parte, el algoritmo de autentificación y/o la clave de autentificación no son legibles por un tercero que esté en posesión del módulo de identificación de abonado (incluso en el interfaz entre el módulo de identificación de abonado y el terminal). Por último, esta etapa de autentificación puede seguir inmediatamente o no a la etapa de lanzamiento por el terminal de la ejecución de la aplicación de servicios.

La invención se refiere también a un Módulo de identificación de abonado, del tipo destinado a cooperar con un terminal para formar una estación móvil comprendida en un sistema de radiocomunicación, pudiendo ejecutar dicho terminal una aplicación de servicios de tal modo que se beneficie del (de los) servicio(s) ofrecido(s) por un módulo de servicios después de que se haya establecido una comunicación entre dicho terminal y dicho módulo de servicios,

comprendiendo dicho módulo de identificación de abonado unos medios de envío al terminal, para que el terminal la ejecute, de una orden de establecimiento de una comunicación entre el terminal y un primer módulo de servicios, estando dicha orden referida a unos parámetros con un primer juego de parámetro(s) que comprende un primer número de teléfono de dicho primer módulo de servicios y, eventualmente, efectuando el terminal las etapas siguientes a la recepción de dicha orden:

- el terminal compara dicho primer juego de parámetro(s) con una lista predeterminada de juego(s) de parámetro(s), que comprende al menos un juego de parámetro(s);

- si dicho primer juego de parámetro(s) forma parte de dicha lista, el terminal ejecuta dicha orden e intenta establecer una comunicación con dicho primer módulo de servicios, según dicho primer juego de parámetro(s);

- si dicha comunicación con dicho primer servidor se establece efectivamente, el terminal lanza la ejecución de dicha aplicación de servicios, de modo que dicho terminal pueda beneficiarse del (de los) servicio(s) ofrecido(s) por dicho primer módulo de servicios.

La invención se refiere también a un terminal del tipo destinado a cooperar con un módulo de identificación de abonado para formar una estación móvil comprendida en un sistema de radiocomunicación, pudiendo ejecutar dicho terminal una aplicación de servicios de manera que se beneficie del (de los) servicio(s) ofrecido(s) por un módulo de servicios después de que se haya establecido una comunicación entre dicho terminal y dicho módulo de servicios,

comprendiendo dicho terminal:

- unos medios de recepción de una orden, procedente del módulo de identificación de abonado y que piden al terminal que establezca una comunicación entre el terminal y un primer módulo de servicios, estando dicha orden referida a parámetros con un primer juego de parámetro(s) que comprende un primer número de teléfono de dicho primer módulo de servicios y, eventualmente, al menos un primer parámetro de llamada;

- unos medios de comparación de dicho primer juego de parámetro(s) con una lista predeterminada de juego (s) de parámetro(s), que comprende al menos un juego de parámetro(s);

- unos medios de ejecución de dicha orden, si dicho primer juego de parámetro(s) forma parte de dicha lista, de manera que intente establecer una comunicación con dicho primer módulo de servicios, según dicho primer juego de parámetro(s);

- unos medios de lanzamiento de la ejecución de dicha aplicación de servicios, si dicha comunicación entre el terminal y dicho primer servidor se establece efectivamente, de modo que dicho terminal pueda beneficiarse del (de los) servicio(s) ofrecido(s) por dicho primer módulo de servicios.

Otras características y ventajas de la invención aparecerán de la lectura de la descripción siguiente de un modo de realización preferente de la invención, que se da a título indicativo y no limitativo, en los cuales:

- la figura 1 presenta un esquema sinóptico global que permite explicar el principio general de un acceso a un módulo de servicios a partir de una estación móvil comprendida en un sistema de radiocomunicación;

- la figura 2 presenta un organigrama simplificado de un modo de realización particular del procedimiento según la invención;

- la figura 3 presenta, de manera parcial, un ejemplo de contenido de la zona de memoria del módulo de identificación de abonado que aparece sobre la figura 1;

- la figura 4 presente con más detalle un modo de realización particular de la etapa de autentificación que aparece sobre la figura 2.

La invención se refiere por tanto a un procedimiento de acceso a un módulo de servicios a partir mi estación móvil comprendida en un sistema de radiocomunicación 1.

Antes de presentar en detalle un modo de realización particular del procedimiento según la invención (en relación con el organigrama de la figura 2), se recuerda el principio general de un acceso a un módulo de servicios a partir de una estación móvil 2 (en relación con el esquema sinóptico de la figura 1).

En la continuación de la descripción, se considera el caso particular de un sistema de radiocomunicación de tipo GSM. Sin embargo, está claro que la presente invención no se limita a este tipo de sistema de radiocomunicación.

En primer lugar, se recuerda, en relación con el esquema sinóptico de la figura 1, la estructura de un sistema de radiocomunicación 1 de tipo GSM. Una pluralidad de estaciones móviles 2 (o MS, de *"Mobile Station"* "Estación Móvil" en inglés, según la terminología GSM) evolucionan en el seno de una red de células geográficas (no representa-

das). Cada célula corresponde a la cobertura de radio de una estación de base 5 (o BTS, de "*Base Transceiver Station*", "Estación Emisora-Receptora", en inglés, según la terminología GSM). La estación móvil 2 comunica, mediante la interfaz aire 8, con la estación de base 5 de la célula donde se encuentra. Las estaciones de base están gestionadas por un controlador de estaciones de base 6 (o BSC, de *"Base Station Controller"*, "Controlador de Estación de Base", en inglés, según la terminología GSM). Varios controladores de estaciones de base 6 pueden ser controlados por un control de conmutación 7 (o MSC. de "*Mobile Service Switching Center*" "Centro de Conmutación de Servicios Móviles", en inglés, según la terminología GSM), que es el elemento principal de una red GSM. La central de conmutación 7 se une a la red telefónica conmutada pública 9 (RTCP). Se tendrá en cuenta que, en aras de la simplificación, sólo se representa en la figura 1 uno de cada tipo de elementos 2, 5, 6 y 7 de la estructura.

La estación móvil 2 comprende un terminal 3 (o ME, de "*Mobile Equipment*", "Equipo Móvil", en inglés, según la terminología GSM) que coopera con un módulo de identificación de abonado 4 (o SIM, de "Subscriber Identity Module", según la terminología GSM). Para más precisiones sobre el terminal 3 y el módulo de identificación de abonado 4, se podrá acudir a las normas "GSM 11.11" y GSM 11.14 (Fase 2+) de la ETSI.

De manera general, y conocida en sí misma, con el fin de poder acceder a un módulo de servicios dado, el terminal debe poder ejecutar una aplicación de servicios, específica a este módulo de servicios dado y que permite al terminal beneficiarse del (o de los) servicio(s) ofrecido(s) por este módulo de servicios dado.

A título de ejemplo, en la figura 1, se supone que existen:

- dos plataformas de acceso 11 (UP1), 12 (UP2), que son dos módulos de servicios particulares que ofrece cada uno un servicio de acceso a una red informática de tipo Internet 10;
- un servidor 13 de pago y/o de reserva y/o de consulta.

En la continuación de la descripción, a título de ejemplo ilustrativo y no restrictivo, se presenta en detalle únicamente el caso de un acceso a una plataforma de acceso 11, 12. Sin embargo, está claro que el mecanismo de acceso descrito a continuación se aplica también al caso de un acceso a cualquier tipo de módulo de servicios, y, en particular, a un servidor que ofrece a uno o varios servicios de pago y/o de reserva y/o de consulta.

Con el fin de acceder a una plataforma de acceso, y a través de ésta, a una red informática de tipo Internet 10, la aplicación de servicios que el terminal 3 debe ejecutar es un navegador 31 ("browser"). Se utiliza por ejemplo el navegador comercializado por la empresa Unwired Planet, bajo el nombre de producto "UP.browser" (marca registrada).

De manera clásica, el navegador 31 utiliza una lenguaje específico y permite al terminal 3 navegar en la red informática de tipo Internet (es decir, conectarse a "sitios Web" con el fin de poder intercambiar con ellos todo tipo de informaciones). Previamente a esta "navegación", el terminal 3 debe haber establecido una comunicación con una plataforma de acceso a esta red informática de tipo Internet 10. Se recuerda que en el ejemplo presentado, están disponibles dos plataformas de acceso 11 (UP1), 12 (UP2). Se trata por ejemplo de plataformas del tipo comercializado por la empresa Unwired Planet, bajo el nombre de producto "UP.link" (marca registrada).

El lenguaje específico utilizado por el navegador 31 es, por ejemplo, el lenguaje "WAP/HDML" (de "Wireless Application Protocol/Handled Device Mark-up Language", "Protocolo de Aplicaciones Inalámbricas/Lenguaje de Señalización de Dispositivo Tratado" en inglés). Para más precisiones relativas a este lenguaje, y más generalmente los conceptos WAP y HDML (marca registrada), se podrá acudir a los documentos siguientes:

- acerca de HDML (se puede consultar estos documentos en el URL: http://www.uplanet.com):
  * "*HDML Specification*" (Especificación de HDML), versión 2.0, 11 de abril de 1997;
  * "*UP.Link (marca registrada) administration guide*", (Guía de administración de UP.Link), versión 3.0, abril de 1998;
- acerca de WAP (se puede consultar estos documentos en el URL: http://www.wapforum.org/):
  * "*WAP Architecture Specification*", ("Especificación de la Arquitectura WAP") WAP Forum, 30 de abril de 1998;
  * *"Wireless Transport Layer Security Specification"*, ("Especificación de Seguridad de la Capa de Transporte Inalámbrico") WAP Foro, 30 de abril de 1998;
  * "*WML Script Language Specification*", ("Especificación de lenguaje de Guión WML") WAP Forum, 9 de abril de 1998;
  * "*WAP Secunty Smart Card*", ("Tarjeta Inteligente de Seguridad WAP") versión borrador O.1 (1998-06).

Generalmente, la aplicación de servicios (ejecutada por el terminal) puede escribirse en un lenguaje cualquiera, tal como, por ejemplo, el lenguaje JAVA (marca registrada).

Según la presente invención, y con el fin de permitir la puesta en práctica del procedimiento describe en detalle más adelante (en relación con la figura 2), el módulo de identificación de abonado 4 y el terminal 3 comprenden unos medios específicos.

Así pues, el módulo de identificación de abonado 4 comprende unos medios 52 de envío al terminal de una orden que pide al terminal establecer una comunicación con un módulo de servicios (por ejemplo una de las plataformas de acceso 11, 12). Esta orden, por ejemplo está referida a parámetros por una parte con el número de teléfono del servidor de servicio (o con uno entre una pluralidad de dichos números), y por otra parte, con el modo de transmisión (por ejemplo modo digital o modo analógico) según el cual se debe establecer la comunicación.

Está claro que un mismo módulo de servicios puede ser accesible de distintas maneras, correspondiendo cada una a un juego de parámetro distinto. En efecto, un mismo módulo de servicios puede poseer varios números de teléfono, o, bajo un mismo número, aceptar distintos procedimientos de transmisión.

Por otra parte, el terminal 3 comprende:

- unos medios 32 de recepción de la orden antes citada procedente del módulo de identificación de abonado 4, estando esta orden referida a unos parámetros con un juego de parámetro dado;

- unos medios 33 de comparación del juego de parámetro que acompaña el orden con una lista predeterminada de juegos de parámetro, de manera que se determine si el juego de parámetros que acompaña a la orden pertenece o no a esta lista;

- unos medios 34 de establecimiento de una comunicación por una parte con el servidor cuyo número de teléfono se precisa como parámetro de la orden, y por otra parte según el modo de transmisión precisado como parámetro de la orden;

- unos medios 35 de lanzamiento de la aplicación de servicios 31, si el resultado de la comparación efectuada por los medios 33 de comparación es positivo y si los medios 34 de establecimiento han establecido efectivamente una comunicación con el módulo de servicios.

En relación con el organigrama de la figura 2, se presenta ahora en detalle un modo de realización particular del procedimiento según la invención.

Como se explica en detalle a continuación, según la invención, la ejecución del procedimiento de acceso se “lanza” por el módulo de identificación de abonado (y no, como en la técnica anterior conocida, por el terminal). Este “lanzamiento” de la ejecución del procedimiento de acceso, por ejemplo, se propone al usuario de la estación móvil en forma de una funcionalidad suplementaria en el seno del “menú de operador”. Se recuerda que el “menú de operador” es la “aplicación de operador” (o la “aplicación de SIM”) ejecutada por el módulo de identificación de abonado y a través de la cual el usuario ve que se le ofrece una pluralidad de funcionalidades consustanciales a su operador.

En este modo de realización particular, se supone, por otra parte, que el terminal 3 y el módulo de identificación de abonado 4 son del tipo que puede aplicar las herramientas “SIM Aplicación Toolkit”, tal como se describe en detalle en la norma “GSM 11.14 (Fase 2+)” de la ETSI. El módulo de identificación de abonado 4 se califica entonces como “SIM proactivo, según la terminología GSM. En resumen, el “SIM Aplicación Toolkit” es un juego de órdenes y procedimientos que permiten al módulo de identificación de abonado 4 “tomar la iniciativa” y enviar órdenes al terminal 3. Especialmente, una de estas órdenes, denominada “SET UP CALL (parámetro)”, permite al módulo de identificación de abonado 4 pedir al terminal 3 que establezca una comunicación marcando un número que le precisa en parámetro y según un modo de transmisión que le precisa igualmente en parámetro.

Se presenta sucesivamente a continuación cada una de las etapas del modo de realización particular del procedimiento según la invención, tal como se ilustra en el organigrama de la figura 2.

Etapa 20: por ejemplo durante cada una (o solamente algunas) de sus inicializaciones, el terminal 3 lee, en una zona de memoria 51 del módulo de identificación de abonado 4, una lista predeterminada de juegos de parámetros, comprendiendo cada uno un número de teléfono de un módulo de servicios, un modo de transmisión, y eventualmente otro(s) parámetro(s) de llamada. Se presenta un ejemplo de estructura de la zona de memoria 51 en detalle más adelante, en relación con la figura 3.

Etapa 21: el módulo de identificación de abonado 4 envía al terminal 3 una orden “SET UP CALL (primer juego de parámetros)”, pidiendo al terminal 3 que establezca una comunicación según las indicaciones del primer juego de parámetros. Se trata, por ejemplo, de establecer una comunicación con la primera plataforma UP1, en modo digital.

Etapa 22: el terminal 3 compara el primer juego de parámetros, precisado en parámetro de la orden, con una lista predeterminada de uno o más juego(s) de parámetros distinto(s).

Etapa 23: el terminal 3 determina si se verifica la primera condición siguiente: “el primer juego de parámetros pertenece a la lista predeterminada”.

Etapa 24: si se verifica la primera condición, el terminal 3 intenta establecer una comunicación según las indicaciones del primer juego de parámetros.

Etapa 25: el terminal 3 determina si se verifica la segunda condición siguiente: se ha establecido efectivamente la comunicación pedida.

Etapa 26: si se verifica la segunda condición, el terminal 3 lanza la aplicación de servicios 31 (en el ejemplo antes citado, se lanza el navegador).

Etapa 27: el módulo de servicios (UP1 en el ejemplo antes citado) autentifica el módulo de identificación de abonado 4.

Como se ha presentado en el organigrama simplificado de la figura 4, en un modo de realización particular, esta etapa 27 de autentificación comprende a su vez las siguientes etapas:

- el módulo de servicios UP1 envía (41) un número aleatorio, denominado de desafío, al módulo de identificación de abonado 4, mediante el terminal 3;

- en función de este desafío y con ayuda de un algoritmo de autentificación y/o al menos una clave de autentificación contenida(s) en unas zonas protegidas 52, 53 del módulo de identificación de abonado (por ejemplo en la zona memoria 51, véase la fig. 3), el módulo de identificación de abonado 4 calcula (42) una primera firma electrónica SI;

- mediante el terminal 3, el módulo de identificación de abonado 4 envía (43) la primera firma electrónica S1 al módulo de servicios UP1;

- en función del desafío y con ayuda del algoritmo de autentificación y/o de la clave de autentificación, que conoce también, el módulo de servicios UP1 calcula (44) una segunda firma electrónica S2;

- el módulo de servicios UP1 compara (45) las primera y segunda firmas electrónicas S1, S2, y si son idénticas, autentifica el módulo de identificación de abonado 4 (y en consecuencia al usuario de esta tarjeta SIM).

Etapa 28: si no se verifica una de las primera y segunda condiciones (véase etapas 23 y 25 respectivamente), el módulo de identificación de abonado 4 envía al terminal 3 una nueva orden “SET UP CALL (segundo juego de parámetros)”, pidiendo al terminal 3 que establezca una comunicación según las indicaciones del segundo juego de parámetros. Se trata, por ejemplo, de establecer una comunicación con la segunda plataforma UP2, en modo analógico. Está claro que podría también tratarse de establecer siempre una comunicación con la primera plataforma UP1, pero en modo analógico. Se comprenderá que son posibles numerosas soluciones, siendo el número de estas soluciones igual al número de juegos de parámetros distintos (comprendiendo cada juego un número de módulo de servicios, un modo de transmisión, ...) para el tipo de módulo de servicios al cual se desea acceder.

Etapas 29 a 34: estas etapas se distinguen de las etapas 22 a 27 solamente en que el primer juego de parámetros y el módulo de servicios UP1 son sustituidos por el segundo juego de parámetros y el módulo de servicios UP2.

Etapa 35: si una de las dos condiciones examinadas en las etapas 30 y 32, pendientes de las etapas 23 y 25 respectivamente, no se verifica, se interrumpe el procedimiento de acceso.

Está claro que si la lista de juegos de parámetros comprende más de dos juegos de parámetros, una variante de la etapa 35 puede consistir en reiterar las etapas 28 a 32 antes citadas con cada uno de los otros juegos de parámetros. En este caso, sólo se interrumpe el procedimiento de acceso si han fallado todas las diferentes tentativas, con los diferentes juegos de parámetros de la lista.

A continuación se presenta, en relación con la figura 3, un ejemplo de contenido de la zona de memoria 51 del módulo de identificación de abonado 4.

Como se ha explicado anteriormente (véase la etapa 20), esta zona de memoria 51 almacena los elementos constitutivos de los juegos de parámetros que permiten referir a parámetros la orden “CALL SET UP”. Se recuerda que estos elementos constitutivos comprenden, por ejemplo:

- la lista de los números de los módulos de servicios (n1, n2, n3...). En el caso de plataformas de acceso UP, estos números, por ejemplo, se guardan en un fichero elemental EF_{UPLN} (de “*Elementary File*$_{\text{UP LINK NUMBER}}$”, “Archivo Elemental$_{\text{NÚMERO DE ENLACE ASCENDENTE}}$”, en inglés);

- la lista de los parámetros de llamadas (p1, p2, p3...) (por ejemplo los modos de transmisión (modo digital, modo analógico, ...) que corresponden a los distintos números de módulos de servicios. Estos parámetros de llamadas, por ejemplo, se guardan en un fichero elemental EF_{CCP} (de *"Elementary File*$_{\text{CAPABILITY CONFIGURATION PARAMETERS}}$*"*, "Archivo Elemental$_{\text{PARÁMETROS DE CONFIGURACION DE CAPACIDADES}}$", en inglés) de la zona de memoria 51. Al igual que los números de plataforma, estos parámetros están destinados a ser leídos de antemano por el terminal (durante la etapa 20).

Opcionalmente, se puede prever que la zona de memoria 51 del módulo de identificación de abonado 4 (y no el terminal 3) almacene también informaciones útiles al navegador 31 después de que haya sido lanzado. Puede tratarse, por ejemplo:

- de números de tipo IP', almacenados en un fichero elemental EF_{IPN} (de "*Elementary File*$_{\text{INTERNET PROTOCOL NUMBER}}$", "Archivo Elemental$_{\text{NÚMERO DE PROTOCOLO DE INTERNET}}$", en inglés);

- de una clave secreta de autentificación del navegador y/o de encriptación de datos en la red informática de tipo Internet, guardada en un fichero elemental EF_K (de "*Elementary File*$_{\text{KEY}}$", "Archivo Elemental$_{\text{CLAVE}}$", en inglés). Esta clave secreta se utiliza durante cada sesión entre el navegador y una de las plataformas de acceso;

- de un identificador del usuario ante cada plataforma de acceso, guardado en un fichero elemental EF_{dev_Id} (de "*Elementary File*$_{\text{device\_Identifier}}$", "Archivo Elemental$_{\text{Identificador_dispistivo}}$", en inglés);

- de números de centro de servicios de mensajes cortos, almacenados en un archivo elemental, EF_{SMS-P} (de "Elementary File$_{\text{Short Message Services−Parameters}}$", "Archivo Elemental$_{\text{Servicio de Mensajes Cortos−Parámetros}}$", en inglés);

- etc.

Está claro que se pueden considerar otros numerosos modos de realización de la invención. Se puede prever, especialmente, un número cualquiera de módulos de servicios (plataforma de acceso o servidor de pago y/o de reserva y/o de consulta). También se puede prever no almacenar, en la zona de memoria 51 del módulo de identificación de abonado 4, más que algunas de las informaciones mencionadas anteriormente. Se observará igualmente que podría modificarse el orden de ejecución de las etapas 22 a 25 (así como el de las etapas 29 a 32).

REIVINDICACIONES

1. Procedimiento de acceso a un módulo de servicios (UP1, UP2, 13) a partir de una estación móvil (2) comprendida en un sistema de radiocomunicación (1), comprendiendo dicha estación móvil un terminal (3) que coopera con un módulo de identificación de abonado (4), pudiendo ejecutar dicho terminal una aplicación de servicios de manera que se beneficie de uno o de varios servicios ofrecidos por dicho módulo de servicios después de que se haya establecido una comunicación entre dicho terminal y dicho módulo de servicios,

caracterizado porque dicho procedimiento comprende las etapas siguientes:

- el módulo de identificación de abonado envía (21) al terminal, para que el terminal la ejecute, una orden de establecimiento de una comunicación entre el terminal y un primer módulo de servicios (UP1), estando dicha orden referida a unos parámetros correspondientes a un primer juego de uno o varios parámetros que comprende un primer número de teléfono de dicho primer módulo de servicios y, eventualmente, al menos un primer parámetro de llamada;

- el terminal compara (22) dicho primer juego de uno o varios parámetros con una lista predeterminada de juegos de uno o varios parámetros, que comprende al menos un juego de uno o varios parámetros;

- si (23) dicho primer juego de uno o varios parámetros forma parte de dicha lista, el terminal ejecuta dicha orden e intenta (24) establecer una comunicación con dicho primer módulo de servicios, según dicho primer juego de uno o varios parámetros;

- si (25) se establece efectivamente dicha comunicación con dicho primer servidor, el terminal lanza la ejecución de dicha aplicación de servicios, de manera que dicho terminal pueda beneficiarse de uno o varios servicios ofrecidos por dicho primer módulo de servicios.

2. Procedimiento según la reivindicación 1, **caracterizado** porque cada juego distinto de uno o varios parámetros que permite referir a parámetros dicha orden de establecimiento de comunicación, comprende al menos:

- un número de teléfono (n1, n2, n3, ...) de un módulo de servicios;

- un parámetro de llamada (p1, p2, p3, ...) que define un modo de comunicación.

3. Procedimiento según una cualquiera de las reivindicaciones 1 y 2, **caracterizado** porque dicho módulo de servicios (UP1, UP2), denominado plataforma de acceso, ofrece al menos un servicio de acceso a una red informática de tipo Internet (10),

y porque dicha aplicación de servicios ejecutada por el terminal es un navegador que permite navegar al terminal en el seno de dicha red informática de tipo Internet, después de que ha sido establecida efectivamente dicha comunicación entre el terminal y dicha plataforma de acceso.

4. Procedimiento según la reivindicación 3, **caracterizado** porque dicho navegador utiliza un lenguaje específico del tipo “WAP/HDML”.

5. Procedimiento según una cualquiera de las reivindicaciones 3 y 4, **caracterizado** porque al menos una información, útil al navegador (31) después de que haya sido lanzado, está igualmente almacenada en dicho módulo de identificación de abonado (4).

6. Procedimiento según la reivindicación 5, **caracterizado** porque dicha al menos una información, útil para el navegador después de que haya sido lanzado, pertenece al grupo que comprende:

- números de tipo IP;

- claves secretas de autentificación del navegador y/o de encriptación de datos;

- identificadores de usuarios ante las plataformas de acceso;

- números de centro de servicio de mensajes cortos.

7. Procedimiento según una cualquiera de las reivindicaciones 1 y 2, **caracterizado** porque dicho módulo de servicios (13) ofrece al menos un servicio de pago y/o de reserva y/o de consulta,

y porque dicha aplicación de servicios ejecutada por el terminal es una aplicación de pago y/o de reserva y/o de consulta, que permite al terminal beneficiarse de dicho al menos un servicio de pago y/o de reserva y/o de consulta ofrecido por dicho módulo de servicios, después de que se haya establecido efectivamente dicha comunicación entre el terminal y dicho módulo de servicios.

8. Procedimiento según una cualquiera de las reivindicaciones 1 a 7, guardando dicho módulo de identificación de abonado (4) al menos una "aplicación de operador" cuya ejecución permite ofrecer al menos una funcionalidad a un usuario de dicha estación móvil,

caracterizada porque dicha etapa de envío por el módulo de identificación de abonado, al terminal, de una orden de establecimiento de una comunicación entre el terminal y el primer módulo de servicios a una funcionalidad suplementaria, cuya elección se ofrece al usuario durante la ejecución por el módulo de identificación de abonado de dicha aplicación de operador.

9. Procedimiento según una cualquiera de las reivindicaciones 1 a 8, **caracterizado** porque dicho sistema de radiocomunicación al cual pertenece dicha estación móvil corresponde al grupo que comprende:

- los sistemas de radiocomunicación de tipo GSM;
- los sistemas de radiocomunicación de tipo DCS 1800;
- los sistemas de radiocomunicación de tipo PCS 1900;
- los sistemas de radiocomunicación de tipo UMTS;
- los sistemas de radiocomunicación de tipo DECT.

10. Procedimiento según una cualquiera de las reivindicaciones 1 a 9, **caracterizado** porque dicha orden de establecimiento de una comunicación, enviada por el módulo de identificación de abonado al terminal, es la orden "SET UP CALL" (ESTABLECER LLAMADA) del juego de órdenes del *"SIM Application Toolkit"* (Herramientas de Aplicación del SIM).

11. Procedimiento según una cualquiera de las reivindicaciones 1 a 10, **caracterizado** porque dicha lista predeterminada de juegos de uno o varios parámetros se almacena en dicho módulo de identificación de abonado (4), comprendiendo cada juego de uno o varios parámetros un número de teléfono de módulo de servicios (n1, n2, n3, ...) y, eventualmente, al menos un parámetro de llamada (p1, p2, p3, ...),

y porque dicho procedimiento comprendiendo además la etapa siguiente, previa a dicha etapa de comparación:

- el terminal lee dicha lista predeterminada de juego de uno o varios parámetros, almacenada en dicho módulo de identificación de abonado.

12. Procedimiento según la reivindicación 11, **caracterizado** porque dicha etapa de lectura por el terminal de dicha lista predeterminada de juego de uno o varios parámetros se ejecuta durante al menos algunas inicializaciones de dicho terminal.

13. Procedimiento según una cualquiera de las reivindicaciones 1 a 12, **caracterizado** porque si las condiciones para que el terminal lance la ejecución de dicha aplicación de servicios no se satisfacen, dicho procedimiento comprende además las etapas complementarias siguientes, que pueden ser eventualmente reiteradas:

- el módulo de identificación de abonado envía (28) al terminal, para que el terminal la ejecute, una nueva orden de establecimiento de una comunicación entre el terminal y dicho primer módulo de servicios o entre el terminal y un segundo módulo de servicios, distinto del primer módulo de servicios, estando referida dicha nueva orden a unos parámetros con un nuevo juego de uno o varios parámetros distinto de dicho primer juego de uno o varios parámetros;
- el terminal compara (29) dicho nuevo juego de uno o varios parámetros con dicha lista predeterminada de juegos de uno o varios parámetros;
- si (30) el resultado de dicha comparación es positivo, el terminal ejecuta dicha orden e intenta (31) establecer una comunicación con dicho primer o segundo módulo de servicios, según dicho nuevo juego de uno o varios parámetros;
- si (32) se establece efectivamente dicha comunicación con dicho primer o segundo módulo de servicios, el terminal lanza (33) la ejecución de dicha aplicación de servicios, de modo que dicho terminal pueda beneficiarse de uno o varios servicios ofrecidos por dicho primer o segundo módulo de servicios.

14. Procedimiento según la reivindicación 13, **caracterizado** porque dicha etapa (28) de envío por el módulo de identificación de abonado, al terminal, de una nueva orden de establecimiento de una comunicación se efectúa automáticamente si, después de una tentativa precedente, no se cumplen las condiciones para que el terminal lance la ejecución de dicha aplicación de servicios.

15. Procedimiento según la reivindicación 13 y la reivindicación 8, **caracterizado** porque dicha etapa (28) de envío por el módulo de identificación de abonado, al terminal, de una nueva orden de establecimiento de una comunicación corresponde a una funcionalidad suplementaria, cuya elección se ofrece al usuario en la ejecución por el módulo de identificación de abonado de dicha aplicación de operador.

16. Procedimiento según una cualquiera de las reivindicaciones 1 a 15, **caracterizado** porque dicha etapa (26) de lanzamiento por el terminal de la ejecución de dicha aplicación de servicios va seguida de una etapa (27) de autentificación de dicho módulo de identificación de abonado por dicho módulo de servicios, que comprende a su vez las siguientes etapas:

- el servidor de servicios envía (41) un número aleatorio, denominado de desafío, al módulo de identificación de abonado, a través del terminal;

- en función de dicho desafío y con ayuda de un algoritmo de autentificación y/o al menos una clave de autentificación contenido en unas zonas protegidas del módulo de identificación de abonado, el módulo de identificación de abonado calcula (42) una primera firma electrónica;

- mediante el terminal, el módulo de identificación de abonado envía (43) dicha primera firma electrónica al módulo de servicios;

- en función de dicho desafío y con la ayuda de dicho algoritmo de autentificación y/o de dicha al menos una clave de autentificación, que conoce también, dicho módulo de servicios calcula (44) una segunda firma electrónica;

- dicho módulo de servicios compara (45) dichas primera y segunda firmas electrónicas, y si son idénticas, autentifica dicho módulo de identificación de abonado.

17. Módulo de identificación de abonado (4), del tipo destinado a cooperar con un terminal (3) para formar una estación móvil (2) comprendida en un sistema de radiocomunicación, pudiendo ejecutar dicho terminal una aplicación de servicios (31) de tal modo que se beneficie de uno o varios servicios ofrecidos por un módulo de servicios (UP1, UP2, 13) después de que se haya establecido una comunicación entre dicho terminal y dicho módulo de servicios,

caracterizado porque dicho módulo de identificación de abonado comprende unos medios (52) de envío al terminal, para que el terminal la ejecute, de una orden de establecimiento de una comunicación entre el terminal y un primer módulo de servicios, estando dicha orden referida a unos parámetros con un primer juego de uno o varios parámetros que comprende un primer número de teléfono de dicho primer módulo de servicios y, eventualmente, efectuando el terminal las etapas siguientes a la recepción de dicha orden:

- el terminal compara dicho primer juego de uno o varios parámetros con una lista predeterminada de juegos de uno o varios parámetros, que comprende al menos un juego de uno o varios parámetros;

- si dicho primer juego de uno o varios parámetros forma parte de dicha lista, el terminal ejecuta dicha orden e intenta establecer una comunicación con dicho primer módulo de servicios, según dicho primer juego de uno o varios parámetros;

- si dicha comunicación con dicho primer servidor se establece efectivamente, el terminal lanza la ejecución de dicha aplicación de servicios, de modo que dicho terminal pueda beneficiarse de uno o varios servicios ofrecidos por dicho primer módulo de servicios.

18. Terminal (3) del tipo destinado a cooperar con un módulo de identificación de abonado (4) para formar una estación móvil (2) comprendida en un sistema de radiocomunicación, pudiendo ejecutar dicho terminal una aplicación de servicios (31) de manera que se beneficie de uno o varios servicios ofrecidos por un módulo de servicios (UP1, UP2, 13) después de que se haya establecido una comunicación entre dicho terminal y dicho módulo de servicios,

caracterizado porque dicho terminal comprendiendo:

- unos medios (32) de recepción de una orden, procedente del módulo de identificación de abonado y que piden al terminal que establezca una comunicación entre el terminal y un primer módulo de servicios, estando dicha orden referida a parámetros con un primer juego de uno o varios parámetros que comprende un primer número de teléfono de dicho primer módulo de servicios y, eventualmente, al menos un primer parámetro de llamada;

- unos medios (33) de comparación de dicho primer juego de uno o varios parámetros con una lista predeterminada de juegos de uno o varios parámetros, que comprende al menos un juego de uno o varios parámetros;

- unos medios (34) de ejecución de dicha orden, si dicho primer juego de uno o varios parámetros forma parte de dicha lista, de manera que intente establecer una comunicación con dicho primer módulo de servicios, según dicho primer juego de uno o varios parámetros;

- unos medios (35) de lanzamiento de la ejecución de dicha aplicación de servicios, si dicha comunicación entre el terminal y dicho primer servidor se ha establecido efectivamente, de modo que dicho terminal pueda beneficiarse de uno o varios servicios ofrecidos por dicho primer módulo de servicios.

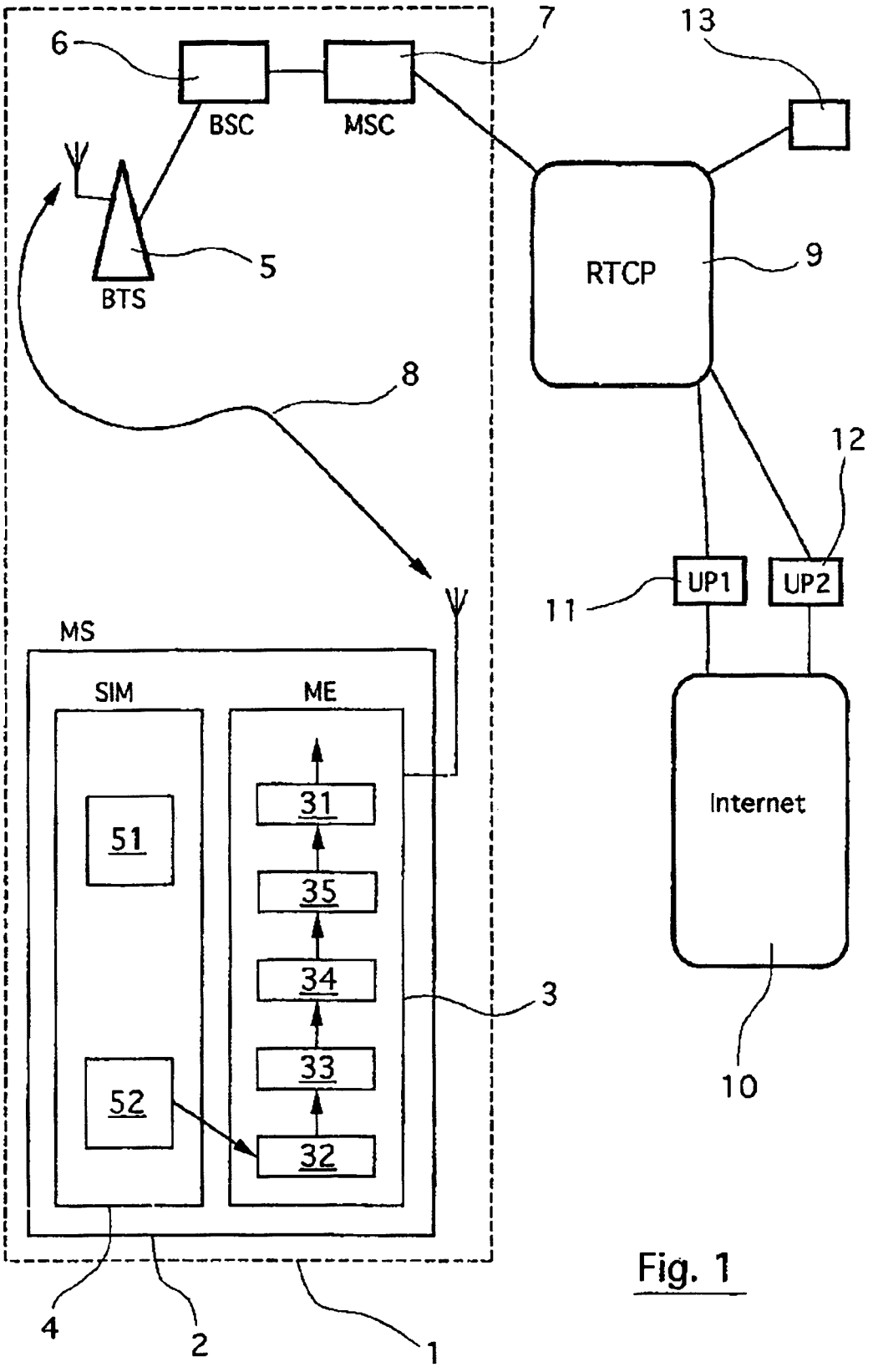
6
BSC
MSC
7
13
BTS
5
RTCP
9
8
12
UP1
UP2
11
MS
SIM
ME
31
51
35
34
3
33
52
32
Internet
10
4
2
1

Fig. 1

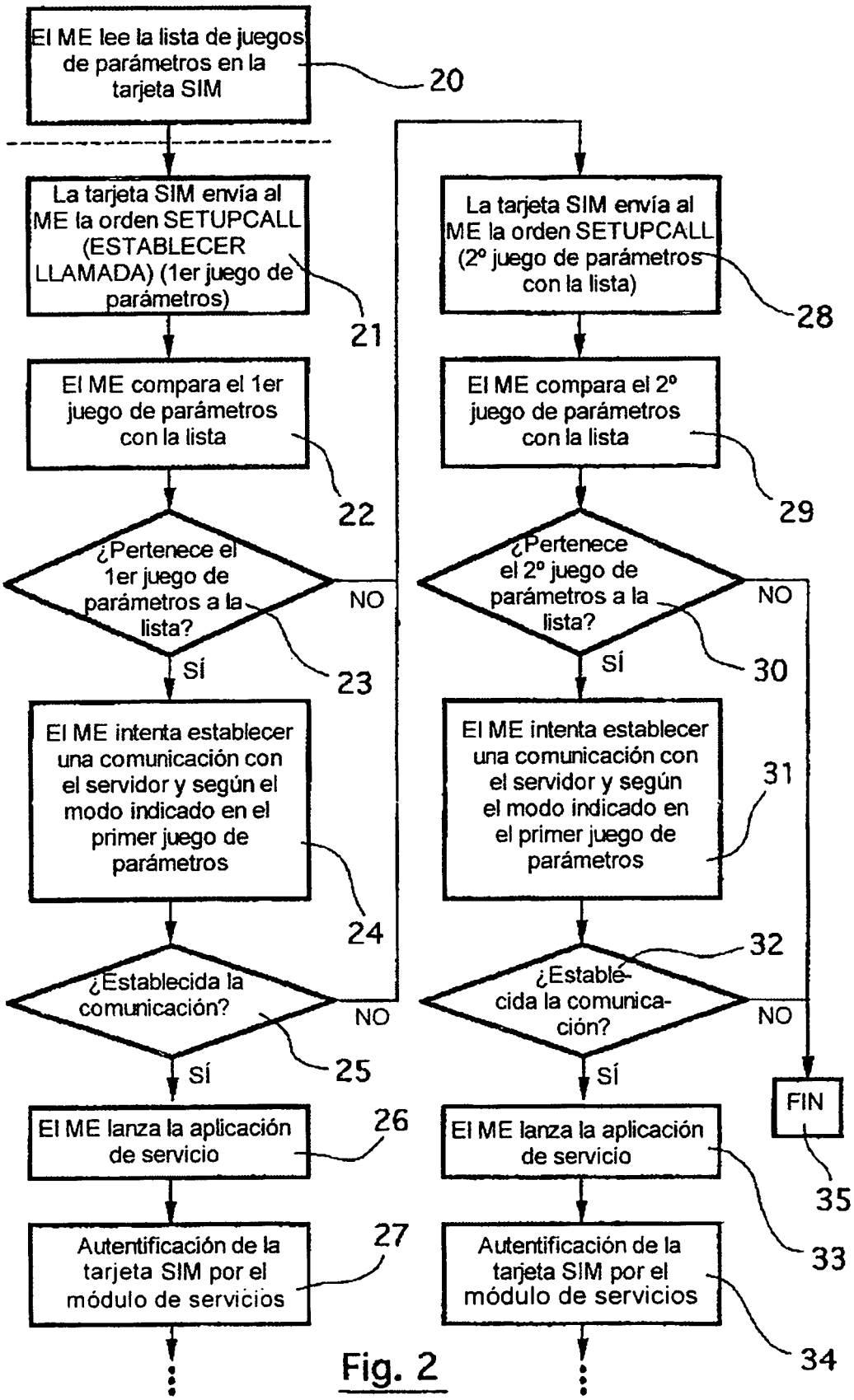
El ME lee la lista de juegos de parámetros en la tarjeta SIM
20
La tarjeta SIM envía al ME la orden SETUPCALL (ESTABLECER LLAMADA) (1er juego de parámetros)
21
El ME compara el 1er juego de parámetros con la lista
22
¿Pertenece el 1er juego de parámetros a la lista?
23
NO
SÍ
El ME intenta establecer una comunicación con el servidor y según el modo indicado en el primer juego de parámetros
24
¿Establecida la comunicación?
25
NO
SÍ
El ME lanza la aplicación de servicio
26
Autentificación de la tarjeta SIM por el módulo de servicios
27
La tarjeta SIM envía al ME la orden SETUPCALL (2º juego de parámetros con la lista)
28
El ME compara el 2º juego de parámetros con la lista
29
¿Pertenece el 2º juego de parámetros a la lista?
30
NO
SÍ
El ME intenta establecer una comunicación con el servidor y según el modo indicado en el primer juego de parámetros
31
¿Establecida la comunicación?
32
NO
SÍ
El ME lanza la aplicación de servicio
33
Autentificación de la tarjeta SIM por el módulo de servicios
34
FIN
35

Fig. 2

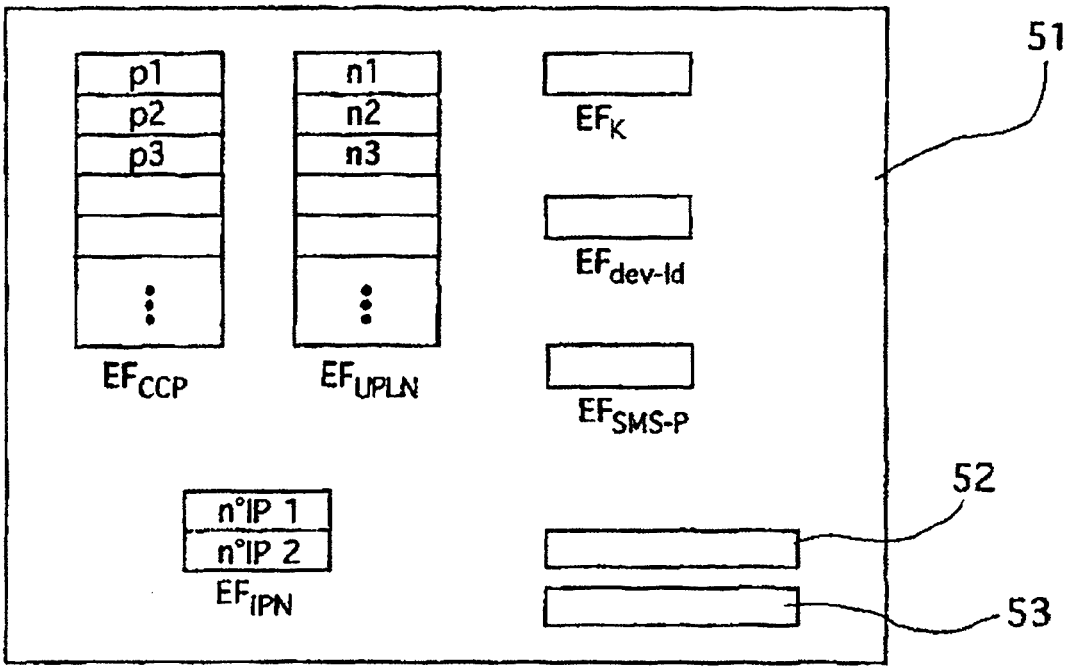
51
p1
p2
p3
n1
n2
n3
EF_K
EF_dev-Id
EF_CCP
EF_UPLN
EF_SMS-P
n°IP 1
n°IP 2
EF_IPN
52
53

Fig. 3

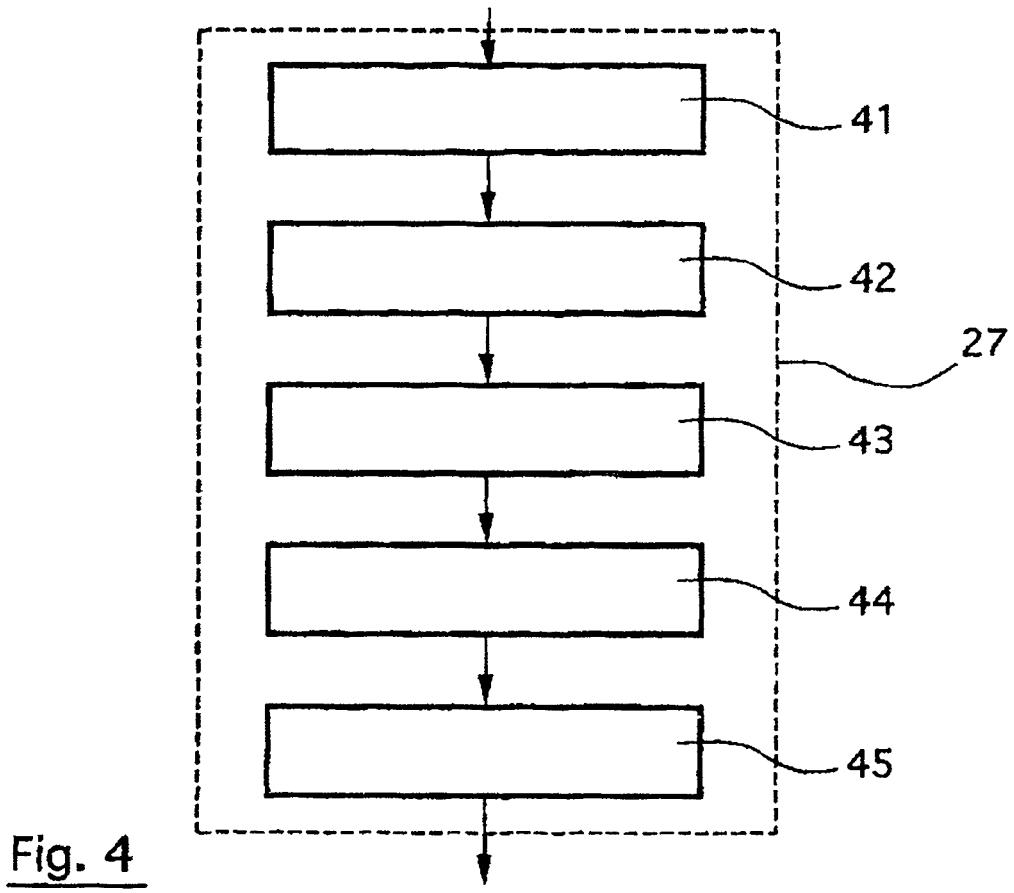
41
42
27
43
44
45

Fig. 4