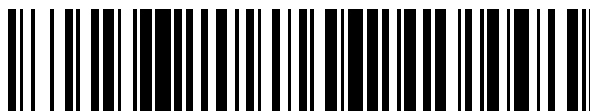


19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 608 493**

51 Int. Cl.:

H04L 29/06 (2006.01)

H04W 12/02 (2009.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **23.01.2009** **PCT/EP2009/050766**

87 Fecha y número de publicación internacional: **06.08.2009** **WO09095354**

96 Fecha de presentación y número de la solicitud europea: **23.01.2009** **E 09705142 (9)**

97 Fecha y número de publicación de la concesión europea: **28.09.2016** **EP 2238730**

54 Título: **Método para la gestión remota de dispositivos móviles y dispositivo móvil adecuado para ello**

30 Prioridad:

30.01.2008 IT PN20080005

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

11.04.2017

73 Titular/es:

INFINITE S.R.L (100.0%)
Via San Gaetano 113
31044 Montebelluna, IT

72 Inventor/es:

BOF, PATRIZIO

74 Agente/Representante:

AZNÁREZ URBIETA, Pablo

ES 2 608 493 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Método para la gestión remota de dispositivos móviles y dispositivo móvil adecuado para ello.

CAMPO TÉCNICO DE LA INVENCION

- 5 La presente invención se refiere a un método para la gestión remota de dispositivos móviles y a un dispositivo móvil adecuado para dicho método, estando destinada la gestión de estos dispositivos en particular a la seguridad general de los datos contenidos en los mismos.

ESTADO DE LA TÉCNICA

- 10 La evolución técnica que ha acompañado al desarrollo de los dispositivos móviles en general a lo largo de estos últimos años ha permitido aumentar considerablemente la capacidad de procesamiento y de almacenamiento de datos de dichos dispositivos, conjuntamente con el número de unidades periféricas de a bordo que son capaces de acomodar, lo que hace que estos dispositivos sean herramientas cada vez más productivas. Como resultado, el uso de los dispositivos móviles se ha extendido rápidamente tanto en entornos corporativos, con el objeto de mejorar la eficiencia, como a nivel personal, para el ocio y fines similares.

- 15 En general, las categorías de los dispositivos móviles a las que se hace referencia en esta especificación incluyen, por ejemplo, dispositivos tales como los denominados PDA o Asistentes Digitales Personales, *Smartphones* (teléfonos inteligentes), *Tablet PC* (PC de tableta) y similares.

- 20 Cada uno de los dispositivos móviles de estas categorías se caracteriza por una heterogeneidad de los componentes tanto de *hardware* como de *software*, interfaces de usuario y plataformas, hasta tal punto que prácticamente puede considerarse como un pequeño ordenador inalámbrico. En particular, todos estos dispositivos móviles tienen en común la posibilidad de utilizar una variedad realmente amplia de interfaces de comunicación inalámbrica que permiten acceder en cualquier caso y de cualquier modo a la red de Internet. Las diversas tecnologías de comunicación inalámbrica que pueden aprovechar los dispositivos móviles se completan e integran entre sí. Éstas incluyen tanto tecnologías de banda ancha, con un radio de cobertura corto o alcance de cobertura pequeño, como tecnologías de banda media o de banda estrecha, con un alcance de cobertura grande.

- 25 Las tecnologías de banda media y de banda estrecha incluyen las típicas de los sistemas móviles de comunicación por radio, como GSM, D-AMPS, GPRS, UMTS, 3G y similares, conocidas en general porque también pueden proporcionar servicios y características particulares. Por ejemplo, la red de telefonía móvil GSM proporciona la característica de transmitir mensajes cortos, el denominado Servicio de Mensajes Cortos (SMS - *Short Message Service*). De todos modos, esta característica de SMS también está actualmente disponible en otras redes, por ejemplo la red de telefonía UMTS o en una red de telefonía fija.

- 30 Como es ampliamente conocido, los sistemas móviles de comunicación por radio cumplen unos criterios claros destinados a garantizar la seguridad general de las conversaciones en el canal de radio, prestando una atención particular a asegurar la autenticación y la confidencialidad de la identidad del usuario, así como la confidencialidad de los datos transmitidos por éste.

- 35 En general se utiliza una tarjeta inteligente, como la denominada tarjeta SIM (*Subscriber Identify Module* - Módulo de Identificación del Abonado), como dispositivo de seguridad para autenticar al usuario. Esta tarjeta SIM telefónica se instala en el dispositivo móvil y, una vez activada, proporciona la capacidad de acceder a los servicios ofrecidos por la red de radio móvil, permitiendo así que el usuario utilice el propio dispositivo móvil. La tarjeta SIM telefónica incluye una memoria de acceso secuencial en la que están almacenados datos que incluyen un código de identificación de usuario unívoco, el denominado código IMSI (*International Mobile Subscriber Identity* - Identidad Internacional de Estación Móvil). El administrador de la red de radio móvil asocia un número de teléfono al código IMSI.

- 40 El propio dispositivo móvil proporciona otro nivel de seguridad. De hecho, cada dispositivo móvil está identificado de forma unívoca por otro código, el denominado código IMEI (*International Mobile Equipment Identity* - Identidad Internacional de Equipo Móvil), que es almacenado de forma permanente en la memoria inherente del dispositivo móvil directamente por el fabricante. Este código es almacenado en una base de datos por el administrador de la red de radio móvil cuando el usuario activa el servicio.

- 45 La necesidad de proporcionar servicios de gestión remota para dispositivos móviles en general es un punto básico en el proceso de convertir un dispositivo móvil en un recurso corporativo real. De hecho, a veces es necesario que el dispositivo móvil realice acciones relativas a la seguridad siguiendo criterios corporativos o, en cualquier caso, que salvaguarden la privacidad en general. Además, por ejemplo debe ser posible descargar e instalar o incluso desinstalar datos y programas. Por otro lado, debe ser posible actualizar y configurar periódicamente el *software* instalado.

Sin embargo, siempre que se requieren dichas acciones ineludibles es necesario manejar y abordar cuestiones inequívocas de naturaleza técnica, como es bien sabido por cualquier especialista en este campo. Como resultado, la tarea de controlar el dispositivo móvil se deja en manos de personal técnico especialista cualificado en materia de TI.

5 Actualmente, algunas compañías telefónicas, las denominadas operadoras de telefonía, suministran sus servicios de comunicación de voz y datos por redes de telefonía tanto fija como móvil en grandes áreas geográficas, facilitando una cobertura capilar extendida a nivel mundial que permite llegar al dispositivo móvil en cualquier lugar con sus propios servicios. Los dispositivos móviles utilizados en este contexto pueden incluir información privada o programas de aplicación propiedad de la operadora de telefonía. El *software* incluido en el dispositivo móvil puede ser asignado, instalado y configurado y también actualizado automáticamente por la operadora de telefonía, quien, con este fin, utiliza herramientas centralizadas que son características de la red del sistema de telefonía del mismo proveedor de servicios.

Además, existen algunas estructuras, como sistemas de procesamiento de datos corporativos o de TI u otras estructuras externas, que están previstas para realizar tareas y actividades de control y servicio en los dispositivos móviles, debiendo entenderse esto principalmente como la posibilidad de instalar y configurar aplicaciones de *software*. Con este fin, dentro del dispositivo móvil se instala una aplicación cliente propietaria.

15 El documento US 2006/236325 describe un cliente de dispositivo que soporta la asistencia al cliente y la distribución de paquetes de actualización a dispositivos electrónicos y que permite gestionar y actualizar eficientemente *firmware* y *software* en dispositivos electrónicos. Un servidor de gestión de terminales/gestión de dispositivos emplea extensiones de un protocolo de gestión de dispositivos estándar industriales para actualizar la información de actualización, abastecer el dispositivo electrónico y gestionarlo, por ejemplo. El dispositivo electrónico puede recibir paquetes de actualización y uno o más agentes de actualización del dispositivo electrónico pueden actualizar el *firmware* y/o *software* del mismo. Un cliente de diagnóstico en el dispositivo electrónico facilita el diagnóstico remoto y un cliente de traps (interrupciones, detección de condición de error) facilita el establecimiento de condiciones de error y la recuperación de información recopilada. Un servidor de gestión de terminales puede invocar a distancia acciones de control dentro del dispositivo electrónico utilizando objetos de gestión no soportados por el protocolo de gestión de los dispositivos estándar industriales. Un usuario del dispositivo electrónico puede emplear un portal de autoasistencia para administrar la autoasistencia y realizar diagnósticos. Una llamada de asistencia de cliente posterior puede utilizar la información recopilada durante la autoasistencia.

Una desventaja de aplicar los criterios de gestión de equipos móviles de acuerdo con los ejemplos arriba mencionados radica en las restricciones que impone la necesidad de recurrir a la asistencia de personal de TI altamente cualificado cada vez que se debe llevar a cabo una tarea de gestión que implique al dispositivo móvil.

Otra desventaja está relacionada con el tipo de servicio ofrecido, que básicamente está orientado a la conexión. Dicho de otro modo, el dispositivo móvil no sólo debe estar conectado a la red cuando se solicita el servicio, sino que también debe permanecer conectado durante todo el tiempo que esté siendo suministrado el mismo servicio.

DESCRIPCIÓN DE LA INVENCION

35 Por consiguiente, un objeto principal de la presente invención es resolver los problemas arriba indicados de las disposiciones del estado anterior de la técnica proporcionando un método para la gestión remota de dispositivos móviles y un dispositivo móvil adecuado para dicho método, dejándose la gestión del dispositivo móvil en manos del usuario final con autonomía plena.

40 Dentro del objeto general arriba indicado, un objetivo de la presente invención es proporcionar un método para la gestión remota de dispositivos móviles y un dispositivo móvil adecuado para dicho método, pudiendo tener lugar la comunicación con el dispositivo móvil de forma asíncrona.

Otro objetivo de la presente invención es proporcionar un método para la gestión remota de dispositivos móviles y un dispositivo móvil adecuado para dicho método, pudiendo ejecutarse algunas funciones o características operativas de forma automática, es decir, el sistema puede detectar ciertas influencias o alteraciones en el dispositivo móvil iniciando automáticamente rutinas de servicio apropiadas como respuesta.

Otro objetivo igualmente importante de la presente invención es proporcionar un método para la gestión remota de dispositivos móviles y un dispositivo móvil adecuado para dicho método, que pueden implementarse y fabricarse a costes competitivos utilizando medios de producción ya disponibles.

50 En las reivindicaciones adjuntas se exponen y definen desarrollos y mejoras ventajosos, debiendo ponerse en este contexto un énfasis especial en el aspecto de seguridad en lo que respecta a la transmisión de señales de instrucción y datos al dispositivo móvil, ya que dicha transmisión se realiza utilizando un protocolo encriptado.

Otra ventaja está relacionada con el modo de recepción de las señales de instrucción en el dispositivo móvil, ya que dichas señales de instrucción se adquieren de un modo silencioso e invisible.

De acuerdo con la presente invención, estos objetivos, ventajas, características y peculiaridades, junto con otros que se evidenciarán a partir de la siguiente descripción, se logran con un método para la gestión remota de dispositivos móviles y un dispositivo móvil adecuado para dicho método, que incorporan las características expuestas y enumeradas en las reivindicaciones independientes adjuntas y en las reivindicaciones dependientes.

5 BREVE DESCRIPCIÓN DE LAS FIGURAS

En cualquier caso, las características y ventajas de la presente invención se entenderán más fácilmente a partir de la descripción de un ejemplo de realización dado más abajo a modo de ejemplo no limitativo en referencia a las figuras adjuntas, en las que:

- Figura 1: vista esquemática del escenario de aplicación del sistema de gestión de un dispositivo móvil;
- 10 Figura 2: vista esquemática de los niveles de abstracción del programa de aplicación cliente;
- Figura 3: diagrama de flujo que muestra esquemáticamente la rutina de activación para controlar el dispositivo móvil;
- Figura 4: diagrama de flujo que muestra esquemáticamente la rutina de gestión del dispositivo móvil;
- Figura 5: diagrama de flujo que muestra esquemáticamente la rutina para detectar el cambio de una tarjeta SIM
- 15 telefónica dentro del dispositivo móvil; y
- Figura 6: vista esquemática que ilustra la sustitución de una tarjeta SIM telefónica en un dispositivo móvil.

DESCRIPCIÓN DETALLADA DE LA INVENCION

- 20 Con referencia a la Figura 1, el sistema de gestión de un dispositivo móvil comprende: al menos una estación de trabajo 12, por ejemplo un ordenador personal de sobremesa o portátil; un centro de servicio remoto 10; y al menos un dispositivo móvil 14. Los elementos incluidos en el sistema de gestión de un dispositivo móvil, tal como se menciona más arriba, dependen de la red de Internet y se conectan a la misma y a una red de telefonía móvil mediante interfaces y tecnologías usuales para con un denominado circuito telemático.

La estación de trabajo 12 comprende al menos un programa para visualizar páginas web e interactuar con las mismas, al que se denominará en adelante en general "navegador".

- 25 El centro de servicio remoto 10 es una unidad de procesamiento y almacenamiento de datos que proporciona un portal web que permite que los usuarios registrados, denominados en adelante "usuarios finales", gestionen el dispositivo móvil 14 de forma autónoma y fiable desde una estación de trabajo 12, con una amplia gama de servicios y contenidos. El centro de servicio remoto 10 comprende herramientas para transmitir señales de instrucciones predefinidas al dispositivo móvil 14 a través de una red de radio móvil, por ejemplo la red de telefonía móvil GMS, donde dichas señales
- 30 de instrucciones preferentemente están encapsuladas siguiendo un estándar de comunicación por radio móvil asíncrona, por ejemplo el estándar SMS. El centro de servicio remoto 10 utiliza además herramientas de encriptado y desencriptado para las señales transmitidas al y recibidas por el dispositivo móvil 14 mismo a través de la red de telefonía móvil.

- 35 El dispositivo móvil 14 comprende una pantalla 22, un soporte de almacenamiento de datos 18 subdividido en múltiples segmentos y una primera tarjeta telefónica SIM 16 (Figura 6) insertada en un receptáculo apropiado. La tarjeta telefónica SIM 16 está activada, de modo que un primer número de teléfono está asociado a un primer código IMSI en la primera tarjeta telefónica SIM 16.

- 40 El dispositivo móvil 14 se puede comunicar con el centro de servicio remoto 10 a través de la red de comunicación por radio móvil, donde las señales transmitidas preferentemente están encapsuladas de acuerdo con un estándar de comunicación por radio móvil asíncrona, por ejemplo el estándar SMS.

El dispositivo móvil 14 incluye un programa de aplicación cliente que se integra a bajo nivel con un sistema operativo instalado en el dispositivo móvil 14, con referencia a una estructura presuntamente jerárquica del mismo sistema operativo. Este programa de aplicación residente cliente en el dispositivo móvil no es visible en la lista de aplicaciones instaladas.

- 45 Con referencia a la Figura 2, el programa de aplicación cliente comprende módulos para desencriptar y encriptar las señales recibidas por y transmitidas al centro de servicio remoto 10 a través de la red de telefonía móvil. El nivel del programa de aplicación cliente situado por debajo comprende módulos para interpretar las señales de instrucción así desencriptadas, completando de este modo una actividad de gestión del dispositivo móvil 14 en la que interviene el sistema operativo. Por consiguiente, el propio programa de aplicación cliente define una interfaz entre las señales de instrucción que han sido intercambiadas a y desde el centro de servicio 10 y el sistema operativo. El programa de
- 50 aplicación cliente comprende además módulos para ejecutar procesos particulares en respuesta a eventos dados, lo que se explicará con mayor detalle más abajo.

El programa de aplicación cliente utiliza el soporte de almacenamiento de datos 18 para guardar ciertos tipos de datos, que se especificarán con mayor detalle más abajo. Además, el programa de aplicación cliente puede adquirir automáticamente (en caso necesario) ciertas características del dispositivo móvil 14 junto con ciertos tipos de datos, como un código de identificación unívoco del dispositivo móvil, es decir, el código IMEI.

- 5 El programa de aplicación cliente puede ser descargado en el dispositivo móvil utilizando la rutina descrita más abajo.

Con referencia a la Figura 3, desde la estación de trabajo 12 conectada con Internet, el usuario final puede visualizar una página web del portal proporcionado por el centro de servicio remoto 10, que después puede ser utilizada por éste para insertar un código de acceso de servicio en una máscara y enviarlo al centro de servicio 10 a través del navegador.

- 10 Dicho código de acceso de servicio incluirá los datos de identificación personal del usuario final, que pueden ser, por ejemplo, un código de identificación, una contraseña y un código de control, y que están disponibles por ejemplo en una tarjeta física, en línea o en de forma soportada en un medio. El código de activación de servicio posibilita el acceso al centro de servicio 10 de forma protegida y controlada, por ejemplo preguntando correspondientemente a una base de datos del mismo centro de servicio 10.

- 15 A continuación, el usuario final puede visualizar otra página web del portal del centro de servicio remoto 10 dentro del navegador. Esta página web incluirá una primera máscara, múltiples tipos de dispositivos móviles, una segunda máscara, una tercera máscara y una cuarta máscara. Por tanto, el usuario final podrá insertar los datos personales requeridos, por ejemplo el nombre, el apellido, etc., en la primera máscara y seleccionar de entre la lista mostrada el tipo de dispositivo móvil correspondiente que debe ser gestionado y controlado. Después, el usuario final podrá enviar esta información al centro de servicio 10 a través del navegador.

- 20 Además, el usuario final podrá insertar el código IMEI del dispositivo móvil 14 en la segunda máscara, mientras que podrá insertar el primer número de teléfono asociado a la primera tarjeta telefónica SIM 16 en la tercera máscara y finalmente enviar dicha información al centro de servicio 10 a través del navegador. Adicionalmente, después de seleccionar una contraseña personal, que en adelante se denominará PIN y que puede ser, por ejemplo, un código de cinco dígitos, el usuario final podrá insertarla en la cuarta máscara y enviar esta información al centro de servicio 10 a través del navegador.

Los datos personales, el código IMEI, el primer número de teléfono y el PIN requeridos se almacenan en una base de datos del centro de servicio 10 en una disposición mutuamente relacionada.

- 30 Una vez adquirido el primer número de teléfono del dispositivo móvil 14, como resultado el centro de servicio 10 puede establecer una conexión con el dispositivo móvil 14 a través de la red de telefonía móvil. Por tanto, enviando la solicitud de descarga al centro de servicio 10 a través del navegador, es posible transferir el programa de aplicación cliente desde el centro de servicio 10 al dispositivo móvil 14.

En una realización modificada de la presente invención, el programa de aplicación cliente puede ser descargado desde el mismo centro de servicio 10 mediante la transmisión de la solicitud de descarga correspondiente al centro de servicio 10 a través de un mensaje SMS que incluye un enlace especial.

- 35 En otras realizaciones modificadas de la presente invención se consideran otras tecnologías para la distribución del programa de aplicación cliente, como el WapProvisioning u otros mecanismos de distribución inalámbrica (*Over-The-Air* - OTA).

En todos los casos, el programa de aplicación cliente se instalará automáticamente al final del proceso de transferencia de datos en el dispositivo móvil 14.

- 40 Una vez concluido dicho procedimiento de instalación automática, el programa de aplicación cliente copiará automáticamente el primer código IMSI incluido en la primera tarjeta telefónica SIM 16 en un primer segmento 30 de la memoria o del soporte de almacenamiento de datos 18 del dispositivo móvil 14.

- 45 Sin embargo, la señal de instrucción encriptada que puede llegar al dispositivo móvil 14 desde el centro de servicio 10 por el momento es ignorada, aun estando el programa de aplicación cliente correctamente instalado. De hecho, el sistema de gestión de dispositivos móviles debe activarse por medio de una rutina de activación que se describe más abajo.

- 50 El usuario final envía la solicitud de activación al centro de servicio 10 a través del navegador. En consecuencia, desde el centro de servicio 10 se envía automáticamente una señal de activación al dispositivo móvil 14. Esta señal de activación está encriptada con una clave rastreable y recuperable por el programa de aplicación cliente, de modo que éste puede descifrar dicha señal.

La señal de activación descriptada resultante proporciona el código IMEI previamente almacenado en la base de datos del centro de servicio 10 en una forma encriptada que puede ser desbloqueada mediante el código PIN y una clave criptográfica generada en el centro de servicio 10. Esta clave criptográfica es única para cada dispositivo móvil 14 individual.

- 5 Después se pide al usuario final que introduzca el PIN en un campo de una ventana de diálogo que puede visualizarse en la pantalla 22 del dispositivo móvil 14 para posibilitar el descriptado del código IMEI. Esta solicitud de introducir en primer lugar el PIN está destinada básicamente a evitar una activación fraudulenta o una activación sin el consentimiento previo del usuario final.

- 10 A continuación, el programa de aplicación cliente adquiere el código IMEI almacenado en el dispositivo móvil 14 por el fabricante y lo compara con el código IMEI descriptado a través del PIN. Si los dos códigos son iguales, la clave criptográfica se almacena en un segundo segmento 32 del soporte de almacenamiento 18 y en una ventana de diálogo de la pantalla 22 se visualiza un mensaje que confirma la activación. Además, el dispositivo móvil 14 transmite al centro de servicio 10 una señal de activación satisfactoria encriptada con la clave criptográfica recién almacenada en memoria.
- 15 Esta señal de activación satisfactoria incluye algunas características del dispositivo móvil 14, por ejemplo el primer código IMSI, el tipo y la versión del sistema operativo, la provisión de un GPS, la provisión de una cámara fotográfica, el estado de la batería, el estado de la memoria y similares, confirmando así de que la señal de activación se ha ejecutado correctamente.

- 20 De aquí en adelante, la clave criptográfica es utilizada tanto por el programa de aplicación cliente residente en el dispositivo móvil 14, para encriptar y descriptar todas las señales transmitidas a y recibidas por el centro de servicio 10 a través de la red de radio móvil, como por el centro de servicio remoto 10 para encriptar y descriptar todas las señales transmitidas a y recibidas por el dispositivo móvil 14 a través de la misma red de radio móvil.

- 25 Por tanto, la seguridad de las comunicaciones en el canal de radio está asegurada gracias a que el protocolo de comunicación está encriptado con una clave criptográfica diferente para cada dispositivo móvil 14 individual. En particular, es prácticamente imposible transmitir una señal de instrucción al dispositivo móvil 14 si se desconoce la clave criptográfica correspondiente.

Por lo demás, si el código IMEI almacenado en el dispositivo móvil 14 por el fabricante es diferente al código IMEI descriptado a través del PIN, el procedimiento de activación falla a la vez que se visualiza un mensaje de aviso correspondiente en la ventana de diálogo de la pantalla 22.

- 30 Todos los mensajes de activación que probablemente entrarían después del primero son rechazados automáticamente, de modo que no será posible cambiar la clave criptográfica almacenada en el segundo segmento del soporte de memoria 18.

En otra realización modificada de la presente invención está previsto que el usuario final pueda transmitir la solicitud de activación al centro de servicio 10 desde el dispositivo móvil 14, permaneciendo inalterado el procedimiento que se debe seguir a continuación.

- 35 La Figura 4 ilustra esquemáticamente el diagrama de flujo del proceso de gestión para un dispositivo móvil 14 que ha sido activado de acuerdo con el procedimiento de activación arriba descrito y que, por tanto, puede ser controlado por el usuario final.

- 40 Desde la estación de trabajo 12, el usuario final puede visualizar en la pantalla la página web del portal proporcionado por el centro de servicio 10 para poder introducir el código de acceso de servicio en la máscara correspondiente y enviarlo al centro de servicio 10 a través del navegador.

- 45 A continuación, el usuario final puede visualizar dentro del navegador otra página web del portal proporcionado por el centro de servicio 10. Esta otra página web incluirá múltiples tareas y operaciones alternativas seleccionables para la gestión del dispositivo móvil 14. Estas tareas de gestión pueden incluir, por ejemplo, la cancelación o la copia de seguridad de los datos contenidos en el dispositivo móvil 14, el bloqueo y el desbloqueo del dispositivo móvil 14, la ejecución de aplicaciones en el dispositivo móvil 14, etc., es decir, todas las tareas necesarias para controlar, comprobar y gestionar por completo el dispositivo móvil 14.

Además, está prevista una tarea para desactivar el dispositivo móvil 14. En este caso particular, la clave criptográfica almacenada en el segundo segmento 32 del soporte de memoria 18 se cancela cuando el programa de aplicación cliente interpreta una señal de instrucción de desactivación.

- 50 Adicionalmente están previstos algunos modos de función que deben ser ejecutados de forma automática si la primera tarjeta SIM telefónica 16 es sustituida por una segunda tarjeta SIM telefónica 20 (Figura 6) dentro del dispositivo móvil 14, tal como se describirá con mayor detalle más abajo.

Por tanto, el usuario final puede enviar la tarea seleccionada al centro de servicio 10 a través del navegador. En caso de un modo de gestión normal, el centro de servicio 10 transmitirá después al dispositivo móvil 14 una señal de instrucción encriptada asociada a la tarea de gestión seleccionada. En caso de un modo de gestión automática relacionado con una sustitución de la tarjeta SIM telefónica, el centro de servicio 10 sólo transmitirá la señal de instrucción encriptada al dispositivo móvil 14 cuando se produzca el evento.

Debido al estándar de comunicación por radio móvil particular utilizado entre el centro de servicio 10 y el dispositivo móvil 14 de acuerdo con la presente invención, la señal de instrucción encriptada se puede definir como asíncrona. De hecho, puede ser ejecutada en el dispositivo móvil en un momento posterior al envío de la solicitud real de la tarea de gestión deseada.

El dispositivo móvil 14 recibe la señal de instrucción encriptada de forma silenciosa e invisible, sin que el propio dispositivo móvil 14 emita ninguna señal acústica relacionada ni ninguna señal de cualquier otro tipo. Esta característica puede resultar bastante útil, por ejemplo en caso de robo. De hecho, el usuario final puede iniciar una acción para bloquear el dispositivo móvil 14 robado desde su propia estación de trabajo 12 sin que esta acción pueda ser reconocida como tal hasta haber sido ejecutada por completo.

Después, el programa de aplicación cliente adquiere la señal de instrucción encriptada. Como resultado, el programa de aplicación cliente, en comunicación con el sistema operativo, descripta dicha señal con la clave criptográfica, la interpreta y la ejecuta.

Esta acción puede ser notificada al usuario final. Para ello, el dispositivo móvil 14 transmite automáticamente el código de control al centro de servicio 10. A continuación, el centro de servicio 10 envía un mensaje correspondiente, por ejemplo en forma de correo electrónico o SMS, a una dirección de correo electrónico o a un número de teléfono móvil predefinidos, según el caso.

El sistema de gestión de un dispositivo móvil de acuerdo con la presente invención está configurado para poder detectar influencias que tienen lugar en el dispositivo móvil 14 o alteraciones que afectan a éste, e iniciar automáticamente rutinas correctoras o de servicio apropiadas en respuesta a ello. Más particularmente, el programa de aplicación cliente incluye procedimientos adicionales que inician un proceso en el que varias partes del sistema de gestión de dispositivos móviles pueden llevar a cabo una secuencia de tareas destinadas a detectar una sustitución de la tarjeta SIM telefónica dentro del dispositivo móvil 14.

Con referencia a las Figuras 5 y 6, cada vez que se conecta el dispositivo móvil 14 se adquiere el código IMSI almacenado en la tarjeta SIM telefónica insertada en el dispositivo móvil 14 y después se compara con el primer código IMSI que ha sido previamente almacenado en el primer segmento 30 del soporte de memoria 18. Si dicha comparación indica que los dos códigos son iguales, esto significa que la primera tarjeta SIM telefónica 16 no ha sido sustituida en el dispositivo móvil 14 y el proceso iniciado para detectar una sustitución de la primera tarjeta SIM telefónica 16 finaliza.

Por el contrario, si dicha comparación indica que los dos códigos son diferentes entre sí, esto significa que la primera tarjeta SIM telefónica 16 ha sido sustituida en el dispositivo móvil 14 por una segunda tarjeta SIM telefónica 20. Como resultado, el dispositivo móvil 14 envía al centro de servicio una señal de cambio de SIM encriptada que contiene el código IMEI del dispositivo móvil 14. Dicha señal de cambio de SIM lleva asociado un segundo número de teléfono correspondiente a la segunda tarjeta SIM telefónica 20. Por tanto, tal como se deduce por la propiedad transitiva, el código IMEI está asociado al segundo número de teléfono.

Sin embargo, en la base de datos del centro de servicio 10, el código IMEI seguirá correspondiendo al número de teléfono relacionado con la primera tarjeta SIM telefónica 16, que ya no se utiliza más. Como consecuencia, el sistema de gestión del dispositivo móvil debe actualizarse para que pueda reconocer cuál es el número de teléfono actual al que se deben enviar las señales de instrucción encriptadas.

Por tanto, en el centro de servicio se almacena ahora el segundo número de teléfono relacionado a la segunda tarjeta SIM telefónica 20 en lugar del primer número de teléfono relacionado con la primera tarjeta SIM telefónica 16.

De modo similar, en el dispositivo móvil 14, el primer segmento 30 del soporte de almacenamiento 18 que contiene el primer código IMSI de la primera tarjeta SIM telefónica 16 es sustituido por un segundo código IMSI de la segunda tarjeta SIM telefónica 20.

Una vez concluido el procedimiento de actualización en el centro de servicio 10, el centro de servicio 10 transmite automáticamente al dispositivo móvil 14 una señal de instrucción encriptada que lleva asociada la tarea de gestión previamente seleccionada por el usuario final.

Dichas tareas de gestión pueden incluir, por ejemplo, el bloqueo por defecto del dispositivo móvil 14, la cancelación de datos introducidos o la notificación arriba mencionada por envío de un correo electrónico o un SMS a una dirección de correo electrónico o a un número de teléfono móvil predefinidos respectivamente, permitiendo así que el usuario final

decida qué acción debe ejecutar en ese momento conforme a lo previsto por la gestión de las señales para el dispositivo móvil de acuerdo con la presente invención.

La sustitución de la tarjeta SIM telefónica puede ser notificada al usuario final con un procedimiento similar al utilizado para notificar la ejecución de la instrucción en el dispositivo móvil 14, por lo que se omite su descripción adicional.

- 5 En un tercer segmento 34 del soporte de almacenamiento 18 está almacenada una lista de tarjetas SIM de teléfono que, si se insertan en el dispositivo móvil 14, no dan lugar a una activación del procedimiento de cambio de tarjeta SIM telefónica arriba descrito. Por consiguiente, dicho procedimiento de cambio de tarjeta SIM sólo se iniciará si se inserta una tarjeta SIM telefónica cuyo código IMSI no está incluido en la lista almacenada en memoria. Esta lista se actualiza a través de una señal de instrucción encriptada enviada por el centro de servicio 10, que está provista de la lista actualizada. Dicha instrucción también puede emplearse para gestionar cambios de tarjeta SIM de teléfono realizados de forma intencionada.

- 15 La anterior descripción muestra de forma totalmente evidente que el método para la gestión remota de dispositivos móviles y el dispositivo móvil adecuado para dicho método de acuerdo con la presente invención permiten lograr los objetivos y ventajas arriba indicados. De hecho, se ha concebido un método para la gestión remota de dispositivos móviles y un dispositivo móvil adecuado para dicho método con los que el usuario final tiene plena capacidad para gestionar y controlar su propio dispositivo móvil 14 desde una estación de trabajo 12 en un modo de operación de autoservicio. Además, el sistema puede detectar automáticamente influencias o alteraciones que se producen en el dispositivo móvil 14, lo que a su vez provoca la ejecución de rutinas de servicio apropiadas en respuesta, con el fin de activar la funcionalidad de gestión de dispositivos móviles preestablecida por el usuario final, como es el caso de una sustitución de la tarjeta SIM telefónica.

- 20 De cualquier modo se entenderá que tanto el método como el dispositivo de acuerdo con la presente invención pueden ser sometidos a una serie de modificaciones destinadas a una serie de aplicaciones diferentes, y pueden ser realizados de diferentes maneras sin salirse del alcance de la presente invención, y que las diversas realizaciones y variantes de los mismos, tal como se describen más arriba, pueden ser utilizadas tanto de forma individual como en cualquier combinación de las mismas.

REIVINDICACIONES

1. Método para la gestión remota de dispositivos móviles, que incluye los siguientes pasos:

- transmitir un código de acceso desde una estación de trabajo (12) a un centro de servicio (10), estando dicha estación de trabajo (12) y dicho centro de servicio (10) interconectados con una red telemática;
- 5 – comprobar la autenticidad del código de acceso en el centro de servicio (10);
- transmitir los datos personales de un usuario final desde la estación de trabajo (12) al centro de servicio (10);
- almacenar dichos datos personales en una memoria en el centro de servicio (10);
- 10 – seleccionar un tipo deseado de dispositivo móvil y enviar dicho tipo seleccionado de dispositivo móvil desde la estación de trabajo (12) al centro de servicio (10);
- transmitir un código de identificación unívoco almacenado en un dispositivo móvil (14) por el fabricante, un primer número de teléfono y una contraseña personal desde la estación de trabajo (12) al centro de servicio (10), estando provisto dicho dispositivo móvil (14) de una primera tarjeta SIM telefónica activada (16) y estando dicho primer número de teléfono asociado a dicha primera tarjeta SIM telefónica activada (16);
- 15 – almacenar en una memoria en el centro de servicio (10) dicho código de identificación unívoco almacenado en el dispositivo móvil (14), el primer número de teléfono y la contraseña personal, estando asociados entre sí dicho código de identificación unívoco almacenado en el dispositivo móvil (14), dicho primer número de teléfono y dicha contraseña personal;
- enviar una solicitud desde la estación de trabajo (12) al centro de servicio (10) para descargar un programa de aplicación cliente en el dispositivo móvil (14);
- 20 – descargar e instalar el programa de aplicación cliente desde el centro de servicio (10) en el dispositivo móvil (14), siendo dicho programa de aplicación cliente autoinstalable;
- copiar en el dispositivo móvil (14) un primer código IMSI contenido en una primera tarjeta SIM telefónica (16), en un primer segmento (30) de un soporte de almacenamiento (18) del dispositivo móvil (14);
- 25 – enviar una solicitud para activar el dispositivo móvil (14) desde la estación de trabajo (12) al centro de servicio (10);
- transmitir una señal de activación encriptada en un primer modo de encriptado desde el centro de servicio (10) al dispositivo móvil (14), incluyendo dicha señal una clave criptográfica y un código de identificación unívoco encriptado correspondiente al código de identificación unívoco previamente almacenado en dicho centro de servicio (10) encriptado en un segundo modo de encriptado, y estando dicho dispositivo móvil (14) interconectado con la red telemática;
- 30 – descryptar la señal de activación encriptada a través del programa de aplicación cliente en el dispositivo móvil (14) y extraer dicha clave criptográfica y dicho código de identificación unívoco encriptado;
- descryptar dicho código de identificación unívoco encriptado mediante la introducción de la contraseña personal en el dispositivo móvil (14) para obtener un código de identificación unívoco descryptado;
- 35 – comparar en el dispositivo móvil (14) dicho código de identificación unívoco descryptado con dicho código de identificación unívoco almacenado en el dispositivo móvil (14);
- almacenar la clave criptográfica en el dispositivo móvil (14), en un segundo segmento (42) del soporte de almacenamiento (18), cuando dicho código de identificación unívoco descryptado es igual a dicho código de identificación unívoco almacenado en el dispositivo móvil (14); y
- 40 – transmitir desde el dispositivo móvil (14) al centro de servicio (10) una señal de activación satisfactoria que está encriptada con la clave criptográfica y que incluye algunas características del dispositivo móvil (14);
- comprobar la señal de activación satisfactoria en el centro de servicio (10);
- 45 – controlar el dispositivo móvil (14) desde la estación de trabajo (12), siendo activado dicho dispositivo móvil (14).

2. Método para la gestión remota de dispositivos móviles según la reivindicación 1, caracterizado porque el control del dispositivo móvil (14) incluye los siguientes pasos:

- transmitir el código de acceso desde la estación de trabajo (12) al centro de servicio (10);
- comprobar la autenticidad del código de acceso en el centro de servicio (10);
- 50 – seleccionar una tarea de gestión del dispositivo móvil (14) y envío de la tarea de gestión seleccionada desde la estación de trabajo (12) al centro de servicio (10);
- transmitir una señal de instrucción encriptada con la clave criptográfica desde el centro de servicio (10) al dispositivo móvil (14), estando asociada dicha señal de instrucción con dicha tarea de gestión del dispositivo móvil (14);
- 55 – descryptar la señal de instrucción encriptada en el dispositivo móvil (14) con la clave criptográfica;
- interpretar y ejecutar automáticamente la señal de instrucción en el dispositivo móvil (14), realizando así la tarea de gestión del dispositivo móvil (14).

3. Método para la gestión remota de dispositivos móviles según la reivindicación 2, caracterizado porque una señal de instrucción encriptada con la clave criptográfica está asociada con una tarea de gestión del dispositivo móvil (14) que se debe ejecutar automáticamente cuando en el dispositivo móvil (14) se produce una sustitución de una primera tarjeta SIM telefónica (16) por una segunda tarjeta SIM telefónica (20).
- 5 4. Método para la gestión remota de dispositivos móviles según la reivindicación 3, caracterizado porque la detección de la sustitución de la tarjeta SIM telefónica incluye los siguientes pasos:
 - comparar en el dispositivo móvil (14) el código IMSI almacenado en el primer segmento (30) del soporte de memoria (18) al conectar el dispositivo móvil (14) con un segundo código IMSI incluido en la segunda tarjeta SIM telefónica (20);
 - 10 – comprobar en el dispositivo móvil (14) si el código IMSI almacenado en el primer segmento (30) del soporte de memoria (18) es diferente al segundo código IMSI incluido en la segunda tarjeta SIM telefónica (20);
 - transmitir una señal de cambio de tarjeta SIM, encriptada con la clave criptográfica, desde el dispositivo móvil (14) al centro de servicio (10), incluyendo dicha señal el código de identificación unívoco del dispositivo móvil (14) y estando ésta asociada a un segundo número de teléfono asociado con dicha
 - 15 segunda tarjeta SIM telefónica (20);
 - sustituir en el centro de servicio (10) el primer número de teléfono asociado a la primera tarjeta SIM telefónica (16) por el segundo número de teléfono asociado a dicha segunda tarjeta SIM telefónica (20), estando asociados tanto dicho primer número de teléfono como dicho segundo número de teléfono con el código de identificación unívoco del dispositivo móvil (14);
 - 20 – sustituir en el dispositivo móvil (14) el primer código IMSI de la primera tarjeta SIM telefónica (16) por el segundo código IMSI de la segunda tarjeta SIM telefónica (20) en el primer segmento (30) del soporte de memoria (18);
 - transmitir desde el centro de servicio (10) la señal de instrucción encriptada con la clave criptográfica asociada al modo de gestión preestablecido del dispositivo móvil (14) en la forma prevista para la
 - 25 sustitución de la primera tarjeta SIM telefónica (16) por la segunda tarjeta SIM telefónica (20);
 - desencriptar la señal de instrucción encriptada con la clave criptográfica en el dispositivo móvil (14);
 - interpretar y ejecutar automáticamente la señal de instrucción en el dispositivo móvil (14), ejecutando así la tarea de gestión del dispositivo móvil (14).
- 30 5. Método para la gestión remota de dispositivos móviles según cualquiera de las reivindicaciones anteriores, caracterizado porque el código de acceso que incluye un código de identificación, una contraseña y un código de control está disponible al menos en uno de los modos de distribución que incluyen una transmisión en línea, el uso de una tarjeta física o una forma soportada en un medio, estando adaptado dicho código de acceso para permitir un acceso protegido al centro de servicio (10).
- 35 6. Método para la gestión remota de dispositivos móviles según cualquiera de las reivindicaciones anteriores, caracterizado porque las señales intercambiadas entre el centro de servicio (10) y el dispositivo móvil (14) están encapsuladas siguiendo un estándar de comunicación por radio móvil asíncrona.
7. Método para la gestión remota de dispositivos móviles según la reivindicación 6, caracterizado porque las señales intercambiadas entre el centro de servicio (10) y el dispositivo móvil (14) son conforme al estándar de Servicio de Mensajes Cortos (SMS - *Short Message Service*).
- 40 8. Método para la gestión remota de dispositivos móviles según cualquiera de las reivindicaciones anteriores, caracterizado porque las señales intercambiadas entre el centro de servicio (10) y el dispositivo móvil (14) están encriptadas con la clave criptográfica, siendo dicha clave criptográfica única para cada dispositivo móvil (14) individual.
- 45 9. Método para la gestión remota de dispositivos móviles según la reivindicación 1, caracterizado porque el dispositivo móvil (14) envía la solicitud para descargar el programa de aplicación cliente a través de un SMS que incluye un enlace.
10. Método para la gestión remota de dispositivos móviles según la reivindicación 1, caracterizado porque el programa de aplicación cliente es distribuido en el dispositivo móvil (14) utilizando un mecanismo de distribución inalámbrico.
- 50 11. Método para la gestión remota de dispositivos móviles según la reivindicación 1, caracterizado porque después de comprobar la señal de activación satisfactoria en el centro de servicio (10) se visualiza un mensaje de activación satisfactoria.

12. Método para la gestión remota de dispositivos móviles según la reivindicación 1, caracterizado porque una solicitud de activación del dispositivo móvil (14) se ignora en un dispositivo móvil (14) ya activado.
13. Método para la gestión remota de dispositivos móviles según la reivindicación 1, caracterizado porque la solicitud de activación es enviada por el dispositivo móvil (14).
- 5 14. Método para la gestión remota de dispositivos móviles según cualquiera de las reivindicaciones anteriores, caracterizado porque las tareas de gestión de dispositivos móviles incluyen un bloqueo por defecto del dispositivo móvil (14), un desbloqueo del dispositivo móvil (14), una cancelación de datos introducidos en el dispositivo móvil (14), una copia de seguridad de datos en el dispositivo móvil (14), un mensaje de sustitución de la tarjeta SIM telefónica (16) a través del envío de un correo electrónico a una dirección de correo electrónico, un
10 mensaje de la sustitución de la tarjeta SIM telefónica (16) a través del envío de un SMS a un número de teléfono.
15. Método para la gestión remota de dispositivos móviles según la reivindicación 14, caracterizado porque las tareas de gestión de dispositivos móviles incluyen además un modo para desactivar el dispositivo móvil (14), que se encarga de cancelar la clave criptográfica almacenada en el segundo segmento (32) de la memoria.
- 15 16. Método para la gestión remota de dispositivos móviles según la reivindicación 2, caracterizado porque la ejecución de una instrucción en el dispositivo móvil (14) se notifica a través de los siguientes pasos:
 - transmisión automática del código de control desde el dispositivo móvil (14) al centro de servicio (10);
 - envío de al menos un correo electrónico a una dirección de correo preestablecida y/o de al menos un SMS desde el centro de servicio (10) a un número de teléfono preestablecido.
- 20 17. Método para la gestión remota de dispositivos móviles según las reivindicaciones 4 y 16, caracterizado porque se notifica una sustitución de la tarjeta SIM (16).
18. Método para la gestión remota de dispositivos móviles según la reivindicación 4, caracterizado porque en un tercer segmento (34) del soporte de memoria (18) está almacenada una lista de tarjetas SIM ignoradas por la detección de la sustitución de la tarjeta SIM telefónica, pudiendo ser actualizada dicha lista desde el centro de servicio (10).
- 25 19. Método para la gestión remota de dispositivos móviles según cualquiera de las reivindicaciones anteriores, caracterizado porque el dispositivo móvil (14) recibe de forma silenciosa las señales de instrucción encriptadas.
20. Método para la gestión remota de dispositivos móviles según cualquiera de las reivindicaciones anteriores, caracterizado porque el programa de aplicación cliente no es visible en la lista de aplicaciones instaladas en el dispositivo móvil (14).
- 30 21. Dispositivo móvil para llevar a cabo el método para la gestión remota de dispositivos móviles según cualquiera de las reivindicaciones anteriores, caracterizado porque incluye medios adaptados para descryptar una señal de instrucción encriptada transmitida por un centro de servicio (10) y medios adaptados para interpretar dicha señal de instrucción descryptada y ejecutar dicha instrucción.
- 35 22. Dispositivo móvil según la reivindicación 21, caracterizado porque una clave criptográfica para encriptar y descryptar señales se almacena en un segmento (32) de un soporte de almacenamiento (18) durante la activación, siendo generada dicha clave criptográfica de un modo único por el centro de servicio (10).

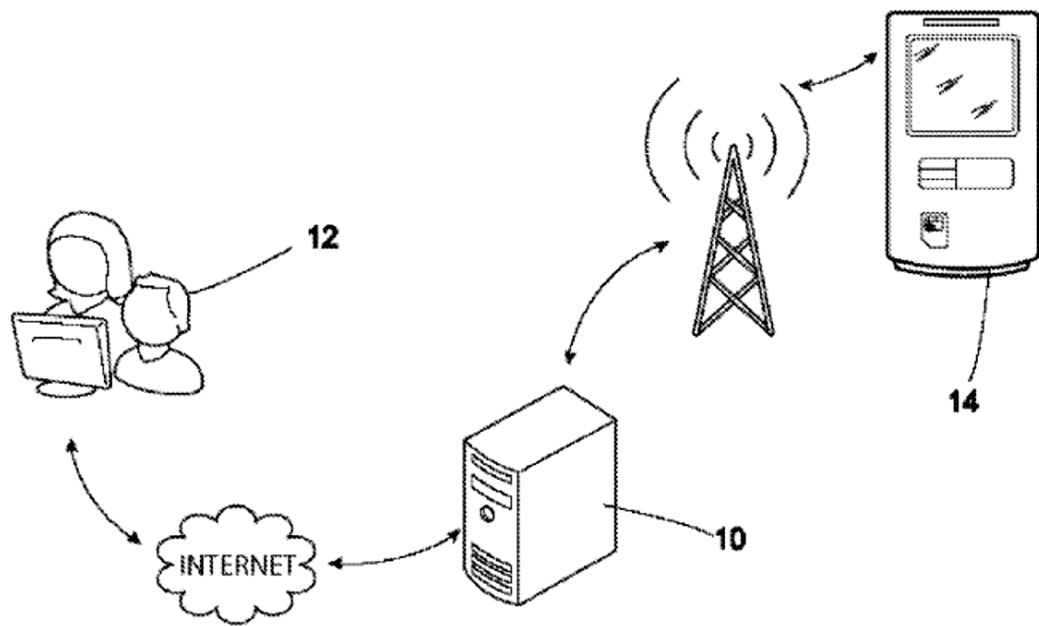


FIG. 1

Interpretador de Instrucciones (encriptado/desencriptado)			
Ejecución de Instrucción de Información	Ejecución de Instrucción de Borrado	Ejecución de Instrucción de Bloqueo/	Ejecución de Instrucción de cambio de tarjeta SIM
Sistema Operativo del Dispositivo			

Fig. 2

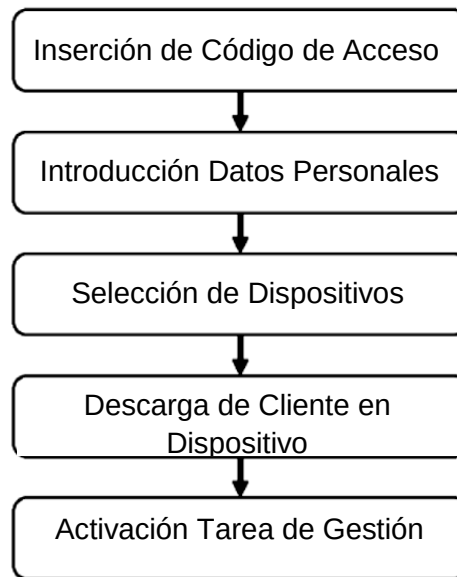


FIG. 3

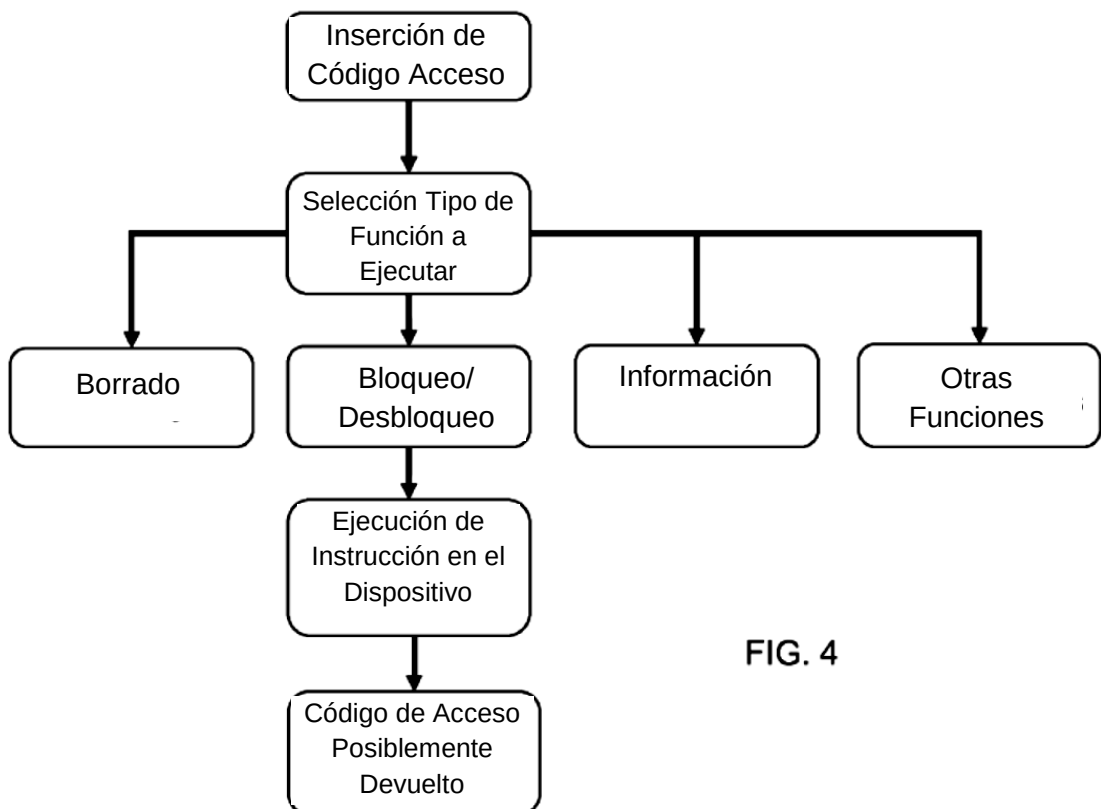


FIG. 4

