(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 390 507**

(51) Int. CI.:
H04L 29/06 (2006.01)
H04L 12/22 (2006.01)
H04W 12/08 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **08155575 .7**
(96) Fecha de presentación: **02.05.2008**
(97) Número de publicación de la solicitud: **2114051**
(97) Fecha de publicación de la solicitud: **04.11.2009**

(54) Título: **Sistemas y métodos de seguridad coordinados para un dispositivo electrónico**

(45) Fecha de publicación de la mención BOPI:
13.11.2012

(45) Fecha de la publicación del folleto de la patente:
13.11.2012

(73) Titular/es:
RESEARCH IN MOTION LIMITED (100.0%)
295 Phillip Street
Waterloo, Ontario N2L 3W8 , CA

(72) Inventor/es:
OULD, CHRISTOPER

(74) Agente/Representante:
DE ELZABURU MÁRQUEZ, Alberto

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

Sistemas y métodos de seguridad coordinados para un dispositivo electrónico.

Campo técnico

Las realizaciones descritas en la presente memoria se refieren generalmente al funcionamiento de una característica o características de seguridad existentes en dispositivos electrónicos y, más particularmente, en dispositivos electrónicos móviles.

Antecedentes

Los dispositivos electrónicos móviles están a menudo equipados con una tarjeta inteligente tal como una tarjeta de Módulo de Identidad de Abonado, o "SIM" ("Subscriber Identity Module") con el fin de enviar y recibir señales de comunicaciones (tales como una llamada de telefonía celular). Típicamente, tales tarjetas de SIM requieren procedimientos de registro y activación de red que implican el uso de palabras de paso. Similarmente, el uso de palabras de paso o de otras características de seguridad puede emplearse para limitar o restringir el acceso a la capacidad funcional de la tarjeta de SIM.

Adicionalmente, algunos dispositivos electrónicos también proporcionan una capacidad funcional de aplicación que es independiente de la tarjeta de SIM. Por ejemplo, algunos dispositivos incluyen aplicaciones de dispositivo que proporcionan la capacidad funcional de libro de direcciones, la capacidad funcional de planificación en el tiempo y de calendario, videojuegos, toma de fotografías con cámara digital y su visionado, y presentaciones multimedia, entre otras. A menudo, tales aplicaciones implican el almacenamiento y el uso de datos o contenido de usuario. El acceso a estas aplicaciones, funciones y datos de usuario está, por lo común, restringido o regulado mediante el uso de palabras de paso u otras características de seguridad.

En el caso de que un usuario no autorizado se haga con el dispositivo e introduzca una palabra de paso no válida en el dispositivo (a menudo al usuario se le dan múltiples oportunidades para introducir una palabra de paso válida), las características de seguridad impiden o restringen de otro modo el acceso a los datos de usuario y pueden impedir un uso adicional de las aplicaciones o la capacidad funcional del dispositivo.

El documento WO 2007/110094 A divulga un sistema para hacer valer políticas o criterios de seguridad en dispositivos de comunicaciones móviles configurados para ser utilizados en una red de comunicaciones móviles, en asociación operativa con un módulo de identidad de abonado. El sistema, que tiene una arquitectura o estructura de cliente-servidor, comprende un servidor que se hace funcionar por parte de un operador de red de comunicaciones móviles y un cliente residente en un dispositivo de comunicaciones móviles en el que se han de hacer valer los criterios de seguridad. El servidor está configurado para determinar criterios de seguridad que se han de aplicar en dicho dispositivo de comunicaciones móviles, y para enviar al mismo un criterio de seguridad que se ha de aplicar. El cliente se ha configurado para recibir el criterio de seguridad que se ha de aplicar desde el servidor, y para aplicar el criterio de seguridad recibido. El servidor incluye una función de autentificación de servidor, configurada para autentificar el criterio de seguridad que se va a enviar al dispositivo de comunicaciones móviles; el cliente está configurado, de manera adicional, para establecer la autenticidad del criterio de seguridad recibido desde el servidor, aprovechando una función de autentificación de cliente residente en el módulo de identidad de abonado.

Breve descripción de los dibujos

Para una mejor comprensión de las realizaciones que se describen en la presente memoria, y para mostrar más claramente el modo como pueden llevarse a efecto, se hará referencia a continuación, a modo de ejemplo, a los dibujos que se acompañan, en los cuales:

La Figura 1 es un diagrama de bloques de un dispositivo móvil en un ejemplo de realización práctica;
La Figura 2 es un diagrama de bloques de un componente de subsistema de comunicación del dispositivo móvil de la Figura 1;
La Figura 3 es un diagrama de bloques de un nodo de una red inalámbrica;
La Figura 4 es un diagrama de bloques que ilustra componentes de un sistema anfitrión o principal, en una configuración a modo de ejemplo; y
La Figura 5 es un diagrama de flujo que ilustra las etapas de un método de coordinación de sistemas de seguridad d de un dispositivo informático, de acuerdo con al menos una realización.

Descripción detallada

Si bien ciertas realizaciones de dispositivos electrónicos móviles existentes hacen posible la inhabilitación de las aplicaciones del dispositivo al recibir una palabra de paso válida, el presente Solicitante ha constatado que la tarjeta de SIM puede permanecer sin afectar. Como resultado de ello, un ladrón del dispositivo puede tener la posibilidad de seguir utilizando la capacidad funcional de comunicación hasta que se le notifique a los administradores de la red de

comunicación y se bloquee la tarjeta de SIM impidiendo su acceso a la red, o se desactive de otro modo.

Por otra parte, el presente Solicitante ha apreciado también que, además de las tarjetas de SIM, pueden utilizarse otros tipos de tarjetas de comunicación en aplicaciones de dispositivos electrónicos móviles. De acuerdo con ello, a modo de ejemplo únicamente, otros tipos de tarjetas de comunicación que pueden utilizarse pueden incluir un R-UIM (módulo de identidad de usuario extraíble –"removable user identity module") o un CSIM (módulo de identidad de abonado de CDMA (acceso múltiple por división de código –"code division multiple access") o de CDMA 2000 ("CDMA or CDMA 2000 subscriber identity module")) o una tarjeta de USIM (módulo de identidad de abonado universal –"universal subscriber identity module").

Realizaciones que se describen en esta memoria están generalmente dirigidas a un sistema y a un método que coordinan dos o más medidas u operaciones de seguridad típicamente independientes de un dispositivo electrónico tal como, por ejemplo, un sistema de comunicaciones móviles. En particular, la activación de una primera medida de seguridad puede disparar o desencadenar la activación de una segunda medida de seguridad.

En un aspecto amplio, se proporciona un método para implementar una característica de seguridad de un dispositivo electrónico, de tal manera que el método comprende: detectar un intento de acceso no válido; iniciar, en respuesta a dicha detección, una primera operación de seguridad para impedir el acceso a, o inhabilitar, una entidad, datos, aplicación o función asociada con dicho dispositivo, y disparar o desencadenar un intento no válido para acceder a otra entidad, datos, aplicación o función asociada con dicho dispositivo, a fin de iniciar una segunda operación de seguridad para impedir el acceso a, o inhabilitar, dicha otra entidad, datos, aplicación o función.

La detección del intento de acceso no válido puede llevarse a cabo por un primer módulo de seguridad.

La etapa de detectar un intento de acceso no válido puede ser iniciada mediante la recepción de un mensaje que comprende instrucciones de control. El mensaje que comprende instrucciones de control puede ser recibido desde un administrador de red.

La primera operación de seguridad puede desencadenar el intento de acceso no válido a dicha otra entidad, datos, aplicación o función asociada con dicho dispositivo.

La segunda operación de seguridad puede comprender impedir el acceso a, o inhabilitar, dicha otra entidad que comprende un dispositivo o un componente que se comunica con, se conecta a, o se inserta en, dicho dispositivo electrónico. La entidad puede ser otro dispositivo de red vinculado al dispositivo electrónico mediante una conexión de red inalámbrica o por conducción de cable, o mediante una conexión local tal como un cable de Bus en Serie Universal. La entidad puede comprender un dispositivo o componente que es susceptible de insertarse en el dispositivo electrónico, y puede extraer o desviar potencia de dicho dispositivo electrónico.

La segunda operación de seguridad puede comprender inhabilitar la capacidad funcional de una entidad que comprende una tarjeta de comunicación del dispositivo electrónico, tal como una tarjeta de SIM u otra tarjeta, que habilite conexiones de red inalámbricas o por conducción de cable a otros dispositivos o aparatos de red similarmente habilitados.

La detección del intento de acceso no válido puede comprender recibir un código de autorización y determinar que el código de autorización no corresponde a datos de autorización previamente almacenados.

El disparo de un intento no válido para acceder a dicha otra entidad, datos, aplicación o función asociada con dicho dispositivo, puede comprender proporcionar a sabiendas un código o datos de autorización no válidos a un segundo módulo de seguridad asociado con dicha otra entidad, datos, aplicación o función. El método reside, generalmente, en detectar un intento no válido de acceder al dispositivo, datos existentes en el dispositivo, una función o aplicación llevada a cabo por el dispositivo, o incluso otro dispositivo o entidad conectada a, insertada en, o que se comunica con el dispositivo, y, en respuesta a la detección del intento de acceso no válido, invocar, esto es, desencadenar o poner en marcha, un procedimiento deliberado para provocar la inhabilitación de, o impedir el acceso a, otros datos, esto es, datos secundarios, existentes en el dispositivo, función o aplicación llevada a cabo por el dispositivo o incluso por aún otro dispositivo o entidad conectada a, insertada en, o que se comunica con el dispositivo. El procedimiento es deliberado hasta el punto de que se proporcionan datos de autorización que se sabe que son incorrectos, como los otros datos del dispositivo, función o aplicación llevada a cabo por el dispositivo, o incluso para aún otro dispositivo o entidad conectada a, insertada en, o en comunicación con el dispositivo. La invención resulta particularmente ventajosa cuando el procedimiento de inhabilitación o prevención de acceso adicional desencadenado se aplica a una entidad que es susceptible de insertarse en el dispositivo electrónico, con lo que este es inhabilitado o ve aplicadas en él medidas de prevención del acceso, de tal manera que, al extraerla del dispositivo electrónico o insertarla en un dispositivo similar, las medidas de inhabilitación o prevención del acceso se encuentran aún en vigor incluso cuando se hace funcionar en asociación con dicho dispositivo similar.

El código o datos de autorización no válidos pueden ser enviados a dicho segundo módulo de seguridad tantas veces como sea necesario para iniciar dicho segundo módulo de seguridad con el fin de impedir el acceso a, o

inhabilitar, dicha otra entidad, datos, aplicación o función. Esto puede comprender, por ejemplo, tres veces.

En otro aspecto amplio, se proporciona un dispositivo electrónico que comprende: un módulo para detectar un intento de acceso no válido; un primer módulo de seguridad acoplado con el módulo, de tal manera que el primer módulo de seguridad está configurado para, en respuesta a un intento de acceso no válido detectado, iniciar una primera operación de seguridad para impedir el acceso a, o inhabilitar, una entidad, datos, aplicación o función asociada con dicho dispositivo, así como para desencadenar un intento no válido para acceder a otra entidad, datos aplicación o función asociada con dicho dispositivo; y un segundo módulo de seguridad asociado con dicha otra entidad, datos, aplicación o función, de tal manera que dicho segundo módulo de seguridad está configurado para impedir el acceso a, o inhabilitar, dicha otra entidad, datos, aplicación o función en respuesta a dicho intento de acceso no válido desencadenado.

En otro aspecto amplio, se proporciona un medio legible por computadora que comprende instrucciones susceptibles de llevarse a cabo en un procesador de un dispositivo electrónico para hacer que dicho dispositivo electrónico implemente el método de la invención.

Estos y otros aspectos y características de diversas realizaciones se describirán con mayor detalle más adelante.

Algunas realizaciones descritas en la presente memoria hacen uso de una estación móvil. Una estación móvil es un dispositivo de comunicación bidireccional o en ambos sentidos con capacidades de comunicación de datos avanzadas, que tiene la capacidad de comunicarse con otros sistemas informáticos, y al que se hace también referencia en la presente memoria generalmente como dispositivo móvil. Un dispositivo móvil puede también incluir la capacidad para comunicaciones de voz. Dependiendo de la capacidad funcional proporcionada por un dispositivo móvil, puede hacerse referencia a él como un dispositivo de mensajería de datos, un localizador portátil o busca en ambos sentidos, un teléfono celular con capacidades de mensajería de datos, un aparato de Internet inalámbrico, o un dispositivo de comunicación de datos (con o sin capacidades de telefonía). Un dispositivo móvil se comunica con otros dispositivos a través una red de estaciones transmisoras-receptoras, o transceptoras.

Con el fin de ayudar al lector a comprender la estructura de un dispositivo móvil y el modo como se comunica con otros dispositivos, se hace referencia a las Figuras 1 a 3.

Refiriéndose, en primer lugar, a la Figura 1, se muestra en ella generalmente con la referencia 100 un diagrama de bloques de un dispositivo móvil en una implementación proporcionada a modo de ejemplo. El dispositivo móvil 100 comprende un cierto número de componentes, siendo el componente de control el microprocesador 102. El microprocesador 102 controla el funcionamiento global del dispositivo móvil 100. Las funciones de comunicación, incluyendo comunicaciones de datos y de voz, se llevan a cabo por medio del subsistema de comunicación 104. El subsistema de comunicación 104 recibe mensajes desde una red inalámbrica 200 y envía mensajes a esta. En esta implementación proporcionada a modo de ejemplo del dispositivo móvil 100, el subsistema de comunicación 104 se ha configurado de conformidad con las normas del Sistema Global para Comunicación Móvil (GSM –"Global System por Mobile Communication") y de los Servicios Generales de Radio en Paquetes (GPRS –"General Packet Radio Services"). La red inalámbrica de GSM / GPRS se utiliza en todo el mundo y se espera que estas normas puedan ser complementadas o, eventualmente, sustituidas por nuevas normas tales como el Entorno de GSM de Datos Mejorado (EDGE –"Enhanced Data GSM Environment") y el Servicio de Telecomunicaciones Móviles Universal (UMTS –"Universal Mobile Telecommunications Service"), el Acceso en Paquetes de Alta Velocidad (HSPA –"High-Speed Packet Access"), que puede incluir el Acceso en Paquetes de Enlace Descendente de Alta Velocidad (HSDPA –"High-Speed Downlink Packet Access"), y la Banda Ancha Ultramóvil (UMB –"Ultra Mobile Broadband"), etc. Se siguen definiendo nuevas normas, pero se cree que estas tendrán similitudes con el comportamiento de red que aquí se describe, y se comprenderá también por las personas expertas en la técnica que la invención está destinada a utilizar cualesquiera otras normas adecuadas que se desarrollen en el futuro. El enlace inalámbrico que conecta el subsistema de comunicación 104 con la red 200 representa un o más canales de Radiofrecuencia (FR) diferentes que funcionan de acuerdo con los protocolos definidos que se especifican para las comunicaciones de GSM / GPRS. Con los nuevos protocolos de red, estos canales son capaces de dar soporte tanto a comunicaciones de voz conmutadas en circuitos como a comunicaciones de datos conmutadas en paquetes.

Si bien la red inalámbrica asociada con el dispositivo móvil 100 es una red inalámbrica de GSM / GPRS en una implementación proporcionada a modo de ejemplo del dispositivo móvil 100, otras redes inalámbricas pueden ser también asociadas con el dispositivo móvil 100 en variantes de implementación. Diferentes tipos de redes inalámbricas que pueden emplearse incluyen, por ejemplo, redes inalámbricas centradas en datos, redes inalámbricas centradas en voz y redes de modo dual que pueden dar soporte tanto a comunicaciones de voz como a comunicaciones de datos a través de las mismas estaciones de base físicas. Redes de modo dual combinadas incluyen, pero no están limitadas por, redes de Acceso Múltiple por División en Código (CDMA –"Code Division Multiple Access"), o redes CDMA2000, redes Solo de Datos de Evolución (EV-DO –"Evolution Data Only"), redes de GSM / GPS (según se ha mencionado anteriormente), y redes de tercera generación (3G) y ulteriores, como la EDGE, UMTS y HSPA, etc. Algunos ejemplos más antiguos de redes centradas en datos incluyen la Red de Radio Mobitex™ y la Red de Radio DataTAC®. Ejemplos de redes de datos centradas en voz más antiguas incluyen las redes de Sistemas de Comunicación Personales (PCS –"Personal Communication Systems") como los sistemas

GSM y de Acceso Múltiple por División en el Tiempo (TDMA –“Time Division Multiple Access”).

El microprocesador 102 también interactúa con subsistemas adicionales tales como una Memoria de Acceso Aleatorio (RAM –“Random Access Memory”) 106m, una memoria de tipo flash o de acceso por impulsos, 108, un dispositivo de presentación visual 110, un subsistema de entrada / salida (E/S –“I/O (input / output)”) 112, un teclado 116, un altavoz 118, un micrófono 120, un subsistema de comunicaciones 122 de corto alcance, y otros subsistemas 124.

Algunos de los subsistemas del dispositivo móvil 100 llevan a cabo funciones relacionadas con la comunicación, en tanto que otros subsistemas pueden proporcionar funciones “residentes” o instaladas en el dispositivo. A modo de ejemplo, el dispositivo de presentación visual 110 y el teclado 116 pueden ser utilizados tanto para funciones relacionadas con la comunicación, tales como la introducción de un mensaje de texto para su transmisión a través de la red 200, como para funciones residentes o emplazadas en el dispositivo, tales como una calculadora o una lista de tareas. El software de sistema operativo utilizado por el microprocesador 102 es, por lo común, almacenado en un dispositivo de almacenamiento permanente tal como una memoria de acceso por impulsos, o del tipo flash, 108, que puede ser, alternativamente, una memoria de solo lectura (ROM –“read-only memory”) o un elemento de almacenamiento similar (no mostrado). Los expertos de la técnica apreciarán que el sistema operativo, aplicaciones específicas de dispositivo, o partes de los mismos, pueden cargarse temporalmente dentro de un dispositivo de almacenamiento volátil tal como una RAM 106.

El microprocesador 102, además de sus funciones de sistema operativo, hace posible la ejecución de aplicaciones de software en el dispositivo móvil 100. Un conjunto de aplicaciones que controlan operaciones de dispositivo básicas, incluyendo aplicaciones de comunicación de datos y voz, pueden instalarse en el dispositivo móvil 100 durante su fabricación. Otra aplicación que pude ser cargada en el dispositivo móvil 100 es un gestor de información personal (PIM –“personal information manager”). Un PIM tiene la capacidad funcional de organizar y gestionar elementos de datos de interés para un abonado, tales como correo electrónico, acontecimientos de calendario, correos o mensajes de voz, citas y elementos de tareas, aunque sin estar limitado por ellos. Una aplicación de PIM tiene la facultad de enviar y recibir elementos de datos a través de una red inalámbrica 200. Los elementos de datos de PIM pueden ser integrados sin discontinuidades, sincronizados y actualizados por medio de una red inalámbrica 200, de tal manera que los elementos de datos correspondientes del abonado del dispositivo móvil se almacenan y/o asocian con un sistema informático anfitrión o principal. Esta capacidad funcional crea una réplica de la computadora principal en el dispositivo móvil 100 con respecto a dichos elementos. Esto puede resultar particularmente ventajoso en el caso de que el sistema informático principal sea el sistema informático de la oficina del abonado del dispositivo móvil.

Pueden cargarse también aplicaciones adicionales en el dispositivo móvil 100 a través de la red 200, el subsistema de E/S auxiliar 112, el acceso o puerta en serie 114, el subsistema de comunicaciones 122 de corto alcance o cualquier otro subsistema adecuado 124. Esta flexibilidad en la instalación de la aplicación aumenta la capacidad funcional del dispositivo móvil 100 y puede hacer posibles funciones emplazadas en el dispositivo, funciones relacionadas con la comunicación, o de ambos tipos, mejoradas. Por ejemplo, aplicaciones de comunicación segura pueden hacer posible la realización de funciones de comercio electrónico y otras transacciones financieras semejantes utilizando el dispositivo móvil 100.

La puerta en serie 114 permite a un abonado establecer preferencias a través de un dispositivo o aplicación de software externa, y amplía las capacidades del dispositivo móvil 100 al hacer posibles descargas de información o de software al dispositivo móvil 100 distintas de a través de una red de comunicación inalámbrica. El recorrido de descarga alternativo puede ser utilizado, por ejemplo, para cargar una clave de cifrado o encriptación en el dispositivo móvil 100 a través de una conexión directa y, por tanto fiable y de confianza, con el fin de proporcionar una comunicación segura del dispositivo.

Los subsistemas 125 pueden incluir al menos un módulo de seguridad 124A de subsistema, adecuadamente programado y configurado para regular el acceso a una o más de las aplicaciones residentes y/o la capacidad funcional 124B. Como se ha hecho notar anteriormente, por ejemplo, tales aplicaciones residentes 124B pueden incluir un PIM para proporcionar una capacidad funcional de libro de direcciones, una capacidad funcional de programación o planificación en el tiempo y de calendario, videojuegos, toma y visualización de fotografías con cámara digital, y presentaciones multimedia, entre otras. A menudo, tales aplicaciones implican el almacenamiento y el uso de datos o contenido 124C de usuario que incluyen preferencias y ajustes de aplicación. Como se comprenderá, tal contenido 124C de usuario puede ser almacenado, en todo o en parte, en la memoria de tipo flash 108, en la ROM o en otro dispositivo de almacenamiento de datos apropiado (típicamente, residente), al que se hace referencia generalmente como 124D.

El acceso a estas aplicaciones 124B y al contenido 124C de usuario puede ser restringido o regulado por el módulo de seguridad 124A, lo que implica el uso de palabras de paso u otras características de seguridad. Tal capacidad funcional de palabra de paso puede incluir el almacenamiento de datos de autorización 124E (que pueden ser almacenados en el dispositivo de almacenamiento 124D de datos o en algún otro lugar). A fin de utilizar las aplicaciones 124B y acceder a los datos 124C de usuario, el módulo de seguridad 124A puede ser programado para

que requiera al usuario a que introduzca una palabra de paso o proporcione, de otro modo, un código de autorización 124F de vez en cuando (típicamente, por medio del dispositivo de presentación visual 110 y el teclado 116, si bien es posible utilizar otros mecanismos), el cual es recibido por el módulo de seguridad 124A y comparado con los datos de autorización 124E.

En ciertas realizaciones, el módulo de seguridad 124A puede ser acoplado operativamente a, o estar de otro modo en comunicación con, un componente de autorización biométrica, por ejemplo, un escáner de retina o un escáner de huellas dactilares (aunque pueden utilizarse otros escáneres biométricos), configurado para recibir información biométrica única o exclusiva desde un usuario con el fin de confirmar la identidad del usuario. En tales realizaciones, los datos de autorización 124E pueden comprender la información biométrica de uno o más usuarios autorizados, en tanto que el código de autorización 124F puede comprender la información biométrica obtenida por exploración de un usuario en ese momento del dispositivo 100.

En el caso de que se reciba un código de autorización 124F por el módulo de seguridad 124A, que no coincida ni se corresponda de otra manera con los datos de autorización 124E (lo que ilustra un ejemplo de “suceso de seguridad”), el acceso a los datos de usuario 124C puede ser restringido (por ejemplo, los datos 124C de usuario pueden ser encriptados o borrados), y puede impedirse al usuario acceder a la capacidad funcional de aplicación 124B (tales procedimientos pueden ser considerados “operaciones de seguridad”). Un ejemplo alternativo de un suceso de seguridad puede ser el envío de un mensaje electrónico especialmente configurado que comprende instrucciones de control, por parte de un administrador de red (tal como un administrador de la LAN [red de área local –“Local Area Network”] 250 que se describe más adelante). La recepción de dicho mensaje puede provocar el desencadenamiento de un suceso de seguridad y de las características de funcionamiento de seguridad correspondientes que se exponen más adelante.

El dispositivo móvil 100 puede enviar y recibir señales de comunicación por la red 200 una vez completados los procedimientos de registro de red o de activación requeridos. El acceso a red está asociado con un abonado o usuario de un dispositivo móvil 100. Para identificar a un abonado, el dispositivo móvil 100 puede posibilitar la inserción de una tarjeta 126 de Módulo de Identidad de Abonado o “SIM” (“Subscriber Identity Module”) en una interfaz de SIM con el fin de comunicarse con una red. El SIM 126 es un tipo de “tarjeta inteligente” o tarjeta de comunicación convencional que se utiliza para identificar a un abonado del dispositivo móvil 100 y para personalizar el dispositivo móvil 100, entre otras cosas. En algunas realizaciones alternativas, el dispositivo móvil 100 puede comprender un equipo de mano de iDEN (Red Mejorada Digital Integrada –“Integrated Digital Enhanced Network”), que incorpora el uso de tarjetas de SIM.

Además de las tarjetas de SIM, pueden utilizarse en aplicaciones de dispositivo electrónico móvil otros tipos de tarjetas de comunicación. A modo de ejemplo únicamente, en realizaciones alternativas, otros tipos de tarjetas de comunicación que podrían utilizarse además de las tarjetas de SIM o en lugar de ellas, pueden incluir un módulo de R-UIM (módulo de identidad de usuario extraíble –“removable user identity module”) o un CSIM (módulo de identidad de abonado de CDMA (acceso múltiple por división de código –“code division multiple access”) (“CDMA subscriber identity module”)) o una tarjeta de USIM (módulo de identidad de abonado universal –“universal subscriber identity module”).

Sin el SIM 126, el dispositivo 100 móvil puede no ser completamente operativo para la comunicación con la red 200. Mediante la inserción del SIM 126 en el interfaz 128 de SIM, un abonado puede acceder a todos los servicios suscritos. Los servicios pueden incluir, sin limitación: exploración de web y mensajería, tal como correo electrónico, mensajería de voz, Servicio de Mensajes Cortos (SMS –“Short Message Service”), y Servicios de Mensajería Multimedia (MMS –“Multimedia Messaging Services”), así como mensajes entre pares o iguales, tales como de PIN a PIN, a los que puede hacerse referencia también simplemente como mensajes de PIN. Tal y como se utiliza en este contexto, un PIN (número de identificación personal –“personal identification number”) se refiere generalmente a un número que identifica de manera única o exclusiva el dispositivo móvil 100, y un mensaje de PIN hace referencia generalmente a un mensaje dirigido a uno o más números de PIN. Servicios más avanzados pueden incluir, sin limitación: punto de venta, servicio sobre el terreno o automatización de las fuerzas de ventas. El SIM 126 incluye un procesador y memoria para almacenar información. Una vez que se ha insertado el SIM 126 en la interfaz 128 de SIM, esta se acopla al microprocesador 102. A fin de identificar al abonado, el SIM 126 contiene algunos parámetros de usuario tales como una Identidad de Abonado Móvil Internacional (IMSI –“International Mobile Subscriber Identity”). Una ventaja de utilizar el SIM 126 es que un abonado no ha de estar necesariamente vinculado a ningún dispositivo móvil físico individual. El SIM 126 puede almacenar, asimismo, información de abonado adicional para un dispositivo móvil, incluyendo información de agenda (o de calendario) e información de las últimas llamadas.

El SIM 126 puede incluir al menos un módulo de seguridad 126A de SIM adecuadamente programado, configurado para regular el acceso a uno o más de las capacidades funcionales de comunicación 124B anteriormente señaladas.

El acceso a las aplicaciones de comunicación de SIM y a la capacidad funcional 126B puede ser restringido o regulado por el módulo de seguridad 126A, lo que implica el uso de palabras de paso u otras características de seguridad. Tal capacidad funcional de palabra de paso puede incluir el almacenamiento de datos 126C de

autorización de SIM, tales como un PIN (número de identificación personal –"personal identification number") (que puede ser almacenado en el dispositivo de almacenamiento 124D de datos, pero que se almacenará a menudo en el dispositivo de almacenamiento 126D de datos de SIM residente en la tarjeta 126 de SIM). Como se comprenderá, dichos datos 126C de PIN se darán a menudo además de los datos de PUK ("clave de desbloqueo personal"), que se asignan de manera exclusiva a la tarjeta 126 de SIM.

A fin de utilizar las aplicaciones de comunicación y la capacidad funcional 126B, el módulo de seguridad 126A de SIM puede haberse programado para requerir al usuario que introduzca una palabra de paso o, en caso contrario, proporcione un código de autorización 126E de vez en cuando (por lo común, a través del dispositivo de presentación visual 110 y del teclado 116, si bien pueden ser utilizados otros mecanismos), que es recibido por el módulo de seguridad 126A y comparado con los datos de autorización 126C. En el caso de que se reciba un código de autorización por parte del módulo de seguridad 126A, que no coincida ni se corresponda de otro modo con los datos de autorización 126C (también un "suceso de seguridad"), puede impedirse todo acceso adicional a la capacidad funcional de comunicación. Típicamente, a un usuario se le proporcionan múltiples intentos (por ejemplo, tres) para introducir un código de autorización 126E aceptable, antes de que la capacidad funcional de comunicación sea desactivada (una "operación de seguridad").

Además, el módulo de seguridad 124A del subsistema se acopla operativamente al módulo de seguridad 125A de SIM, típicamente a través del microprocesador 102. En el caso de que se detecte un suceso de seguridad por parte del módulo de seguridad 124A del subsistema, el módulo de seguridad 124A se programa de manera que incluya en sus operaciones de seguridad el desencadenamiento o puesta en marcha de un suceso de seguridad para la detección del módulo de seguridad 126A de SIM. Por ejemplo, el módulo de seguridad 124A del subsistema puede ser programado para desencadenar la función de palabra de paso del sistema de seguridad 126A de SIM e introducir una o más códigos de autorización no válidos 126E, hasta que se inhabilite la capacidad funcional de comunicación.

El dispositivo móvil 100 puede ser un dispositivo alimentado por batería y puede incluir una interfaz 132 de batería destinada a recibir una o más baterías recargables 130. La interfaz 132 de batería puede ser acoplada a un regulador (no mostrado), que ayuda a la batería 130 a proporcionar potencia V+ al dispositivo móvil 100. Si bien la tecnología actual hace uso de una batería, tecnologías futuras tales como las microceldas de combustible pueden proporcionar la energía al dispositivo móvil 100. En algunas realizaciones, el dispositivo móvil 100 puede ser alimentado por energía solar.

El subsistema de comunicaciones 122 de corto alcance hace posible la comunicación entre el dispositivo móvil 100 y diferentes sistemas o dispositivos, sin tener que hacer uso de la red 200. Por ejemplo, el subsistema 122 puede incluir un dispositivo de infrarrojos y sus circuitos y componentes asociados para la comunicación de corto alcance. Ejemplos de comunicación de corto alcance incluirán normas desarrolladas por la Asociación de Datos de Infrarrojos (IrDA –"Infrared Data Association"), Bluetooh, y la familia de normas 802.11 desarrolladas por el IEEE (Instituto de Ingeniería Eléctrica y Electrónica –"Institute of Electrical and Electronics Engineering").

Durante el uso, una señal recibida, tal como un mensaje de texto, un mensaje de correo electrónico o una descarga de página web, será procesado o tratado por el subsistema de comunicación 104 y suministrado como entrada al microprocesador 102. El microprocesador 102 tratará entonces la señal recibida para suministrarla como salida al dispositivo de presentación visual 110 o, alternativamente, al subsistema de E/S auxiliar 112. Un abonado puede también componer elementos de datos, tales como mensajes de correo electrónico, por ejemplo, utilizando el teclado 116 en combinación con el dispositivo de presentación visual 110 y, posiblemente, un subsistema de E/S auxiliar 112. El subsistema auxiliar 112 puede incluir dispositivos tales como: una pantalla táctil, un ratón, una bola de seguimiento, un detector de huella dactilar por infrarrojos o una rueda de rodadura con una capacidad de pulsación de un botón dinámico. El teclado 116 puede comprender un teclado alfanumérico y/o una placa o cuadro de teclas del tipo de teléfono. El teclado 116 puede comprender un teclado virtual o un teclado físico, o ambos. Un elemento compuesto puede ser transmitido por la red 200, a través del subsistema de comunicación 104.

Para las comunicaciones de voz, el funcionamiento global del dispositivo móvil 100 es sustancialmente similar, a excepción de que las señales recibidas pueden ser tratadas y suministradas como salida al altavoz 118, y pueden generarse por el micrófono 120 señales para ser transmitidas. Pueden implementarse también subsistemas de E/S de voz o audio alternativos, tales como un subsistema de grabación de mensajes de voz, en el dispositivo móvil 100. Si bien la salida de señal de voz o de audio se lleva a cabo fundamentalmente a través del altavoz 118, el dispositivo de presentación visual 110 puede también ser utilizado para proporcionar información adicional tal como la identidad de una parte llamante, la duración de una llamada de voz u otra información relacionada con llamadas de voz.

Haciendo referencia, a continuación, a la Figura 2, se muestra en ella un diagrama de bloques del componente 104 de subsistema de comunicación de la Figura 1. El subsistema de comunicación 104 comprende un receptor 150, un transmisor 152, uno o más elementos de antena empotrados o internos 154, 156, Osciladores Locales (LOs –"Local Oscillators") 158 y un módulo de procesamiento o tratamiento tal como un Procesador de Señal Digital (DSP – "Digital Signal Processor") 160.

El diseño concreto del subsistema de comunicación 104 depende de la red 200 en la que esté destinado a funcionar el dispositivo móvil 100, por lo que ha de comprenderse que el diseño ilustrado en la Figura 2 sirve únicamente como un ejemplo. Las señales recibidas por la antena 154 a través de la red 200 se suministran como salida al receptor 150, el cual puede llevar a cabo funciones de receptor común tales como la amplificación de señal, la conversión en sentido descendente de la frecuencia, la filtración, la selección de canal y la conversión de analógica a digital (A/D). La conversión de A/D de una señal recibida permite que se lleven a cabo funciones de comunicación más complejas tales como la desmodulación y la descodificación en el DSP 160. De una forma similar, las señales que se han de transmitir son tratadas, incluyendo su modulación y codificación, por el DSP 160. Estas señales tratadas por el DSP se suministran como entrada al transmisor 152 para su conversión de digitales a analógicas (D/A), la conversión en sentido ascendente de la frecuencia, la filtración, la amplificación y la transmisión por la red 200 a través de la antena 156. El DSP 160 no sólo trata señales de comunicación, sino que también proporciona un control del receptor y del transmisor. Por ejemplo, las ganancias aplicadas a las señales de comunicación en el receptor 150 y el transmisor 152 pueden ser controladas de forma adaptativa a través de algoritmos de control de ganancia automáticos implementados en el DSP 160.

El enlace inalámbrico entre el dispositivo móvil 100 y la red 200 puede contener uno o más canales diferentes, típicamente canales de RF diferentes, así como protocolos asociados utilizados entre el dispositivo móvil 100 y la red 200. Un canal de RF es un recurso limitado que debe ser conservado, típicamente debido a los límites en la anchura de banda total y la potencia de batería limitada del dispositivo móvil 100.

Cuando el dispositivo 100 se encuentra completamente operativo, el transmisor 152 puede ser armonizado o puesto en funcionamiento únicamente cuando está enviando a la red 200, y puede, en caso contrario, ser desconectado para conservar recursos. De forma similar, el receptor 150 puede ser periódicamente desconectado para ahorrar energía, hasta que sea necesario para recibir señales o información (si es que la hay) durante los periodos de tiempo designados.

Haciendo referencia, a continuación, a la Figura 3, se muestra en ella, indicado por la referencia 202, un diagrama de bloques de un nodo de una red inalámbrica proporcionada a modo de ejemplo. El dispositivo móvil 100 se comunica con un nodo 202 situado dentro de la red inalámbrica 200. En la implementación proporcionada a modo de ejemplo en la Figura 3, el nodo 202 se ha configurado de conformidad con las tecnologías de Servicio General de Radio en Paquetes (GPRS –“General Packet Radio Service”) y de Sistemas Globales para Móviles (GSM –“Global Systems for Mobile”); sin embargo, en otras realizaciones, pueden llevarse a efecto diferentes normas según se ha expuesto anteriormente con mayor detalle. El nodo 202 incluye un controlador de estación de base (BSC –“base station controller”) 204 con una estación de torre asociada 206, una Unidad de Control de Paquetes (PCU –“Packet Control Unit”) 208, añadida para el soporte de GPRS en GSM, una Central de Conmutación Móvil (MSC –“Mobile Switching Center”) 210, un Registro de Posición Doméstica (HLR –“Home Location Register”) 212, un Registro de Posición de Visitante (VLR –“Visitor Location Register”) 214, un Nodo de Soporte de GPRS en Servicio (SGSN –“Serving GPRS Support Node”) 216, un Nodo de Soporte de GPRS de Pasarela (GGSN –“Gateway GPRS Support Node”) 218, y un Protocolo de Configuración de Anfitrión Dinámico (DHCP –“Dynamic Host Configuration Protocol”) 220. La lista de componentes no pretende ser una lista exhaustiva de los componentes de cada nodo 202 dentro de una red de GSM / GPRS, sino que, en lugar de ello, sirve como una lista de componentes que se utilizan por lo común en comunicaciones a través de la red 200, para facilidad de ilustración.

En una red de GSM, la MSC 210 está conectada al BSC 204 y a una red de líneas o conducciones instaladas en tierra, tal como una Red de Telefonía Pública Conmutada (PSTN –“Public Switched Telephone Network”) 222, a fin de satisfacer requisitos de la conmutación en circuitos. La conexión a través de la PCU 208, el SGSN 216 y el GGSN 218, a la red pública o privada (Internet) 224 (a la que se hace referencia también en la presente memoria generalmente como infraestructura de red compartida), representa el recorrido de los datos para dispositivos móviles con capacidad para GPRS. En una red de GSM ampliada con capacidades para GPRS, el BSC 204 también contiene una Unidad de Control de Paquetes (PCU) 208 que se conecta al SGSN 216 para controlar la segmentación, la asignación de canales de radio, y con el fin de satisfacer los requisitos de la conmutación en paquetes. A fin de realizar un seguimiento de la ubicación del dispositivo móvil y de la disponibilidad de gestión tanto de la conmutación en circuitos como de la conmutación en paquetes, el HLR 212 se comparte entre la MSC 210 y el SGSN 216. El acceso al VLR 214 es controlado por la MSC 210.

La estación 206 comprende una estación fija. La estación 206 y el BSC 204 forman, juntos, el equipo transmisor-receptor, o transceptor, fijo. El equipo transceptor fijo proporciona una cobertura de red inalámbrica para un área de cobertura particular a la que se hace referencia comúnmente como “celda”. El equipo transceptor fijo trasmite señales de comunicación a, y recibe señales de comunicación de, dispositivos móviles situados dentro de su celda a través de la estación 206. El equipo transceptor fijo lleva a cabo, normalmente, funciones tales como la modulación y, posiblemente, la codificación y/o la encriptación o cifrado de señales que se van a transmitir al dispositivo móvil de acuerdo con protocolos y parámetros de comunicación particulares, habitualmente predeterminados, bajo el control de su controlador. Similarmente, el equipo transceptor fijo desmodula y, posiblemente, descodifica y descifra, si es necesario, cualesquiera señales de comunicación recibidas desde el dispositivo móvil 100 situado dentro de su celda. Los protocolos y parámetros de comunicación pueden variar entre diferentes nodos. Por ejemplo, un nodo puede emplear un esquema de modulación diferente y funcionar a frecuencias diferentes de otros nodos.

Para todos los dispositivos móviles 100 registrados con una red específica, se almacenan datos de configuración permanentes, tales como un perfil de usuario, en el HLR 212. El HLR 212 también contiene información de posición para cada dispositivo móvil registrado y puede ser requerido para determinar la posición en ese momento de un dispositivo móvil. La MSC 210 es responsable de un grupo de áreas de posición y almacena los datos de los dispositivos móviles situados en ese momento dentro de su área de responsabilidad, en el VLR 214. Por otra parte, el VLR 214 también contiene información sobre dispositivos móviles que están visitando otras redes. La información contenida en el VLR 214 incluye parte de los datos de dispositivo móvil permanentes transmitidos desde el HLR 212 al VLR 214 para un acceso más rápido. Al trasladar información adicional desde un nodo remoto del HLR 12 al VLR 14, la magnitud del tráfico entre estos nodos puede ser reducida de tal manera que puedan proporcionarse servicios de voz y de datos con tiempos de respuesta más rápidos y, al mismo tiempo, que requieran menos uso de los recursos informáticos.

El SGSN 216 y el GGSN 218 son elementos añadidos para el soporte de GPRS, a saber, el soporte de los datos conmutados en paquetes, dentro del GSM. El SGSN 216 y la MSC 210 tienen responsabilidades similares dentro de la red inalámbrica 200, al efectuar un seguimiento de la posición de cada dispositivo 100. El SGSN 216 también lleva a cabo funciones de seguridad y de control de acceso para el tráfico de datos por la red 200. El GGSN 218 proporciona conexiones de comunicación entre redes con redes externas conmutadas en paquetes, y se conecta a uno o más SGSNs 216 a través de una red troncal de Protocolo de Internet (IP –“Internet Protocol”) que se hace funcionar dentro de la red 200. Durante las operaciones normales, un dispositivo móvil 100 dado lleva a cabo un “Enganche de GPRS” con el fin de captar una dirección de IP y acceder a servicios de datos. Este normalmente no está presente en canales de voz conmutados en circuitos, ya que se utilizan direcciones de Red Digital de Servicios Integrados (ISDN –“Integrated Services Digital network”) para encaminar las llamadas entrantes y salientes. En la actualidad, todas las redes con capacidad para GPRS utilizan direcciones de IP privadas, asignadas dinámicamente, por lo que requieren un servidor 220 de DHCP conectado al GGSN 218. Existen muchos mecanismos para la asignación de IP dinámica, incluyendo el uso de una combinación de un servidor de Servicio de Usuario de Marcación para Autentificación a Distancia (RADIUS –“Remote Authentication Dial-In User Service”) y un servidor de DHCP. Una vez que se ha completado el Enganche de GPRS, se establece una conexión lógica desde un dispositivo móvil 100, a través de una PCU 208, un SGSN 216, a un Nodo de Punto de Acceso (APN –“Access Point Node”) ubicado dentro del GGSN 218. El APN representa un terminal lógico de un túnel de IP que puede acceder, bien a servicios directos compatibles con la Internet o bien a conexiones de red privadas. El APN representa también un mecanismo de seguridad para la red 200, en la medida en que cada dispositivo móvil 100 ha de ser asignado a uno o más APNs y los dispositivos móviles 100 no pueden intercambiar datos sin llevar a cabo primero un Enganche de GPRS a un APN que haya sido autorizado para su uso. Puede considerarse el APN como similar a un nombre de dominio de Internet tal como “myconnection.wireless.com”.

Una vez completado el Enganche de GPRS, se crea un túnel y todo el tráfico es intercambiado dentro de paquetes de IP estándar utilizando cualquier protocolo al que pueda darse soporte en paquetes de IP. Esto incluye métodos de formación de túneles tales como IP sobre IP, como es el caso con algunas conexiones de IPSecurity (IPsec (Seguridad de IP)) que se emplean con Redes Privadas Virtuales (VPN –“Virtual Private Networks”). Se hace referencia también a estos túneles como Contextos de Protocolo de Datos en Paquetes (PDP –“Packet Data Protocol”), y existe un número limitado de estos, disponibles en la red 200. Con el fin de maximizar el uso de Contextos de PDP, la red 200 hará funcionar un temporizador libre para cada Contexto de PDP, al objeto de determinar si existe una falta de actividad. Cuando un dispositivo móvil 100 no está utilizando su Contexto de PDP, puede revertirse la asignación del Contexto de PDP y devolverse la reserva o fondo de direcciones de IP gestionado por el servidor 220 de DHCP.

Haciendo referencia, a continuación, a la Figura 4, se muestra en ella un diagrama de bloques que ilustra los componentes de un sistema anfitrión, en un ejemplo de configuración. El sistema anfitrión 250 puede ser, típicamente, por ejemplo, una oficina de empresa u otra red de área local (LAN –“local area network”), aunque puede ser, en vez de eso, una computadora de oficina doméstica u otro sistema privado, por ejemplo, en variantes de implementación. A modo de otros ejemplos, el sistema anfitrión 250 puede comprender una LAN controlada por una institución gubernamental, sanitaria, financiera o educativa. En este ejemplo mostrado en la Figura 4, el sistema anfitrión 250 se ha representado como una LAN de una organización a la que pertenece un usuario del dispositivo móvil 100.

La LAN 250 comprende un cierto número de componentes de red conectados entre sí por unas conexiones 260 de LAN. Por ejemplo, una computadora de sobremesa 262a del usuario, que puede estar conectada a un receptáculo accesorio 164 para el dispositivo móvil 100 del usuario, está situada en la LAN 250. El receptáculo 264 para el dispositivo móvil 100 puede ser acoplado a la computadora 262a por medio de, por ejemplo, una conexión de Bus en Serie Universal (USB –“Universal Serial Bus”). Otras computadoras 262b de usuario se encuentran también emplazadas en la LAN 250, y cada una de ellas puede estar equipada o no con un receptáculo accesorio 264 para un dispositivo móvil. El receptáculo 264 facilita la carga de información (por ejemplo, datos de PIM, claves de cifrado simétricas privadas para facilitar las comunicaciones seguras entre el dispositivo móvil 100 y la LAN 250) procedente de la computadora 262a de usuario en un dispositivo móvil 100, y puede ser particularmente útil para las actualizaciones de información masivas que se llevan a cabo a menudo a la hora de analizar el dispositivo móvil 100 para su uso. La información descargada al dispositivo móvil 100 puede incluir certificados que se utilizan en el

intercambio de mensajes. Se comprenderá por parte de las personas expertas en la técnica que las computadoras 262a, 262b de usuario estarán también conectadas, típicamente, a otros dispositivos periféricos no explícitamente mostrados en la Figura 4.

Por otra parte, únicamente se ha mostrado en la Figura 4 un subconjunto de componentes de red de la LAN 250 por facilidad de exposición, y se comprenderá por las personas expertas en la técnica que la LAN 250 comprenderá componentes adicionales que no se muestran explícitamente en la Figura 4, para este ejemplo de configuración. Más generalmente, la LAN 250 puede representar una parte más pequeña de una red mayor (no mostrada) de la organización, y puede comprender diferentes componentes y/o estar dispuesta en topologías diferentes de la mostrada en el ejemplo de la Figura 4.

En este ejemplo, el dispositivo móvil 100 se comunica con la LAN 250 a través de un nodo 202 de la red inalámbrica 2 y una infraestructura de red compartida 224, tal como una red de proveedor de servicios o la Internet pública. El acceso a la LAN 250 puede proporcionarse a través de uno o más dispositivos de encaminamiento o *routers* (no mostrados), y dispositivos de computación de la LAN 250 pueden operar desde detrás de un cortafuego o un servidor 266 de representante.

En una variante de implementación, la LAN 250 comprende un dispositivo de encaminamiento de VPN inalámbrico (no mostrado) para facilitar el intercambio de datos entre la LAN 250 y el dispositivo móvil 100. El concepto de un dispositivo de encaminamiento de VPN inalámbrico es nuevo en la industria inalámbrica e implica que puede establecerse una conexión de VPN directamente a través de una red inalámbrica específica, con un dispositivo móvil 100. La posibilidad de utilizar un dispositivo de encaminamiento de VPN inalámbrico tan solo ha llegado a estar disponible recientemente y podrá ser empleada cuando la nueva Versión 6 del Protocolo de Internet (IP) (IPV6 –“Internet Protocol Version 6”) llegue a las redes inalámbricas basadas en IP. Este nuevo protocolo proporcionará suficientes direcciones de IP como para dedicar una dirección de IP a cada dispositivo móvil, haciendo posible hacer pasar información a un dispositivo móvil en cualquier momento. Una ventaja de utilizar un dispositivo de encaminamiento de VPN inalámbrico es que este puede consistir en un componente de VPN prefabricado y disponible en el mercado, que no requiere el uso de una pasarela inalámbrica independiente ni de una infraestructura inalámbrica independiente. Una conexión de VPN puede incluir, por ejemplo, una conexión de Protocolo de Control de Transmisión (TCP –“Transmission Control Protocol”) / IP o de Protocolo de Datagrama [diagrama de datos] de Usuario (UDP –“User Datagram Protocol”) / IP para suministrar los mensajes directamente al dispositivo móvil 100 en esta variante de implementación.

Los mensajes destinados a un usuario del dispositivo móvil 100 son inicialmente recibidos por un servidor 268 de mensajes de la LAN 250. Tales mensajes pueden originarse desde cualquiera de un cierto número de recursos. Por ejemplo, puede haberse enviado un mensaje por parte de un remitente desde una computadora 262b ubicada dentro de la LAN 250, desde un dispositivo móvil diferente (no mostrado) conectado a la red inalámbrica 200 o a una red inalámbrica diferente, o bien desde un dispositivo informático diferente u otro dispositivo capaz de enviar mensajes, a través de la infraestructura 224 de red compartida y, posiblemente, a través de un proveedor de servicios de aplicación (ASP –“application service provider”) o un proveedor de servicios de Internet (ISP –“Internet service provider”), por ejemplo.

El servidor 268 de mensajes actúa, por lo común, como la interfaz primaria para el intercambio de mensajes, particularmente mensajes de correo electrónico, dentro de la organización y a través de la infraestructura de red compartida 224. Cada usuario de la organización que se ha establecido para enviar y recibir mensajes está asociado, típicamente, con una cuenta de usuario gestionada por el servidor 268 de mensajes. Un ejemplo de servidor 268 de mensajes es un Servidor de Microsoft Exchange®. En algunas implementaciones, la LAN 250 puede comprender múltiples servidores 268 de mensajes. El servidor 268 de mensajes puede también haberse configurado para proporcionar funcionales adicionales más allá de la gestión de mensajes, incluyendo la gestión de datos asociada, por ejemplo, con calendarios y listas de tareas.

Cuando se reciben los mensajes por el servidor 268 de mensajes, estos son, por lo común, almacenados en un dispositivo de almacenamiento de mensajes (no mostrado explícitamente), desde el que los mensajes pueden ser subsiguientemente recuperados y suministrados a los usuarios. Por ejemplo, una aplicación de cliente de correo electrónico que opera en una computadora 262a de usuario puede solicitar los mensajes de correo electrónico asociados con la cuenta de ese usuario almacenada en el servidor 268 de mensajes.

Estos mensajes pueden ser entonces, típicamente, recuperados desde el servidor 268 de mensajes y almacenados localmente en la computadora 262a.

Cuando se hace funcionar el dispositivo móvil 100, el usuario puede desear hacer que se recuperen mensajes de correo electrónico para su entrega al dispositivo de mano. Una aplicación de cliente de correo electrónico que opera en el dispositivo móvil 100 puede también solicitar mensajes asociados con la cuenta del usuario desde el servidor 268 de mensajes. El cliente de correo electrónico puede haberse configurado (ya sea por el usuario o por un administrador, posiblemente de acuerdo con un criterio de tecnología de información (IT –“Information technology”) de la organización) para realizar esta petición en la dirección del usuario, a un cierto intervalo de tiempo predefinido

o al producirse algún suceso predefinido. En algunas implementaciones, al dispositivo móvil 10 se le asigna su propia dirección de correo electrónico, y los mensajes dirigidos específicamente al dispositivo móvil 100 son automáticamente redirigidos al dispositivo móvil 100 a medida que son recibidos por el servidor 268 de mensajes.

Para facilitar la comunicación inalámbrica de mensajes y de datos relacionados con mensajes entre el dispositivo móvil 100 y los componentes de la LAN 250, es posible proporcionar diversos componentes 270 de soporte de las comunicaciones inalámbricas. En esta implementación proporcionada a modo de ejemplo, los componentes 270 de soporte de las comunicaciones inalámbricas comprenden, por ejemplo, un servidor 272 de gestión de mensajes y un servidor 288 de datos móvil. El servidor 272 de gestión de mensajes se utiliza para proporcionar específicamente soporte para la gestión de mensajes, tales como mensajes de correo electrónico, que han de ser manejados por dispositivos móviles. En general, si bien los menajes siguen siendo almacenados en el servidor 268 de mensajes, puede utilizarse el servidor 272 de gestión de mensajes para controlar cuándo, si y cómo han de ser enviados los mensajes el dispositivo móvil 100. El servidor 272 de gestión de mensajes también facilita el manejo de mensajes compuestos en el dispositivo móvil 100, los cuales son enviados al servidor 268 de mensajes para su subsiguiente entrega.

Por ejemplo, el servidor 272 de gestión de mensajes puede: supervisar el “buzón de correo” del usuario (por ejemplo, el dispositivo de almacenamiento de mensajes asociado con la cuenta de usuario existente en el servidor 268 de mensajes) en busca de nuevos mensajes de correo electrónico; aplicar filtros definibles por el usuario a los nuevos mensajes para determinar si, y cómo, han de ser reemitidos los mensajes al dispositivo móvil 100 del usuario; comprimir y encriptar o cifrar nuevos mensajes (por ejemplo, utilizando una técnica de cifrado tal como la Norma de Cifrado de Datos (DES –“Data Encryption Standard”) o la Triple DES) y hacerlos pasar al dispositivo móvil 100 a través de la infraestructura de red compartida 224 y de la red inalámbrica 20; y recibir mensajes compuestos en el dispositivo móvil 100 (por ejemplo, cifrados utilizando la Triple DES), descifrar y descomprimir los mensajes compuestos, reformatear los mensajes compuestos, si se desea, de tal manera que parezca que se han originado desde la computadora 262a del usuario, y reencaminar los mensajes compuestos al servidor 268 de mensajes para su entrega.

Ciertas propiedades o restricciones asociadas con los mensajes que se han de enviar desde, y/o recibir por, el dispositivo móvil 100 pueden definirse (por ejemplo, por medio de un administrador de acuerdo con el criterio de IT) y hacerse valer por el servidor 272 de gestión de mensajes. Estas pueden incluir las alternativas referentes a si el dispositivo móvil 100 puede recibir mensajes cifrados y/o firmados, tamaños mínimos de clave de cifrado, si los mensajes salientes han de ser cifrados y/o firmados, y si se deben enviar a una dirección de copia predefinida copias de todos los mensajes seguros enviados desde el dispositivo móvil 100, por ejemplo.

El servidor 272 de gestión de mensajes puede también haberse configurado para proporcionar otras funciones de control, tales como hacer pasar únicamente cierta información del mensaje o porciones predefinidas (por ejemplo, “bloques”) de un mensaje almacenados en el servidor 268 de mensajes, al dispositivo móvil 100. Por ejemplo, cuando un mensaje es inicialmente recuperado por el dispositivo móvil 100 desde el servidor 268 de mensajes, el servidor 272 de gestión de mensajes se configura para hacer pasar únicamente la primera parte de un mensaje al dispositivo móvil 100, de tal manera que la parte es de un tamaño predefinido (por ejemplo, 2 kB). El usuario puede entonces solicitar más del mensaje, que se ha de entregar, en bloques dimensionados con un tamaño similar, por parte del servidor 272 de gestión de mensajes, al dispositivo móvil 100, posiblemente hasta un tamaño máximo predefinido de los mensajes.

De acuerdo con ello, el servidor 272 de gestión de mensajes facilita un mejor control sobre el tipo de datos y la cantidad de datos que se comunica al dispositivo móvil 100, y puede ayudar a minimizar el derroche potencial de banda o de otros recursos.

Se comprenderá por las personas expertas en la técnica que el servidor 272 de gestión de mensajes no necesita ser implementado en un servidor físico independiente ubicado en una LAN 250 o en otra red. Por ejemplo, algunas o todas las funciones asociadas con el servidor 272 de gestión de mensajes pueden estar integradas con el servidor 268 de mensajes o con alguno otro servidor existente en la LAN 250. Por otra parte, la LAN 250 puede comprender múltiples servidores 272 de gestión de mensajes, particularmente en variantes de implementación en las que se da soporte a un gran número de dispositivos móviles.

Haciendo referencia, a continuación, a la Figura 5, se muestra en ella generalmente como la referencia 500 un diagrama de flujo que ilustra las etapas de un método para implementar las características de seguridad de un dispositivo móvil de acuerdo con al menos una realización. Detalles adicionales de algunas de las características que se describen más adelante con respecto a las etapas del método 500, pueden haberse descrito anteriormente en la presente memoria.

Las etapas del método 500 se llevan a cabo en el dispositivo informático. En una realización, al menos algunas de las etapas del método se llevan a cabo mediante uno o más módulos de seguridad que se llevan a cabo, y residen, en un dispositivo (por ejemplo, el dispositivo móvil 100 de la Figura 1). Por otra parte, los módulos de seguridad no necesitan ser aplicaciones autónomas, y la capacidad funcional de los módulos de seguridad puede ser

implementada en una o más aplicaciones que se ejecutan, y residen, en el dispositivo móvil o en otro dispositivo informático.

En general, en el método 50, un suceso de seguridad detectado por un módulo de seguridad provoca el disparo o desencadenamiento de las características de seguridad proporcionadas por otro módulo de seguridad. Las etapas del método 500 se describen con mayor detalle más adelante.

El método 500 comienza por el bloque 510, en el que el módulo de seguridad 124A determina si se ha producido un suceso de seguridad. Por ejemplo, la detección de tal suceso de seguridad puede resultar del hecho de que el usuario trate de acceder a la capacidad funcional de aplicación 124B y se le haya instado, por parte del módulo de seguridad del subsistema 124A, a suministrar como entrada un código de autorización 124F, tal como una palabra de paso. El módulo de seguridad 124A determina si el código de autorización 124F corresponde a los datos de autorización 124E. Alternativamente, tal y como se ha señalado en lo anterior, un administrador de red puede desencadenar un suceso de seguridad al enviar al dispositivo 100 un mensaje de seguridad apropiadamente configurado.

Como se ha señalado anteriormente, en ciertas realizaciones, el código de autorización 124F puede comprender, de manera alternativa o adicional, datos biométricos obtenidos del usuario en curso. De acuerdo con ello, en dicha realización, un código de autorización no válido según se recoge en el bloque 510 puede implicar, por ejemplo, una toma de huella dactilar del usuario que no coincide con una toma de huella dactilar almacenada en el dispositivo 124D de almacenamiento de datos.

Si no se detecta ningún suceso de seguridad, en el bloque 512, se permite al usuario acceder a la capacidad funcional de aplicación. Por ejemplo, si el código de autorización 124F recibido por el módulo de seguridad 124A coincide o se corresponde de otra manera con los datos de autorización 124E, se confirma la autorización por parte del usuario. De esta forma, se permite al usuario acceder a la capacidad funcional de aplicación 124B. Sin embargo, si se detecta un suceso de seguridad, se inicia, en el bloque 514, la primera operación de seguridad. Por ejemplo, si el código de autorización 124F no es válido porque no coincide o no se corresponde de otra manera con los datos de autorización 124E, el módulo de seguridad 124A se programa para efectuar una o más operaciones de seguridad. Dichas operaciones de seguridad pueden incluir impedir el acceso a los datos de usuario 124C y a las aplicaciones 124B. Como se ha señalado anteriormente, esta etapa puede implicar el cifrado o el borrado de los datos 124C de usuario. Asimismo, como se ha sugerido anteriormente, pueden proporcionarse al usuario múltiples oportunidades para introducir un código de autorización 124F que corresponde a los datos de autorización 124E.

En el bloque 516, la primera operación de seguridad también incluye desencadenar un segundo suceso de seguridad. En el bloque 518, el segundo suceso de seguridad inicia la segunda operación de seguridad. Por ejemplo, dicho segundo suceso de seguridad puede ser desencadenado por el primer módulo de seguridad 124A al introducir una o más códigos de autorización de SIM no válidos hasta que la programación del módulo de seguridad 126A de SIM inicia su operación de seguridad, tal como, por ejemplo, la inhabilitación la tarjeta 126 de SIM y su capacidad funcional de comunicación.

Subsiguientemente a la inhabilitación de la tarjeta 126 de SIM en el bloque 516, en ciertas realizaciones, el usuario puede contactar con los administradores de la red de comunicación para desbloquear la tarjeta 126 de SIM, a fin de restablecer su capacidad funcional de comunicación y permitir que la tarjeta 126 de SIM acceda a la red.

Si bien las realizaciones proporcionadas a modo de ejemplo y que se han expuesto en esta memoria ilustran la interconexión de un módulo de seguridad 124A de subsistema con un módulo de seguridad 126A de SIM, ha de comprenderse que pueden interconectarse dos o más módulos de seguridad que regulan el acceso a la capacidad funcional de múltiples aplicaciones, de acuerdo con las enseñanzas expuestas en la presente memoria.

Como se comprenderá, en el caso de que un ladrón o una persona de otro modo inautorizada obtenga la posesión del dispositivo 100, mediante dicha introducción individual de una palabra de paso no válida para acceder a una capacidad funcional de aplicación, o desencadenando de otro modo un suceso de seguridad, se tendrá como resultado un efecto dominó en el que se activen uno o más módulos de seguridad distintos para detectar un suceso de seguridad correspondiente e implementar sus características de seguridad y restringir el acceso a sus capacidades funcionales de aplicación correspondientes.

La invención se ha descrito en relación con un cierto número de realizaciones. Sin embargo, se comprenderá por parte de las personas expertas en la técnica que pueden realizarse otras variantes y modificaciones sin apartarse del ámbito de la invención, según se define en las reivindicaciones que se acompañan a la presente memoria.

REIVINDICACIONES

1.- Un método para implementar una característica de seguridad de un dispositivo electrónico (100), de tal manera que el método comprende:

detectar un intento de acceso no válido;
iniciar, en respuesta a dicha detección, una primera operación de seguridad para impedir el acceso a, o inhabilitar, una entidad, datos, aplicación o función asociada con dicho dispositivo, y disparar o desencadenar un intento no válido para acceder a otra entidad, datos, aplicación o función asociada con dicho dispositivo, a fin de iniciar una segunda operación de seguridad para impedir el acceso a, o inhabilitar, dicha otra entidad, datos, aplicación o función.

2.- El método de acuerdo con la reivindicación 1, en el cual la detección del intento de acceso no válido se lleva a cabo por un primer módulo de seguridad (124A).

3.- El método de acuerdo con la reivindicación 1 o la reivindicación 2, en el cual la etapa de detectar un intento de acceso no válido se inicia con la recepción de un mensaje que comprende instrucciones de control.

4.- El método de acuerdo con la reivindicación 3, en el cual el mensaje que comprende instrucciones de control es recibido desde un administrador de red.

5.- El método de acuerdo con la reivindicación 2, o la reivindicación 3 o la reivindicación 4 cuando dependen de la reivindicación 2, en el cual la primera operación de seguridad desencadena el intento de acceso no válido a dicha otra entidad, datos, aplicación o función asociada con dicho dispositivo.

6.- El método de acuerdo con una cualquiera de las reivindicaciones precedentes, en el cual la segunda operación de seguridad comprende impedir el acceso a, o inhabilitar, dicha otra entidad que comprende un dispositivo o componente que se comunica con, se conecta a, o se inserta dentro de, dicho dispositivo electrónico.

7.- El método de acuerdo con una cualquiera de las reivindicaciones 1 a 5, en el cual la segunda operación de seguridad comprende inhabilitar la capacidad funcional de una entidad que comprende una tarjeta de comunicación (126) del dispositivo electrónico.

8.- El método de acuerdo con una cualquiera de las reivindicaciones precedentes, en el cual detectar el intento de acceso no válido comprende recibir un código de autorización (124F) y determinar que el código de autorización (124F) no se corresponde con datos de autorización previamente almacenados.

9.- El método de acuerdo con cualquiera de las reivindicaciones precedentes, en el cual desencadenar un intento no válido de acceder a dicha otra entidad, datos, aplicación o función asociada con dicho dispositivo, comprende proporcionar a sabiendas un código o datos de autorización no válidos a un segundo módulo de seguridad (126A) asociado con dicha otra entidad, datos, aplicación o función.

10.- El método de acuerdo con la reivindicación 9, en el cual el código o datos de autorización no válidos son enviados a dicho segundo módulo de seguridad (126A) tantas veces como sea necesario para iniciar dicho segundo módulo de seguridad (126A) con el fin de impedir el acceso a, o inhabilitar, dicha otra entidad, datos, aplicación o función.

11.- Un dispositivo electrónico (100) que comprende:

un módulo (124B) para detectar un intento de acceso no válido; un primer módulo de seguridad (124A), conectado con el módulo (124B),de tal manera que el primer módulo de seguridad está configurado para iniciar, en respuesta a un intento de acceso no válido detectado, una primera operación de seguridad para impedir el acceso a, o inhabilitar, una entidad, datos, aplicación o función asociada con dicho dispositivo, y para disparar o desencadenar un intento no válido de acceder a otra entidad, datos, aplicación o función asociada con dicho dispositivo; y
un segundo módulo de seguridad (126A), asociado con dicha otra entidad, datos, aplicación o función, de tal manera que dicho segundo módulo de seguridad (126A) está configurado para impedir el acceso a, o inhabilitar, dicha otra entidad, datos, aplicación o función en respuesta a dicho intento de acceso no válido desencadenado.

12.- El dispositivo electrónico (100) de acuerdo con la reivindicación 11, en el cual el primer módulo de seguridad (124A) está configurado para detectar un intento de acceso no válido en respuesta a la recepción de un mensaje que comprende instrucciones de control.

13.- El dispositivo electrónico (100) de acuerdo con la reivindicación 12, en el cual el primer módulo de seguridad (124A) está configurado para recibir el mensaje que comprende instrucciones de control desde un administrador de

red.

14.- El dispositivo electrónico (100) de acuerdo con una cualquiera de las reivindicaciones 11 a 13, en el cual el primer módulo de seguridad (124A) está configurado para desencadenar dicho intento de acceso no válido a dicha otra entidad, datos, aplicación o función asociada con dicho dispositivo.

15.- El dispositivo electrónico (100) de acuerdo con una cualquiera de las reivindicaciones 11 a 14, en el cual el segundo módulo de seguridad (126A) está configurado para impedir el acceso a, o inhabilitar, dicha otra entidad que comprende un dispositivo o componente que se comunica con, se conecta a, o se inserta dentro de, dicho dispositivo electrónico.

16.- El dispositivo electrónico (100) de acuerdo con una cualquiera de las reivindicaciones 11 a 15, en el cual el segundo módulo de seguridad (126A) está configurado para inhabilitar la capacidad funcional de una entidad que comprende una tarjeta de comunicación (126) del dispositivo electrónico.

17.- El dispositivo electrónico (100) de acuerdo con una cualquiera de las reivindicaciones 11 a 16, en el cual el segundo módulo de seguridad (126A) se ha configurado para impedir el acceso a, o inhabilitar, dicha otra entidad que comprende un dispositivo o componente que se comunica con, se conecta a, o se inserta dentro de, dicho dispositivo electrónico.

18.- El dispositivo electrónico (100) de acuerdo con una cualquiera de las reivindicaciones 11 a 17, en el cual el primer módulo de seguridad (124A) está configurado para disparar o desencadenar un intento no válido de acceder a dicha otra entidad, datos, aplicación o función asociada con dicho dispositivo, al proporcionar a sabiendas un código o datos de autorización no válidos a dicho segundo módulo de seguridad (126A).

19.- El dispositivo electrónico (100) de acuerdo con la reivindicación 18, en el cual el primer módulo de seguridad (124A) está configurado para enviar un código o datos de autorización no válidos a dicho segundo módulo de seguridad (126A) tantas veces como sea necesario para iniciar dicho segundo módulo de seguridad (126A), con el fin de impedir el acceso a, o inhabilitar, dicha otra entidad, datos, aplicación o función.

20.- El dispositivo electrónico (100) de acuerdo con una cualquiera de las reivindicaciones 11 a 19, de tal modo que el dispositivo comprende adicionalmente un dispositivo de almacenamiento (124D) de datos de usuario, configurado para almacenar datos (124C) de usuario, y de tal manera que el primer módulo de seguridad (124A) está configurado adicionalmente para inhabilitar el acceso a, o para borrar, los datos (124C) de usuario cuando se implementa la primera operación de seguridad.

21.- El dispositivo electrónico (100) de acuerdo con una cualquiera de las reivindicaciones 11 a 20, de tal manera que el dispositivo comprende, adicionalmente, un dispositivo de almacenamiento (124D) de datos de autorización, destinado a almacenar datos de autorización (124E), y de modo que el primer módulo de seguridad (124A) está configurado, de manera adicional, para recibir un primer código de autorización (124F) y comparar el primer código de autorización (124F) con los primeros datos de autorización (124E) almacenados en el dispositivo de almacenamiento (124D) de datos de autorización, a fin de detectar un intento de acceso no válido.

22.- El dispositivo electrónico (100) de acuerdo con la reivindicación 21, en el cual el primer módulo de seguridad (124A) está configurado, de manera adicional, para implementar dicha primera operación de seguridad al determinarse que el primer código de autorización (124F) no se corresponde con los primeros datos de autorización (124E).

23.- El dispositivo electrónico (100) de acuerdo con la reivindicación 22, en el cual el segundo módulo de seguridad (126A) está configurado, de manera adicional, para recibir un segundo código de autorización (126E) y comparar el segundo código de autorización (126E) con los segundos datos de autorización (126C) almacenados en el dispositivo de almacenamiento (126D) de datos de autorización.

24.- El dispositivo electrónico de acuerdo con la reivindicación 23, en el cual el segundo modulo de seguridad (126A) está configurado, de manera adicional, para implementar dicha segunda operación de seguridad al determinarse que el segundo código de autorización (126E) no se corresponde con los segundos datos de autorización (126C).

25.- El dispositivo electrónico de acuerdo con una cualquiera de las reivindicaciones 11 a 24, de tal manera que el dispositivo comprende un dispositivo electrónico móvil.

26.- Un medio legible por computadora, que comprende instrucciones susceptibles de llevarse a cabo en un procesador (102) de un dispositivo electrónico (100) para hacer que dicho dispositivo electrónico implemente el método de acuerdo con una cualquiera de las reivindicaciones 1 a 10.

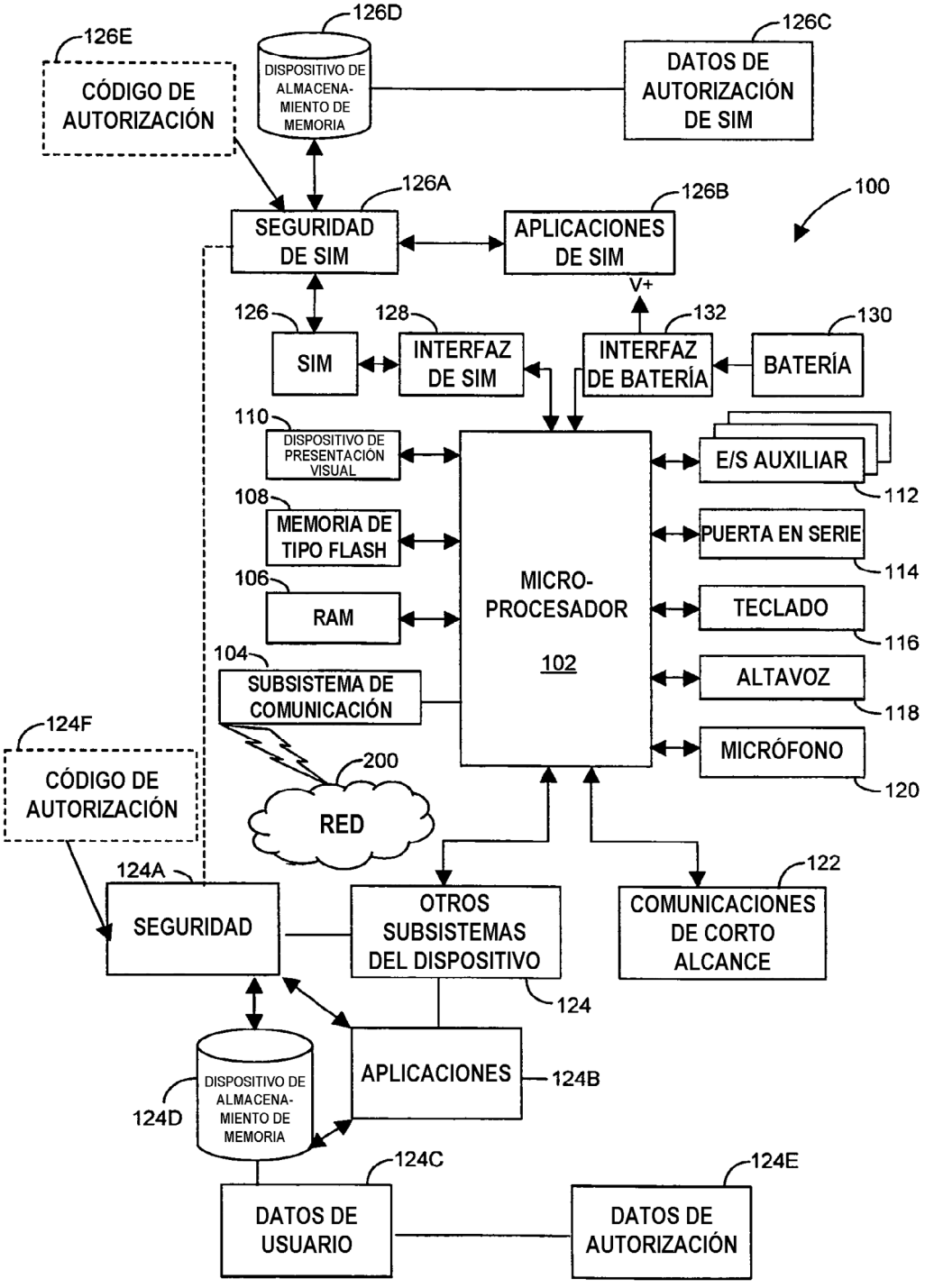
126D
126E
126C
DISPOSITIVO DE ALMACENA-MIENTO DE MEMORIA
CÓDIGO DE AUTORIZACIÓN
DATOS DE AUTORIZACIÓN DE SIM
126A
126B
100
SEGURIDAD DE SIM
APLICACIONES DE SIM
V+
126
128
132
130
SIM
INTERFAZ DE SIM
INTERFAZ DE BATERÍA
BATERÍA
110
DISPOSITIVO DE PRESENTACIÓN VISUAL
E/S AUXILIAR
112
108
MEMORIA DE TIPO FLASH
PUERTA EN SERIE
114
106
RAM
MICRO-PROCESADOR
102
TECLADO
116
104
SUBSISTEMA DE COMUNICACIÓN
ALTAVOZ
118
MICRÓFONO
120
124F
CÓDIGO DE AUTORIZACIÓN
200
RED
124A
122
SEGURIDAD
OTROS SUBSISTEMAS DEL DISPOSITIVO
COMUNICACIONES DE CORTO ALCANCE
124
APLICACIONES
124B
DISPOSITIVO DE ALMACENA-MIENTO DE MEMORIA
124D
124C
124E
DATOS DE USUARIO
DATOS DE AUTORIZACIÓN

FIG. 1

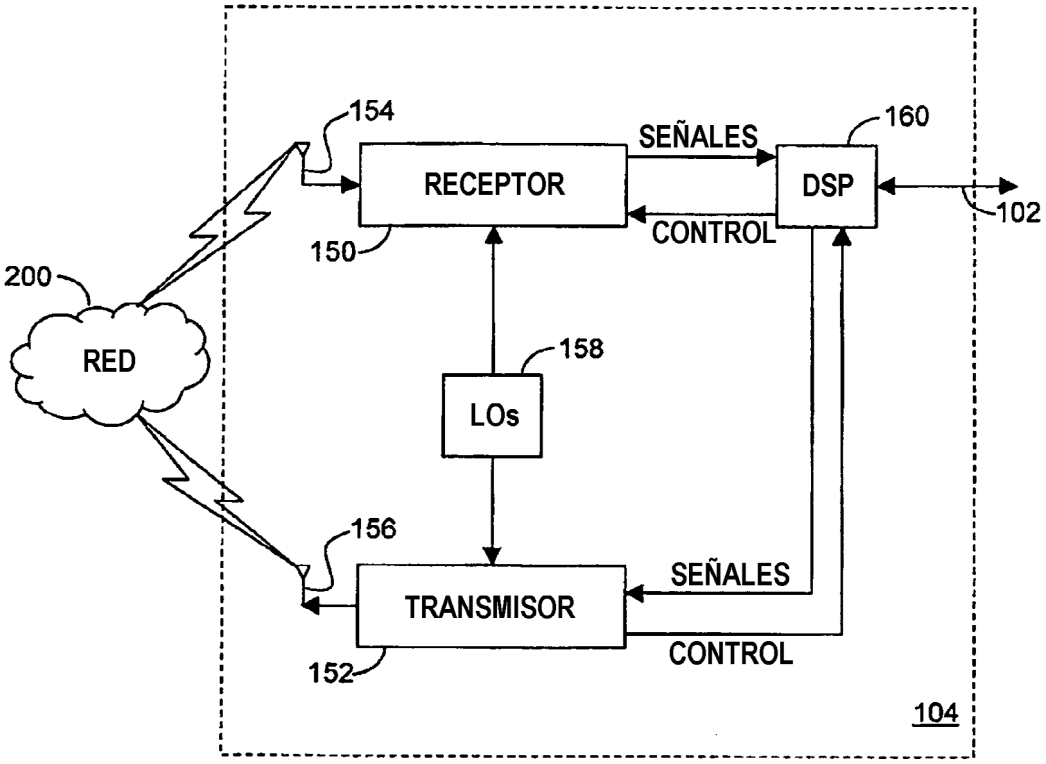
154
SEÑALES
160
RECEPTOR
DSP
102
CONTROL
150
200
RED
158
LOs
156
SEÑALES
TRANSMISOR
CONTROL
152
104

FIG. 2

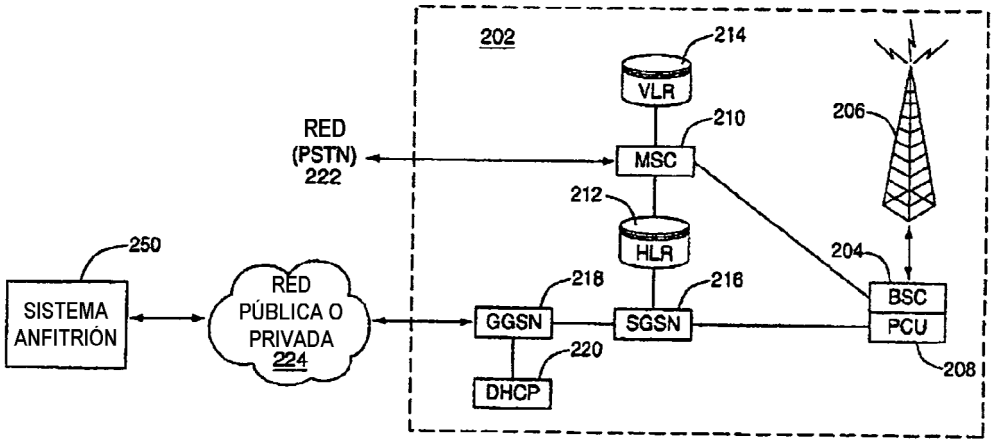
202
214
VLR
210
MSC
206
RED
(PSTN)
222
212
HLR
204
250
218
216
BSC
SISTEMA
ANFITRIÓN
RED
PÚBLICA O
PRIVADA
224
GGSN
SGSN
PCU
220
208
DHCP

FIG. 3

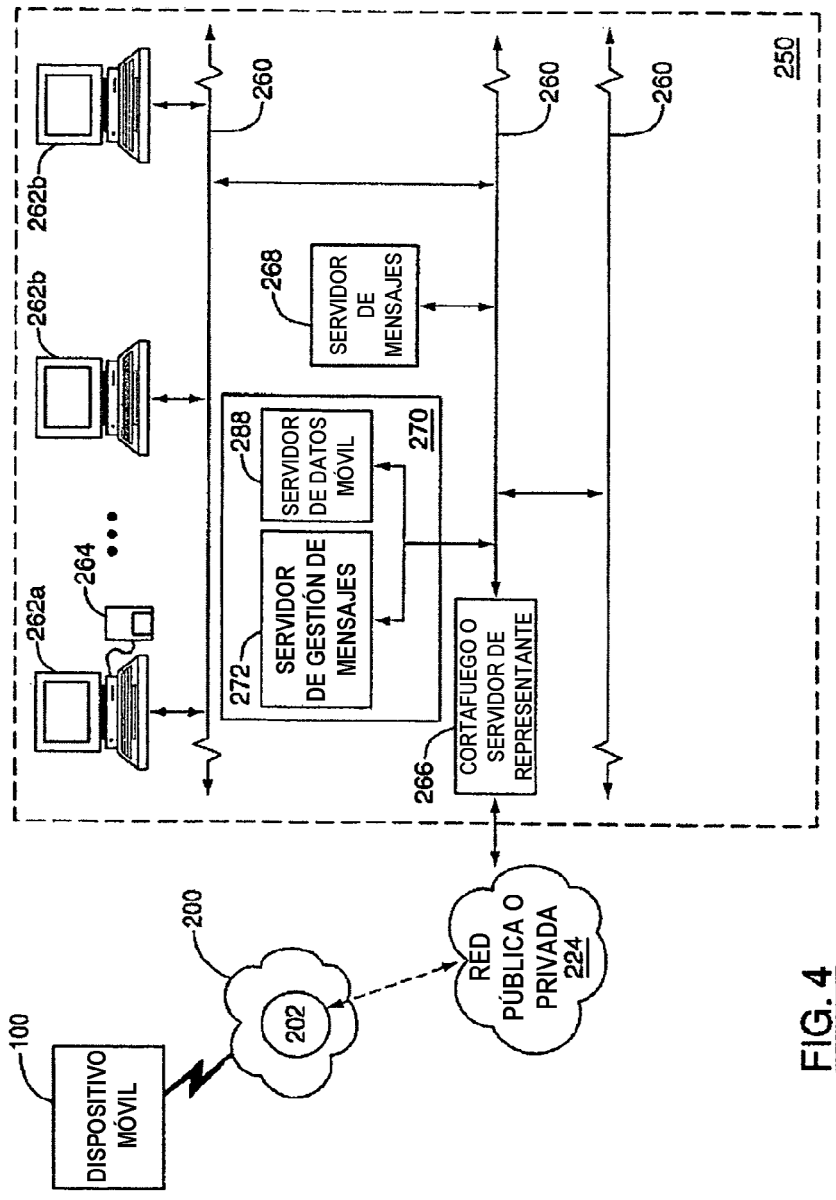
100
DISPOSITIVO MÓVIL
200
202
RED PÚBLICA O PRIVADA 224
266
CORTAFUEGO O SERVIDOR DE REPRESENTANTE
272
SERVIDOR DE GESTIÓN DE MENSAJES
288
SERVIDOR DE DATOS MÓVIL
270
268
SERVIDOR DE MENSAJES
262a
264
262b
262b
260
260
260
250

FIG. 4

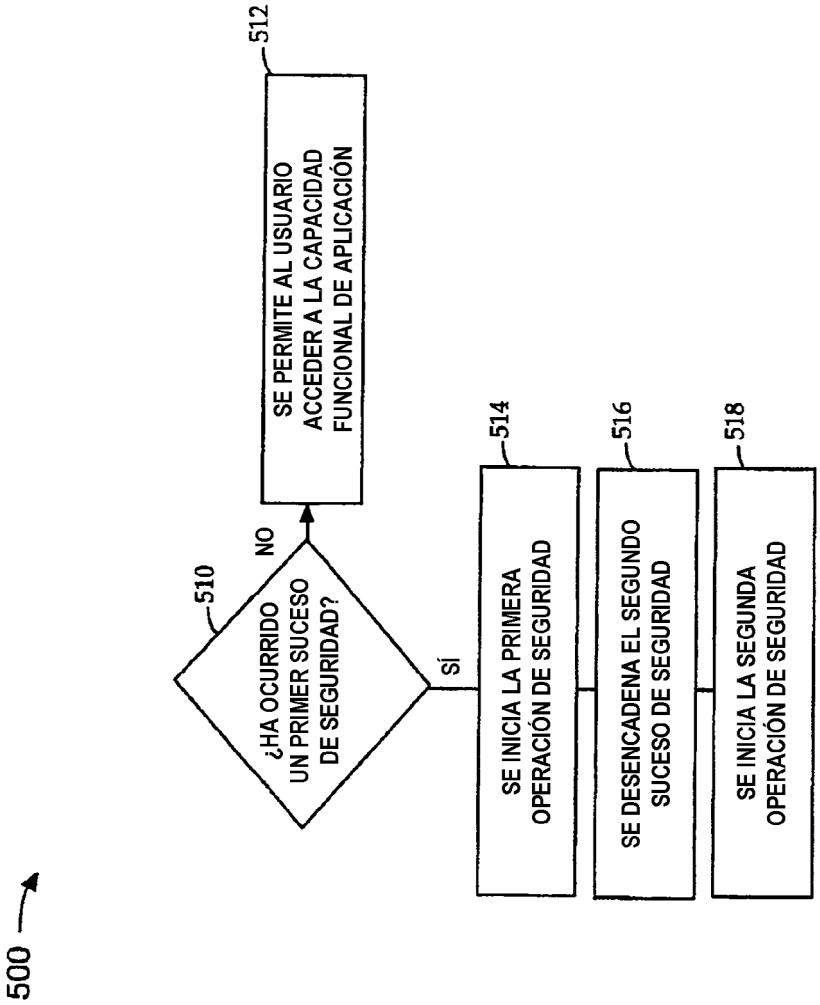
500
510
¿HA OCURRIDO UN PRIMER SUCESO DE SEGURIDAD?
NO
SÍ
512
SE PERMITE AL USUARIO ACCEDER A LA CAPACIDAD FUNCIONAL DE APLICACIÓN
514
SE INICIA LA PRIMERA OPERACIÓN DE SEGURIDAD
516
SE DESENCADENA EL SEGUNDO SUCESO DE SEGURIDAD
518
SE INICIA LA SEGUNDA OPERACIÓN DE SEGURIDAD

FIG. 5