(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 357 414**

(51) Int. Cl.:
G06F 21/00 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **06115509 .9**
(96) Fecha de presentación : **28.02.2003**
(97) Número de publicación de la solicitud: **1734723**
(97) Fecha de publicación de la solicitud: **20.12.2006**

(54) Título: **Sistema y método de protección de datos en un dispositivo de comunicación.**

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

(45) Fecha de publicación de la mención BOPI:
26.04.2011

(72) Inventor/es: **Adams, Neil y**
Little, Herb

(45) Fecha de la publicación del folleto de la patente:
26.04.2011

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

DESCRIPCIÓN

Campo del Invento

Este invento se refiere en general a la protección de datos, y en particular a la protección de datos en un dispositivo de comunicación.

Descripción del Estado de la Técnica

En un entorno de empresa, los empleados tienen frecuentemente posibilidad de acceso a suministros de equipo de oficina a ser utilizado para realizar su trabajo, que incluye típicamente al menos un ordenador personal (PC) y frecuentemente incluye también dispositivos de comunicaciones móviles inalámbricas y otros tipos de dispositivos electrónicos. En cualquiera de esos equipos puede haber almacenada información confidencial o sensible de otro modo, información sobre el patrono, o ambas. Aunque el equipo del usuario, tal como un PC, que permanece en las instalaciones del patrono esté físicamente asegurado por el patrono, los dispositivos portátiles o móviles, por su propia naturaleza, es más probable que se extravíen o sean robados, y por lo tanto son menos seguros. Es por lo tanto frecuentemente deseable proteger la información sensible que haya en los dispositivos móviles para impedir que una parte no autorizada tenga acceso a tal información en equipo del usuario perdido o robado.

Un tipo corriente de medida de seguridad para dispositivos móviles habilitados o capacitados para comunicaciones, tal como los dispositivos móviles inalámbricos, por ejemplo, es la de asegurar que la información sensible es transferida a tales dispositivos móviles con seguridad. Aunque la transferencia de la información sea segura, estas medidas solamente protegen la información durante la transferencia, y no después de que haya sido recibida la información por un dispositivo móvil.

De acuerdo con otro esquema de seguridad conocido, la información recibida es cifrada o encriptada cuando se almacena en una memoria, o antes de hacerlo. El descifrado o desencriptado de la información cifrada almacenada requiere acceso a una clave criptográfica. En general, se prefiere una criptografía de clave simétrica, en la cual se utiliza una sola clave tanto para el cifrado o encriptado como para el descifrado o desencriptado, para los dispositivos móviles que tienen recursos limitados para el procesado, ya que las operaciones criptográficas con clave simétrica son más rápidas y requieren menos tareas del procesador que las asociadas con otros esquemas criptográficos. El acceso a esa única clave puede ser controlado utilizando protección por contraseña, por ejemplo, de modo que un usuario no autorizado no pueda simplemente leer la clave de la memoria en un dispositivo móvil perdido o robado y descifrar luego todo el contenido cifrado o encriptado almacenado en el dispositivo móvil. Sin embargo, esto puede dar por resultado situaciones en las que la clave no sea accesible cuando se haya recibido la información en un dispositivo móvil. Es deseable que se requiera un empleado para operar un dispositivo móvil provisto por su empleador de manera segura mediante lo cual los datos recibidos en el dispositivo sean protegidos.

Otro antecedente de la técnica incluye:

1) El Credant Mobile Guardian Shield (Escudo Guardián Móvil Credant), diseñado para asegurar la confidencialidad de la información almacenada en un dispositivo móvil. En el caso de que un empleado deje o abandone una compañía, por ejemplo, un administrador autorizado puede recuperar la información

2) El SafeGuard PDA (PDA Salvaguardi) de Ultimaco Safeware AG

3) TRUST DIGITAL (DIGITAL CONFIANZA) de Trust Digital Security Software; y

4) un documento de PALM titulado “Securing the handheld environment – An Enterprise Perspective” (Asegurando el entorno portátil – Una perspectiva de Empresa).

En un primer aspecto del invento, hay provisto preferiblemente un dispositivo de comunicación que comprende: una memoria configurada para almacenar datos; un módulo de protección de datos de dicho dispositivo de comunicación configurado para recibir datos, para proteger los datos recibidos mediante el cifrado o encriptación de dichos datos recibidos, y almacenar los datos recibidos protegidos en la memoria, en el que el sistema comprende además medios para habilitar o capacitar el módulo de protección de datos, estando configurados dichos medios para restringir algunas o todas las demás operaciones del dispositivo de comunicación hasta que la protección de datos haya sido habilitada; en el que el sistema tiene un primer estado operativo y un segundo estado operativo; y un almacén de claves configurado para almacenar una pluralidad de claves criptográficas; en el que el módulo de protección de datos está configurado para determinar si el dispositivo de comunicación está en el primer estado operativo o en el segundo estado operativo, para cifrar o encriptar los datos recibidos utilizando una primera de la pluralidad de claves criptográficas si el dispositivo de comunicación está en el primer estado operativo, o una segunda de la pluralidad de claves criptográficas si el dispositivo de comunicación está en el segundo estado operativo, y para almacenar los datos recibidos cifrados o encriptados en la memoria; y en el que la primera de la pluralidad de claves criptográficas está protegida.

En un segundo aspecto del invento, hay provisto preferiblemente un método para proteger los datos recibidos en un dispositivo de comunicación, el método comprende los pasos de: recibir los datos en un sistema de protección de

datos de dicho dispositivo de comunicación, en el que dicho sistema de protección de datos, al recibir los datos, procesa dichos datos cifrándolos o encriptándolos para protegerlos; almacenar dichos datos recibidos protegidos en una memoria de dicho dispositivo de comunicación; habilitar o capacitar el sistema de protección de datos antes de que dichos datos sean recibidos en dicho sistema de protección de datos o si no, restringir algunas o todas las demás operaciones del dispositivo de comunicación hasta que el sistema de protección de datos haya sido habilitado; almacenar una primera clave criptográfica y una segunda clave criptográfica en el dispositivo de comunicación, estando protegida la primera clave criptográfica; determinar si el dispositivo de comunicación (30) está en un primer estado operativo o en un segundo estado operativo; cifrar o encriptar los datos recibidos utilizando la primera clave criptográfica si el dispositivo de comunicación (30) está en el primer estado operativo; encriptar los datos recibidos utilizando la segunda clave criptográfica si el dispositivo de comunicación (30) está en el segundo estado operativo; y almacenar los datos recibidos cifrados o encriptados en la memoria del dispositivo de comunicación.

Aún en un aspecto adicional del invento, hay provisto preferiblemente un producto de programa de ordenador que comprende un medio o soporte legible por ordenador que incorpora un código de programa ejecutable mediante el procesador de un dispositivo informático para implementar el método del segundo aspecto del invento.

Otras características de los sistemas y métodos de protección de datos se describirán o se harán evidentes en el curso de la descripción detallada que sigue y de la reivindicaciones adjuntas.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La Fig. 1 es un diagrama de bloque que ilustra un sistema de comunicación en el cual se pueden utilizar dispositivos móviles.

La Fig. 2 es un diagrama de bloque de un dispositivo móvil en el cual se han incorporado un sistema y un método de protección de datos.

La Fig. 3 es un organigrama o diagrama de flujo que ilustra un método de habilitar o capacitar la protección de datos.

La Fig. 4 es un organigrama o diagrama de flujo que ilustra un método de protección de datos recibidos en un dispositivo móvil.

La Fig. 5A es un diagrama de bloque de un formato de datos.

La Fig. 5B es un diagrama de bloque de un formato de datos alternativo.

La Fig. 6 es un organigrama o diagrama de flujo en el que se ha ilustrado un método para obtener acceso a datos protegidos.

Las Figs. 7-11, son reproducciones de pantallas de una presentación de un dispositivo móvil en el cual se han incorporado un sistema y un método de protección de datos.

La Fig. 12 es un diagrama de bloque de un dispositivo de comunicación móvil inalámbrico.

DESCRIPCIÓN DE LAS REALIZACIONES PREFERIDAS

La Fig. 1 es un diagrama de bloque en el que se ha ilustrado un sistema de comunicación en el cual se pueden utilizar dispositivos móviles. El sistema de comunicación 10 incluye una Wide Area Network (WAN - Red de Área Extendida) 12, acoplada a un sistema de ordenador 14, una puerta o pasarela de red inalámbrica 16 y una Local Area Network (LAN - Red de Área Local) de empresa 18. La puerta o pasarela de red inalámbrica 16 está también conectada a una red de comunicaciones inalámbricas 20, en la cual está configurado para operar un dispositivo de comunicación móvil inalámbrico, el dispositivo móvil 22.

El sistema de ordenador 14 puede ser un PC de sobremesa o uno portátil, que esté configurado para comunicar con la WAN 12, la red Internet por ejemplo. Los PCs tales como el sistema de ordenador 14, tienen normalmente acceso a la red de Internet a través de un Proveedor de Servicios de Internet (ISP), de un Proveedor de Servicios de Aplicaciones (ASP), o similar.

La red LAN de empresa 18 es un ejemplo de un entorno de trabajo en el cual múltiples ordenadores 28 están conectados en una red. Tal red está frecuentemente situada detrás de un cortafuegos de seguridad 24. Dentro de la LAN 30 de empresa, un servidor de datos 26, que opera en un ordenador detrás del cortafuegos 24, actúa como la interfaz primaria para la empresa, para intercambiar datos tanto dentro de la LAN 18 como con otros sistemas y dispositivos externos, a través de la WAN 12. El servidor de datos 26 puede ser, por ejemplo, un servidor de mensajería tal como un Servidor de Intercambio Microsoft™, o un servidor de Lotus Domino™. Estos servidores proporcionan también funcionalidad adicional, tal como la de almacenamiento de base de datos dinámica para datos tales como de calendario, listas de lo que se ha de hacer, listas de tareas, correo electrónico, y documentación. Aunque solamente se ha ilustrado un servidor de datos 26 en la LAN 18, quienes sean expertos en la técnica apreciarán que una LAN puede

incluir más de un servidor, incluyendo otros tipos de servidor que soportan recursos que son compartidos entre los sistemas de ordenador 28 acoplados en la red.

El servidor de datos 28 proporciona capacidades de comunicación de datos a los sistemas de ordenador 28 acoplados en la red, acoplados en la LAN 18. Una LAN 18 típica incluye múltiples sistemas de ordenador 28, cada uno de los cuales materializa un cliente apropiado para comunicaciones con el servidor de datos 26. En el anterior ejemplo de mensajería electrónica, dentro de la LAN 18, los mensajes son recibidos por el servidor de datos 26, son distribuidos a los buzones apropiados para las cuentas de usuario dirigidas en el mensaje recibido, y son luego accedidos por un usuario a través de un cliente de mensajería que opera en un sistema de ordenador 28. El intercambio de otros tipos de datos distintos a los mensajes electrónicos es habilitado o capacitado de un modo similar utilizando clientes compatibles con el servidor de datos 26. Los clientes de fines múltiples, tales como el Lotus Botes, por ejemplo, manejan mensajes electrónicos, así como otros tipos de archivos y de datos.

La puerta o pasarela inalámbrica 16 proporciona una interfaz a una red inalámbrica 20, a través de la cual se pueden intercambiar datos, incluyendo los datos que deban ser protegidos, con un dispositivo móvil 22. El dispositivo móvil 22 puede ser, por ejemplo, un dispositivo de comunicación de datos, un dispositivo de comunicación de modo doble, tal como muchos teléfonos móviles con módem que tienen funcionalidad de comunicaciones tanto de datos como de voz, un dispositivo de múltiples modos capaz de comunicaciones de voz, de datos y de otros tipos, un asistente digital personal (PDA) habilitado o capacitado para comunicaciones inalámbricas, o un módem inalámbrico que opere conjuntamente con un sistema de ordenador, portátil o de sobremesa, o con algún otro dispositivo. En lo que sigue se describe con más detalle un dispositivo móvil que sirve de ejemplo.

Funciones tales como las de direccionamiento del dispositivo móvil 22, la de codificación o la de transformación de otro modo de mensajes para transmisión inalámbrica, u otras funciones de interfaz necesarias, se realizan mediante la puerta o pasarela de red inalámbrica 16. Cuando la puerta o pasarela de red inalámbrica 16 está configurada para operar con más de una red inalámbrica 20, también determina la misma una red que sea la más probable para localizar un dispositivo móvil dado 22, y posiblemente sigue los dispositivos móviles a medida que los usuarios se desplacen entre países o redes. Aunque solamente se ha representado una única puerta o pasarela de red inalámbrica 16 en la Fig. 1, el dispositivo móvil 22 podría ser configurado para comunicar con más de una puerta o pasarela, tal como una puerta o pasarela de red de empresa y una puerta o pasarela de WAP (Wireless Access Point o Punto de Acceso Inalámbrico), por ejemplo.

Cualquier sistema de ordenador con acceso a la WAN 12 puede potencialmente intercambiar datos con el dispositivo móvil 22 a través de la puerta o pasarela de red inalámbrica 16, con tal de que el dispositivo móvil 22 esté habilitado o capacitado para tales comunicaciones. Como alternativa, podrían también incorporarse puertas o pasarelas de redes inalámbricas privadas, tales como los “routers” (“enrutadores o encaminadores”) de la red privada virtual (VPN) inalámbrica, para proporcionar una interfaz privada con una red inalámbrica. Por ejemplo, una VPN inalámbrica incorporada en la LAN 18 puede proporcionar una interfaz privada de la LAN 18 con uno o más dispositivos móviles, tales como el 33, a través de la red inalámbrica 20, sin que para ello se requiera la puerta o pasarela de red inalámbrica 16. Tal interfaz privada a un dispositivo móvil 22 a través de la puerta o pasarela de red inalámbrica 16, y/o la red inalámbrica 20, puede también extenderse de un modo efectivo a entidades fuera de la LAN 18, proporcionándose para ello un sistema de envío o de modificación de la dirección de datos que opere conjuntamente con el servidor de datos 26.

Una red inalámbrica 20 entrega normalmente datos a y desde dispositivos de comunicación tales como el dispositivo móvil 22, a través de transmisiones de RF (radiofrecuencia) entre estaciones de base y dispositivos. La red inalámbrica 20 puede ser, por ejemplo, una red inalámbrica céntrica de datos, una red inalámbrica céntrica de voz, o una red de doble modo que pueda soportar comunicaciones tanto de voz como de datos con la misma infraestructura. Las redes de voz y de datos recientemente desarrolladas incluyen las redes de Acceso Múltiple con División de Código (CDMA), los Grupos Móviles Especiales, o el Sistema Global para comunicaciones móviles (GSM) y las redes de Servicio de Paquetes de Radio Generales (GPRS), y las redes de tercera generación (3G) como la de Datos Mejorados para Evolución Global (EDGE) y los Sistemas de Telecomunicaciones Móviles Universales (UMTS), que están actualmente en desarrollo. Las redes céntricas de datos más antiguas incluyen, aunque sin quedar limitadas a ellas, la Red de Radio Movitex™ (“Movitex”) y la Red de Radio Data TAC™ “Data TAC”), y las redes de datos céntricas de voz incluyen las redes de Sistemas de Comunicación Personal (PCS) como la de los sistemas de GSM y de Acceso Múltiple con División del Tiempo (TDMA) que han estado disponibles en Norteamérica y en todo el mundo durante varios años.

En el sistema 10, una compañía que posea la LAN de empresa 18 puede proporcionar a un empleado un dispositivo móvil 22 y acceso a la LAN 18 de la empresa. Se puede entonces obtener acceso a los datos de la empresa y almacenarlos en el dispositivo móvil 22. Cuando el usuario del dispositivo móvil 22 tenga acceso a la LAN 18 a través de un sistema de ordenador 28 con el cual pueda también comunicarse el dispositivo móvil 22, quedan disponibles otros caminos para obtener acceso a los datos de la empresa y almacenarlos en el dispositivo móvil 22. Aunque tales datos están corrientemente protegidos mientras son transferidos al dispositivo móvil 22, utilizando para ello técnicas de comunicación segura, esas técnicas no protegen los datos una vez que éstos hayan sido recibidos y almacenados en el dispositivo móvil 22.

Como se ha descrito anteriormente, el cifrado o encriptado de los datos cuando están almacenados en la memoria del dispositivo móvil 22 o antes de hacerlo, ofrece una cierta medida de seguridad. Para reducir los retrasos en el tiempo de acceso a los datos y la carga en el procesador asociada al descifrado o desencriptado de los datos, se prefiere una criptografía de clave simétrica. Sin embargo, las medidas de seguridad incorporadas para proteger la clave simétrica pueden también hacer que la clave sea inaccesible cuando hayan sido recibidos los datos. Por ejemplo, cuando el dispositivo móvil 22 incorpora protección por contraseña, una clave simétrica utilizada para el cifrado o encriptado de datos podría ser accesible únicamente cuando el dispositivo móvil 22 hubiese sido desbloqueado mediante la correcta entrada de una contraseña o frase de paso de seguridad. En este ejemplo, si el dispositivo móvil 22 recibe los datos cuando está bloqueado, cuando los datos son empujados al dispositivo móvil 22 sin haber sido solicitados, la clave simétrica no es accesible, y los datos no pueden ser cifrados o encriptados para almacenamiento.

Los sistemas y métodos de acuerdo con los aspectos del presente invento proporcionan protección de los datos recibidos cuando un dispositivo móvil está en cualquiera de una pluralidad de estados.

La Fig. 2 es un diagrama de bloque de un dispositivo móvil en el cual están incorporados un sistema y un método de protección de datos. Para quienes sean expertos en la técnica, será evidente que solamente se han ilustrado en la Fig. 2 los componentes que intervienen en el sistema de protección de datos. Un dispositivo móvil incluye, típicamente, otros componentes además de los ilustrados en la Fig. 2.

El dispositivo móvil 30 comprende una memoria 32, un sistema de protección de datos 49, un procesador 30, una interfaz de usuario (UI) 52, un transceptor inalámbrico 54 y una interfaz o conectador 56. La memoria 52 incluye, preferiblemente, un área de almacenamiento 34 para aplicaciones de software, un almacén de claves 42, y una pluralidad de almacenes de datos 36-40 y 44-48.

La memoria 32 es, o al menos incluye, un almacén gravable tal como una RAM, dentro del cual otros componentes del dispositivo pueden grabar datos. El almacén de aplicaciones de software 34 incluye aplicaciones de software que han sido instaladas en el dispositivo móvil 30, y puede incluir, por ejemplo, una aplicación de mensajería electrónica, una aplicación de gestión de información personal (PIM), juegos, así como otras aplicaciones. El almacén 36 de datos de aplicaciones almacena la información asociada con las aplicaciones de software en el dispositivo móvil 30, incluyendo no solamente datos, tales como las páginas web de almacenamiento intermedio o rápido (“caché”) para una aplicación de navegador, o archivos utilizados por aplicaciones de software, sino también datos de configuración para aplicaciones de software. Los mensajes electrónicos, tales como los mensajes recibidos y/o enviados por correo electrónico, son almacenados en el almacén de mensajes 38. Los datos tales como la información de programas, citas, y recordatorios, son almacenados en el almacén de calendario 40. El almacén de tareas 44 se utiliza para almacenar las tareas que un usuario desee seguir. Las notas y los memorándums entrados por un usuario se almacenan en el almacén de memorándums 46. El almacén 48 de entrada de textos almacena una lista de palabras o diccionario que soporta, por ejemplo, la entrada de texto de predicción y la corrección de errores automática cuando se entra texto en el dispositivo móvil 30. Aunque se han ilustrado como almacenes de datos separados, quienes sean expertos en la técnica apreciarán que algunos o todos los almacenes podrían ser consolidados en un solo almacén de datos en la memoria 32. También será evidente que un dispositivo móvil puede incluir además un número menor o diferente de almacenes de datos de los ilustrados en la Fig. 2.

El almacén de claves 42 almacena las claves criptográficas utilizadas para soportar la protección de datos en el dispositivo móvil 30, y preferiblemente reside en un componente de la memoria seguro en una parte asegurada de la memoria 32, a la cual se controla el acceso. Por ejemplo, un usuario de una aplicación de software no deberá poder borrar ni cambiar una clave de protección de datos en el almacén de claves 42. En una realización, el acceso al almacén de claves 42 está limitado al sistema de protección de datos 49. El sistema de protección de datos 49 cifra los datos recibidos y descifra los datos cifrados o encriptados almacenados en la memoria 32, como se describe con más detalle en lo que sigue.

El procesador 50 está conectado al transceptor inalámbrico 54 y por lo tanto habilita o capacita al dispositivo móvil 30 para comunicaciones a través de una red inalámbrica. La interfaz/conectador 56 proporciona un camino de comunicación alternativo para un PC u otro dispositivo que tenga una interfaz o conectador cooperante. La interfaz/conectador 56 podría ser cualquiera de una pluralidad de componentes de transferencia de datos, incluyendo, por ejemplo, una interfaz de transferencia de datos ópticos, tal como un puerto de Asociación de Datos de Infrarrojos (IrDA), alguna otra interfaz de comunicaciones inalámbricas de corto alcance, o bien una interfaz cableada, tal como un puerto en serie, un puerto de Universal Serial Bus (USB - Bus en Serie Universal), o bien una ranura Digital Segura (SD). Como interfaces para comunicaciones inalámbricas de corto alcance conocidas se incluyen, por ejemplo, los módulos Bluetooth™ y los módulos 802.11. Para quienes sean expertos en la técnica será evidente que el “Bluetooth” y el “802.11” designan conjuntos de especificaciones, disponibles en el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) de los EE.UU., relativas a las LANs inalámbricas y a las redes de área personal inalámbricas, respectivamente. Por lo tanto, un enlace de comunicación establecido a través de la interfaz/conectador 56 puede ser una conexión inalámbrica, o bien una conexión cableada física.

La UI 52 incluye componentes de la UI tales como un teclado, o un teclado numérico, o una pantalla de presentación, u otros componentes que acepten entradas desde, o proporcionen salidas a, un usuario del dispositivo

móvil 30. Aunque se ha ilustrado como un solo bloque en la Fig. 2, será evidente que un dispositivo móvil incluye, típicamente, más de una UI, y la UI 52 está por lo tanto destinada a representar una o más interfaces de usuario.

Los datos en cualquier almacén de datos, o en todos ellos, en un dispositivo móvil, pueden ser protegidos como se ha descrito aquí. En la mayor parte de las realizaciones prácticas, no es probable que las aplicaciones de software instaladas en un dispositivo móvil estén protegidas, aunque los otros almacenes de datos 36-38 y 44-48 almacenen corrientemente datos que un usuario, para datos personales, o un patrono, para datos de la empresa, pueda desear proteger.

En el dispositivo móvil 30, el acceso a la memoria 32 está controla por el sistema de protección de datos 49, el cual cifra los datos recibidos y almacena en la memoria 32 los datos cifrados o encriptados, y descifra los datos almacenados para otros componentes del dispositivo móvil. Todos los demás componentes del dispositivo móvil 30 están conectados al sistema de protección de datos 49, y las operaciones de leer y grabar en la memoria por esos otros componentes se efectúan a través del sistema 49 de protección de datos. Los datos recibidos por el sistema de protección de datos 49 desde el transceptor inalámbrico 54 o la UI 52, a través del procesador 50, desde una aplicación de software que esté siendo ejecutada por el procesador 50, o bien desde la interfaz/conectador 56, son cifrados o encriptados utilizando una clave almacenada en el almacén de claves 42. Análogamente, cuando se recibe una petición de datos protegidos por el sistema 49 de protección de datos desde un componente o aplicación de software en el dispositivo móvil 30, el sistema 49 de protección de datos descifra los datos cifrados o encriptados y pasa los datos descifrados o desencriptados al componente que los solicita. El sistema 49 de protección de datos se incorpora ya sea como un módulo de software, o ya sea como una utilidad que puede ser capacitada o incapacitada, como se describe con más detalle en lo que sigue, o bien un módulo de equipo físico configurado para gestionar la memoria 32, partes específicas de la memoria 32, o almacenes de datos o tipos de datos particulares.

Se apreciará que la disposición representada en la Fig. 2 está destinada a fines ilustrativos únicamente, y que el invento no queda en modo alguno limitado a ella. Por ejemplo, en una realización alternativa, el procesador 50, la interfaz/conectador 56, y otros sistemas del dispositivo, tienen acceso a la memoria 32, e interactúan con un sistema de protección de datos cuando datos cifrados o encriptados recuperados de la memoria 32 hayan de ser descifrados o desencriptados, y los datos recibidos hayan de ser cifrados o encriptados antes de ser almacenados en la memoria 32. En este caso, los sistemas y componentes del dispositivo móvil pasan los datos al sistema de protección de datos para cifrado y descifrado cuando sea necesario, pero acceden directamente a la memoria 32. Aunque la disposición ilustrada en la Fig. 2 proporciona un más estrecho control de la protección de datos por cuanto se controla el acceso a la memoria 32 mediante el sistema 49 de protección de datos, esta realización alternativa simplifica el soporte para los almacenes de datos no protegidos, ya que los datos no protegidos son recuperados directamente de la memoria 32, sin implicación alguna del sistema de protección de datos.

En funcionamiento, el sistema 49 de protección de datos accede a las claves criptográficas en el almacén de claves 42. De acuerdo con un aspecto del invento, el almacén de claves 42 almacena varias claves. Como se ha descrito anteriormente, se prefiere en general la criptografía simétrica para los dispositivos móviles limitados por el procesador, de tal modo que en al almacén de claves 42 se almacena una clave simétrica utilizada tanto para el cifrado o encriptado como para el descifrado o desencriptado de los datos protegidos, cuando se habilita o capacita la protección de datos. Aunque una contraseña o frase de paso de seguridad asegura el dispositivo móvil 30 contra su uso no autorizado, se prefieren en general otras medidas para proteger las claves simétricas, y por lo tanto los datos cifrados o encriptados, contra los denominados ataques al equipo físico. Por ejemplo, la protección mediante contraseña no protege el contenido de la memoria cuando los componentes físicos que comprende la memoria 32 son retirados del dispositivo móvil 30 para leer directamente los datos almacenados en los mismos. La clave simétrica es por lo tanto almacenada, preferiblemente, en el almacén de claves 42, en forma cifrada. Para el descifrado o desencriptado de la clave simétrica se requiere la correcta entrada de una contraseña del usuario.

Una vez descifrada, la clave simétrica es típicamente almacenada en el almacén de claves 42 o en otra área o almacén intermedio (“caché”) de la memoria, de modo que no haya de ser necesariamente descifrada cada vez que se necesite. Sin embargo, la clave simétrica descifrada se borra, preferiblemente, cuando se bloquea el dispositivo móvil 30, en respuesta a una orden del usuario, o bien automáticamente después de un período de tiempo de inactividad de seguridad previamente establecido, o bien cuando se almacena el dispositivo móvil 30 en una caja o bolsa de transporte, por ejemplo. La siguiente vez que se desbloquee el dispositivo móvil 30 con una contraseña correcta, se descifra de nuevo la clave simétrica cifrada.

Aunque el anterior esquema de cifrado o encriptado con clave proporciona un alto nivel de protección para una clave simétrica, y por lo tanto para los datos cifrados o encriptados utilizando la clave simétrica, no se dispone de una versión descifrada de la clave simétrica cuando el dispositivo móvil 30 está bloqueado. Como tal, cualesquiera datos recibidos cuando el dispositivo móvil 30 está bloqueado no pueden ser cifrados o encriptados utilizando la clave simétrica. Manteniendo la clave simétrica descifrada en la memoria después de bloqueado el dispositivo móvil 30, de modo que los datos puedan ser cifrados o encriptados cuando esté bloqueado el dispositivo móvil 30, se dejan los datos almacenados en la memoria 32 expuestos a ataques en el equipo físico. De acuerdo con un aspecto del invento, los datos descifrados o desencriptados almacenados en la memoria 32 se borran cuando el dispositivo móvil 30 entra en el estado de bloqueado. Alternativamente, el usuario podría ser apremiado para que entrase la contraseña cada vez que se reciban datos. Sin embargo, a menos que el usuario entre inmediatamente la contraseña, los datos recibidos deben

ser almacenados en la parte de libre acceso, al menos hasta la siguiente vez en que el usuario desbloquee el dispositivo móvil 30, o simplemente no ser almacenados en el dispositivo móvil 30. En este último caso, los datos recibidos se dejan en el dispositivo móvil 30 y deben ser retransmitidos al dispositivo.

De acuerdo con un aspecto del invento, el almacén de claves 42 almacena también un par de claves pública/privada. Una clave pública no es secreta, y es por lo tanto almacenada en la parte de libre acceso, incluso cuando el dispositivo móvil 30 esté bloqueado. Los datos cifrados o encriptados utilizando la clave pública solamente pueden ser descifrados o desencriptados utilizando la clave privada, la cual puede estar protegida de una manera similar a como lo está una clave simétrica. Por lo tanto, se utiliza la clave pública para cifrar datos recibidos cuando el dispositivo móvil 30 está bloqueado.

Por lo tanto, se utiliza una primera clave criptográfica, la clave simétrica, para cifrar los datos recibidos cuando el dispositivo móvil 30 está en un primer estado operativo, desbloqueado, y se utiliza una segunda clave criptográfica, la clave pública, para cifrar los datos recibidos cuando el dispositivo móvil 30 está en un segundo estado operativo, bloqueado. Los beneficios de la criptografía de clave simétrica se consiguen, por lo tanteo, para cualesquiera datos recibidos cuando el dispositivo móvil 30 está desbloqueado. El descifrado o desencriptado de tales datos es más rápido y requiere menos intervención del procesador, en comparación con otros esquemas criptográficos. Por otra parte, se evita el antes citado inconveniente de utilizar una clave simétrica protegida, almacenando para ello una clave pública para el cifrado o encriptado de datos cuando el dispositivo móvil 30 está bloqueado. Los datos cifrados o encriptados utilizando la clave pública son descifrados o desencriptados utilizando la correspondiente clave privada. Aunque la criptografía de clave pública es en general más lenta que la criptografía de clave simétrica, los retrasos para el acceso a los datos asociado al descifrado o desencriptado de datos son preferiblemente reducidos eligiendo para ello un esquema criptográfico de clave pública en el que las operaciones de descifrado o desencriptado son rápidas. Por ejemplo, la criptografía de curva elíptica (ECC) ofrece un descifrado o desencriptado significativamente más rápido que el de las técnicas de Rivest-Shamir-Adleman (RSA).

Como se ha descrito brevemente anteriormente, el sistema de protección de datos 49 puede ser implementado como un módulo de software o utilidad que se habilita o capacita cuando se hayan de proteger datos. La Fig. 3 es un organigrama o diagrama de flujo que ilustra un método de habilitar o capacitar la protección de datos. En el paso 60, la operación para habilitar o capacitar la protección de datos la ejecuta un dispositivo móvil. Esta operación es preferiblemente reclamada por un usuario del dispositivo móvil entrando para ello una orden, o bien seleccionando un elemento de un menú utilizando un teclado, un teclado numérico, un ratón, una rueda rastreadora de accionamiento con el pulgar, u otro dispositivo de entrada, por ejemplo. Sin embargo, deberá también apreciarse que un dispositivo móvil es preferiblemente configurable para requerir que un usuario habilite o capacite la protección de datos. Por ejemplo, cuando un patrono proporciona un dispositivo móvil a un usuario empleado, pero desea tener la seguridad de que todos los datos de la sociedad que estén en el dispositivo móvil quedan protegidos, se insertan en el dispositivo móvil, ya sea antes de que el dispositivo móvil sea proporcionado al usuario, o ya sea cuando se configure por primera vez el dispositivo móvil para operación por el usuario, un módulo de software o utilidad de control de la configuración e información de control de la configuración que especifique qué protección debe ser habilitada o capacitada. El módulo de control de la configuración reclama entonces automáticamente la operación en el paso 60, ó bien limita algunas o todas las demás operaciones del dispositivo móvil hasta que haya sido habilitada o capacitada la protección de datos.

Con objeto de proteger una clave simétrica utilizada para el cifrado o encriptado de datos y una clave privada utilizada para el descifrado o desencriptado de datos, deberá también capacitarse o habilitarse una protección mediante contraseña cuando se habilite o capacite la protección de datos, o antes de hacerlo. En el paso 62, se realiza una determinación acerca de si ha sido ya habilitada o capacitada la protección mediante contraseña. Cuando no haya sido habilitada o capacitada la protección mediante contraseña, se apremia al usuario para que habilite o capacite la protección mediante contraseña y establezca una contraseña en el paso 64. Se generan entonces claves de protección de datos y se almacenan en un almacén de claves en el paso 66, cuando ha sido ya habilitada o capacitada la protección mediante contraseña, o bien cuando el usuario haya habilitado o capacitado la protección mediante contraseña en el paso 64.

En las claves para protección de datos generadas en el paso 66 se incluye una clave simétrica utilizada tanto para cifrar los datos recibidos cuando el dispositivo móvil está en un estado de desbloqueado, antes de ser almacenados los datos en la memoria del dispositivo móvil, como para descifrar esos datos cifrados o encriptados cuando se recuperen de la memoria. Como se ha descrito anteriormente, esta clave simétrica es a su vez cifrada utilizando la contraseña establecida por el usuario. En el paso 66 se generan también un par de claves pública/privada. La clave pública se almacena en la parte de libre acceso, dado que no tiene que ser mantenida secreta, y se utiliza para cifrar los datos recibidos cuando el dispositivo móvil esté en estado de bloqueado. Los datos cifrados o encriptados utilizando la clave pública solamente pueden ser descifrados o desencriptados utilizando la clave privada, de tal modo que el compromiso de la clave público no es preocupante en cuanto a seguridad. Sin embargo, la clave privada, al igual que la clave simétrica, se almacena preferiblemente en el almacén de claves en una forma cifrada, cifrando para ello la clave privada utilizando la contraseña, por ejemplo.

Cualesquiera datos recibidos en un dispositivo móvil después de haber sido habilitada o capacitada la protección de datos son cifrados o encriptados antes de ser almacenados en la memoria. La Fig. 4 es un organigrama o diagrama de flujo que ilustra un método de protección de datos recibidos en un dispositivo móvil.

En el paso 72, los datos son recibidos en el dispositivo móvil. Con referencia a la Fig. 2, el dispositivo móvil 30 está configurado para recibir datos a través del transceptor inalámbrico 54, ó de la interfaz/conectador 56, así como por entrada del usuario a través de la UI 52. Las aplicaciones de software generan también típicamente datos para almacenamiento en la memoria 32. Cuando se hayan proporcionado otras interfaces, tales como una unidad de disco o una lectora de tarjeta de memoria extraíble por ejemplo, el paso 72 incluye también operaciones de recepción de datos desde esas interfaces.

En el paso 74 se determina entonces el estado operativo actual del dispositivo móvil. Cuando el dispositivo esté bloqueado, se recupera la clave pública y se cifran los datos recibidos utilizando la clave pública en el paso 78. Si el dispositivo móvil está desbloqueado, queda entonces disponible la clave simétrica. La clave simétrica descifrada se recupera del almacén de claves o de un almacenamiento intermedio si fue descifrada cuando se desbloqueó el dispositivo móvil, entrando para ello correctamente una contraseña. Por lo demás, la clave simétrica cifrada se recupera del almacén de claves, se descifra, y se utiliza luego para cifrar los datos recibidos en el paso 76.

De acuerdo con otro aspecto del invento, se hace en el paso 80 una determinación acerca de si los datos recibidos están relacionados con datos existentes que hayan sido ya almacenados en el dispositivo móvil, En el paso 82, los datos recibidos cifrados o encriptados se almacenan en la memoria, cuando no estén relacionados con datos existentes. Si los datos recibidos están relacionados con datos existentes, se agregan como apéndice los datos recibidos cifrados o encriptados a los datos existentes, en el paso 84. Por ejemplo, cuando el remitente de los datos recibidos, o bien un sistema intermedio tal como el servidor de datos 26 o la puerta o pasarela de red inalámbrica 16 de la Fig. 1, está configurado para enviar los datos al dispositivo móvil en bloques de hasta un tamaño predeterminado, se divide entonces un elemento de datos grande en bloques separados que son enviados al dispositivo móvil. En este caso, cada bloque de datos asociado con un elemento de datos particular recibido después de un primer bloque de datos para el mismo elemento de datos, es relacionado con cualesquiera bloques de datos previamente recibidos para el elemento de datos.

Quienes sean expertos en la técnica apreciarán que cuando un elemento de datos está separado en bloques de datos, cada bloque incluye información que permite al receptor reconstruir el elemento de datos. Esta información se tiene típicamente en forma de un identificador de sesión, un identificados de elemento de datos, un nombre de archivo, un número de secuencia, o algún otro identificador que se use del receptor para identificar otros bloques de datos para el elemento de datos. Aunque cada bloque de datos es cifrado o encriptado cuando se recibe en el dispositivo móvil, preferiblemente se almacena un identificador del elemento de datos o versión transformada del mismo, tal como un direccionamiento calculado del identificador, en el dispositivo móvil en la parte de libre acceso, y se utiliza en el paso 80 para determinar si los datos recibidos están relacionados con los datos existentes.

Si un elemento de datos incluye múltiples bloques de datos, se cifra entonces cada bloque de datos y se almacena a medida que se va recibiendo. Aunque cada bloque de datos comprende una parte del mismo elemento de datos, los bloques de datos son cifrados o encriptados por separado, utilizando un algoritmo y con dependencia de la clave sobre el estado operativo del dispositivo móvil cuando se recibe ese bloque de datos. Por lo tanto, un elemento de datos de múltiples bloques recibido, es almacenado como una serie de bloques de datos cifrados o encriptados independientemente. La Fig. 5A es un diagrama de bloque de un formato de datos que soporta tales elementos de datos.

El elemento de datos 85 incluye una referencia 86 del elemento de datos y tres partes 87, 88 y 89 del elemento de datos. Las partes 87, 88 y 89 del elemento de datos son preferiblemente almacenadas en una disposición ordenada de octetos a la que se hace referencia mediante la referencia 86 del elemento de datos. La referencia 86 del elemento de datos incluye un identificador del elemento de datos, tal como un identificador de mensaje de correo electrónico, o un identificador de sesión, por ejemplo, y una localización, o indicador, de la disposición ordenada de octetos en la cual está almacenadas las partes 87, 88 y 89 del elemento de datos. El identificador del elemento de datos soporta la determinación, en el paso 80, de la Fig. 4, y, conjuntamente con la localización, permite que sean recuperadas las partes 87, 88 y 89 del elemento de datos. Cada parte 87, 88 y 89 de elemento de datos incluye un cabecero 87A, 88A u 89A del bloque de datos, y un bloque de datos 87B, 88B u 89B. Los cabeceros 87A, 88A y 89A del bloque de datos incluyen una longitud y un identificador de clave correspondientes a cada bloque de datos 87B, 88B y 89B en el elemento de datos 85. La longitud del bloque de datos en un cabecero de bloque de datos indica la longitud, o alternativamente una localización o un indicador de un extremo del correspondiente bloque de datos, de modo que pueda ser debidamente recuperado cada bloque de datos. El identificador de la clave indica la clave, el algoritmo de cifra, o ambas cosas, que se utilizaron para cifrar un bloque de datos o que se requieren para descifrar el bloque de datos. Los bloques de datos 87B, 88B y 89B, representan bloques de datos recibidos que comprenden un solo elemento de datos, que han sido cifrados o encriptados.

En el ejemplo ilustrado en la Fig. 5A, el bloque de datos 1 fue recibido cuando estaba desbloqueado el dispositivo móvil, y como tal fue cifrado o encriptado utilizando la clave simétrica para generar el bloque de datos cifrado o encriptado 87B. Se determina la longitud del bloque de datos cifrado o encriptado 87B, y esa longitud y un identificador de clave “simétrica” se añaden al bloque de datos cifrado o encriptado 87B como el cabecero 87A del bloque. El cabecero 87A del bloque y el bloque de datos cifrado o encriptado 87B son luego almacenados en la memoria.

Preferiblemente, se crea una referencia del elemento de datos y se almacena cuando se recibe en un dispositivo móvil un elemento de datos, o bien el primer bloque de datos de un elemento de datos de múltiples bloques, de modo que el elemento de datos pueda ser recuperado, y subsiguientemente los bloques de datos relacionados o recibidos pueden ser identificados y añadidos como apéndice a la correspondiente disposición ordenada de octetos a la que se ha hecho referencia mediante la referencia del elemento de datos. Por consiguiente, la referencia 86 del elemento de datos fue creada cuando se recibió el bloque de datos 1, o posiblemente después de haber sido cifrado o encriptado el bloque de datos 1 y almacenado en el dispositivo móvil, e incluye un identificador del elemento de datos y una localización que indica dónde ha sido o será almacenada la parte 87 del elemento de datos.

El segundo bloque de datos del elemento de datos, el bloque de datos 2, fue recibido cuando el dispositivo móvil estaba bloqueado, y por lo tanto fue cifrado o encriptado utilizando la clave pública. El cabecero 88A del bloque 2 se genera y se añade al bloque de datos cifrado o encriptado 88B como se ha descrito anteriormente, y la parte 88 del elemento de datos resultante, que incluye el cabecero 88A del bloque y el bloque 88B de datos cifrados o encriptados, se añade como apéndice a la parte 87 del elemento de datos en la disposición ordenada a la que se ha hecho referencia mediante la referencia 86 del elemento de datos. El tercer bloque de datos, el bloque de datos 3, al igual que el bloque de datos 1, fue recibido mientras el dispositivo móvil estaba desbloqueado, y fue cifrado o encriptado utilizando la clave simétrica. La parte de datos 89, que comprende el cabecero 89A del bloque y el bloque de datos cifrado o encriptado 88B, es añadida como apéndice, de un modo similar, a la parte 88 del elemento de datos en la disposición ordenada a que se ha hecho referencia mediante la referencia 86 del elemento de datos.

De esta manera, los bloques de datos subsiguientes de un elemento de datos son cifrados o encriptados, se genera un cabecero del bloque, y se añade al bloque de datos cifrado o encriptado, y el cabecero del bloque y el bloque de datos cifrado se añaden como apéndice a un bloque de datos cifrado o encriptado precedente. En un esquema conocido para añadir de un modo efectivo nuevos datos a una disposición ordenada de octetos existente, se define una nueva disposición ordenada, se copia el contenido de la disposición ordenada existente en la nueva disposición ordenada, y se graban los nuevos datos en la nueva disposición ordenada. Se suprime entonces la referencia al espacio de la memoria ocupado por la disposición ordenada existente, o se reclama de otro modo para almacenamiento de otros datos. El proceso de copia en esta técnica tiende a ser lento, y es exigente en cuanto a memoria, por cuanto requiere suficiente espacio de memoria disponible para dos copias de la disposición ordenada de datos existente. El esquema de adición como apéndice descrito anteriormente es más rápido y requiere menos espacio de memoria que por esta técnica conocida.

Cuando se haya de obtener acceso al elemento de datos 85, tal como cuando un usuario seleccione el elemento de datos para su presentación, se localizan en la memoria la disposición ordenada de octetos en la cual se hallan las partes 87, 88 y 89 del elemento de datos, utilizando la localización de la referencia 86 del elemento de datos. Para cada bloque de datos cifrado o encriptado 87B, 88B y 89B, se determinan el esquema de descifrado o desencriptado apropiado y la longitud del bloque de datos cifrado o encriptado, a partir del identificador de clave y de la longitud en el correspondiente cabecero 87A, 88A y 89A del bloque. Cada uno de los bloques de datos cifrados o encriptados 87B, 88B y 89B es leído de la disposición ordenada de octetos y descifrado o desencriptado, y los bloques de datos descifrados o desencriptados se combinan en un solo elemento de datos descifrados o desencriptados, el cual corresponde al elemento de datos que fue transmitido al dispositivo móvil.

Quienes sean expertos en la técnica apreciarán que aunque las partes 87, 88 y 89 del elemento de datos se han representado en la Fig. 5A y se han descrito anteriormente como almacenadas en una disposición ordenada de octetos, las partes del elemento de datos no han de estar necesariamente almacenadas en localizaciones contiguas en la memoria. Típicamente, se utilizan indicadores de memoria u otros identificadores para enlazar lógicamente los bloques.

La Fig. 5B es un diagrama de bloque de un formato de datos alternativo. El elemento de datos 90 representa la estructura lógica de un elemento de datos, e incluye un cabecero 92 del elemento de datos y tres bloques de datos cifrados o encriptados 94, 96 y 98. El cabecero 92 incluye un identificador del elemento de datos e información tal como la de la longitud, la localización y el identificador de clave, para cada bloque de datos 94, 96 y 98 del elemento de datos 90. El cabecero 82 y los bloques de datos 94, 96 y 98 están de preferencia enlazados lógicamente, pero no han de estar necesariamente almacenados en lugares contiguos en la memoria.

Como en el ejemplo descrito anteriormente con referencia a la Fig. 5A, los bloques de datos 1, 2 y 3 fueron recibidos cuando el dispositivo móvil estaba desbloqueado, bloqueado, y desbloqueado, respectivamente. Los bloques de datos 1 y 3 fueron cifrados o encriptados utilizando la clave simétrica, y el bloque de datos 2 fue cifrado o encriptado utilizando la clave pública. El cabecero 92 fue preferiblemente creado y almacenado cuando se recibió el primer bloque de datos 94, se cifró, y se almacenó en el dispositivo móvil, de modo que el primer bloque de datos 94 pueda ser debidamente recuperado y descifrado o desencriptado, y subsiguientemente se puedan identificar los bloques de datos relacionados recibidos. La información para los bloques de datos cifrados o encriptados segundo y tercero 96 y 98 fue añadida al cabecero 92 cuando se recibieron esos bloques de datos. Cuando el dispositivo móvil está desbloqueado y se obtiene acceso al elemento de datos 90 en el dispositivo móvil, se localiza cada bloque utilizando la localización y la longitud en el cabecero 92, se determina el esquema de descifrado o desencriptado apropiado a partir del identificador de clave en el cabecero 92, y se recupera después cada bloque de datos, se descifra, y se combina para reconstruir el elemento de datos.

Como se ha descrito anteriormente y se ha ilustrado en las Figs. 5A y 5B, un solo elemento de datos puede incluir bloque de datos que fueron cifrados o encriptados utilizando diferentes esquemas de cifrado o encriptado, en donde los bloques de datos fueron recibidos en el dispositivo móvil cuando el dispositivo móvil estaba en diferentes estados operativos. Es también posible que el dispositivo móvil esté en el mismo estado operativo cuando se reciban los bloques de datos para el mismo elemento de datos. Por ejemplo, si el bloque de datos 2 hubiera sido recibido cuando el dispositivo móvil estaba en el estado de desbloqueado, habría sido entonces también cifrado o encriptado utilizando la clave simétrica. De acuerdo con otro aspecto del invento, antes de que sea cifrado o encriptado un bloque de datos recibido, se determina si el estado operativo actual del dispositivo móvil es el mismo que el estado operativo del dispositivo móvil cuando se recibió el bloque de datos precedente del mismo elemento de datos. Cuando el estado operativo, y por lo tanto la clave de protección de datos, sea el mismo para los datos recibidos que para un bloque de datos precedente de un elemento de datos, tanto el bloque precedente como los datos recibidos son cifrados o encriptados de la misma manera. En tal caso, el bloque de datos precedente se descifra de preferencia, si es posible, se añade como apéndice el bloque de datos recibido al bloque de datos precedente descifrado o desencriptado para formar un bloque de datos combinado, y se cifra el bloque de datos combinado y se almacena en la memoria. Puesto que el bloque de datos precedente es parte del bloque de datos combinado cifrado o encriptado, el espacio que ocupa en la memoria el bloque de datos precedente o bien se graba encima del mismo con el bloque de datos combinado cifrado o encriptado, o bien queda disponible para almacenar otros datos.

Este tipo de operación es posible, por ejemplo, cuando un bloque precedente y los datos recibidos se hayan recibido mientras está accesible la clave simétrica. Cuando el bloque precedente y los datos recibidos se hayan recibido cuando el dispositivo estaba bloqueado y se cifran utilizando la clave pública, la clave privada no es accesible, y no se puede descifrar el bloque precedente. Sin embargo, es posible un proceso similar de descifrado o desencriptado y vuelta a cifrar cuando se haga accesible la clave privada, tal como cuando se obtenga acceso al bloque precedente y a los datos recibidos, tal como se describe con más detalle en lo que sigue.

Aunque este cifrado o/vuelta a cifrar hace posible combinar más de un bloque de datos en un solo bloque de datos cifrado o encriptado, la adición como apéndice de bloques de datos cifrados o encriptados, tal como se ha descrito anteriormente, implica menos tiempo, menos memoria, y menor procesado de datos, y es por lo tanto preferido en general en los dispositivos móviles limitados con potencia, memoria y recursos de procesado limitados.

La Fig. 6 es un organigrama o diagrama de flujo en el que se muestra un método para obtener acceso a datos protegidos. En el paso 102, un sistema de protección de datos o un sistema o componente de dispositivo móvil, dependiendo de cómo hayan sido implementados el sistema de protección de datos y el esquema de acceso a la memoria, recupera los datos cifrados o encriptados. El sistema de protección de datos determina entonces si los datos cifrados o encriptados fueron cifrados o encriptados utilizando una clave simétrica o una clave pública, sobre la base de un identificador de clave. Se utiliza una clave privada correspondiente para descifrar los datos cifrados o encriptados en el paso 106 cuando los datos cifrados o encriptados fueron cifrados o encriptados utilizando una clave pública. Se utiliza la clave simétrica para descifrar los datos cifrados o encriptados en el paso 108, cuando los datos cifrados o encriptados fueron cifrados o encriptados utilizando la clave simétrica. Los datos descifrados o desencriptados son luego dados de salida al sistema o componente de dispositivo móvil que recuperó o solicitó los datos. Si los datos recuperados comprenden una pluralidad de bloques de datos, se realizan entonces los pasos 104 a 110 para cada bloque de datos.

Los pasos de descifrado o desencriptado 106 y 108 suponen que la clave pública o la clave simétrica son accesibles. En tanto que el dispositivo móvil sea desbloqueado cuando se obtiene acceso a datos protegidos, esas claves están o bien disponibles en la memoria, o bien pueden ser descifradas. Si las claves no son accesibles, los datos protegidos no pueden ser entonces descifrados o desencriptados.

Como se ha descrito anteriormente, la criptografía de la clave pública es típicamente más lenta que la criptografía de la clave simétrica. Cada vez que se reciben datos mientras el dispositivo móvil está bloqueado, o bien se descifra un elemento de datos que incluye tales datos, se deben efectuar las operaciones de descifrado o desencriptado de la clave pública en el dispositivo móvil. Cuando tales datos son descifrados o desencriptados en el paso 106, están entonces disponibles los datos descifrados o desencriptados en el dispositivo móvil. Durante las operaciones de descifrado o desencriptado, el dispositivo móvil está en un estado de desbloqueado; de tal modo que la clave simétrica es también accesible. De acuerdo con otro aspecto del invento, los datos descifrados o desencriptados que fueron previamente cifrados o encriptados utilizando la clave pública, son vueltos a cifrar utilizando la clave simétrica. Si es necesario, se actualiza también, en consecuencia, un cabecero del elemento de datos. Como alternativa, cuando cualesquiera bloques de datos de un elemento de datos hubieran sido cifrados o encriptados utilizando ka clave pública, los bloques de datos descifrados o desencriptados son concatenados para formar un solo bloque de datos combinado, el cual es luego vuelto a cifrar utilizando la clave simétrica. El elemento de datos original se reemplaza entonces en la memoria por el elemento de datos vuelto a cifrar. De esta manera, se evitan más operaciones de descifrado o desencriptado de la clave pública cuando se obtiene subsiguientemente acceso al elemento de datos.

Deberá también apreciarse que puede en cambio preferirse mantener bloques de datos cifrados o encriptados separados para un elemento de datos de múltiples bloques. Por ejemplo, cuando un elemento de datos de bloques de datos sea un mensaje de correo electrónico, la presentación del mensaje en un “buzón de entrada” o una lista de mensajes podría requerir datos de solamente un primer bloque de datos. En ese caso, la construcción del mensaje es mucho más rápida si se descifra solamente el primer bloque de datos de cada mensaje, en vez de cada mensaje entero.

La implementación particular y la configuración de un sistema y un método de protección de datos dependen del tipo de dispositivo en el cual se establezca la protección de datos. La interacción entre un usuario y un sistema de protección de datos puede ser diferente para los diferentes tipos de dispositivo. Las Figs. 7-11 son reproducciones o instantáneas de pantallas de una presentación en un dispositivo móvil en el cual se han implementado un sistema y un método de protección de datos, como un ejemplo ilustrativo de una posible implementación. Las reproducciones de pantallas de las Figs. 7-11 son representaciones de pantallas presentadas a un usuario en una presentación de un dispositivo móvil, en varias etapas durante la configuración de las características de seguridad. En las Figs. 7-11, a la protección de datos se la ha denominado como una protección del contenido.

En la Fig.7, un usuario ha seleccionado una operación para habilitar o capacitar la protección del contenido en el dispositivo móvil. Sin embargo, como se ha ilustrado en la parte superior de la Fig. 7, todavía no ha sido habilitada o capacitada la protección mediante contraseña, y al usuario se le apremia para que habilite o capacite la protección mediante contraseña. Si el usuario habilita o capacita la protección mediante contraseña, moviendo para ello un cursor desde “No” hasta “Sí”, y seleccionando “Sí”, entonces el usuario establece una contraseña y un período de tiempo de espera de seguridad, de 2 minutos en este ejemplo (Fig. 8), y se habilita o capacita la protección mediante contraseña. Si la protección mediante contraseña no está habilitada o capacitada y no se dispone de medios alternativos para asegurar las claves de la protección de datos, no se puede entonces habilitar o capacitar la protección del contenido. Estas operaciones anteriores son sustancialmente como se ha ilustrado en los pasos 60, 62 y 64 de la Fig. 3.

Una vez que haya sido habilitada o capacitada la protección mediante contraseña, se generan las claves de protección del contenido. En la Fig. 8, el par de claves de protección del contenido son un par de claves pública/privada. Los datos pseudo aleatorios se reúnen para la operación de generación de clave desde que el usuario pulsa la clave en un teclado o en un teclado numérico, y con el movimiento de un dispositivo de entrada de accionamiento con el pulgar en el dispositivo móvil. En un PC, tales datos se reúnen típicamente utilizando movimientos del ratón. Sin embargo, la mayor parte de los dispositivos móviles tienen pequeñas pantallas de presentación y no disponen de ratón, de tal modo que se utilizan las claves de teclado conjuntamente con el dispositivo de entrada con la rueda rastreadora de accionamiento con el pulgar, para proporcionar más datos aleatorios que podrían ser generados utilizando ya sea pulsaciones de la clave o ya sea las entradas con la rueda rastreadora de accionamiento con el pulgar, sola. En la Fig. 9 se ha ilustrado una pantalla que proporciona realimentación a un usuario, que indica el progreso de la recogida de información pseudo aleatoria. En una realización preferida, se recogen 160 bits de datos utilizados como clave privada, a partir de la cual se genera la pública. Análogamente, se genera una clave simétrica cuando se habilita o capacita la protección del contenido, utilizando ya sea la misma información pseudo aleatoria o ya sea otra información pseudo aleatoria recogida de una manera similar. El número de pulsaciones de clave y los movimientos con la rueda rastreadora de accionamiento con el pulgar se reduce, preferiblemente, utilizando para ello la misma información pseudo aleatoria para ambas operaciones de generación de clave. Cuando un sistema de protección de datos está configurado para utilizar una clave privada de 160 bits y una clave simétrica de 128 bits, por ejemplo, se recogen 160 bits de información aleatoria y se utilizan como la clave privada, y se utilizan 128 de los 160 bits como la clave simétrica.

Cuando las claves de protección de datos hayan sido generadas y almacenadas, se habilita o capacita la protección de datos, y aparece una pantalla de opciones de seguridad, como se ha ilustrado en la Fig. 10. Cuando el dispositivo móvil materialice otras características de seguridad, la pantalla de opciones de seguridad proporciona acceso para habilitar o capacitar, inhabilitar o incapacitar, o configurar, esas características, así como la protección del contenido. En la Fig. 10, una característica de seguridad de bloqueo del dispositivo móvil cuando se lleva en una bolsa de transporte, es accesible a través de la pantalla de opciones de seguridad.

Como otra medida de seguridad, cualesquiera requisitos de configuración para la protección del contenido no pueden ser preferiblemente inhabilitados o incapacitados mientras está habilitada o capacitada la protección del contenido. Por ejemplo, la inhabilitación o incapacitación de la protección de la contraseña sacrifica la seguridad de la clave privada y de la clave simétrica. Cuando un usuario trate de inhabilitar o incapacitar la protección de la contraseña mientras está habilitada o capacitada la protección del contenido, se presenta el mensaje de alerta representado en la Fig. 11. La protección de la contraseña no se habilita o capacita a menos que se habilite o capacite también la protección del contenido. Algunos tipos de dispositivo móvil soportan también información de control de la configuración para controlar aún más que características pueden ser capacitadas o incapacitadas por un usuario.

Cuando se inhabilita o incapacita la protección del contenido, son posibles varias operaciones. En una realización, los datos cifrados o encriptados almacenados se mantienen en forma cifrada. Las claves de protección de datos se descifran, y después se vuelven a cifrar con una contraseña predeterminada conocida por o accesible para el sistema de protección de datos. Aunque se mantienen los datos cifrados o encriptados almacenados, el descifrado o desencriptado de las claves de protección de datos, y por consiguiente el descifrado o desencriptado de los datos cifrados o encriptados cuando se tiene acceso a ellos, no requieren la entrada de una contraseña de usuario. En este esquema, se pueden utilizar las mismas claves de protección de datos si se habilita o capacita de nuevo la protección del contenido. En una realización alternativa, todos los datos cifrados o encriptados almacenados son descifrados o desencriptados y sustituidos en la memoria cuando se inhabilita o incapacita la protección del contenido. No se requiere entonces ninguna operación de descifrado o desencriptado para el subsiguiente acceso a los datos almacenados. Si se vuelve a habilitar o capacitar la protección del contenido, se generan entonces o se obtienen nuevas claves de protección de datos, se pueden cifrar los datos almacenados cuando sea posible, y subsiguientemente se cifran los datos recibidos, como se ha descrito anteriormente.

La Fig. 12 es un diagrama de bloque de un dispositivo de comunicación móvil inalámbrico. El dispositivo móvil 500 es preferiblemente un dispositivo de comunicación de dos vías, que tiene al menos capacidades de comunicación de voz y de datos. El dispositivo móvil 500 tiene preferiblemente la capacidad de comunicar con otros sistemas de ordenador en Internet. Dependiendo de la funcionalidad proporcionada por el dispositivo móvil 500, puede denominarse a éste como un dispositivo de mensajería de datos, un buscapersonar de dos vías, un teléfono móvil con capacidades de mensajería de datos, un aparato inalámbrico para Internet, o un dispositivo de comunicación de datos (con o sin capacidades de telefonía). Como se ha mencionado anteriormente, a tales dispositivos se les denomina aquí en general simplemente como dispositivos móviles.

El dispositivo móvil 500 incluye un transceptor 511, un microprocesador 538, una pantalla de presentación 522, una memoria no volátil 524, una memoria de acceso directo (RAM) 526, dispositivos 528 de entrada/salida (I/O) auxiliares, un puerto en serie 530, un teclado 532, un altavoz 534, un micrófono 536, un subsistema 540 de comunicaciones inalámbricas de corto alcance, y otros subsistemas 542 del dispositivo. El transceptor 511 incluye, preferiblemente, antenas de transmisión y de recepción 516, 518, un receptor (Rx) 512, un transmisor (Tx) 514, uno o más osciladores locales (Los) 513, y un procesador de señales digitales (DSP) 520. Dentro de la memoria no volátil 524, el dispositivo móvil 500 incluye una pluralidad de módulos de software 524A-524N, que pueden ser ejecutados por el microprocesador 538 (y/o por el DSP 520), incluyendo un módulo de comunicación de voz 524A, un módulo de comunicación de datos 524B, y una protección de datos de otros módulos operativos 524N para realizar una pluralidad de otras funciones.

El dispositivo móvil 500 es preferiblemente un dispositivo de comunicación de dos vías, que tiene capacidades de comunicación de voz y de datos. Así, por ejemplo, el dispositivo móvil 500 puede comunicar por una red de voz, tal como cualquiera de las redes celulares analógicas p digitales, y puede también comunicar por una red de datos. Las redes de voz y de datos se han representado en la Fig. 12 mediante la torre de comunicación 519. Estas redes de voz y de datos pueden ser redes de comunicación separadas que usen infraestructuras separadas, tales como estaciones de base, controladores de red, etc., o bien pueden estar integradas en una sola red inalámbrica. Las referencias a la red 519 deberán por lo tanto interpretarse como que abarcan tanto una sola red de voz y de datos, como redes separadas.

El subsistema de comunicación 511 se utiliza para comunicar con la red 519. Se utiliza el DSP 520 para enviar y recibir señales de comunicación a y desde el transmisor 514 y el receptor 512, y también para intercambiar información de control con el transmisor 514 y el receptor 512. Si las comunicaciones de voz y de datos tienen lugar en una sola frecuencia, o en un conjunto de frecuencias estrechamente espaciadas, puede utilizarse entonces un solo LO 513 conjuntamente con el transmisor 514 y el receptor 512. Alternativamente, si se utilizan diferentes frecuencias para comunicaciones de voz frente a las comunicaciones de datos, o si el dispositivo móvil está habilitado o capacitado para comunicaciones en más de una red 519, se pueden utilizar entonces una pluralidad de Los 513 para generar frecuencias correspondiente a las utilizadas en la red 519. Aunque en la Fig. 12 se han representado dos antenas 516, 518, el dispositivo móvil 500 podría utilizarse con una sola estructura de antena. La información, que incluye información tanto de voz como de datos, se comunica a y desde el módulo de comunicación 511, a través de un enlace entre el DSP 520 y el microprocesador 538.

El diseño detallado del subsistema 511 de comunicación, tal como el de la banda de frecuencia, la selección de componentes, el nivel de potencia, etc., dependen de la red de comunicaciones 519 en la cual esté destinado a operar el dispositivo móvil 500. Por ejemplo, un dispositivo móvil 500 destinado a operar en un mercado de América del Norte, puede incluir un subsistema de comunicación 511 diseñado para cooperar con las redes de comunicación de datos móviles Mobitex o Data TAC, y estar diseñado también para operar con cualquiera de entre una diversidad de redes de comunicación de voz, tales como las AMPS, la TDMA, la CDMA, la PCS, etc., mientras que un dispositivo móvil 500 destinado para uso en Europa puede estar configurado para operar con la red de comunicación de datos GPRS y con la red de comunicación de voz GSM. También pueden utilizarse otros tipos de redes de datos y de voz, tanto separadas como integradas, con el dispositivo móvil 500.

Los requisitos de acceso a la red de comunicaciones para el dispositivo móvil 500 varían también, dependiendo del tipo de red 519. Por ejemplo, en las redes de datos Mobitex y Data TAC, los dispositivos móviles se registran en la red utilizando un número de identificación único asociado a cada dispositivo. En las redes de datos GPRS, sin embargo, el acceso a la red va asociado a un abonado o usuario del dispositivo móvil 500. Un dispositivo GPRS requiere típicamente un módulo de identidad del abonado (“SIM”), el cual se requiere con objeto de operar el dispositivo móvil 500 en una red GPRS. Las funciones de comunicación locales o fuera de la red (si las hay) pueden ser operables, sin el SIM, pero el dispositivo móvil 500 es incapaz de desempeñar funciones en que intervengan comunicaciones por la red 519, aparte de cualesquiera de las operaciones legalmente requeridas, tales como la llamada de emergencia ‘911’.

Después de que se hayan completado cualesquiera procedimientos requeridos de activación o de registro, el dispositivo móvil 500 es capaz de enviar y recibir señales de comunicación, incluyendo, preferiblemente, tanto señales de voz como señales de datos, por la red 519. Las señales recibidas por la antena 516 desde la red de comunicaciones 519 son encaminadas al receptor 512, el cual proporciona la amplificación de la señal, la conversión de la frecuencia, el filtrado, la selección de canal, etc., y la conversión de analógica a digital. La conversión de analógica a digital de la señal recibida permite funciones más complejas de comunicaciones, tales como la de desmodulación y descodificación digital, a ser efectuadas utilizando el DSP 520. De una manera similar, las señales a ser transmitidas a la red 519 son procesadas, incluyendo la modulación y la codificación, por ejemplo, por el DSP 520, y son luego proporcionadas al

transmisor 514 para conversión de digital a analógica, conversión de frecuencia, filtrado, amplificación y transmisión a la red de comunicaciones 519, a través de la antena 518. Aunque se ha ilustrado un solo transceptor 511 para comunicaciones tanto de voz como de datos, en realizaciones alternativas el dispositivo móvil 500 puede incluir múltiples transceptores distintos, tales como un primer transceptor para transmitir y recibir señales de voz, y un segundo transceptor para transmitir y recibir señales de datos, o bien un primer transceptor configurado para operar dentro de una primera banda de frecuencia, y un segundo transceptor configurado para operar dentro de una segunda banda de frecuencia.

Además de procesar las señales de comunicaciones, el DSP 520 proporciona también control para el receptor y el transmisor. Por ejemplo, los niveles de ganancia aplicados a las señales de comunicación en el receptor 512 y en el transmisor 514 pueden controlarse adaptándolos a través de algoritmos de control automático de la ganancia, implementados en el DSP 520. También se podrían materializar otros algoritmos de control del transceptor en el DSP 520, con objeto de proporcionar un control más perfeccionado del transceptor 511.

El microprocesador 538 gestiona y controla, preferiblemente, la operación general del dispositivo móvil 500. Podrían utilizarse aquí muchos tipos de microprocesadores o de microcontroladores, o bien, alternativamente, se podría utilizar un solo DSP 520 para realizar las funciones del microprocesador 538. Las funciones de comunicación de bajo nivel, incluyendo al menos las comunicaciones de datos y de voz, se realizan a través del DSP 520 en el transceptor 511. Las aplicaciones de comunicación de alto nivel, incluyendo la aplicación de comunicación de voz 524A, y la aplicación de comunicación de datos 524B se almacenan en la memoria no volátil 524, para su ejecución por el microprocesador 538. Por ejemplo, el módulo 524A de comunicación de voz, proporciona una interfaz de usuario de alto nivel operable para transmitir y recibir llamadas de voz entre el dispositivo móvil 500 y una pluralidad de otros dispositivos de voz, a través de la red 529. Análogamente, el módulo 52aB de comunicación de datos proporciona una interfaz de usuario de alto nivel operable para enviar y recibir datos, tales como cortos mensajes de correo electrónico, archivos, información del organizador, mensajes cortos de texto, etc., entre el dispositivo móvil 500 y una pluralidad de otros dispositivos de datos, a través de la red 519.

El microprocesador 538 interactúa también con otros subsistemas del dispositivo, tales como la pantalla de presentación 522, la RAM 526, los dispositivos 528 de I/O auxiliar, el puerto en serie 530, el teclado 532, el altavoz 534, el micrófono 536, el subsistema de comunicaciones de corto alcance 540, y cualesquiera otros subsistemas del dispositivo designados en general por 542. Por ejemplo, los módulos 524A-N son ejecutados por el microprocesador 538 y pueden proporcionar una interfaz de alto nivel entre un usuario del dispositivo móvil y el dispositivo móvil. Esta interfaz incluye, típicamente, un componente gráfico que se proporciona a través de la pantalla de presentación 522, y un componente de entrada/salida que se proporciona a través de los dispositivos de I/O (entrada/salida) auxiliares 528, el teclado 532, el altavoz 534, o el micrófono 536.

Algunos de los subsistemas representados en la Fig. 12 realizan funciones relacionadas con la comunicación, mientras que otros subsistemas pueden realizar funciones de “residente” o de “en el dispositivo”. Notablemente, algunos subsistemas, tales como el teclado 532 y la pantalla de presentación 522 pueden utilizarse para ambas funciones relacionadas con la comunicación, tales como la de entrar un mensaje de texto para su transmisión por una red de comunicación de datos, y funciones residentes en el dispositivo tales como la de una calculadora o la de una lista de tareas, u otras funciones del tipo de PDA.

El software del sistema operativo utilizado por el microprocesador 538 está preferiblemente almacenado en un almacén persistente, tal como la memoria no volátil 524. Además del sistema operativo y de los módulos de comunicación 524A-N, la memoria no volátil 524 puede incluir un sistema de archivo para almacenar datos. La memoria no volátil 524 incluye también al menos un almacén de claves, así como los datos protegidos descritos anteriormente. El sistema operativo, las aplicaciones o módulos del dispositivo específico, o partes del mismo, están típicamente cargados temporalmente en una memoria volátil, tal como la RAM 526, para una más rápida operación. Además, las señales de comunicación recibidas pueden ser también almacenadas temporalmente en la RAM 526, antes de grabarlas permanentemente en un sistema de archivo situado en la memoria no volátil 524. La memoria no volátil 524 puede materializarse, por ejemplo, con una memoria rápida de estado sólido, una RAM no volátil, o una RAM con el apoyo de una batería.

Un módulo de aplicación que sirve de ejemplo, 524N, que puede ser cargado en el dispositivo móvil 500, es una aplicación PIM que proporciona funcionalidad de PDA, tal como de acontecimientos de calendario, citas, y elementos de tarea. Este módulo 524N puede también interactuar con el módulo de comunicación de voz 524A para gestionar llamadas de teléfono, correos de mensaje de voz, etc., y puede también interactuar con el módulo de comunicación de voz 524B para gestionar comunicaciones de correo electrónico y otras transmisiones de datos. Alternativamente, toda la funcionalidad del módulo de comunicación de voz 524A y del módulo de comunicación de datos 524B, puede ser integrada en el módulo de PIM.

La memoria no volátil 524 proporciona preferiblemente un sistema de archivo para facilitar el almacenamiento de los elementos de datos de PIM en el dispositivo. La aplicación de PIM incluye, preferiblemente, la capacidad para enviar y recibir elementos de datos, ya sea por sí misma o ya sea conjuntamente con los módulos de comunicación de voz y de datos 524A, 524B, a través de la red inalámbrica 519. Los elementos de datos de PIM son preferiblemente integrados sin solución de continuidad, sincronizados y actualizador, a través de la red inalámbrica 519, con un conjunto

correspondiente de elementos de datos almacenados o asociados con un sistema de ordenador central, creando con ello un sistema con simetría de espejo para los elementos de datos asociados con un usuario particular.

El dispositivo móvil 500 se sincroniza manualmente con un sistema central, colocando para ello el dispositivo móvil 500 en una cuna de interfaz, la cual acopla el puerto en serie 530 del dispositivo móvil 500 con un puerto en serie del sistema central. El puerto en serie 530 puede ser utilizado también para descargar otros módulos de aplicación 524N para su instalación en el dispositivo móvil 500. Este camino de descarga cableado puede además ser utilizado para cargar claves de cifrado o encriptado en el dispositivo móvil 500, para uso en comunicaciones seguras, lo cual es un método más seguro que el de intercambio de la información cifrada a través de la red inalámbrica 519. Como una alternativa a la generación de clave de protección de datos en el dispositivo descrita anteriormente, las claves de protección de datos podrían ser generadas por otro sistema y transferidas al dispositivo móvil 500 de esta manera.

Los módulos de aplicación de software 524N pueden ser cargados en el dispositivo móvil 500 a través de la red 519, a través de un subsistema de I/O auxiliar 528, a través del subsistema de corto alcance 540, o a través de cualquier otro subsistema adecuado 542, e instalados por un usuario en la memoria no volátil 524 ó en la RAM 526. Tal flexibilidad en la instalación de la aplicación aumenta la funcionalidad del dispositivo móvil 500, y puede proporcionar mejores funciones del dispositivo, funciones relacionadas con la comunicación, o ambas. Por ejemplo, las aplicaciones de comunicación segura pueden habilitar o capacitar funciones de comercio electrónico y otras de tales transacciones financieras, para que sean efectuadas utilizando el dispositivo móvil 500.

Cuando el dispositivo móvil 500 está operando en un modo de comunicación de datos, una señal recibida, tal como un mensaje de texto o una descarga de una página web, se procesa por el transceptor 511 y se proporciona al microprocesador 538, el cual preferiblemente procesa además la señal recibida para darle salida a la pantalla de presentación 522, o bien, alternativamente, a un dispositivo de I/O auxiliar 528. Cuando está habilitada o capacitada la protección de datos, los datos recibidos son cifrados o encriptados tal como se ha descrito anteriormente antes de ser almacenados en el dispositivo móvil 500. Un usuario del dispositivo móvil 500 puede también componer elementos de datos, tales como mensajes de correo electrónico, utilizando el teclado 532, el cual es preferiblemente un teclado alfanumérico completo dispuesto en el estilo QWERTY, aunque se pueden utilizar también otros estilos de teclados alfanuméricos completos, tales como el conocido DVORAK. La entrada del usuario al dispositivo móvil 500 se mejora además con la pluralidad de dispositivos de I/O auxiliar 528, los cuales pueden incluir un dispositivo de entrada de rueda rastreadora de accionamiento con el pulgar, una pantalla táctil, una diversidad de conmutadores, un conmutador de entrada basculante, etc. Los elementos de datos compuestos dados de entrada por el usuario son luego transmitidos por la red de comunicaciones 519 a través del transceptor 511, y pueden ser también almacenados en forma cifrada en el dispositivo móvil 500.

Cuando el dispositivo móvil 500 está operando en un modo de comunicación de voz, la operación total del dispositivo móvil 500 es sustancialmente similar al modo de datos, excepto en que las señales recibidas son dadas de salida al altavoz 534 y se generan señales de voz para su transmisión mediante un micrófono 536. En el dispositivo móvil 500 se pueden incorporar también dispositivos de I/O de audio o de voz alternativos, tales como un subsistema de registro de mensajes de voz. La pantalla de presentación 522 puede ser también utilizada para proporcionar una indicación de la identidad de una parte que llame, la duración de una llamada de voz, u otra información relacionada con una llamada de voz. Por ejemplo, el microprocesador 538, conjuntamente con el módulo de comunicación de voz 524A y el software del sistema operativo, pueden detectar la información de identificación de quien llama, correspondiente a una llamada de voz que llegue, y presentarla en la pantalla de presentación 522. Aunque las técnicas de protección de datos descritas anteriormente podrían no tener que ser necesariamente aplicadas a comunicaciones de voz, ya que las señales de comunicación de voz no son típicamente almacenadas, algunas informaciones relacionadas con la comunicación de voz, tales como la información de contacto, pueden ser protegidas.

En el dispositivo móvil 500 está también incluido un subsistema de comunicaciones de corto alcance 540. Por ejemplo, el subsistema 540 puede incluir un dispositivo de infrarrojos y circuitos y componentes asociados, o bien un módulo de comunicación Bluetooth u 802.11 inalámbrico de corto alcance, para permitir comunicación con sistemas y dispositivos habilitados o capacitados de un modo similar.

Se apreciará que la descripción hecha anteriormente se refiere a realizaciones preferidas, únicamente a modo de ejemplos. Para aquellos que son expertos y conocen este campo, serán evidentes muchas variaciones en los sistemas y métodos descritos anteriormente, y tales variaciones lógicas están dentro del alcance del invento tal como se describe y reivindica.

Por ejemplo, un dispositivo en el cual puedan estar incorporados los sistemas y métodos descritos anteriormente puede incluir menos, más o diferente número de componentes de los representados en los dibujos. Aunque la protección de datos es quizás más pertinente para dispositivos móviles, los cuales por su propia naturaleza son difíciles de asegurar físicamente, las técnicas aquí descritas son también aplicables a PCs, así como a otros sistemas típicamente fijos.

El invento no es de ningún modo dependiente de cualesquiera características particulares de la comunicación. La protección de datos como la que aquí se ha descrito podría ser incorporada a dispositivos de comunicación de dos vías o de una vía (de recepción únicamente).

Además, aunque anteriormente se ha descrito principalmente la protección de datos en el contexto de los datos recibidos después de haber sido habilitada o capacitada la protección de datos, los datos existentes que hayan sido ya almacenados en el dispositivo móvil antes de haber habilitado o capacitado la protección de datos, son también preferiblemente cifrados o encriptados cuando se habilita o capacita la protección de datos, cuando el formato de los datos almacenados lo permita.

REIVINDICACIONES

1. Un dispositivo de comunicación (30) para proteger los datos recibidos en dicho dispositivo de comunicación (30), comprendiendo el dispositivo de comunicación (30):

una memoria (32) configurada para almacenar datos;

un módulo de protección de datos (49) de dicho dispositivo de comunicación (30) configurado para recibir datos, para proteger los datos recibidos mediante el cifrado o encriptación de dichos datos recibidos, y para almacenar los datos recibidos protegidos en la memoria (32);

medios para habilitar o capacitar el módulo de protección de datos (49), estando dichos medios configurados para restringir algunas o todas las demás operaciones del dispositivo de comunicación (30) hasta que la protección de datos haya sido habilitada;

en el que el dispositivo de comunicación (30) tiene un primer estado operativo y un segundo estado operativo; y

un almacén de claves (42) configurado para almacenar una pluralidad de claves criptográficas;

en el que el módulo de protección de datos (49) está configurado para determinar si el dispositivo de comunicación (30) está en el primer estado operativo o en el segundo estado operativo, para cifrar o encriptar los datos recibidos utilizando una primera de la pluralidad de claves criptográficas si el dispositivo de comunicación está en el primer estado operativo o una segunda de la pluralidad de claves criptográficas si el dispositivo de comunicación está en el segundo estado operativo, y almacenar los datos recibidos cifrados o encriptados en la memoria (32); y

en el que la primera de la pluralidad de claves criptográficas está protegida.

2. El dispositivo de comunicación (30) de la reivindicación 1, en el que los medios que habilitan el módulo de protección de datos están configurados para invocar automáticamente una operación para habilitar o capacitar la protección de datos en el dispositivo de comunicación (30) o si no, restringir algunas o todas las demás operaciones del dispositivo de comunicación (30) hasta que la protección de datos haya sido habilitada.

3. El dispositivo de comunicación (30) de la reivindicación 2, en el que los medios que habilitan el módulo de protección de datos están configurados para invocar automáticamente una operación para requerir que un usuario habilite o capacite la protección de datos en el dispositivo de comunicación (30) o si no, restringir algunas o todas las demás operaciones del dispositivo de comunicación (30) hasta que la protección de datos haya sido habilitada por el usuario.

4. El dispositivo de comunicación (30) de una cualquiera de las reivindicaciones anteriores, en el que los medios que habilitan el módulo de protección de datos comprenden un módulo de control de configuración implementada de software.

5. El dispositivo de comunicación (30) de una cualquiera de las reivindicaciones anteriores, en el que la primera clave criptográfica es inaccesible cuando el dispositivo de comunicación (30) está en el segundo estado operativo.

6. El dispositivo de comunicación (30) de la reivindicación 5, en el que el primer estado operativo es un estado de desbloqueado, y en el que el segundo estado operativo es un estado de bloqueado.

7. El dispositivo de comunicación (30) de la reivindicación 5 ó de la reivindicación 6, en el que la primera clave criptográfica es una clave simétrica, y en el que la segunda clave criptográfica es una clave pública.

8. El dispositivo de comunicación (30) de la reivindicación 7, en el que la clave pública está asociada con una clave privada, y en el que el módulo de protección de datos (49) está además configurado para determinar si los datos cifrados o encriptados fueron cifrados o encriptados utilizando la clave pública o la clave simétrica, para descifrar o desencriptar los datos cifrados o encriptados utilizando la clave privada si los datos cifrados o encriptados hubieran sido cifrados o encriptados utilizando la clave pública, y para descifrar o desencriptar los datos cifrados o encriptados utilizando la clave simétrica si los datos cifrados o encriptados hubieran sido cifrados o encriptados utilizando la clave simétrica.

9. El dispositivo de comunicación (30) de una cualquiera de las reivindicaciones anteriores, en el que el dispositivo de comunicación (30) comprende un dispositivo de comunicación móvil inalámbrico seleccionado del grupo consistente en: un dispositivo de comunicación de datos, un teléfono móvil que tiene funcionalidad de comunicaciones tanto de datos como de voz, un dispositivo de modo múltiple capaz de comunicaciones de voz, de datos y de comunicaciones de otros tipos, un dispositivo de mensajería, un asistente digital personal (PDA) habilitado o capacitado para comunicaciones inalámbricas, un módem inalámbrico, un dispositivo de comunicación de una vía, y un dispositivo de comunicación de dos vías.

10. Un método de protección de datos recibidos en un dispositivo de comunicación (30), comprendiendo el métodos los pasos de:

recibir los datos en un sistema de protección de datos (49) de dicho dispositivo de comunicación (30), en el que dicho sistema de protección de datos, al recibir los datos, los procesa mediante el cifrado o encriptación de los mismos para protegerlos;

almacenar dichos datos recibidos protegidos en una memoria (32) de dicho dispositivo de comunicación (30);

habilitar o capacitar el sistema de protección de datos (49) antes de que dichos datos sean recibidos en dicho sistema de protección de datos (49) o si no, restringir algunas o todas las demás operaciones del dispositivo de comunicación (30) hasta que el sistema de protección de datos (49) haya sido habilitado;

almacenar (66) una primera clave criptográfica y una segunda clave criptográfica en el dispositivo de comunicación (30), estando protegida la primera clave criptográfica;

determinar (74) si el dispositivo de comunicación (30) está en un primer estado operativo o en un segundo estado operativo;

encriptar (78) los datos recibidos utilizando la primera clave criptográfica si el dispositivo de comunicación (30) está en el primer estado operativo;

encriptar (76) los datos recibidos utilizando la segunda clave criptográfica si el dispositivo de comunicación (30) está en el segundo estado operativo; y

almacenar (82) los datos recibidos encriptados en la memoria (32) del dispositivo de comunicación (30).

11. El método de la reivindicación 10, que comprende además invocar automáticamente una operación para habilitar o capacitar la protección de datos en el dispositivo de comunicación (30) o si no, restringir algunas o todas las operaciones del dispositivo de comunicación (30) hasta que la protección de datos haya sido habilitada.

12. El método de la reivindicación 11, que comprende además invocar automáticamente una operación para requerir a un usuario que habilite o capacite la protección de datos en el dispositivo de comunicación (30) o si no, restringir algunas o todas las demás operaciones del dispositivo de comunicación (30) hasta que la protección de datos haya sido habilitada por el usuario.

13. El método de una cualquiera de las reivindicaciones 10 a 12, en el que un medio para habilitar o capacitar el sistema de protección de datos (49) es proporcionado o provisto como un módulo de control de configuración implementada de software.

14. El método de la reivindicación 13, en el que los medios que habilitan el sistema de protección de datos son proporcionados al dispositivo de comunicación (30) antes de que dicho dispositivo sea provisto o proporcionado a un usuario o cuando el dispositivo de comunicación (30) está primero configurado para ser operado por un usuario.

15. El método de una cualquiera de las reivindicaciones 10 a 12, en el que el segundo estado operativo es un estado operativo de bloqueado en el cual la primera clave criptográfica es inaccesible y el primer estado operativo es un estado operativo de desbloqueado en el cual la primera clave criptográfica es accesible.

16. El método de la reivindicación 15, que además comprende el paso de almacenar la clave privada en el dispositivo de comunicación (30), en el que la primera clave criptográfica es una clave simétrica que está almacenada de forma cifrada o encriptada, y la segunda clave criptográfica es una clave pública asociada con una clave privada.

17. El método de la reivindicación 16, que además comprende determinar si los datos cifrados o encriptados fueron cifrados o encriptados utilizando la clave pública o la clave simétrica, descifrando o desencriptando los datos cifrados o encriptados utilizando la clave privada si los datos cifrados o encriptados fueron cifrados o encriptados utilizando la clave pública, y descifrando o desencriptando los datos cifrados o encriptados utilizando la clave simétrica si los datos cifrados o encriptados fueron cifrados o encriptados utilizando la clave simétrica.

18. Un producto de programa de ordenador para proteger los datos recibidos en un dispositivo de comunicación (30), comprendiendo dicho producto de programa de ordenador un medio legible por ordenador que incorpora un código de programa ejecutable mediante el procesador de un dispositivo informático para implementar el método de una cualquiera de las reivindicaciones 10 a 17.

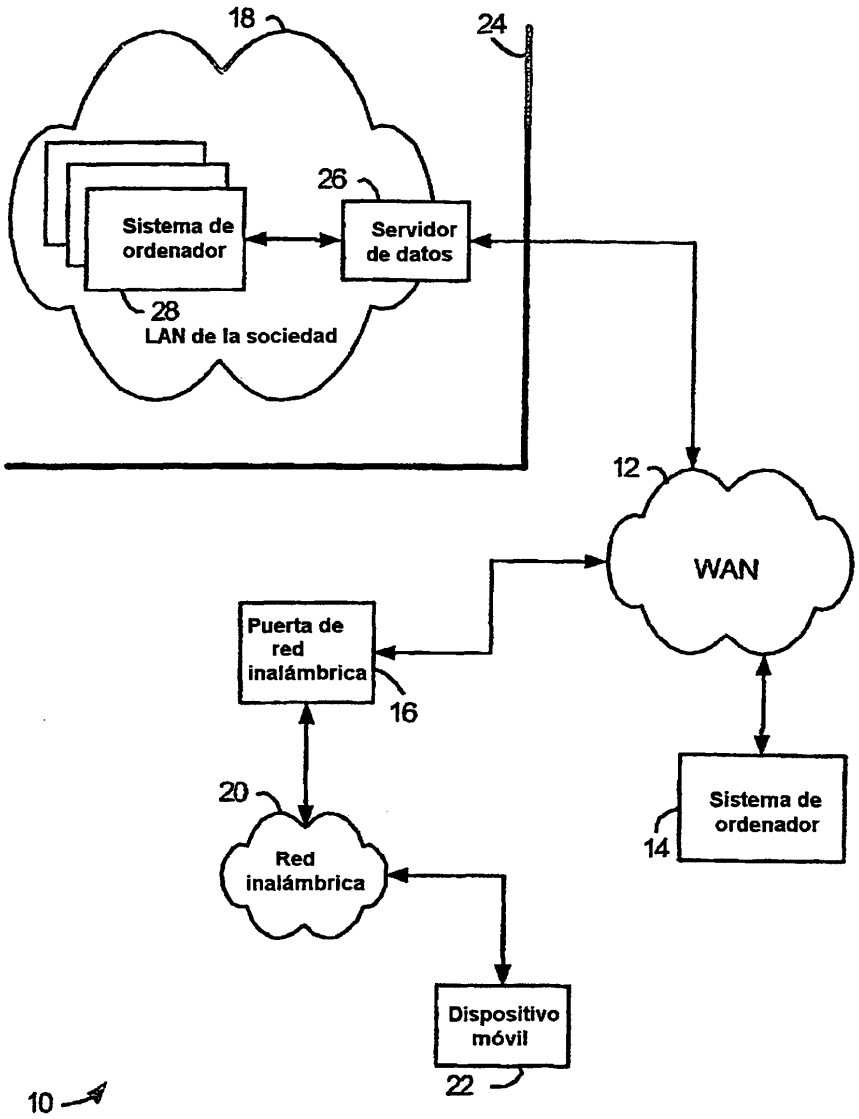
18
24
26
Sistema de ordenador
Servidor de datos
28
LAN de la sociedad
12
WAN
Puerta de red inalámbrica
16
20
Red inalámbrica
Sistema de ordenador
14
Dispositivo móvil
22
10

FIG. 1

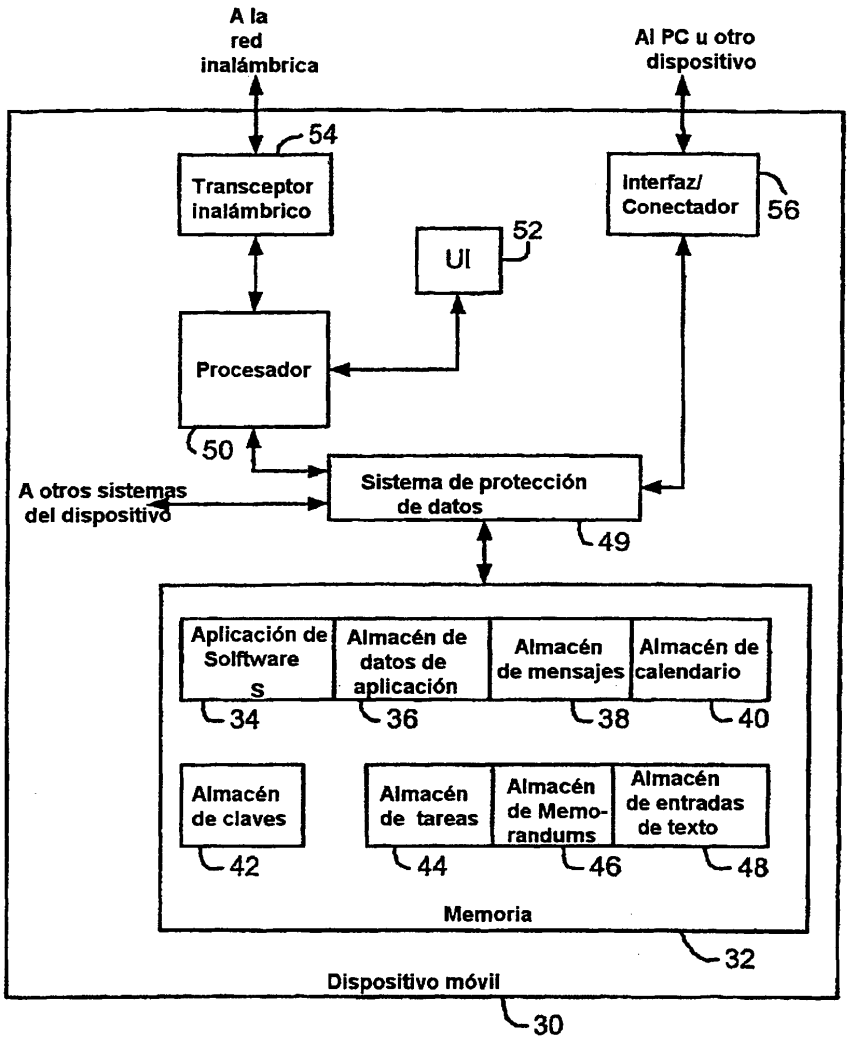
A la red inalámbrica
Al PC u otro dispositivo
54
Transceptor inalámbrico
Interfaz/ Conectador
56
52
UI
Procesador
50
A otros sistemas del dispositivo
Sistema de protección de datos
49
Aplicación de Solftware s
Almacén de datos de aplicación
Almacén de mensajes
Almacén de calendario
34
36
38
40
Almacén de claves
Almacén de tareas
Almacén de Memo-randums
Almacén de entradas de texto
42
44
46
48
Memoria
32
Dispositivo móvil
30

FIG. 2

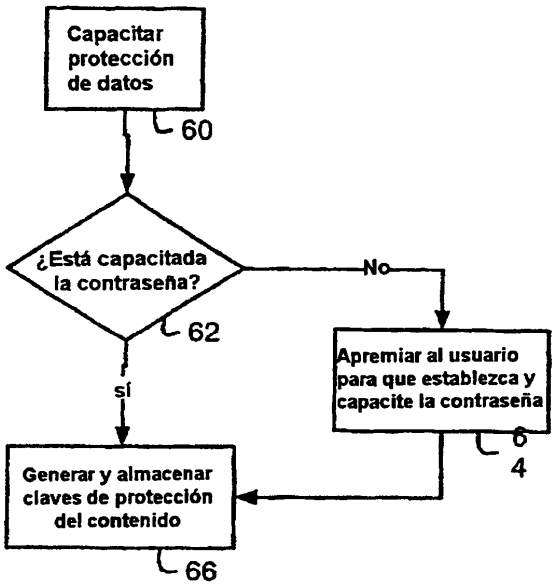
Capacitar protección de datos
60
¿Está capacitada la contraseña?
62
No
Apremiar al usuario para que establezca y capacite la contraseña
64
sí
Generar y almacenar claves de protección del contenido
66

FIG. 3

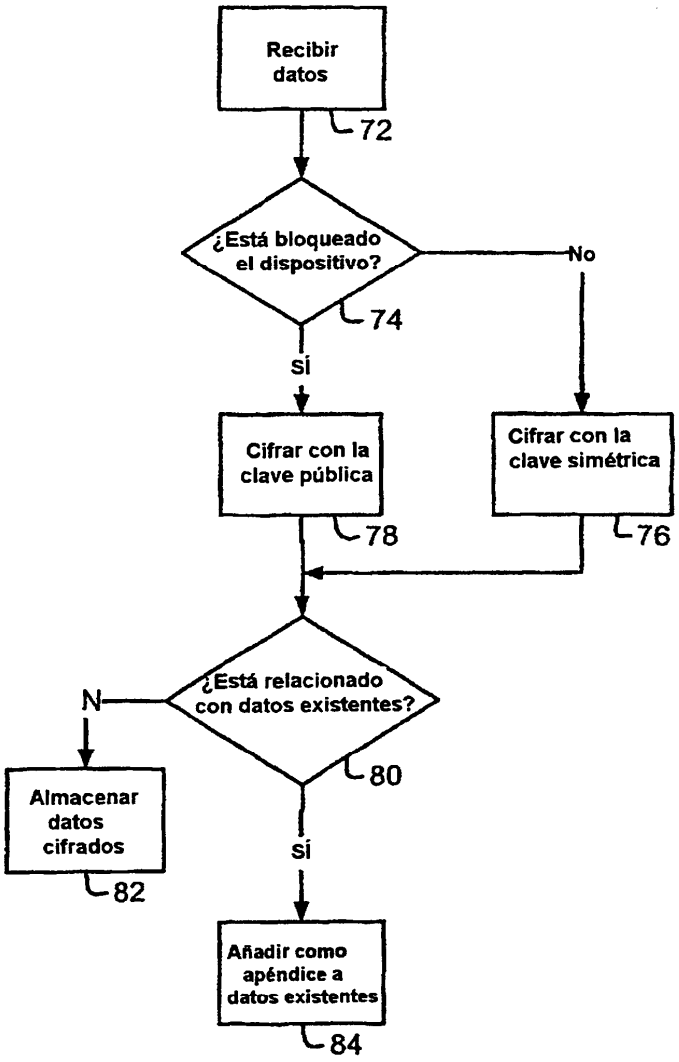
Recibir datos
72
¿Está bloqueado el dispositivo?
74
No
Sí
Cifrar con la clave pública
78
Cifrar con la clave simétrica
76
¿Está relacionado con datos existentes?
80
N
Sí
Almacenar datos cifrados
82
Añadir como apéndice a datos existentes
84

FIG. 4

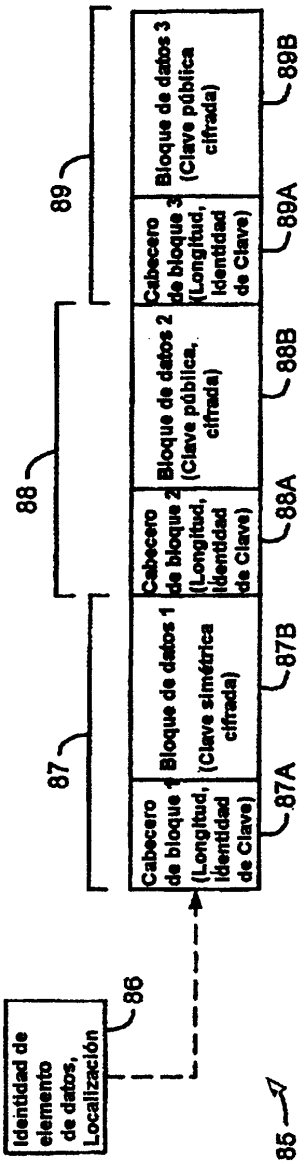
Identidad de elemento de datos, Localización
86
85
87
87A
Cabecero de bloque 1 (Longitud, Identidad de Clave)
87B
Bloque de datos 1 (Clave simétrica cifrada)
88
88A
Cabecero de bloque 2 (Longitud, Identidad de Clave)
88B
Bloque de datos 2 (Clave pública, cifrada)
89
89A
Cabecero de bloque 3 (Longitud, Identidad de Clave)
89B
Bloque de datos 3 (Clave pública cifrada)

FIG. 5A

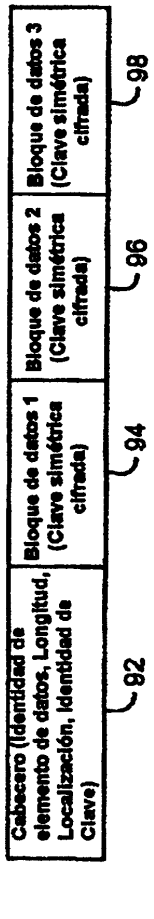
Cabecero (Identidad de elemento de datos, Longitud, Localización, Identidad de Clave)
92
Bloque de datos 1 (Clave simétrica cifrada)
94
Bloque de datos 2 (Clave simétrica cifrada)
96
Bloque de datos 3 (Clave simétrica cifrada)
98
90

FIG. 5B

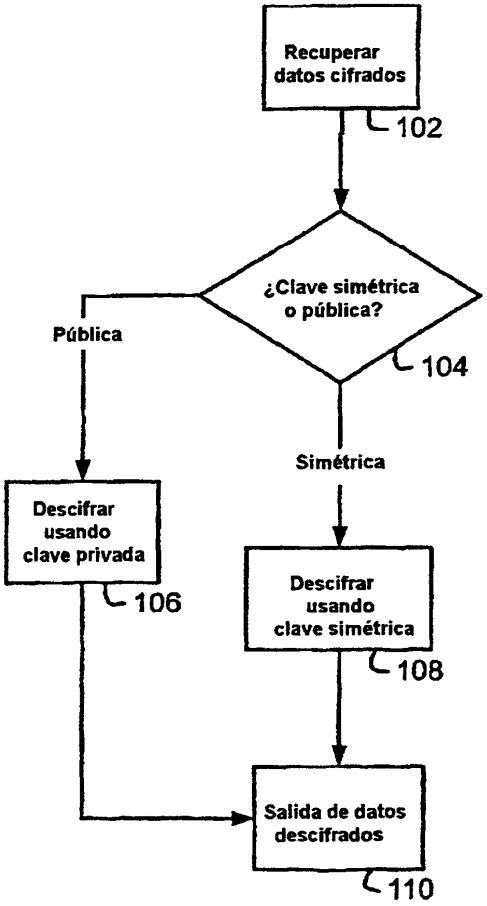
Recuperar datos cifrados
102
¿Clave simétrica o pública?
104
Pública
Simétrica
Descifrar usando clave privada
106
Descifrar usando clave simétrica
108
Salida de datos descifrados
110

FIG. 6

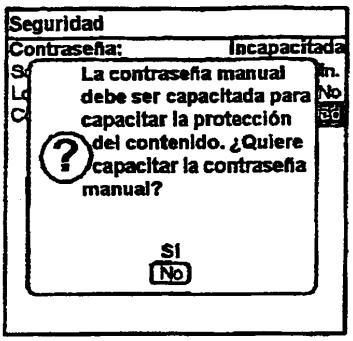

FIG. 7

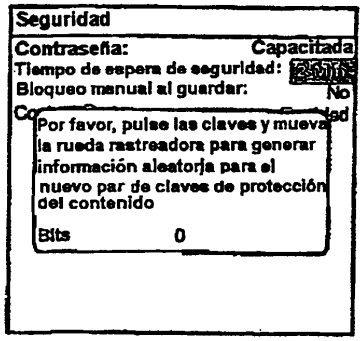

FIG. 8

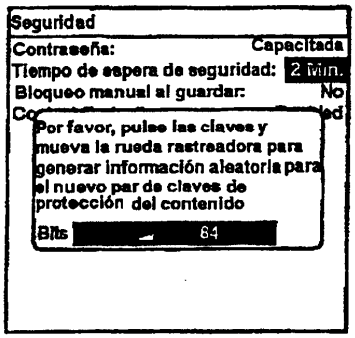

FIG. 9

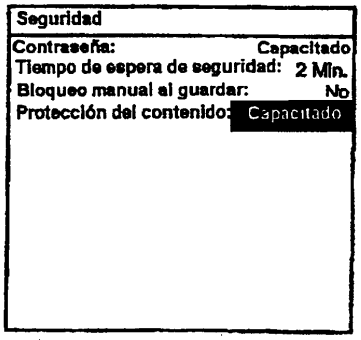

FIG. 10

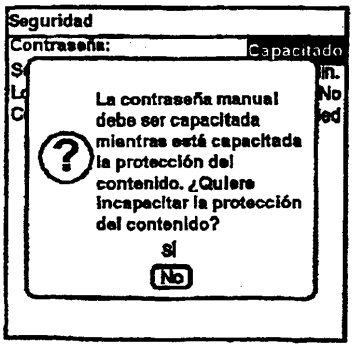

FIG. 11

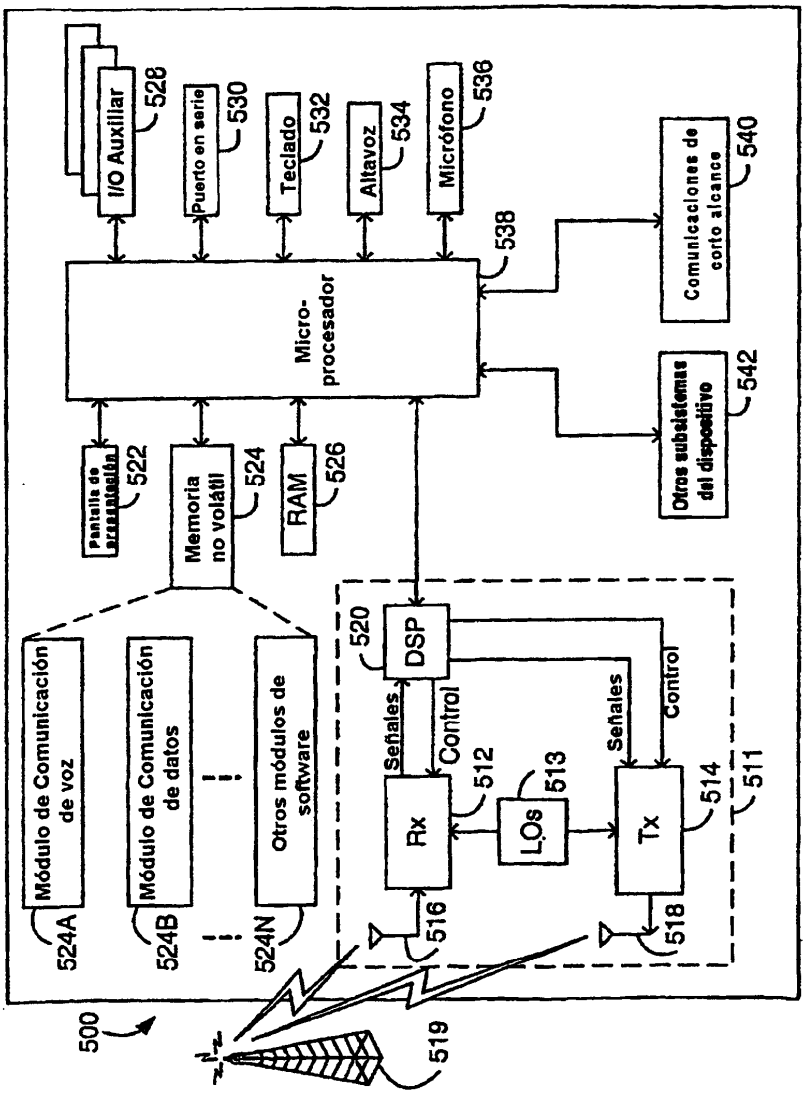
I/O Auxiliar
528
Puerto en serie
530
Teclado
532
Altavoz
534
Micrófono
536
538
Micro-procesador
Comunicaciones de corto alcance
540
Otros subsistemas del dispositivo
542
Pantalla de presentación
522
Memoria no volátil
524
RAM
526
Módulo de Comunicación de voz
524A
Módulo de Comunicación de datos
524B
Otros módulos de software
524N
520
DSP
Señales
Control
Rx
512
LOs
513
Señales
Control
Tx
514
511
516
518
500
519

FIG. 12