(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 383 607**

(51) Int. CI.:
H04L 9/08 (2006.01)
G06F 21/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **06113904 .4**
(96) Fecha de presentación: **13.05.2006**
(97) Número de publicación de la solicitud: **1855414**
(97) Fecha de publicación de la solicitud: **14.11.2007**

(54) Título: **Sistema y método para la reinicialización remota de contraseña y de clave de cifrado**

(45) Fecha de publicación de la mención BOPI:
22.06.2012

(45) Fecha de la publicación del folleto de la patente:
22.06.2012

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

(72) Inventor/es:
Brown, Michael K;
Little, Herb y
Brown, Michael S

(74) Agente/Representante:
de Elzaburu Márquez, Alberto

DESCRIPCIÓN

Sistema y método para la reinicialización remota de contraseña y de clave de cifrado.

La presente invención se refiere de manera general al campo de la seguridad informática y de red, y en particular a la administración de contraseñas.

Los datos almacenados en la memoria de un dispositivo de comunicación y/o informático, tal como un dispositivo de comunicación móvil, se pueden asegurar mediante cifrado usando una clave de protección de contenido. Esta clave, a su vez, está protegida preferentemente por, o derivada en parte de, una contraseña de introducida por el usuario, PIN, u otra pieza de datos suministrada por el usuario. Este es un medio para asegurar que los datos sensibles almacenados en el dispositivo de comunicación son accesibles solamente por un usuario designado.

Debido a que las contraseñas introducidas por el usuario a menudo son dependientes del usuario que recuerda mentalmente la contraseña, algunas veces es necesario para el usuario, un administrador u otra persona reinicializar la contraseña del usuario a otro valor cuando el usuario olvida la contraseña existente. El procedimiento de reinicialización se puede invocar remotamente desde otro dispositivo en comunicación con el dispositivo de usuario, por ejemplo desde un servidor situado en la misma red que el dispositivo de usuario. No obstante, cuando la protección de contenido está habilitada y los datos en el dispositivo de comunicación se cifran usando una clave de protección de contenido protegida por o deducida de la contraseña de usuario existente, la clave de protección de contenido no se puede recuperar sin la contraseña de usuario existente. Si el usuario no puede recordar la contraseña existente, los datos protegidos se hacen inaccesibles.

Es por lo tanto deseable proporcionar un sistema y método para reinicializar una contraseña que se usa para proteger o deducir una clave de protección de contenido en un dispositivo desde una ubicación remota, mientras que se continúa proporcionando acceso al contenido del dispositivo que está cifrado usando la clave de protección de contenido.

La US-A-5768373 revela un método para proporcionar acceso a datos cuando un usuario ha olvidado una contraseña. En esta adaptación, se proporciona una pareja de clave privada/pública “una vez”. El usuario entonces tiene que ir a través de pasos adicionales de autenticación antes de que se permita el acceso a los datos.

La EP-A-1079565 se dirige a un medio de asegurar un enlace de comunicación entre un servidor y cliente proporcionando una clave compartida para impedir un ataque de hombre en el medio. Esto permite que los datos sean recuperados incluso si se pierde la contraseña.

En un aspecto hay proporcionado un método para asegurar los datos en un dispositivo de almacenamiento de datos capaz de que se asegure por una primera contraseña, el dispositivo de almacenamiento de datos que se proporciona con una clave de cifrado de contenido ***K***, el método que comprende los pasos de:

recibir, en un dispositivo de almacenamiento de datos, una clave pública ***B*** generada a partir de una clave privada ***b*** en una ubicación remota, la clave privada ***b*** que se almacena en la ubicación remota;
generar, en el dispositivo de almacenamiento de datos, una clave privada ***d*** y una clave pública ***D*** a partir de la clave privada ***d***;
generar, en el dispositivo de almacenamiento de datos, una clave de cifrado de claves ***L*** a partir de la clave privada ***d*** y la clave pública ***B***;
cifrar la clave de protección de contenido ***K*** con la clave de cifrado de claves ***L*** para proporcionar una primera clave de protección de contenido cifrada, cifrando la clave de protección de contenido ***K*** con la primera contraseña para proporcionar una segunda clave de protección de contenido cifrada, y almacenar la primera y la segunda claves de protección de contenido cifradas en el dispositivo de almacenamiento de datos;
destruir ***d*** y ***K*** en el dispositivo de almacenamiento de datos; y
recuperar la clave de cifrado de claves ***L***:

generando, en el dispositivo de almacenamiento de datos, un valor clave r y una clave pública ***D’*** a partir del valor de clave ***r*** y la clave pública ***D***;
transmitir la clave pública ***D’*** a la ubicación remota;
recibir, en el dispositivo de almacenamiento de datos, una clave pública ***L’*** generada a partir de la clave privada ***b*** y la clave pública ***D’*** en la ubicación remota; y
obtener, en el dispositivo de almacenamiento de datos, la clave de cifrado de claves ***L*** a partir del valor de clave inverso r^{-1} y ***L’***.

El método puede además comprender recibir desde la ubicación remota una nueva contraseña; transmitir a la ubicación remota una clave pública ***D’***, en la que ***D’ = rD***; recibir, desde la ubicación remota, una clave pública ***L’***, en la que ***L’*** comprende una clave pública generada a partir del valor de clave ***b*** y ***D’***; calcular $r^{-1}L'$ para deducir ***L***; descifrar la primera clave de protección de contenido cifrada; deducir una nueva clave de protección de contenido; y

cifrar la nueva clave de protección de contenido usando la nueva contraseña para proporcionar una nueva segunda clave de protección de contenido cifrada.

En otro aspecto hay proporcionado un dispositivo de almacenamiento de datos para almacenar datos cifrados, el dispositivo de almacenamiento de datos que se adapta para permitir acceso a las operaciones del dispositivo de almacenamiento de datos tras la introducción con éxito de una contraseña, el dispositivo de almacenamiento de datos que comprende:

una memoria volátil para almacenar datos que comprenden los datos a ser cifrados o descifrados, contraseñas, y claves;
una memoria no volátil para almacenar los datos cifrados y las claves cifradas; y
un procesador adaptado para:

recibir desde una ubicación remota una clave pública ***B*** en donde ***B = bP***, generar un valor aleatorio ***d*** y almacenar temporalmente ***d*** en la memoria volátil o no volátil, calcular una clave pública ***D = dP***, y almacenar la clave pública ***D*** en la memoria no volátil; calcular una clave de cifrado de claves ***L = dB***, cifrar una clave de protección de contenido K usando L, usar la clave de protección de contenido ***K*** para cifrar y descifrar los datos a ser almacenados en la memoria no volátil, y cifrar y descifrar la clave de protección de contenido ***K*** usando una contraseña almacenada en la memoria volátil; y borrar ***L, d*** y copias no cifradas de ***K***; y generar un valor aleatorio r y almacenar temporalmente ***r*** en la memoria volátil o no volátil, calcular una clave pública ***D' = rD***, y transmitir ***D'*** a la ubicación remota; recibir desde la ubicación remota una clave pública ***L'=bD'*** y calcular r^1L' para deducir la clave de cifrado de claves ***L***, y usar ***L*** para descifrar la clave de protección de contenido ***K***.

En otro aspecto hay proporcionado un método para asegurar datos en un dispositivo de almacenamiento de datos capaz de ser asegurado por una primera contraseña, el dispositivo de almacenamiento de datos que se proporciona con una clave de cifrado de contenido ***K***, el método que comprende los pasos de:

recibir, en un dispositivo de almacenamiento de datos, una clave pública ***B*** generada a partir de una clave privada ***b*** en una ubicación remota, la clave privada ***b*** que se almacena en la ubicación remota;
generar, en el dispositivo de almacenamiento de datos, una clave privada ***d*** y una clave pública ***D*** a partir de la clave privada ***d***;
generar, en el dispositivo de almacenamiento de datos, una clave de cifrado de claves ***L*** a partir de la clave privada ***d*** y la clave pública ***B***;
cifrar la clave de protección de contenido ***K*** con la primera contraseña para proporcionar una clave de protección de contenido cifrada, y almacenar la clave de protección de contenido cifrada en el dispositivo de almacenamiento de datos;
cifrar la primera contraseña con la clave de cifrado de claves ***L*** para proporcionar una primera contraseña cifrada, y almacenar la contraseña cifrada en el dispositivo de almacenamiento de datos;
destruir ***d*** y la clave de cifrado de contenido no cifrada ***K*** en el dispositivo de almacenamiento de datos; y
recuperar la clave de cifrado de claves ***L***:

generando, en el dispositivo de almacenamiento de datos, un valor clave ***r*** y una clave pública ***D'*** a partir del valor de clave ***r*** y la clave pública ***D***;
transmitiendo la clave pública D' a la ubicación remota;
recibiendo, en el dispositivo de almacenamiento de datos, una clave pública ***L'*** generada a partir de la clave privada ***b*** y la clave pública ***D'*** en la ubicación remota; y
obteniendo, en el dispositivo de almacenamiento de datos, la clave de cifrado de claves ***L*** a partir del valor de clave inverso r^1 y ***L'***.

El método descrito en el párrafo precedente además puede comprender recibir desde la ubicación remota una segunda contraseña en el dispositivo de almacenamiento de datos;
transmitir a la ubicación remota una clave pública ***D'***, en la que ***D' = rD***;
recibir, desde la ubicación remota, una clave pública ***L'***, en la que ***L'*** comprende una clave pública generada a partir del valor de clave ***b*** y ***D'***;
calcular r^1L' para deducir ***L***;
descifrar la primera contraseña cifrada para obtener una primera contraseña descifrada;
descifrar la clave de protección de contenido cifrada usando la primera contraseña descifrada;
deducir una nueva clave de protección de contenido; y
cifrar la nueva clave de protección de contenido usando la segunda contraseña para proporcionar una nueva clave de protección de contenido cifrada.

En otro aspecto hay proporcionado un dispositivo de almacenamiento de datos para almacenar datos cifrados, el dispositivo de almacenamiento de datos que está adaptado para permitir el acceso a las operaciones del dispositivo de almacenamiento de datos tras la introducción con éxito de una contraseña, el dispositivo de almacenamiento de

datos que comprende:

una memoria volátil para almacenar datos que comprende los datos a ser cifrados o descifrados, contraseñas, y claves;
una memoria no volátil para almacenar los datos cifrados y las claves cifradas; y
un procesador adaptado para:

recibir desde una ubicación remota una clave pública ***B*** en donde ***B = bP***, generar un valor aleatorio d y almacenar temporalmente ***d*** en la memoria volátil o no volátil, calcular una clave pública ***D = dP***, y almacenar la clave pública ***D*** en la memoria no volátil; calcular una clave de cifrado de claves ***L = dB***, cifrar una clave de protección de contenido ***K*** usando una contraseña introducida por el usuario, cifrar la contraseña introducida por el usuario usando ***L***, usar la clave de protección de contenido ***K*** para cifrar y descifrar datos a ser almacenados en la memoria no volátil; y borrar ***d*** y las copias no cifradas de ***K***; y generar un valor aleatorio ***r*** y almacenar temporalmente ***r*** en la memoria volátil o no volátil, calcular una clave pública ***D' = rD***, y transmitir ***D'*** a la ubicación remota; recibir desde la ubicación remota una clave pública ***L'= bD'*** y calcular $r^{1}L'$ para deducir la clave de cifrado de claves ***L***, y usar ***L*** para descifrar la contraseña introducida por el usuario cifrada.

La invención también proporciona un medio legible por ordenador que comprende código ejecutable por un dispositivo informático para llevar a cabo cualquiera de los métodos descritos anteriormente.

Breve descripción de los dibujos

En los dibujos que ilustran a modo de ejemplo solamente una realización preferente de la invención,

La Figura 1 es un esquema de una red para llevar a cabo un método para establecer y reinicializar remotamente una contraseña y una clave de cifrado.
La Figura 2 es una representación esquemática de un método para establecer una contraseña y una clave de cifrado.
La Figura 3 es una representación esquemática de un método para reinicializar una contraseña y una clave de cifrado.
La Figura 4 es un diagrama de bloques de un dispositivo de comunicación móvil para usar con los métodos ilustrados en las Figuras 2 y 3.

Descripción de las realizaciones preferidas

Con referencia a la Figura 1, se muestra una descripción de un sistema de comunicación ejemplar para usar con las realizaciones descritas más adelante. Un experto en la técnica apreciará que puede haber muchas topologías diferentes, pero el sistema mostrado en la Figura 1 ayuda a demostrar el funcionamiento de los sistemas y métodos descritos en la presente solicitud. Puede haber muchos dispositivos de comunicación conectados al sistema, que no se muestran en la descripción simple de la Figura 1.

La Figura 1 muestra el primer dispositivo de comunicación 1, aquí un ordenador personal 10, una red, aquí Internet 20, un sistema servidor 40, una pasarela inalámbrica 85, infraestructura inalámbrica 90, una red inalámbrica 105 y un segundo dispositivo de comunicación, aquí un dispositivo de comunicación móvil 100. Se apreciará por aquellos expertos en la técnica que los dispositivos conocidos aquí dentro como dispositivos de comunicación o dispositivos de almacenamiento de datos pueden comprender dispositivos cuya función principal se dirige a comunicación de voz o datos sobre una red y almacenamiento de datos, pero también puede ser proporcionado con aplicaciones personales o de productividad, o dispositivos cuya función principal se dirige a calcular o ejecutar aplicaciones de productividad, pero también se adaptan para permitir a un usuario comunicar sobre una red.

Un ordenador personal 10 puede, por ejemplo, estar conectado a un ISP (Proveedor de Servicios de Internet) en el cual un usuario del sistema tiene una cuenta, situada dentro de una empresa, posiblemente conectado a una red de área local (LAN), y conectado a Internet 20, o conectado a Internet 20 a través de un ASP (proveedor de servicios de aplicaciones) grande. Aquellos expertos en la técnica apreciarán que los sistemas mostrados en la Figura 1 en su lugar se pueden conectar a una red de área extendida (WAN) distinta de Internet.

La pasarela inalámbrica 85 y la infraestructura 90 proporcionan un enlace entre Internet 20 y la red inalámbrica 105. La infraestructura inalámbrica 90 determina la red más probable para localizar un usuario dado y hacer el seguimiento del usuario según deambula (itinerante) entre países o redes. Los mensajes y otros datos se pueden entregar al dispositivo móvil 100 a través de transmisión inalámbrica, típicamente en una radiofrecuencia (RF), desde una estación base en la red inalámbrica 105 al dispositivo móvil 100. La red particular 105 puede ser cualquier red inalámbrica sobre la cual se pueden intercambiar mensajes con un dispositivo de comunicación móvil. El dispositivo móvil 100 también puede recibir datos por otros medios, por ejemplo a través de una conexión directa a un puerto proporcionado en el dispositivo móvil 100, tal como un enlace de Canal Principal Universal Serie (USB).

El servidor 40 se puede implementar, por ejemplo, en un ordenador en red dentro del cortafuegos de una

corporación, un ordenador dentro de un sistema de ISP o ASP o similar. El servidor 40 puede actuar como la aplicación, el acceso de red, y/o servidor de archivos para uno o más dispositivos de comunicación. El dispositivo móvil 100, si se configura para recibir y posiblemente enviar correo electrónico, se asociará normalmente con una cuenta en el servidor 40. Los productos de soporte lógico y otros componentes que a menudo se usan en conjunto con las funciones del servidor 40 descritas aquí dentro no se muestran en la Figura 1, ya que no juegan directamente un papel en el sistema y método descrito más adelante. Si el servidor 40 actúa como un servidor de mensajes, el servidor 40 puede soportar o bien un denominado esquema de acceso de mensajes "de empuje" o "de tracción", en el que el dispositivo móvil 100 debe requerir que los mensajes almacenados sean reenviados por el servidor de mensajes al dispositivo móvil 100, o el servidor 40 puede ser dotado con medios para redirigir automáticamente mensajes direccionados al usuario del dispositivo móvil 100 según son recibidos, respectivamente.

Como se puede ver a partir de la siguiente descripción, el servidor 40 se puede usar para proporcionar funciones administrativas para los dispositivos de comunicación 10 y 100, por ejemplo estableciendo y transmitiendo políticas de tecnologías de la información (IT). En la realización preferente, se proporciona el acceso del administrador al servidor 40 para reinicializar las contraseñas del dispositivo, aunque el sistema y el método descrito aquí dentro se puede implementar a partir de otro dispositivo en la red, si tal acceso a nivel de administrador se proporciona en el otro dispositivo.

Los datos almacenados en una memoria en el dispositivo móvil 100 o el otro dispositivo de comunicación 10, tal como el contenido proporcionado por el usuario o administrador o las claves de cifrado, se pueden asegurar en parte por medio de una contraseña introducida por el usuario, PIN, o método de control de acceso similar. El contenido puede incluir mensajes electrónicos, información personal, u otros datos provocados para ser introducidos o creados por el usuario del dispositivo 100 o 10. Los métodos de control de acceso adecuados pueden incluir aumentar la seguridad proporcionando un lector de tarjetas inteligentes para acceder a datos de seguridad desde una tarjeta inteligente en posesión del usuario tras una petición expedida por el dispositivo móvil 100 u otro dispositivo de comunicación 10. Tales mecanismos de seguridad impiden que un usuario no autorizado obtenga acceso a los datos a través de la interfaz de usuario proporcionada por el dispositivo.

Preferentemente, una contraseña introducida por el usuario no es el único medio por el cual el contenido en el dispositivo 100 o 10 se asegura. Más bien, la contraseña, que usa métodos conocidos en la técnica, se usa sola o en conjunto con otros datos de cifrado para asegurar otra clave, tal como una clave de protección de contenido o una clave en masa de protección de contenido K, que se usa a su vez para cifrar datos. La clave de protección de contenido K en sí misma puede ser una clave criptográfica de Estándar de Cifrado Avanzado (AES) con una longitud de 128, 192, o 256 bit, u otra clave para usar con programas informáticos de cifrado de acuerdo con otro estándar. Como apreciarán aquellos expertos en la técnica, se pueden usar otros estándares de cifrado para definir la naturaleza de la clave de protección de contenido K, aunque preferentemente se usa un método de cifrado de bloque simétrico. Además, la clave de protección de contenido K no puede ser usada directamente para convertir datos en texto cifrado; en su lugar, el dispositivo 100 o 10 se puede configurar para usar la clave de protección de contenido K para generar una o más claves de cifrado de contenido adicional para cifrar y/o descifrar datos almacenados en el dispositivo 100 o 10. No obstante, preferentemente ni la clave de protección de contenido K ni ninguna clave adicional derivada de la clave K están almacenadas en el espacio en la memoria del dispositivo de comunicación 100 o 10.

Por ejemplo, la contraseña se puede usar para cifrar la clave de protección de contenido K, y la clave de protección de contenido cifrada K puede ser almacenada en la memoria no volátil del dispositivo 100 o 10. La memoria no volátil se trata más adelante con referencia a la Figura 4. Cuando se accede al dispositivo 100 o 10 primero por el usuario, el usuario es avisado para introducir una contraseña. La contraseña introducida se puede comparar con una contraseña almacenada en la memoria del dispositivo de comunicación 100 o 10. Preferentemente, no obstante, la contraseña en sí misma no está almacenada en el espacio en la memoria; más bien, una función para generar claves (o alguna otra función) de la contraseña introducida por el usuario se compara con una función para generar claves (o alguna otra función) de la contraseña almacenada en memoria. Si los datos comparados coinciden, entonces el usuario es autentificado y la contraseña introducida se puede almacenar en memoria volátil, también descrita más adelante con referencia a la Figura 4, en el dispositivo 100 o 10. La contraseña puede ser almacenada en memoria volátil durante la duración de una sesión de usuario, que se puede terminar mediante el "cierre de sesión" del dispositivo, suspendiendo las operaciones del dispositivo 100 o 10 situando el dispositivo en un modo de espera activa, apagando el dispositivo 100 o 10 o desconectando de otro modo una fuente de alimentación de la memoria volátil, o de acuerdo con otras políticas de IT, por ejemplo borrando la contraseña de la memoria volátil después de un periodo de tiempo establecido o inmediatamente después de la autentificación del usuario.

Si es deseable proteger los datos almacenados en la memoria del dispositivo 100 o 10 usando la clave de protección de contenido ***K***, cuando el dispositivo 100 o 10 determina que se requiere una clave de cifrado para convertir los datos a ser protegidos a texto cifrado, accede a la clave de protección de contenido cifrada ***K*** y descifra la clave usando la contraseña almacenada en la memoria volátil. La clave de protección de contenido descifrada ***K*** se almacena en la memoria volátil y se usa o bien para cifrar los datos a ser protegidos y almacenados, o bien para generar claves de cifrado adicionales para cifrar los datos a ser protegidos y almacenados. No obstante se usa la

clave de protección de contenido ***K***, puede ser borrada de la memoria volátil después que se cifran los datos. En ese caso, cuando el dispositivo 100 o 10 requiere datos que fueron cifrados previamente, el dispositivo 100 o 10 de nuevo accede a la clave de protección de contenido cifrada ***K***, la descifra y la almacena en la memoria volátil, entonces o bien descifra los datos requeridos usando la clave ***K*** directamente o derivando las claves adicionales necesarias para descifrar los datos. Después de que la clave ***K*** se ha usado, se borra de nuevo de la memoria volátil. La clave de protección de contenido ***K*** solamente se almacena de esta manera en el espacio en la memoria volátil de una forma transitoria. Alternativamente, una vez que la clave de protección de contenido ***K*** ha sido descifrada una primera vez durante una sesión de usuario, se puede retener en la memoria volátil hasta que se termina la sesión de usuario.

El dispositivo de comunicación 100 o 10 se puede conectar a una red tal como aquella descrita en la Figura 1, y se puede dotar con políticas de IT con relación a la protección de contenido. Preferentemente, algunas políticas y rasgos de seguridad en el dispositivo 100 o 10 se pueden controlar desde una ubicación remota en la red, por ejemplo desde el servidor 40. Esto es particularmente útil en el caso de que un usuario olvide su contraseña para acceder al dispositivo 100 o 10, ya que un administrador u otra persona con suficientes privilegios puede forzar un reinicialización de contraseña en el dispositivo 100 o 10 sobre la red.

No obstante, si la contraseña se usa para cifrar la clave de protección de contenido ***K***, entonces cuando una contraseña se reinicializa la clave de protección de contenido ***K*** deja de estar disponible para el dispositivo 100 o 10. Por lo tanto, de acuerdo con la realización preferente, la clave de protección de contenido ***K*** se restablece por el dispositivo 100 o 10 usando información proporcionada por el servidor 40 como sigue, con referencia a la Figura 2.

Cuando una clave de protección de contenido ***K*** se establece para un dispositivo de almacenamiento de datos tal como el dispositivo de comunicaciones 100 o 10, el dispositivo de reinicialización, tal como el servidor 40, primero selecciona o genera una clave privada ***b*** en el paso 205. La clave privada ***b*** se genera preferentemente como un número aleatorio o pseudo-aleatorio y es adecuada para usar en un algoritmo de criptografía de curva elíptica, por ejemplo de acuerdo con un algoritmo de cifrado aprobado por el Instituto Nacional de Estándares y Tecnología (NIST). No obstante, se puede emplear cualquier algoritmo de criptografía de clave asimétrico alternativo. Preferentemente, se usa un algoritmo de criptografía de curva elíptica, y más preferentemente se usa al menos una clave de 521 bit y la curva elíptica usada tiene un cofactor de 1. Usando ***b*** y un punto elíptico predeterminado ***P***, el servidor 40 calcula ***B = bP*** en el paso 210 y almacena ***b*** de manera segura en el paso 215. ***b*** se puede cifrar por sí mismo usando medios conocidos en la técnica, y almacenar como texto de cifrado. En el paso 220, el resultado ***B*** se transmite al dispositivo de comunicaciones 100 o 10. En este punto, el servidor 40 y el dispositivo 100 o 10 pueden estar de acuerdo con un algoritmo de cifrado seleccionado, o alternativamente un algoritmo de cifrado puede haber sido previamente establecido por las políticas de IT entre el servidor 40 al dispositivo 100 o 10.

El dispositivo 100 o 10 recibe ***B*** en el paso 225 y preferentemente verifica que ***B*** es una clave pública válida en el paso 230, usando técnicas conocidas en la técnica. Por ejemplo, si se usa un algoritmo de criptografía de curva elíptica, entonces el dispositivo 100 o 10 puede verificar que ***B*** es un punto en la curva predeterminada definido para esta implementación del algoritmo. El dispositivo 100 o 10 entonces selecciona o genera un valor de clave ***d*** en el paso 235. ***d*** es preferentemente un valor generado aleatoriamente o pseudo-aleatoriamente, de nuevo, preferentemente al menos de 521 bits de largo. El dispositivo calcula una nueva clave pública ***D = dP*** en el paso 240, y almacena ***D*** en el paso 245. El dispositivo 100 o 10 también calcula una clave de cifrado de claves ***L = dB*** en el paso 250, donde ***B*** es el valor de clave recibido desde el servidor 40. La clave de protección de contenido ***K*** entonces se cifra con la clave de cifrado de claves ***L*** en el paso 260, y esta versión cifrada de ***K, enc(K)***$_1$, se almacena en el dispositivo. La clave de protección de contenido ***K*** también se cifra con la contraseña de usuario, y esta segunda versión cifrada de ***K, enc(K)***$_2$, también se almacena en el dispositivo. Este segundo paso de cifrado se indica en la Figura 2 en el paso 255, anterior al cifrado de ***K*** por ***L*** en el paso 260; no obstante, aquellos expertos en la técnica apreciarán que estos pasos de cifrado pueden ocurrir en orden inverso. (Señalar que la contraseña en sí misma se proporciona a o por el dispositivo 100 o 10 en el paso 200, por ejemplo por el usuario o por algún otro medio conocido en la técnica; el dispositivo en sí mismo se puede configurar para generar una contraseña y proporcionar la contraseña al usuario). Cualquier copia no cifrada de ***K*** y ***d*** se destruye por el dispositivo en el paso 265. De esta manera, la clave de protección de contenido ***K*** se almacena en dos formas de texto cifrado en el dispositivo, y preferentemente no se almacena en ningún otro lugar. El dispositivo 100 o 10 y el servidor 40 también pueden destruir ***B***.

Los pasos ilustrados en la Figura 2 se muestran en la tabla de más abajo:

Dispositivo de Almacenamiento de Datos		**Dispositivo de Reinicialización**
		Elegir ***b*** aleatoriamente. Calcular ***B = bP***. Almacenar ***b*** de manera segura.
Recibir ***B***.	← ***B***	Enviar ***B*** al dispositivo de almacenamiento de datos

Elegir contraseña. Verificar que ***B*** es una clave pública válida. Elegir ***d*** aleatoriamente. Calcular ***D = dP***. Almacenar ***D***. Calcular ***K = dB***. Cifrar ***K*** con ***L***. Cifrar ***K*** con la contraseña. Destruir ***d***. Destruir ***K***.		

Después de este procedimiento, la clave de protección de contenido ***K*** se puede recuperar en una de dos formas. Durante el funcionamiento normal, el usuario puede proporcionar la contraseña de usuario para ingresar en o desbloquear el dispositivo, y el dispositivo puede usar la contraseña para descifrar la segunda versión cifrada de ***K, enc(K)***$_2$, almacenada en el dispositivo. En el caso de que la contraseña ya no esté disponible para descifrar la clave de protección de contenido ***K***, por ejemplo si el usuario no puede recordar la contraseña, se puede seguir un procedimiento tal como aquel ilustrado en la Figura 3.

Cuando se determina que una nueva contraseña debería ser establecida para el dispositivo 100 o 10, un usuario o administrador en el servidor 40 puede seleccionar o generar una nueva contraseña en el paso 305. El servidor 40 entonces requiere la clave pública desde el dispositivo 100 o 10 en el paso 310. No obstante, más que proporcionar la clave pública ***D*** en el espacio, tras la recepción de la petición de la clave pública en el paso 415 el dispositivo 100 o 10 selecciona o genera un valor aleatorio o pseudo-aleatorio ***r*** y almacena temporalmente ***r*** en el paso 320, y calcula ***D' = rD*** en el paso 325, preferentemente usando criptografía de curva elíptica. Esta clave pública ciega ***D'*** se transmite al servidor 40 en el paso 430.

Después de la recepción de la clave pública ciega ***D'*** en el servidor 40 en el paso 435, el servidor 40 verifica preferentemente que ***D'*** es una clave pública válida en el paso 340, entonces calcula una clave ciega ***L' = bD'*** en el paso 345, ***b*** que se ha almacenado previamente en el servidor 40. El servidor 40 entonces transmite esta nueva clave ciega calculada ***L'*** y la nueva contraseña al dispositivo de comunicaciones 100 o 10 en el paso 350. La nueva contraseña se destruye preferentemente en el servidor 40 en el paso 390. Después el dispositivo 100 o 10 recibe ***L'*** en el paso 355, preferentemente verifica que ***L'*** es una clave pública válida en el paso 360; el dispositivo 100 o 10, calcula la función inversa $r^{-1}L' = L$ en el paso 365. El dispositivo entonces puede usar ***L*** para descifrar la primera versión cifrada de ***K, enc(K)***$_1$, almacenada en el dispositivo en el paso 370.

El dispositivo 100 o 10 de esta manera deduce la clave de protección de contenido original ***K***, y puede usar ***K*** para descifrar cualquier contenido seguro almacenado en el dispositivo 100 o 10. Después del descifrado, preferentemente la clave de protección de contenido existente ***K*** se destruye en el paso 375, y una nueva clave de protección de contenido, ***K'***, se genera en el paso 380 para volver a cifrar el contenido a ser asegurado en el dispositivo 100 o 10. Esta nueva clave de protección de contenido ***K'*** está preferentemente protegida de una manera similar a aquella descrita con relación con la Figura 2; preferentemente, el servidor inicia esta protección generando una nueva clave privada ***b*** como en el paso 205 en la Figura 2, y luego procediendo con los pasos posteriores para provocar una nueva clave de cifrado de claves M; la nueva contraseña, transmitida en el paso 350 en la Figura 3, se usaría en el paso 200 en la Figura 2.

Los pasos ilustrados en la Figura 3 se muestran en la tabla de más abajo:

Dispositivo de Almacenamiento de Datos		**Dispositivo de Reinicialización**
		Introducir una nueva contraseña.
	← Petición de Clave Pública	Transmitir la petición para la clave pública del dispositivo.
Elegir ***r*** aleatoriamente. Mantener ***r*** en la RAM. Calcular ***D' = rD = rdP***.		
Enviar ***D'***.	***D'*** →	Recibir ***D'***.
		Verificar que ***D'*** es una clave pública válida. Calcular ***L' = bD' = brdP = rdB = rL***
Recibir ***L'***, nueva contraseña	← ***L'***, nueva contraseña	Enviar ***L'*** y la nueva contraseña.
Verificar que ***L'*** es una clave pública válida. Calcular $r^{-1}L' = r^{-1}rL = L$.		

Destruir ***r***. Usar ***L*** para descifrar ***K***. Destruir ***K***. Generar la nueva ***K'***. Usar la nueva contraseña para cifrar la nueva ***K'***.		

Si la nueva clave de protección de contenido ***K'*** va a ser protegida usando una nueva clave de cifrado de claves ***M***, el servidor 40 puede generar una nueva clave privada b_1 y deducir una nueva clave pública B_1 a partir de b_1 y un punto de generación P_1, que puede ser el mismo punto de generación P que aquél usado previamente. El proceso restante para cifrar la nueva clave de protección de contenido ***K'*** con M se describe en la siguiente tabla:

Dispositivo de Almacenamiento de Datos		**Dispositivo de Reinicialización**
		Elegir b_1 aleatoriamente. Calcular $B_1 = b_1P_1$. Almacenar b_1 de manera segura.
Recibir B_1.	← B_1	Enviar B_1 al dispositivo de almacenamiento de datos
Verificar que B_1 es una clave pública válida. Elegir d_1 aleatoriamente. Calcular $D_1 = d_1P_1$. Almacenar D_1. Calcular $M = d_1B_1$. Cifrar ***K'*** con ***M***. Cifrar ***K'*** con la nueva contraseña. Destruir d_1. Destruir ***M***.		

De esta manera, se apreciará que un medio se ha proporcionado para una clave de protección de contenido ***K*** a ser recuperada, incluso si la clave ***K*** está cifrada por una contraseña que se pierde posteriormente, almacenando una versión cifrada alternativa de ***K***.

En una realización alternativa, el dispositivo de reinicialización puede proporcionar inmediatamente la nueva contraseña seleccionada en el paso 305 como parte de un comando de contraseña de reinicialización en el paso 385 sin requerir la clave pública del dispositivo, desviando por ello los pasos 310 y 315 en la Figura 3. Si el dispositivo es incapaz de reinicializar inmediatamente la contraseña al nuevo valor porque la protección de contenido está habilitada y ***K*** se almacena solamente en forma cifrada como se determina en el paso 390, el dispositivo puede responder con la clave pública ciega ***D'***, indicando por ello al servidor que el protocolo de recuperación de clave se debería iniciar. El resto del protocolo puede proceder como se describió anteriormente, con el servidor proporcionando opcionalmente la nueva contraseña una segunda vez en el paso 350.

En una realización adicional, la clave de cifrado de claves ***L*** puede ser usada para cifrar la contraseña del usuario en lugar de cifrar la clave de protección de contenido ***K*** directamente. En tal realización así, tanto la contraseña cifrada con L y la clave de protección de contenido ***K*** cifrada con la contraseña, o en otras palabras $enc(K)_2$, son almacenadas en el dispositivo. Si la contraseña ya no está disponible, el procedimiento en la Figura 3 puede ser llevado a cabo, excepto si una vez que la clave de cifrado de claves ***L*** haya sido recuperada en el paso 365, puede ser usada para descifrar primero la contraseña de usuario, y luego la contraseña de usuario puede ser usada para descifrar la clave de protección de contenido cifrada $enc(K)_2$.

Aquellos expertos en la técnica apreciarán que la clave de protección de contenido ***K*** se asegura de esta manera contra un ataque basado en componentes físicos. Mientras que el servidor 40 almacena información útil para la reconstrucción de la clave de cifrado de claves ***L***, un usuario malicioso con acceso al servidor 40 pero no al dispositivo 100 o 10 será incapaz de reconstruir ***L*** a partir de la clave privada ***b*** sola. El proceso de reconstrucción adicionalmente blinda el contenido protegido de un usuario malicioso en el servidor 40, dado que la clave pública ***D*** no es transmitida al servidor 40; solamente la clave ***D'***, la cual es una versión escondida de ***D***, es transmitida al servidor 40 de manera que el servidor 40 permanece incapaz de calcular ***L***. Se puede ver que el método de reinicialización de una contraseña que es usada para cifrar una clave de protección de contenido ***K***, como se ilustra en la Figura 3, proporciona el medio para recuperar y volver a cifrar los datos almacenados en el dispositivo 100 o 10.

Como otro ejemplo, los sistemas y métodos revelados aquí dentro pueden ser usados con muchos ordenadores y dispositivos diferentes, tal como un dispositivo de comunicaciones móvil inalámbrico mostrado en la Figura 4. Con

referencia a la Figura 4, el dispositivo móvil 100 es un dispositivo móvil de modo doble e incluye un transceptor 411, un microprocesador 438, una pantalla 422, una memoria no volátil 424, memoria de acceso aleatorio (RAM) 426, uno o más dispositivos de entrada/salida (I/O) auxiliares 428, un puerto serie 430, un teclado 432, un altavoz 434, un micrófono 436, un subsistema de comunicaciones inalámbrico de corto alcance 440, y otros subsistemas de dispositivo 442.

El transceptor 411 incluye un receptor 412, un transmisor 414, las antenas 416 y 418, uno o más osciladores locales 413, y un procesador digital de señal (DSP) 420. Las antenas 416 y 418 pueden ser elementos de antena de una antena de múltiples elementos, y son preferentemente antenas integradas. No obstante, los sistemas y métodos aquí descritos no están restringidos en ningún modo a un tipo particular de antena, o incluso a dispositivos de comunicación inalámbricos.

El dispositivo móvil 100 es preferentemente un dispositivo de comunicación de dos vías que tiene capacidades de comunicación de voz y datos. De esta manera, por ejemplo, el dispositivo móvil 100 puede comunicarse sobre una red de voz, tal como cualquiera de las redes celulares analógica o digital, y puede también comunicar sobre una red de datos. Las redes de voz y datos están representadas en la Figura 4 mediante la torre de comunicación 419. Estas redes de voz y dato pueden ser redes de comunicación separadas usando infraestructura separada, tal como estaciones base, controladores de red, etc., o pueden ser integradas dentro de una red inalámbrica única.

El transceptor 411 es usado para comunicar con la red 319, e incluye el receptor 412, el transmisor 414, el uno o más osciladores locales 313 y el DSP 320. El DSP 320 es usado para enviar y recibir señales a y desde el transceptor 416 y 418, y también proporciona información de control al receptor 412 y al transmisor 414. Si las comunicaciones de voz y dato se llevan a cabo en una única frecuencia, o conjuntos de frecuencias cercanamente separadas, entonces se puede usar un oscilador local único 413 en conjunto con el receptor 412 y el transmisor 414. Alternativamente, si se utilizan diferentes frecuencias para comunicaciones de voz frente a comunicaciones de datos por ejemplo, la pluralidad de osciladores locales 413 puede ser usada para generar una pluralidad de frecuencias correspondiente a las redes de voz y dato 419. La información, la cual incluye información tanto de voz como de datos, es comunicada a y desde el transceptor 311 mediante un enlace entre el DSP 420 y el microprocesador 438.

El diseño detallado del transceptor 411, tal como su banda de frecuencia, selección de componentes, nivel de potencia, etc., será dependiente de la red de comunicación 419 en la que el dispositivo móvil 100 está pretendiendo funcionar. Por ejemplo, un dispositivo móvil 100 que intenta funcionar en el mercado Norte Americano puede incluir un transceptor 411 diseñado para funcionar con cualquiera de una variedad de redes de comunicación de voz, tal como las redes de comunicación de datos móvil Mobitex o DataTAC, AMPS, TDMA, CDMA, PCS, etc., mientras un dispositivo móvil 100 destinado a usar en Europa puede ser configurado para funcionar con la red de comunicación de datos GPRS y la red de comunicación de voz GSM. Otros tipos de redes de voz y datos, tanto separadas como integradas, pueden ser también utilizadas con un dispositivo móvil 100.

Dependiendo del tipo de red o redes 419, los requerimientos de acceso para el dispositivo móvil 100 también pueden variar. Por ejemplo, en las redes de datos Mobitex y DataTAC, los dispositivos móviles se registran en la red usando un único número de identificación asociado con cada dispositivo móvil. En las redes de datos GPRS, no obstante, el acceso a la red está asociado con un abonado o usuario de un dispositivo móvil. Un dispositivo GPRS típicamente requiere un módulo de identidad de abonado (“SIM”), el cual es requerido para hacer funcionar un dispositivo móvil en una red GPRS. Las funciones de comunicación de red locales o no de red (en su caso) pueden ser operable, sin el dispositivo SIM, pero un dispositivo móvil será incapaz de llevar a cabo cualesquiera funciones que implican comunicaciones sobre la red de datos 319, distintas de cualquier operación requerida legalmente, tal como llamadas de emergencia ‘911’.

Después de que se han completado cualesquiera procedimientos de registro o activación de red requeridos, el dispositivo móvil 100 puede enviar y recibir señales de comunicación, incluyendo tanto señales de voz como de datos, sobre las redes 419. Las señales recibidas por la antena 416 desde la red de comunicación 419 se encaminan al receptor 412, el cual proporciona amplificación de señal, conversión de reducción de frecuencia, filtrado, selección de canal, etc., y también puede proporcionar conversión analógica a digital. La conversión analógica a digital de la señal recibida permite funciones de comunicación más complejas, tales como demodulación y descodificación digital a ser realizada usando el DSP 420. De una manera similar, las señales a ser transmitidas a la red 419 se procesan, incluyendo la modulación y codificación, por ejemplo, por el DSP 420 y entonces se proporcionan al transmisor 414 para conversión digital a analógica, conversión de aumento frecuencia, filtrado, amplificación y transmisión a la red de comunicación 419 a través de la antena 418.

Además de procesar las señales de comunicación, el DSP 420 también proporciona control del transceptor. Por ejemplo, los niveles de ganancia aplicados a las señales de comunicación en el receptor 412 y el transmisor 414 se puede controlar adaptativamente a través de algoritmos de control automático de ganancia implementados en el DSP 420. Otros algoritmos de control del transceptor también se podrían implementar en el DSP 420 para proporcionar control más sofisticado del transceptor 411.

El microprocesador 438 preferentemente gestiona y controla el funcionamiento total del dispositivo móvil 100. Muchos tipos de microprocesadores o microcontroladores se podrían usar aquí, o, alternativamente, se podría usar un DSP 420 único para llevar a cabo las funciones del microprocesador 438. Las funciones de comunicación de bajo nivel, incluyendo al menos las comunicaciones de voz y datos, se realizan a través del DSP 420 en el transceptor 411. Otras, aplicaciones de comunicación de alto nivel, tal como una aplicación de comunicación de voz 424A, y una aplicación de comunicación de datos 424B se pueden almacenar en la memoria no volátil 424 para la ejecución por el microprocesador 438. Por ejemplo, el módulo de comunicación de voz 424A puede proporcionar una interfaz de usuario de alto nivel operable para transmitir y recibir llamadas de voz entre el dispositivo móvil 100 y la pluralidad de otros dispositivos de voz o de modo doble a través de la red 419. De manera similar, el módulo de comunicación de datos 424B puede proporcionar una interfaz de usuario de alto nivel operable para enviar y recibir datos, tales como mensajes de correo electrónico, archivos, información de organización, mensajes cortos de texto, etc., entre el dispositivo móvil 100 y una pluralidad de otros dispositivos de datos a través de las redes 419. El microprocesador 438 también interactúa con otros subsistemas del dispositivo, tales como la pantalla 422, la RAM 426, los subsistemas de entrada/salida (I/O) auxiliares 428, el puerto serie 430, el teclado 432, el altavoz 434, el micrófono 436, el subsistema de comunicaciones de corto alcance 440 y cualquier otro subsistema de dispositivo generalmente designado como 442.

Algunos de los subsistemas mostrados en la Figura 4 realizan funciones relacionadas con la comunicación, mientras que otros subsistemas pueden proporcionar funciones “residentes” o en el dispositivo. Señaladamente, algunos subsistemas, tales como el teclado 432 y la pantalla 422 se pueden usar tanto para funciones relacionadas con la comunicación, tal como introducir un mensaje de texto para transmisión sobre una red de comunicación de datos, como funciones residentes en el dispositivo tales como una calculadora o lista de tareas u otras funciones tipo PDA.

El soporte lógico del sistema operativo usado por el microprocesador 438 se almacena preferentemente en un almacén persistente tal como la memoria no volátil 424. La memoria no volátil 424 se puede implementar, por ejemplo, como un componente de memoria Rápida, o como una RAM respaldada por batería. Además del sistema operativo, el cual controla las funciones de bajo nivel del dispositivo móvil 410, la memoria no volátil 424 incluye una pluralidad de módulos de soporte lógico 424A-424N que se pueden ejecutar por el microprocesador 438 (y/o el DSP 420), incluyendo un módulo de comunicación de voz 424N, un módulo de comunicación de datos 424B, y una pluralidad de otros módulos operacionales 424N para llevar a cabo una pluralidad de otras funciones. Estos módulos se ejecutan por el microprocesador 438 y proporcionan una interfaz de alto nivel entre un usuario y el dispositivo móvil 100. Esta interfaz típicamente incluye un componente gráfico proporcionado a través de la pantalla 422, y un componente de entrada/salida proporcionado a través de la I/O auxiliar 428, teclado 432, altavoz 434, y micrófono 436. El sistema operativo, las aplicaciones o módulos de dispositivo específicos, o partes de los mismos, se pueden cargar temporalmente en un almacén volátil, tal como una RAM 426 para funcionamiento más rápido. Además, las señales de comunicación recibidas también pueden ser almacenadas temporalmente en la RAM 426, antes de escribirlas permanentemente a un sistema de ficheros situado en un almacén persistente tal como la memoria Rápida 424.

La memoria no volátil 424 preferentemente proporciona un sistema de ficheros para facilitar el almacenamiento de elementos de datos PIM en el dispositivo. La aplicación PIM preferentemente incluye la capacidad de enviar y recibir elementos de datos, o bien por sí misma, o bien en conjunto con los módulos de comunicación de voz y datos 424A, 424B, a través de las redes inalámbricas 419. Los elementos de datos PIM son preferentemente integrados, sincronizados y actualizados sin problemas, a través de las redes inalámbricas 419, con un conjunto correspondiente de elementos de datos almacenados o asociados con un sistema de ordenador central, creando por ello un sistema reflejado para los elementos de datos asociados con un usuario particular.

Los objetos de contexto que representan al menos elementos de datos parcialmente descodificados, así como elementos de datos completamente descodificados, se almacenan preferentemente en el dispositivo móvil 100 en un almacén volátil y no persistente tal como la RAM 426. Tal información puede en su lugar ser almacenada en la memoria no volátil 424, por ejemplo, cuando los intervalos de almacenamiento son relativamente cortos, de manera que la información se elimina de la memora pronto después de que se almacena. No obstante, es preferente el almacenamiento de esta información en la RAM 426 u otro almacén volátil y no persistente, para asegurar que la información se borra de la memoria cuando el dispositivo móvil 100 pierde potencia. Esto impide que una parte no autorizada obtenga ninguna información descodificada o parcialmente descodificada almacenada quitando una pastilla de memoria del dispositivo móvil 100, por ejemplo.

El dispositivo móvil 100 se puede sincronizar manualmente con un sistema central situando el dispositivo 100 en una plataforma de interfaz, que acople el puerto serie 430 del dispositivo móvil 100 al puerto serie de un sistema o dispositivo informático. El puerto serie 430 también se puede usar para permitir a un usuario establecer preferencias a través de un dispositivo externo o aplicación informática, o descargar otros módulos de aplicaciones 324N para instalación. Este camino de descarga cableado se puede usar para cargar una clave de cifrado en el dispositivo, lo cual es un método más seguro que intercambiar información de cifrado a través de la red inalámbrica 419. Como se apreciará por aquellos expertos en la técnica, los métodos descritos en relación con las Figuras 2 y 3 se pueden

llevar a cabo con un dispositivo de comunicación móvil 100 o bien sobre el camino cableado o bien una red inalámbrica. Las interfaces para otros caminos de descarga cableados se pueden proporcionar en el dispositivo móvil 100, además de o en lugar del puerto serie 430. Por ejemplo, un puerto USB proporcionaría una interfaz a un ordenador personal equipado de manera similar.

Un subsistema de comunicaciones de corto alcance 440 también se incluye en el dispositivo móvil 100. El subsistema 440 puede incluir un dispositivo de infrarrojos y circuitos y componentes asociados, o un módulo de comunicación de RF de corto alcance tal como un módulo Bluetooth® o un módulo 802.11, por ejemplo, para proporcionar comunicación con sistemas y dispositivos habilitados de manera similar. Aquellos expertos en la técnica apreciarán que “Bluetooth” y “802.11” se refieren a conjuntos de especificaciones, disponibles en el Instituto de Ingenieros Eléctricos y Electrónicos, con referencia a las redes de área personal inalámbricas y las redes de área local inalámbricas, respectivamente.

Los sistemas y métodos revelados aquí dentro se presentan solamente a modo de ejemplo y no suponen limitar el alcance de la invención. Otras variaciones de los sistemas y métodos descritos anteriormente serán evidentes para aquellos expertos en la técnica y como tal se consideran que están dentro del alcance de la invención. Por ejemplo, se debería entender que los pasos y el orden de los pasos en el proceso descrito aquí dentro se pueden alterar, modificar y/o aumentar y todavía logar el resultado deseado. Solamente como ejemplo, la secuencia de pasos representados en la Figura 2 y Figura 3 se puede alterar con respecto a la temporización de la destrucción de las diversas claves y los valores provisionales, a condición de que esas claves y valores estuvieran disponibles para su propósito previsto.

Los datos de los sistemas y métodos se pueden almacenar en uno o más almacenes de datos. Los almacenes de datos pueden ser de muchos tipos diferentes de dispositivos de almacenamiento y construcciones de programación, tal como RAM, ROM, memoria Rápida, estructuras de datos de programación, variables de programación, etc. Se señala que las estructuras de datos describen formatos para usar en organizar y almacenar los datos en bases de datos, programas, memoria, u otro medio legible por ordenador para usar por un programa informático.

El código adaptado para proporcionar los sistemas y métodos descritos anteriormente se pueden proporcionar en muchos tipos diferentes de medios legibles por ordenador que incluyen mecanismos de almacenamiento informático (por ejemplo, CD-ROM, disco flexible, RAM, memoria rápida, disco duro de ordenador, etc.) que contienen instrucciones para usar en la ejecución por un procesador para realizar las operaciones de los métodos e implementar los sistemas descritos aquí dentro.

Los componentes informáticos, módulos de programa, funciones y estructuras de datos descritos aquí dentro se pueden conectar directamente o indirectamente uno con otro para permitir el flujo de datos necesario para sus funcionamientos. También se señala que un módulo o procesador incluye pero no se limita a una unidad de código que realiza una operación de soporte lógico, y se puede implementar por ejemplo como una unidad de subrutina de código, o como una unidad de función de soporte lógico de código, o como un objeto (como en un paradigma orientado a objeto), o como un programita, o en un lenguaje de escritura informático, o como otro tipo de código de ordenador.

Diversas realizaciones de la presente invención que han sido descritas de esta manera en detalle a modo de ejemplo, serán evidentes a aquellos expertos en la técnica que se pueden hacer variaciones y modificaciones sin salirse de la invención. La invención incluye todas de tales variaciones y modificaciones como que caen dentro del alcance de las reivindicaciones anexas.

REIVINDICACIONES

1. Un método para asegurar datos en un dispositivo de almacenamiento de datos (10, 100) capaz de estar asegurado por una primera contraseña, el dispositivo de almacenamiento de datos (10, 100) que se proporciona con una clave de protección de contenido ***K***, el método que comprende:

recibir (225), en el dispositivo de almacenamiento de datos (10, 100), una clave pública ***B*** generada a partir de una clave privada ***b*** en una ubicación remota (40), la clave privada ***b*** que se almacena en la ubicación remota (40);
generar (235, 240), en el dispositivo de almacenamiento de datos (10, 100), una clave privada ***d*** y una clave pública ***D*** a partir de la clave privada ***d***;
generar (250), en el dispositivo de almacenamiento de datos (10, 100), una clave de cifrado de claves ***L*** a partir de la clave privada ***d*** y la clave pública ***B***;
cifrar (260) la clave de protección de contenido ***K*** con la clave de cifrado de claves ***L*** para proporcionar una primera clave de protección de contenido cifrada, cifrando (255) la clave de protección de contenido ***K*** con la primera contraseña para proporcionar una segunda clave de protección de contenido cifrada, y almacenar la primera y la segunda claves de protección de contenido cifradas en el dispositivo de almacenamiento de datos (10, 100);
destruir (265) ***d*** y ***K*** en el dispositivo de almacenamiento de datos (10, 100); y
recuperar la clave de cifrado de claves ***L***:

generando (320, 325), en el dispositivo de almacenamiento de datos, un valor de clave ***r*** y una clave pública ***D'*** a partir del valor de clave ***r*** y la clave pública ***D***;
transmitiendo (330) la clave pública ***D'*** a la ubicación remota;
recibiendo, (355), en el dispositivo de almacenamiento de datos, una clave pública ***L'*** generada a partir de la clave privada ***b*** y la clave pública ***D'*** en la ubicación remota; y
obteniendo (365), en el dispositivo de almacenamiento de datos, la clave de cifrado de claves ***L*** a partir de un inverso r^{-1} del valor de clave ***r*** y a partir de la clave pública ***L'***.

2. El método de la reivindicación 1 que además comprende cifrar el contenido almacenado en el dispositivo de almacenamiento de datos usando la clave de protección de contenido ***K*** antes de cifrar la clave de protección de contenido ***K*** y almacenar las claves de protección de contenido cifradas en el dispositivo de almacenamiento de datos.

3. El método de la reivindicación 1 que además comprende:

recibir una contraseña de entrada;
determinar que la contraseña de entrada coincide con la primera contraseña, y si la contraseña de entrada coincide con la primera contraseña,
descifrar la segunda clave de protección de contenido cifrada usando la contraseña de entrada para obtener la clave de protección de contenido ***K***; y
usar la clave de protección de contenido ***K*** obtenida de esta manera para cifrar el contenido para almacenamiento en el dispositivo de almacenamiento de datos.

4. El método de la reivindicación 3 que además comprende usar la clave de protección de contenido ***K*** obtenida de esta manera para descifrar el contenido cifrado almacenado en el dispositivo de almacenamiento de datos.

5. El método de la reivindicación 1, que además comprende descifrar la primera clave de protección de contenido cifrada usando la clave de cifrado de claves ***L*** recuperada de esta manera para obtener la clave de protección de contenido ***K***.

6. El método de la reivindicación 5, que además comprende:

descifrar el contenido previamente cifrado usando una clave de protección de contenido ***K*** y almacenada en el dispositivo de almacenamiento de datos usando la clave de protección de contenido ***K*** obtenida de esta manera;
proporcionar una nueva clave de protección de contenido ***K'***;
cifrar el contenido descifrado de esta manera usando la nueva clave de protección de contenido ***K'***;
cifrar la nueva clave de protección de contenido ***K'*** usando la clave de cifrado de claves ***L*** para proporcionar una nueva primera clave de protección de contenido cifrada, y cifrar la nueva clave de protección de contenido ***K'*** con la primera contraseña para proporcionar una nueva segunda clave de protección de contenido cifrada.

7. El método de la reivindicación 5, que además comprende:

proporcionar una nueva clave de cifrado de claves ***M***;
recibir una segunda contraseña;
cifrar la clave de protección de contenido ***K*** usando la nueva clave de cifrado de claves ***M*** para proporcionar una nueva primera clave de protección de contenido cifrada, y cifrar la clave de protección de contenido ***K*** con la segunda contraseña para proporcionar una nueva segunda clave de protección de contenido cifrada.

8. El método de la reivindicación 7 en el que proporcionar una nueva clave de cifrado de claves ***M*** comprende:

recibir, en un dispositivo de almacenamiento de datos, una clave pública B_1 generada a partir de una clave privada b_1 en la ubicación remota, la clave privada b_1 que se almacena en la ubicación remota;
generar, en el dispositivo de almacenamiento de datos, una clave privada d_1 y una clave pública D_1 a partir de la clave privada d_1;
generar, en el dispositivo de almacenamiento de datos, una clave de cifrado de claves ***M*** a partir de la clave privada d_1 y la clave pública B_1; y
destruir, en el dispositivo de almacenamiento de datos, ***M***, d_1 y ***K*** mientras que retiene la nueva primera y la nueva segunda claves de protección de contenido cifradas.

9. El método de cualquiera de las reivindicaciones 1 a 8, que además comprende recibir, en el dispositivo de almacenamiento de datos, una petición de la clave pública ***D'*** desde la ubicación remota, anterior a generar el valor de clave ***r*** y la clave pública ***D'***.

10. El método de cualquiera de las reivindicaciones 1 a 8, que además comprende recibir, en el dispositivo de almacenamiento de datos, un comando de reinicialización de contraseña desde la ubicación remota, anterior a generar el valor de clave ***r*** y la clave pública ***D'***.

11. El método de la reivindicación 5, que además comprende:

descifrar el contenido previamente cifrado usando la clave de protección de contenido ***K*** y almacenada en el dispositivo de almacenamiento de datos usando la clave de protección de contenido ***K*** obtenida de esta manera;
proporcionar una nueva clave de protección de contenido ***K'***;
cifrar el contenido descifrado de esta manera usando la nueva clave de protección de contenido ***K'***;
proporcionar una nueva clave de cifrado de claves ***M***;
cifrar la nueva clave de protección de contenido ***K'*** usando la contraseña para proporcionar una nueva primera clave de protección de contenido cifrada, y cifrar la nueva clave de protección de contenido ***K'*** con la nueva clave de cifrado de claves ***M*** para proporcionar una nueva segunda clave de protección de contenido cifrada.

12. El método de la reivindicación 11 en el que proporcionar una nueva clave de cifrado de claves ***M*** comprende:

recibir, en un dispositivo de almacenamiento de datos, una clave pública B_1 generada a partir de una clave privada b_1 en la ubicación remota, la clave privada b_1 que se almacena en la ubicación remota;
generar, en el dispositivo de almacenamiento de datos, una clave privada d_1 y una clave pública D_1 a partir de la clave privada d_1;
generar, en el dispositivo de almacenamiento de datos, una clave de cifrado de claves ***M*** a partir de la clave privada d_1 y la clave pública B_1; y
destruir, en el dispositivo de almacenamiento de datos, la clave de cifrado de claves ***M***, la clave privada d_1 y la nueva clave de protección de contenido ***K'*** mientras que retiene la nueva primera y la nueva segunda claves de protección de contenido cifradas.

13. El método de la reivindicación 8 o la reivindicación 12 en el que la clave pública ***B*** también se genera desde un punto elíptico predeterminado ***P***, y la clave pública B_1 también se genera a partir de un punto elíptico predeterminado P_1.

14. El método de cualquiera de las reivindicaciones precedentes, que además comprende:

recibir desde la ubicación remota una nueva contraseña;
transmitir a la ubicación remota la clave pública ***D'***, en donde ***D' = rD***;
recibir, desde la ubicación remota, la clave pública ***L'***, en donde ***L'*** comprende una clave pública generada a partir del valor de clave ***b*** y la clave pública ***D'***;
calcular r^1L' para deducir la clave de cifrado de claves ***L***;
descifrar la primera clave de protección de contenido cifrada;
deducir una nueva clave de protección de contenido; y
cifrar la nueva clave de protección de contenido usando la nueva contraseña para proporcionar una segunda clave de protección de contenido cifrada.

15. El método de la reivindicación 14 cuando no depende directamente o indirectamente de ninguna de las reivindicaciones 7, 8, 12 o 13, que además comprende:

recibir una clave pública B_1 desde la ubicación remota, la clave pública B_1 que se genera a partir de una clave privada b_1 y un punto elíptico predeterminado P_1 en la ubicación remota;
generar una clave privada d_1, y una clave pública D_1 a partir de la clave privada d_1 y el punto elíptico predeterminado P_1;
generar una clave de cifrado de claves ***M*** a partir de la clave privada d_1 y la clave pública B_1;
destruir la clave privada d_1; y
cifrar la nueva contraseña usando la nueva clave de cifrado de claves ***M.***

16. Un dispositivo de almacenamiento de datos (10, 100) para almacenar datos cifrados, el dispositivo de almacenamiento de datos (10, 100) que se adapta para permitir el acceso a las operaciones del dispositivo de almacenamiento de datos al introducir con éxito una contraseña, el dispositivo de almacenamiento de datos (10, 100) que comprende:

una memoria volátil (426) para almacenar datos que comprenden los datos a ser cifrados o descifrados, contraseñas, y claves;
una memoria no volátil (424) para almacenar datos cifrados y claves cifradas; y
un procesador (438) adaptado para:

recibir desde una ubicación remota (40) una clave pública ***B*** en donde ***B = bP*** en donde ***b*** es una clave privada y ***P*** es un punto elíptico predeterminado, generar un valor aleatorio ***d*** y almacenar temporalmente el valor aleatorio ***d*** en la memoria volátil o no volátil, calcular una clave pública ***D = dP***, y almacenar la clave pública ***D*** en la memoria no volátil;
calcular una clave de cifrado de claves ***L = dB***, cifrar una clave de protección de contenido ***K*** usando la clave de cifrado de claves ***L***, usar la clave de protección de contenido ***K*** para cifrar y descifrar los datos a ser almacenados en la memoria no volátil, y cifrar y descifrar la clave de protección de contenido ***K*** usando una contraseña almacenada en la memoria volátil; y borrar la clave de cifrado de claves ***L***, el valor aleatorio ***d*** y las copias no cifradas de la clave de protección de contenido ***K***; y
generar un valor aleatorio ***r*** y almacenar temporalmente el valor aleatorio ***r*** en la memoria volátil o no volátil, calcular una clave pública ***D' = rD***, y transmitir la clave pública ***D'*** a la ubicación remota; recibir desde la ubicación remota una clave pública ***L' = bD'*** y calcular r^1L', en donde r^1 es un inverso del valor de clave ***r***, para deducir la clave de cifrado de claves ***L***, y usar la clave de cifrado de claves ***L*** derivada de esta manera para descifrar la clave de protección de contenido ***K***.

17. Un método para asegurar datos en un dispositivo de almacenamiento de datos (10, 100) capaz de estar asegurado por una primera contraseña, el dispositivo de almacenamiento de datos (10, 100) que se proporciona con una clave de protección de contenido ***K***, el método que comprende:

recibir (225), en un dispositivo de almacenamiento de datos, una clave pública ***B*** generada a partir de una clave privada ***b*** en una ubicación remota, la clave privada ***b*** que está almacenada en la ubicación remota;
generar (235, 240), en el dispositivo de almacenamiento de datos, una clave privada ***d*** y una clave pública ***D*** a partir de la clave privada ***d***;
generar (250), en el dispositivo de almacenamiento de datos, una clave de cifrado de claves ***L*** a partir de la clave privada ***d*** y la clave pública ***B***;
cifrar (255) la clave de protección de contenido ***K*** con la primera contraseña para proporcionar una clave de protección de contenido cifrada, y almacenar la clave de protección de contenido cifrada en el dispositivo de almacenamiento de datos;
cifrar la primera contraseña con la clave de cifrado de claves ***L*** para proporcionar una primera contraseña cifrada, y almacenar la contraseña cifrada en el dispositivo de almacenamiento de datos;
destruir (265) la clave privada ***d*** y la clave de protección de contenido no cifrada ***K*** en el dispositivo de almacenamiento de datos; y
recuperar la clave de cifrado de claves ***L***:

generando (320, 325), en el dispositivo de almacenamiento de datos, un valor de clave ***r*** y una clave pública ***D'*** a partir del valor de clave r y la clave pública ***D***;
transmitiendo (330) la clave pública ***D'*** a la ubicación remota;
recibiendo (355), en el dispositivo de almacenamiento de datos, una clave pública ***L'*** generada a partir de la clave privada ***b*** y la clave pública ***D'*** en la ubicación remota; y
obteniendo (365), en el dispositivo de almacenamiento de datos, la clave de cifrado de claves ***L*** a partir del inverso r^1 del valor de clave ***r*** y la clave pública ***L'***.

18. El método de la reivindicación 17 que además comprende cifrar el contenido almacenado en el dispositivo de

almacenamiento de datos usando la clave de protección de contenido ***K*** antes de cifrar la clave de protección de contenido ***K*** y almacenar la clave de protección de contenido cifrada en el dispositivo de almacenamiento de datos.

19. El método de la reivindicación 18 que además comprende:

recibir una contraseña de entrada;
determinar que la contraseña de entrada coincide con la primera contraseña, y si la contraseña de entrada coincide con la primera contraseña,
descifrar la clave de protección de contenido cifrada usando la contraseña de entrada para obtener la clave de protección de contenido ***K***; y
usar la clave de protección de contenido ***K*** obtenida de esta manera para cifrar el contenido para almacenamiento en el dispositivo de almacenamiento de datos.

20. El método de la reivindicación 19 que además comprende usar la clave de protección de contenido ***K*** obtenida de esta manera para descifrar el contenido cifrado almacenado en el dispositivo de almacenamiento de datos.

21. El método de la reivindicación 17, que además comprende descifrar la primera contraseña cifrada ***L*** recuperada de esta manera para obtener la primera contraseña, y descifrar la clave de protección de contenido cifrada usando la primera contraseña obtenida descifrando la primera contraseña cifrada para obtener la clave de protección de contenido ***K***.

22. El método de la reivindicación 21, que además comprende:

descifrar el contenido cifrado previamente usando la clave de protección de contenido ***K*** y almacenada en el dispositivo de almacenamiento de datos usando la clave de protección de contenido ***K*** obtenida de esta manera;
proporcionar una nueva clave de protección de contenido ***K'***;
cifrar el contenido descifrado de esta manera usando la clave de protección de contenido ***K'***;
cifrar la nueva clave de protección de contenido ***K'*** usando la primera contraseña para proporcionar una nueva clave de protección de contenido cifrada.

23. El método de la reivindicación 21, que además comprende:

proporcionar una nueva clave de cifrado de claves ***M***;
recibir una segunda contraseña;
cifrar la clave de protección de contenido ***K*** obtenida de esta manera usando la segunda contraseña para proporcionar una nueva clave de protección de contenido cifrada, y cifrar la segunda contraseña usando la nueva clave de cifrado de claves ***M*** para proporcionar una segunda contraseña cifrada.

24. El método de la reivindicación 23 en el que proporcionar una nueva clave de cifrado de claves ***M*** comprende:

recibir, en un dispositivo de almacenamiento de datos, una clave pública B_1 generada a partir de una clave privada b_1 en la ubicación remota, la clave privada b_1 que se almacena en la ubicación remota;
generar, en el dispositivo de almacenamiento de datos, una clave privada d_1 y una clave pública D_1 a partir de la clave privada d_1;
generar, en el dispositivo de almacenamiento de datos, una clave de cifrado de claves ***M*** a partir de la clave privada d_1 y la clave pública B_1; y
destruir la clave privada d_1, destruyendo la clave de protección de contenido ***K*** después de que se proporciona la nueva clave de protección de contenido cifrada, y destruir la clave de cifrado de claves ***M*** después de que se proporciona la segunda contraseña cifrada, en el dispositivo de almacenamiento de datos.

25. El método de cualquiera de las reivindicaciones 17 a 24, que además comprende recibir, en el dispositivo de almacenamiento de datos (10, 100), una petición de la clave pública ***D'*** desde la ubicación remota (40), anterior a generar el valor de clave ***r*** y la clave pública ***D'***.

26. El método de cualquiera de las reivindicaciones 17 a 24, que además comprende recibir, en el dispositivo de almacenamiento de datos, un comando de reinicialización de contraseña desde la ubicación remota, anterior a generar el valor de clave ***r*** y la clave pública ***D'***.

27. El método de la reivindicación 21, que además comprende:

descifrar el contenido previamente cifrado usando la clave de protección de contenido ***K*** y almacenada en el dispositivo de almacenamiento de datos usando la clave de protección de contenido ***K*** obtenida de esta manera;
proporcionar una nueva clave de protección de contenido ***K';***

cifrar el contenido descifrado de esta manera usando la nueva clave de protección de contenido ***K'***;
proporcionar una nueva clave de cifrado de claves ***M***;
cifrar la nueva clave de protección de contenido ***K'*** usando la contraseña para proporcionar una nueva clave de protección de contenido cifrada, y cifrar la primera contraseña con la nueva clave de protección de claves ***M*** para proporcionar una nueva primera contraseña cifrada.

28. El método de la reivindicación 27 en el que proporcionar una nueva clave de cifrado de claves ***M*** comprende:

recibir, en un dispositivo de almacenamiento de datos, una clave pública B_1 generada a partir de una clave privada b_1 en la ubicación remota, la clave privada b_1 que se almacena en la ubicación remota;
generar, en el dispositivo de almacenamiento de datos, una clave privada d_1 y una clave pública D_1 a partir de la clave privada d_1;
generar, en el dispositivo de almacenamiento de datos, una clave de cifrado de claves ***M*** a partir de la clave privada d_1 y la clave pública B_1; y
destruir la clave privada d_1, destruyendo la nueva clave de protección de contenido ***K'*** después de que se proporciona la nueva clave de protección de contenido cifrada, y destruyendo la clave de cifrado de claves ***M*** después de que se proporciona la nueva primera contraseña cifrada, en el dispositivo de almacenamiento de datos.

29. El método de la reivindicación 24 o la reivindicación 28 en el que la clave pública ***B*** también se genera a partir de un punto elíptico predeterminado ***P***, y la clave pública B_1 también se genera a partir de un punto elíptico predeterminado P_1.

30. El método de cualquiera de las reivindicaciones 17 a 29, que además comprende
recibir desde la ubicación remota una segunda contraseña en el dispositivo de almacenamiento de datos (10, 100);
transmitir a la ubicación remota la clave pública ***D'***, en donde ***D' = rD***;
recibir, desde la ubicación remota, la clave pública ***L'***, en donde la clave pública ***L'*** comprende una clave pública generada a partir del valor de clave ***b*** y la clave pública ***D'***;
calcular r^1L' , en el que r^1 es un inverso del valor de clave ***r***, para deducir la clave de cifrado de claves ***L***;
descifrar la primera contraseña cifrada para obtener una primera contraseña descifrada; descifrar la clave de protección de contenido cifrada usando la primera contraseña descifrada; deduciendo una nueva clave de protección de contenido; y
cifrar la nueva clave de protección de contenido usando la segunda contraseña para proporcionar una nueva clave de protección de contenido cifrada.

31. El método de la reivindicación 30 cuando no depende directamente o indirectamente de ninguna de las reivindicaciones 23, 24, 27, 28 o 29, que además comprende:

deducir una nueva clave de cifrado de claves ***M***:

recibiendo una clave pública B_1 generada a partir de una clave privada b_1 y un punto elíptico predeterminado P_1 en la ubicación remota, la clave privada b_1 que se almacena en la ubicación remota;
generar una clave privada d_1, y una clave pública D_1 a partir de la clave privada d_1 y el punto elíptico predeterminado P_1;
generando la nueva clave de cifrado de claves ***M*** a partir de la clave privada d_1 y la clave pública B_1; y
destruir la clave privada d_1; y
cifrando la segunda contraseña usando la nueva clave de cifrado de claves ***M.***

32. Un medio legible por ordenador que comprende código ejecutable por un dispositivo informático (40) para llevar a cabo el método de cualquiera de las reivindicaciones 1 a 15 o 17 a 31.

33. Un dispositivo de almacenamiento de datos (10, 100) para almacenar datos cifrados, el dispositivo de almacenamiento de datos que se adapta para permitir el acceso a operaciones del dispositivo de almacenamiento de datos en la introducción con éxito de una contraseña, el dispositivo de almacenamiento de datos (10, 100) que comprende:

una memoria volátil (426) para almacenar datos que comprenden los datos a ser cifrados o descifrados, contraseñas, y claves;
una memoria no volátil (424) para almacenar los datos cifrados y las claves cifradas; y
un procesador (438) adaptada para:

recibir desde una ubicación remota (40) una clave pública ***B*** en donde ***B = bP*** en donde ***b*** es una clave privada y ***P*** es un punto elíptico predeterminado, generar un valor aleatorio ***d*** y almacenar temporalmente el valor aleatorio ***d*** en la memoria volátil o no volátil, calcular una clave pública ***D = dP***, y almacenar la clave pública ***D*** en la memoria no volátil;

calcular una clave de cifrado de claves ***L = dB***, cifrar una clave de protección de contenido ***K*** usando una contraseña introducida por el usuario, cifrar la contraseña introducida por el usuario usando la clave de cifrado de claves ***L***, usar la clave de protección de contenido ***K*** para cifrar y descifrar los datos a ser almacenados en la memoria no volátil; y borrar el valor aleatorio ***d*** y las copias no cifradas de la clave de protección de contenido ***K***; y

generar un valor aleatorio ***r*** y almacenar temporalmente ***r*** en la memoria volátil o no volátil, calcular una clave pública ***D' = rD,*** y transmitir la clave pública ***D'*** a la ubicación remota; recibir desde la ubicación remota una clave pública ***L' = bD'*** y calcular $r^{1}L'$, en donde r^{1} es un inverso de ***r***, para deducir la clave de cifrado de claves ***L***, y usar la clave de cifrado de claves ***L*** deducida de esta manera para descifrar la contraseña cifrada introducida por el usuario.

34. El dispositivo de almacenamiento de datos (10, 100) de la reivindicación 16 o la reivindicación 33, en el que el dispositivo de almacenamiento de datos es un dispositivo de comunicación móvil.

35. El dispositivo de almacenamiento de datos (10, 100) de la reivindicación 16 o la reivindicación 33, en el que el dispositivo de almacenamiento de datos es un ordenador personal.

36. El método de la reivindicación 13 o la reivindicación 29 en el que el punto elíptico predeterminado P_1 es el mismo que el punto elíptico predeterminado ***P***.

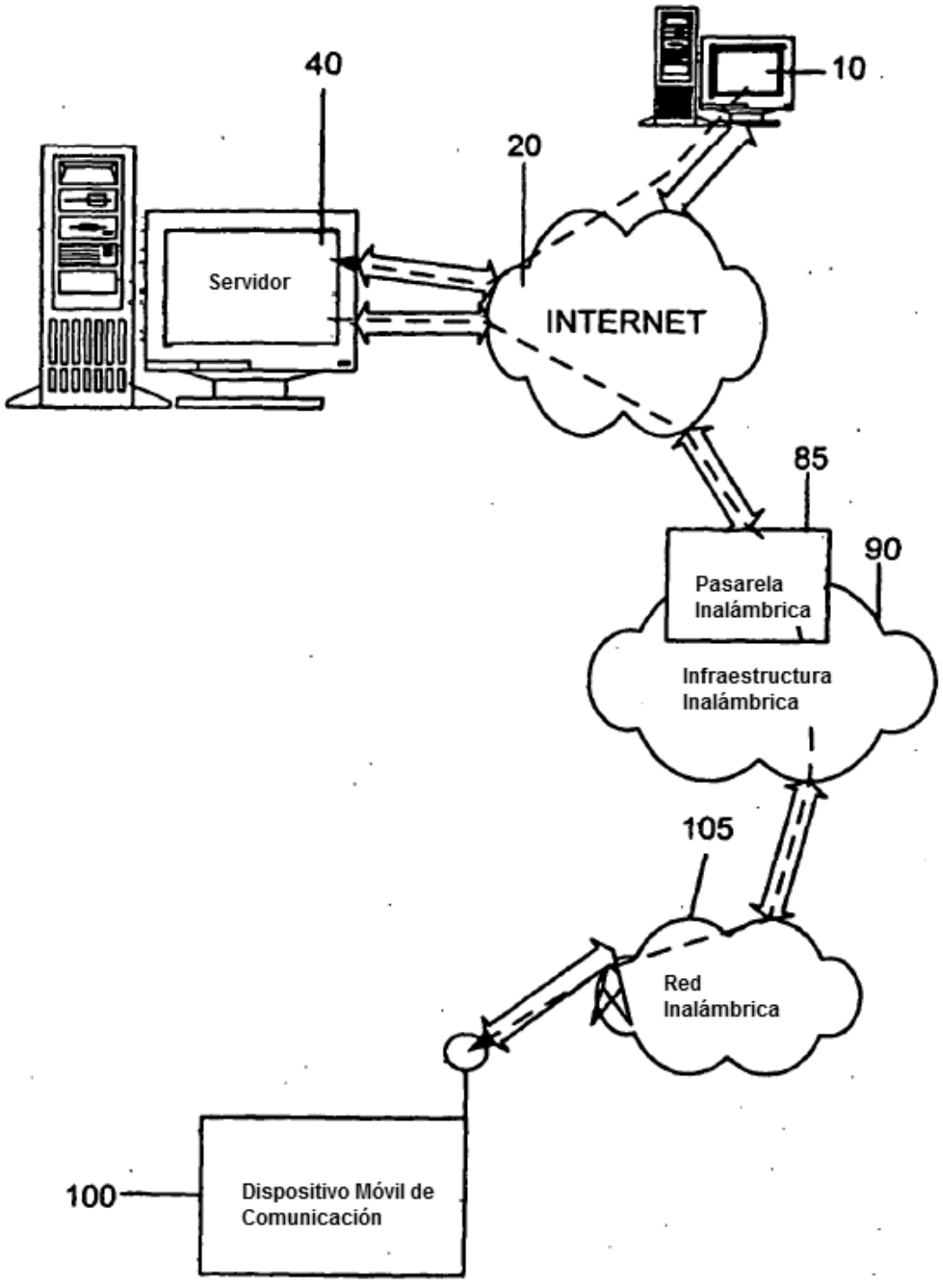

40
10
20
Servidor
INTERNET
85
90
Pasarela
Inalámbrica
Infraestructura
Inalámbrica
105
Red
Inalámbrica
100
Dispositivo Móvil de
Comunicación

Figura 1

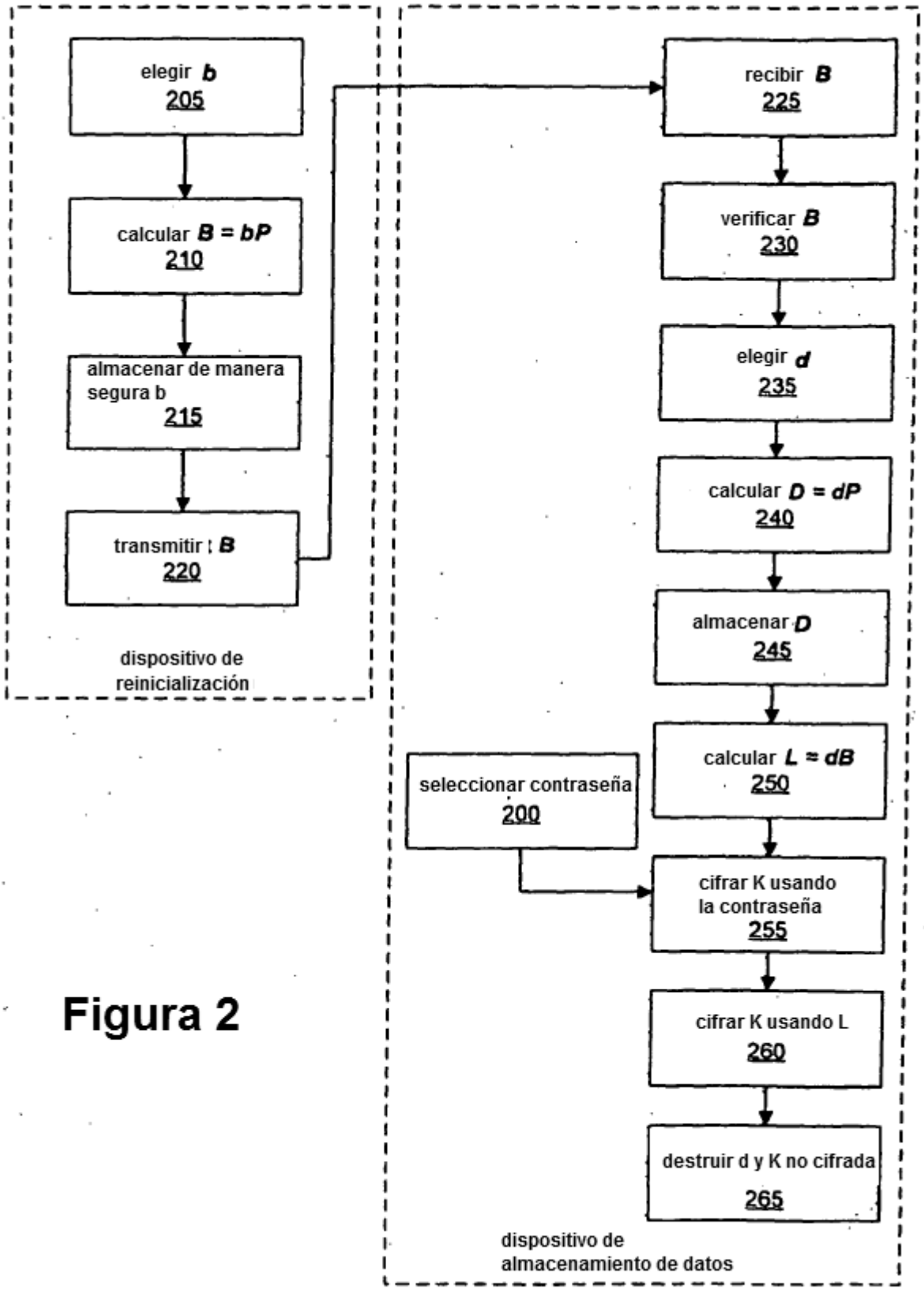
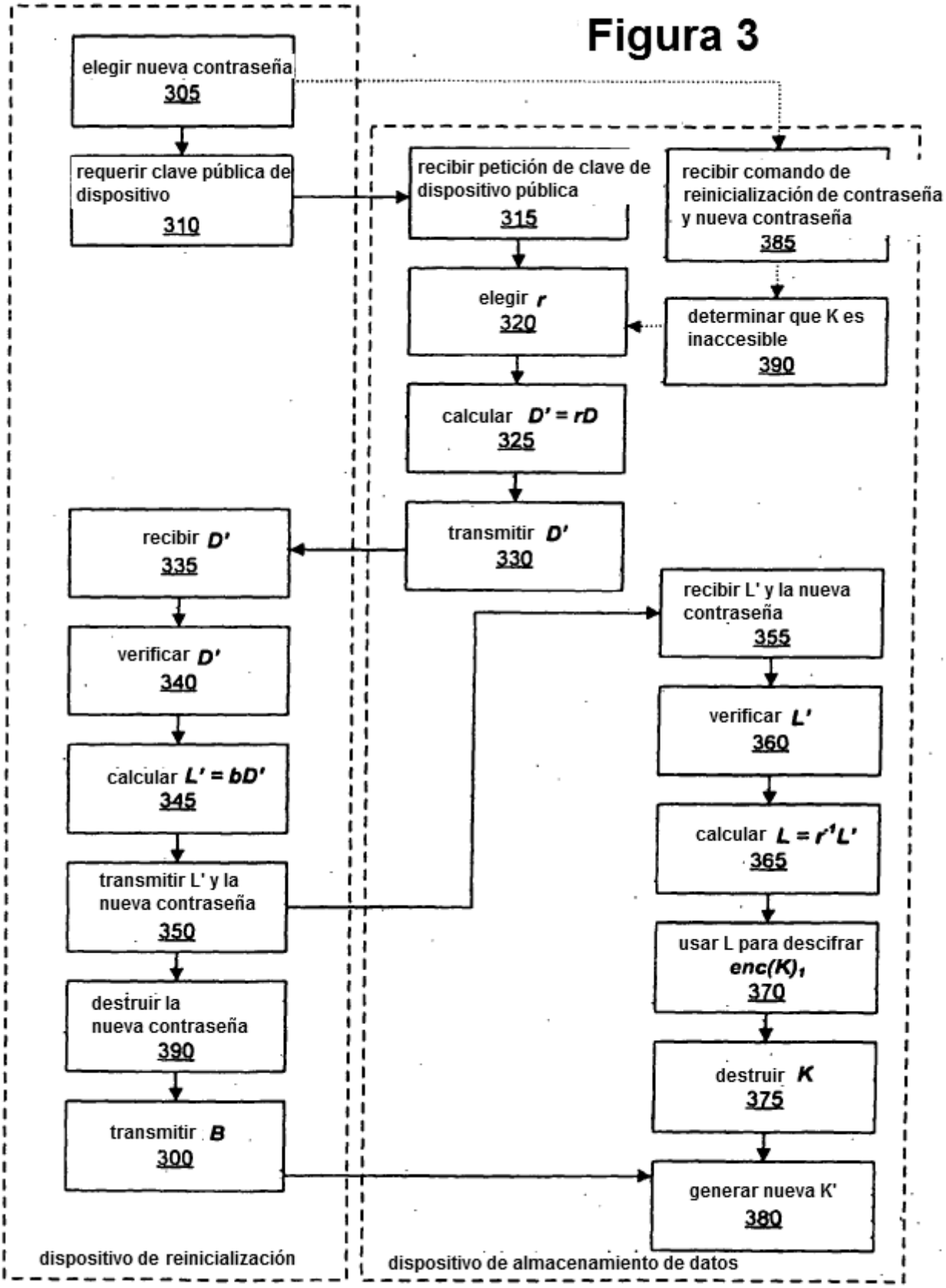

elegir b
205
calcular B = bP
210
almacenar de manera segura b
215
transmitir B
220
dispositivo de reinicialización
recibir B
225
verificar B
230
elegir d
235
calcular D = dP
240
almacenar D
245
calcular L = dB
250
seleccionar contraseña
200
cifrar K usando la contraseña
255
cifrar K usando L
260
destruir d y K no cifrada
265
dispositivo de almacenamiento de datos

Figura 2

Figura 3


elegir nueva contraseña
305
requerir clave pública de dispositivo
310
recibir petición de clave de dispositivo pública
315
recibir comando de reinicialización de contraseña y nueva contraseña
385
elegir r
320
determinar que K es inaccesible
390
calcular D' = rD
325
transmitir D'
330
recibir D'
335
verificar D'
340
calcular L' = bD'
345
transmitir L' y la nueva contraseña
350
destruir la nueva contraseña
390
transmitir B
300
recibir L' y la nueva contraseña
355
verificar L'
360
calcular L = r⁻¹L'
365
usar L para descifrar enc(K),
370
destruir K
375
generar nueva K'
380
dispositivo de reinicialización
dispositivo de almacenamiento de datos

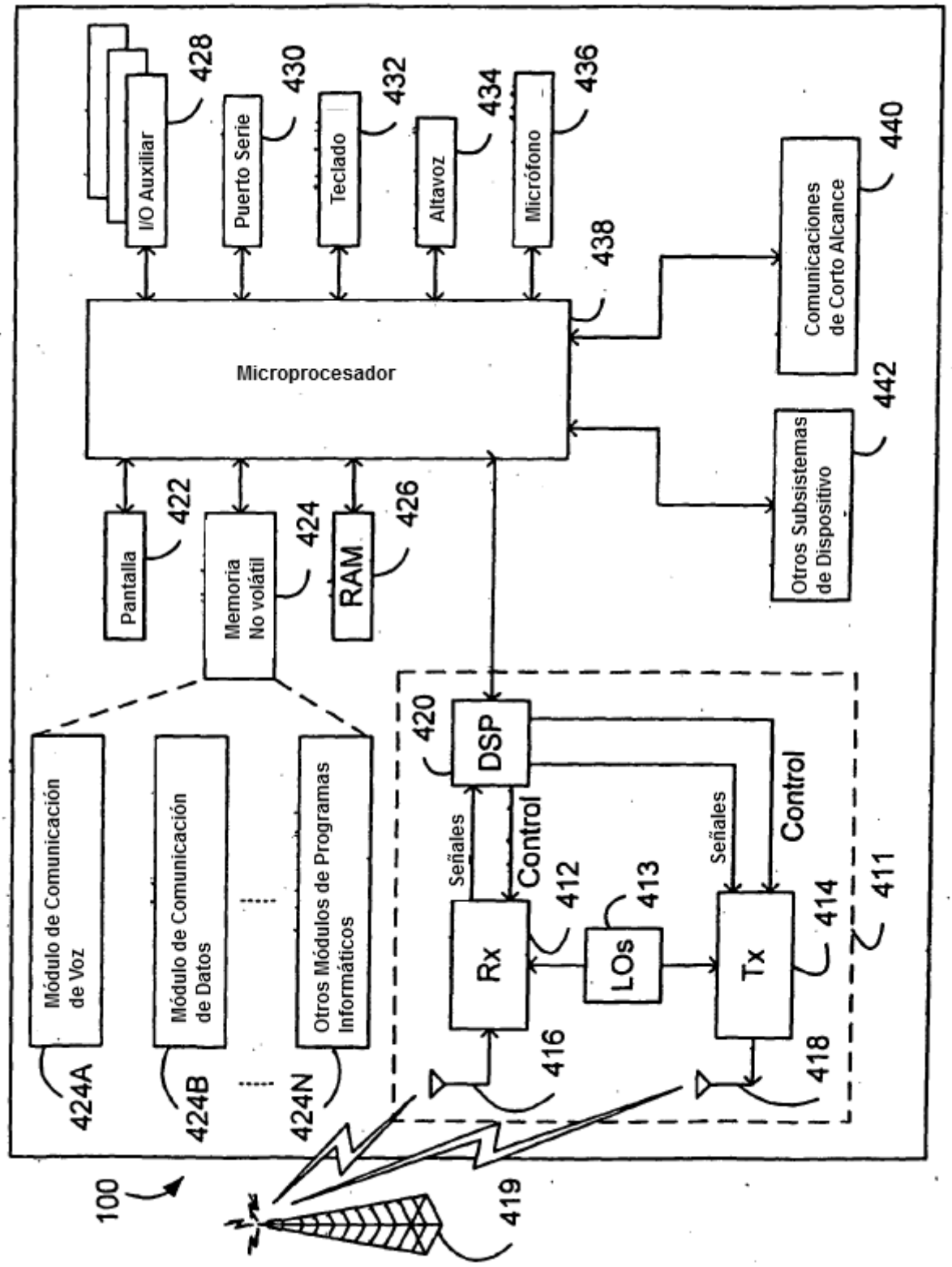

I/O Auxiliar
428
Puerto Serie
430
Teclado
432
Altavoz
434
Micrófono
436
438
Microprocesador
Comunicaciones de Corto Alcance
440
Otros Subsistemas de Dispositivo
442
Pantalla
422
Memoria No volátil
424
RAM
426
Módulo de Comunicación de Voz
Módulo de Comunicación de Datos
Otros Módulos de Programas Informáticos
424A
424B
424N
420
DSP
Señales
Control
412
Rx
LOs
413
Señales
Control
414
Tx
411
416
418
419
100

Figura 4