

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 604 457**

51 Int. Cl.:

G06F 21/10

(2013.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **30.09.2005 PCT/FI2005/000416**

87 Fecha y número de publicación internacional: **06.04.2006 WO06035111**

96 Fecha de presentación y número de la solicitud europea: **30.09.2005 E 05794620 (4)**

97 Fecha y número de publicación de la concesión europea: **28.09.2016 EP 1794729**

54 Título: **Método, dispositivo y producto de programa informático para activar el derecho de uso de al menos un elemento de contenido protegido**

30 Prioridad:

30.09.2004 US 957191

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

07.03.2017

73 Titular/es:

**NOKIA TECHNOLOGIES OY (100.0%)
Karaportti 3
02610 Espoo, FI**

72 Inventor/es:

**VATAJA, TIMO y
INGET, VIRVE**

74 Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

ES 2 604 457 T3

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

DESCRIPCIÓN

Método, dispositivo y producto de programa informático para activar el derecho de uso de al menos un elemento de contenido protegido

Antecedentes de la invención

Campo de la invención:

La invención se refiere a los dispositivos terminales. En particular, la invención se refiere a un método, un dispositivo y un producto de programa informático nuevos y mejorados para activar el derecho de uso de al menos un elemento de contenido protegido almacenado en una memoria del dispositivo o en una memoria extraíble que puede conectarse al dispositivo.

Descripción de la técnica relacionada:

Desde la introducción de las tecnologías de almacenamiento digital, la aplicación más efectiva de los derechos de autor se ha convertido en un problema. Especialmente, la aparición de Internet como un canal de distribución ilícita de contenidos protegidos por derechos de autor ha creado una fuerte demanda de nuevas tecnologías en materia de protección de los derechos de autor. Una de estas tecnologías es la gestión de derechos digitales (DRM). El DRM es un término común para estándares y sistemas propietarios en los que un elemento de contenido determinado se aumenta con información que especifica los derechos de usuario asociados con el mismo. El elemento de contenido puede ser, por ejemplo, una grabación de audio, un video, una imagen, un programa de ordenador o simplemente un documento. Los derechos de usuario pueden comprender varias reglas relativas al uso del elemento de contenido. Por ejemplo, a un usuario se le puede dar un límite de tiempo durante el cual puede presentarse el elemento de contenido, es decir, reproducido para el usuario. El número de veces que se permite escuchar, las identidades de dispositivo permitidas y los derechos de visualización parcial son otros ejemplos de reglas relacionadas con el uso de un elemento de contenido. El DRM requiere que el dispositivo de presentación y el software de presentación en el mismo no sean hostiles, es decir, participen en la aplicación de los derechos digitales. En el dispositivo de presentación suele haber un agente DRM, o en otras palabras, un motor DRM, que hace cumplir los derechos de DRM y protege los elementos de contenido de una copia ilícita. Con el fin de evitar que un elemento de contenido protegido por DRM esté disponible para copiar, el elemento de contenido puede encriptarse mientras está en tránsito desde la red al dispositivo de presentación y mientras está almacenado en el dispositivo de presentación en el exterior del motor DRM, por ejemplo, en un disco duro.

Un estándar para el DRM es el que se basa en la especificación DRM de la alianza móvil abierta (OMA). El objetivo de la DRM OMA es permitir el consumo controlado de objetos de medios digitales permitiendo a los proveedores de contenido expresar los derechos de contenido. Los objetos de medios son elementos de contenido tales como clips de audio, videoclips, imágenes, aplicaciones Java y documentos.

Si un fabricante, licenciario u operador desea diferenciar sus teléfonos, es difícil hacerlo en terminales abiertos, por ejemplo en terminales de sistema operativo Symbian. Symbian es una compañía de licencias de software que desarrolla y suministra un sistema operativo estándar avanzado y abierto para teléfonos móviles con capacidad de datos. Por ejemplo, si algún fabricante de teléfonos móviles desea fabricar un teléfono premium que incluya un editor de vídeo y un teléfono móvil de bajo coste que no incluya el editor de vídeo, no hay medios para detener la copia de la aplicación de editor de vídeo desde el teléfono móvil premium al teléfono móvil de bajo coste. El fabricante del teléfono móvil o un operador también puede querer ofrecer aplicaciones que tengan restricciones en su uso (por ejemplo, que se use 10 veces, una aplicación válida por un mes, etc.) y después de que se hayan consumido los derechos, el propietario del terminal puede ganar más derechos para la aplicación.

El DRM OMA ofrece restricciones para el uso de aplicaciones, pero actualmente no hay un medio para ofrecer un contenido DRM OMA que esté listo al comprar el teléfono. Una solución normal en este momento es comprar y activar el contenido a través de la interfaz aérea.

La publicación US 2003/0226026 desvela un método y un aparato para encriptar un medio de almacenamiento reescribible sin encriptar cuando el medio de almacenamiento está conectado a un aparato de procesamiento. El aparato de procesamiento obtiene un número de identificación que es único para el aparato de procesamiento. Comprobando un indicador de encriptado del medio de almacenamiento, el aparato de procesamiento verifica si el medio de almacenamiento está encriptado. Si el medio de almacenamiento está sin encriptar, el aparato de procesamiento encripta y sobrescribe el medio de almacenamiento usando el número de identificación.

Sumario de la invención:

La invención ofrece un contenido DRM en un dispositivo que está listo cuando, por ejemplo, se compra el dispositivo.

De acuerdo con un aspecto de la invención, la invención es un método para activar el derecho de uso de al menos una pieza protegida de contenido en un dispositivo cuando el dispositivo se enciende por primera vez. El método se caracteriza por que el método comprende: proporcionar un dispositivo con al menos un archivo de derechos sin encriptar, en el que el al menos un archivo de derechos asigna el derecho de uso de la al menos una pieza protegida de contenido, cada uno del al menos un archivo de derechos que incorpora los derechos a una pieza de contenido, comprendiendo el al menos un archivo de derechos una descripción de la pieza de contenido, una descripción de los derechos de la pieza de contenido y una clave de encriptado de contenido usada para encriptar la pieza de contenido; almacenar al menos uno de los al menos un archivo de derechos sin encriptar en una base de datos de derechos; y ejecutar un programa residente en el dispositivo que encripte al menos un archivo de derechos con una clave de encriptado asimétrica específica del dispositivo.

En una realización de la invención, al menos un elemento de contenido se almacena en una memoria del dispositivo.

En una realización de la invención, al menos un elemento de contenido se almacena en una memoria extraíble que puede conectarse al dispositivo, por ejemplo en una tarjeta de memoria extraíble.

En una realización de la invención, al menos uno del al menos un objeto de derechos se almacena en una base de datos de derechos.

En una realización de la invención, el al menos un objeto de derechos se almacena en al menos un archivo.

En una realización de la invención, un elemento de contenido es una aplicación, una imagen, un archivo de audio, un documento o un archivo de vídeo.

En una realización de la invención, el dispositivo comprende un terminal móvil.

De acuerdo con un aspecto adicional de la invención, la invención es un dispositivo para activar el derecho de uso de al menos una pieza protegida de contenido en el dispositivo cuando el dispositivo se enciende por primera vez. El dispositivo se caracteriza por que los dispositivos comprenden: al menos un archivo de derechos para permitir el uso de la al menos una pieza protegida de contenido, cada uno del al menos un archivo de derechos que incorpora los derechos a una pieza de contenido, cada uno del al menos un archivo de derechos que comprende una descripción de la pieza de contenido, la descripción de los derechos de la pieza de contenido y una clave de encriptado de contenido usada para encriptar la pieza de contenido; un módulo de almacenamiento para almacenar un programa de activación; una unidad de procesamiento configurada para ejecutar el programa de activación cuando el dispositivo se arranca por primera vez, en el que la ejecución del programa de activación comprende: encriptar al menos un archivo de derechos con una clave de encriptado asimétrica específica del dispositivo.

En una realización de la invención, al menos un elemento de contenido se almacena en una memoria del dispositivo.

En una realización de la invención, al menos un elemento de contenido se almacena en una memoria extraíble que puede conectarse al dispositivo, por ejemplo, en una tarjeta de memoria extraíble.

En una realización de la invención, el dispositivo comprende además una base de datos de derechos configurada para almacenar al menos un objeto de derechos.

En una realización de la invención, el dispositivo comprende además al menos un archivo configurado para almacenar el al menos un objeto de derechos.

En una realización de la invención, un elemento de contenido es una aplicación, una imagen, un archivo de audio, un documento o un archivo de vídeo.

En una realización de la invención, el dispositivo comprende un terminal móvil.

De acuerdo con un aspecto adicional de la invención, la invención es un producto de programa informático para activar el derecho de uso de al menos una pieza protegida de contenido en un dispositivo, que comprende un código almacenado en al menos un medio legible del dispositivo de procesamiento de datos, estando el código configurado para realizar la siguiente etapa cuando se ejecuta en un dispositivo de procesamiento de datos: activar el derecho de uso de al menos una pieza protegida de contenido en un dispositivo cuando el dispositivo se enciende por primera vez, estando el producto de programa informático caracterizado por que el producto de programa está configurado para realizar las siguientes etapas cuando se ejecuta en un dispositivo de procesamiento de datos: proporcionar un dispositivo con al menos un archivo de derechos sin encriptar, en el que al menos un archivo de derechos asigna el derecho de uso de la al menos una pieza de contenido, incorporando cada uno del al menos un archivo de derechos los derechos a una pieza de contenido, comprendiendo el al menos un archivo de derechos una descripción de la pieza de contenido, una descripción de los derechos de la pieza de contenido y una clave de encriptado de contenido usada para encriptar la pieza de contenido; almacenar al menos uno del al menos un archivo de derechos sin encriptar en una base de datos de derechos; y ejecutar un programa residente en el

dispositivo (202) que encripta al menos un archivo de derechos con una clave de encriptado asimétrica específica del dispositivo.

- 5 La invención desvela una solución donde puede activarse el contenido protegido DRM cuando se compra, por ejemplo, un terminal móvil en lugar de hacerlo posteriormente sobre el aire. Además, usando la solución desvelada en la invención, un fabricante de terminales móviles o un operador es capaz de diferenciar los productos.

Breve descripción de los dibujos:

- 10 Los dibujos adjuntos, que se incluyen para proporcionar una comprensión adicional de la invención y que constituyen una parte de esta memoria descriptiva, ilustran las realizaciones de la invención y junto con la descripción ayudan a explicar los principios de la invención. En los dibujos:

- 15 la **figura 1** es un diagrama de flujo que ilustra una realización de un método de acuerdo con la invención, las **figuras 2a - 2c** son diagramas de bloques que ilustran las realizaciones de un dispositivo de acuerdo con la invención, y la **figura 3** es un diagrama de bloques que ilustra una realización de un archivo de derechos que puede usarse en la invención.

20 Descripción detallada de las realizaciones preferidas

A continuación se hará referencia en detalle a las realizaciones de la presente invención, cuyos ejemplos se ilustran en los dibujos adjuntos.

- 25 La figura 1 desvela un diagrama de flujo que ilustra una realización de un método de acuerdo con la invención. Un dispositivo, por ejemplo, un terminal móvil, está provisto de al menos un objeto de derechos sin encriptar antes de que el terminal móvil se arranque por primera vez, etapa 10. El al menos un objeto de derechos incluye uno o más archivos de derechos que proporcionan el derecho de uso o de muestra de uno o más contenidos de datos, por ejemplo, aplicaciones, archivos de audio, archivos de vídeo, documentos, etc. con el terminal móvil. En la figura 3 se desvela una estructura a modo de ejemplo de un archivo de derechos.

- 30 En la etapa 12, el terminal móvil se arranca (se conecta) por primera vez. El terminal móvil está configurado para ejecutar un programa residente en el terminal móvil, que encripte al menos un objeto de derechos con una clave de encriptado específica del terminal móvil en respuesta al arranque del terminal móvil por primera vez, etapa 14. Al hacer esto, los elementos de contenido, por ejemplo, las aplicaciones en cuestión, solo puede usarse en este terminal móvil. La clave específica del terminal móvil puede ser una clave de encriptado simétrica o asimétrica.

- 35 La figura 2a desvela un diagrama de bloques que ilustra una realización de un dispositivo de acuerdo con la invención. Un terminal móvil 200 se divide aproximadamente en dos partes, un sistema de funcionamiento del fabricante y una parte abierta, por ejemplo un sistema operativo Symbian. El sistema de funcionamiento del fabricante incluye un almacenamiento de clave protegida 28, que comprende una clave de encriptado específica del terminal. Además, en esta realización el sistema de funcionamiento del fabricante incluye también un software de activación 202. La parte del sistema operativo Symbian incluye un sistema de archivos 26 que comprende una base de datos de derechos 20. La base de datos de derechos 20 comprende uno o más archivos de derechos que se desvelan con más detalle en la figura 3. En definitiva, cada archivo de derechos incorpora los derechos para una pieza de contenido, así como proporciona el medio para acceder al contenido de la manera definida por los derechos. Un motor DRM 22 puede acceder a la base de datos de derechos 20 (RDB) en el sistema de archivos 26. El terminal móvil 200 comprende además una unidad de procesamiento 212, por ejemplo, un procesador, configurado para ejecutar el programa de activación, cuando el dispositivo se arranca por primera vez.

- 40 A veces los proveedores/operadores desean ofrecer varias aplicaciones "extra" (por ejemplo, en una tarjeta multimedia (MMC)) a un cliente que compra un nuevo terminal móvil, por ejemplo un teléfono móvil. Por ejemplo, un operador puede querer dar un período de prueba gratuito para algunas aplicaciones. Después del período de prueba, el usuario puede decidir si quiere usar las aplicaciones también en el futuro. También el operador podría vender dos versiones diferentes del mismo teléfono: un teléfono barato y un teléfono más caro que tenga algunas aplicaciones adicionales listas para usar. Debería haber algún mecanismo para controlar los derechos de uso de tales aplicaciones.

- 45 En esta realización, el contenido valioso se protege con el fin de preservar el negocio generador de ingresos para los productores de contenidos (por ejemplo, artistas, músicos, autores, etc.), así como para los minoristas de contenido (por ejemplo, operadores de redes, mISP, etc.). De acuerdo con la invención, el operador, el proveedor de servicios de Internet móvil (mISP) u otra entidad puede proporcionar un paquete de ventas que incluya las memorias extraíbles apropiadas, tal como una tarjeta multimedia (MMC) 24.

- 50 Cada tarjeta de memoria puede tener una identificación de tarjeta de memoria (ID) que sea única para cada tarjeta de memoria. Las tarjetas de memoria están precargadas con contenido, tales como, por ejemplo, tonos de llamada,

logos, protectores de pantalla, Java, música, juegos, etc. De acuerdo con la invención, el contenido se proporciona en la tarjeta de memoria 24 en un formato protegido. Por ejemplo, en la realización ilustrada, el contenido está en un formato protegido creado por Nokia Corporation denominado en el presente documento como contenedor de contenido protegido (SCC). El SCC como se usa en el presente documento se refiere, en general, a un formato de contenedor que encapsula el contenido digital encriptado y opcionalmente unos metadatos asociados relacionados con el contenido. Por ejemplo, el contenido puede estar encriptado con una clave simétrica, aunque en algunos casos el contenido digital puede no estar encriptado. El SCC está asociado lógicamente con uno o más archivos de derechos, de tal manera que los archivos SCC pueden abrirse con el archivo de derechos correcto. Un archivo de derechos tal como se usa en el presente documento se refiere, en general, a un objeto que define los derechos que rigen el uso de una pieza específica de contenido digital.

Cuando el terminal móvil 200 se arranca por primera vez, el software de activación 202 activa la encriptación de la base de datos de derechos 20 con una clave de encriptado específica del terminal móvil, que se almacena en el almacenamiento de clave protegida 28. La clave específica del terminal móvil puede ser una clave de encriptado simétrica o asimétrica.

Aunque la invención se describe en general en relación con las tarjetas de memoria extraíbles, tales como la tarjeta de memoria 24 y una interfaz de memoria 204 a través de la cual la tarjeta de memoria 24 puede estar conectada al terminal móvil 200, la invención puede aplicarse igualmente cuando la tarjeta de memoria se fabrica integralmente en el terminal móvil 200. También es posible que el contenido pueda incluirse tanto en memorias extraíbles como no extraíbles asociadas con un terminal móvil. La invención también puede aplicarse igualmente a las realizaciones en las que la tarjeta de memoria 24 es o una memoria de lectura/escritura o una memoria de solo lectura (ROM).

Es obvio que el terminal móvil 200 puede incluir también otras aplicaciones o componentes de software que no se describen con más detalle y que no se desvelan en la figura 2a.

Aunque se desvela en las figuras 1 y 2 que el dispositivo es un terminal móvil, es obvio que el dispositivo puede ser cualquier otro dispositivo apropiado, por ejemplo, un ordenador o un asistente digital personal (PDA), etc.

La figura 2a desvela que todos los objetos de derechos están dispuestos en la base de datos de derechos 20. En otra realización, los objetos de derechos son archivos separados fuera de la base de datos de objetos de derechos (véanse las figuras 2b, 206, 208 y 210). Todos los objetos de derechos se encriptan por separado con una clave de encriptado específica del dispositivo cuando se arranca el dispositivo por primera vez. En otra realización, los objetos de derechos pueden almacenarse en la base de datos de derechos 20 pero solo se encripta una parte de la base de datos 20, por ejemplo, los objetos de derechos, cuando se arranca el dispositivo por primera vez. Por lo tanto, por ejemplo, los encabezados de bases de datos de derechos pueden permanecer sin encriptar. Sin embargo, en otra realización también otras partes de la base de datos de derechos 20 (además de los objetos de derechos) pueden encriptarse cuando se arranca el dispositivo por primera vez.

Las figuras 2a y 2b desvelan que el sistema de funcionamiento del fabricante comprende un software de activación 202. En otra realización de la invención, el sistema de funcionamiento Symbian u otra parte apropiada del sistema de funcionamiento puede comprender como alternativa un software de activación 202 (véase la figura 2c). En este caso, debe garantizarse que el software de activación 202 no pueda eliminarse o de otro modo desactivarse antes de que el dispositivo se haya arrancado por primera vez. De manera similar, si el software de activación 202 no está en la parte del sistema de funcionamiento del fabricante, debe garantizarse que el software de activación 202 no pueda eliminarse o de otro modo desactivarse antes de que haya concluido el procedimiento de encriptado. Si el software de activación 202 se almacena, por ejemplo, en una memoria de solo lectura (ROM), entonces el software no tiene que residir en la parte del sistema de funcionamiento del fabricante.

Debería observarse que aunque la base de datos de derechos está en texto plano (y por lo tanto puede considerarse vulnerable al uso indebido) durante la fase de fabricación, las instalaciones de fabricación pueden considerarse un lugar protegido y, por lo tanto, la posibilidad de que la base de datos de derechos se filtre en la forma de texto plano es casi inexistente.

La figura 3 ilustra una realización de un posible archivo de derechos en una base de datos de derechos que puede usarse en la invención. Es evidente que el formato o contenido específico de un archivo de derechos puede variar. Por lo tanto, puede usarse cualquier número de formatos de archivo de derechos en los que un usuario accede al contenido.

El fin primordial de un archivo de derechos es que incorpora los derechos a una pieza de contenido, así como que proporciona los medios para acceder al contenido de la manera definida por los derechos. Haciendo referencia al archivo de derechos a modo de ejemplo 30, puede proporcionarse una descripción 32 del contenido con el archivo de derechos, tal como el tipo de contenido (por ejemplo, audio, vídeo, texto, multimedia, etc.). Cada pieza de contenido, o partes seleccionadas de contenido, tendrá un archivo de derechos correspondiente 30, y la descripción 32 proporciona una descripción de su contenido respectivo.

- Para una pieza específica de contenido, existe una descripción 34 de los derechos para ese contenido. Estos derechos pueden incluir derechos tales como los derechos de transferencia y los derechos de uso. Por ejemplo, los derechos de transferencia pueden incluir el derecho (o no) a dar o vender el contenido a otro usuario, o a dar o vender una vista previa u otro uso limitado del contenido a otro usuario. Los derechos de transferencia también
- 5 pueden incluir reglas sobre si el contenido puede copiarse a otro dispositivo propiedad del usuario. Cualquier número de derechos de transferencia puede incluirse. Los derechos de uso son políticas que especifican cómo puede usarse esta copia del contenido. Por ejemplo, los derechos de uso pueden incluir derechos de acceso completo al contenido, derechos de no acceso al contenido, derechos de vista previa o algunos otros derechos de uso limitados. Por ejemplo, los derechos de uso de "vista previa" pueden proporcionarse a los usuarios para cierto
- 10 contenido tras recibir la tarjeta de memoria precargada, para permitir al usuario tener acceso al contenido durante un tiempo limitado (por ejemplo, una semana), una cantidad limitada de usos (por ejemplo, tres veces), una cantidad limitada del contenido (por ejemplo, treinta segundos de una canción MP3), etc.
- El archivo de derechos 30 también incluye el medio para acceder al contenido de acuerdo con lo dictado por las reglas de uso. En una realización, esto se proporciona mediante una clave de encriptado de contenido 36 que se ha
- 15 usado para encriptar el contenido. El archivo de derechos también puede contener otra información, tal como números de secuencia 38 para garantizar frescura, y un código de autenticación de mensajes (MAC) 310 en todos los otros campos, usando la clave de encriptado de contenido.
- 20 Es evidente para un experto en la materia que con el avance de la tecnología, la idea básica de la invención puede implementarse de diversas maneras. Por lo tanto, la invención y sus realizaciones no se limitan a los ejemplos descritos anteriormente, sino que pueden variar dentro del alcance de las reivindicaciones.

REIVINDICACIONES

1. Un método, que comprende:

proporcionar (10) un dispositivo con un archivo de datos de derechos sin encriptar (20), en donde el archivo de datos de derechos sin encriptar está configurado para asignar un derecho de uso de una pieza protegida de contenido de datos antes de arrancar el dispositivo por primera vez, en donde el archivo de datos de derechos está configurado para incorporar el derecho a la pieza protegida de contenido de datos y para proporcionar un medio para acceder a la pieza protegida de contenido de datos;

encender (12) el dispositivo;
determinar (12) si el dispositivo se arranca por primera vez;
arrancar (12) el dispositivo por primera vez; y en respuesta al arranque del dispositivo por primera vez
ejecutar (14) un programa residente en el dispositivo (202) que encripte el archivo de datos de derechos con una clave de encriptado específica del dispositivo.

2. El método de acuerdo con la reivindicación 1, que comprende además: almacenar la pieza protegida de contenido de datos en una memoria (26) del dispositivo.

3. El método de acuerdo con la reivindicación 1, que comprende además: almacenar la pieza protegida de contenido de datos en una memoria extraíble (24) que puede conectarse al dispositivo.

4. El método de acuerdo con la reivindicación 1, en el que la pieza protegida de contenido de datos comprende una aplicación, una imagen, un archivo de audio, un documento o un archivo de vídeo.

5. El método de acuerdo con la reivindicación 1, en el que el dispositivo comprende un terminal móvil.

6. El método de acuerdo con la reivindicación 1, que comprende además: almacenar el archivo de datos de derechos sin encriptar en una base de datos de derechos.

7. El método de la reivindicación 1, que comprende además: almacenar el archivo de datos de derechos sin encriptar en un archivo de datos.

8. Un dispositivo (200), que comprende:

medios para almacenar un archivo de datos de derechos sin encriptar (20) para permitir el uso de una pieza protegida de contenido de datos, en donde el archivo de datos de derechos sin encriptar está configurado para asignar un derecho de uso de una pieza protegida de contenido de datos antes de arrancar el dispositivo por primera vez, en donde el archivo de datos de derechos está configurado para incorporar el derecho a la pieza protegida de contenido de datos y proporcionar un medio para acceder a la pieza protegida de contenido de datos;
un módulo de almacenamiento para almacenar un programa de activación (202);
una unidad de procesamiento (212) configurada para ejecutar el programa de activación cuando el dispositivo se arranca por primera vez, configurándose la unidad de procesamiento para determinar si el dispositivo se arranca por primera vez cuando se enciende el dispositivo;

en donde la ejecución del programa de activación, en respuesta al arranque del dispositivo por primera vez, hace que el dispositivo: encripte el archivo de datos de derechos con una clave de encriptado específica del dispositivo.

9. El dispositivo de acuerdo con la reivindicación 8, que comprende además una memoria configurada para almacenar la pieza protegida de contenido de datos.

10. El dispositivo de acuerdo con la reivindicación 8, que comprende además una interfaz de memoria configurada para recibir una memoria extraíble en la que se almacena la pieza protegida de contenido de datos.

11. El dispositivo de acuerdo con la reivindicación 8, en el que la pieza protegida de contenido de datos comprende una aplicación, una imagen, un archivo de audio, un documento o un archivo de vídeo.

12. El dispositivo de acuerdo con la reivindicación 8, en donde el dispositivo comprende un terminal móvil.

13. Un producto de programa informático que comprende un código almacenado en al menos un medio legible por un dispositivo de procesamiento de datos, estando el código configurado para realizar las siguientes etapas cuando se ejecuta en un dispositivo de procesamiento de datos:

proporcionar (10) un dispositivo con un archivo de datos de derechos sin encriptar (20), en donde el archivo de datos de derechos sin encriptar está configurado para asignar un derecho de uso de una pieza protegida de

contenido de datos antes de que el dispositivo se arranque por primera vez, en donde el archivo de datos de derechos está configurado para incorporar el derecho a la pieza protegida de contenido de datos y para proporcionar un medio para acceder a la pieza protegida de contenido de datos;

- 5 encender (12) el dispositivo;
 determinar (12) si el dispositivo se arranca por primera vez;
 arrancar (12) el dispositivo por primera vez; y en respuesta al arranque del dispositivo por primera vez
 ejecutar (14) un programa residente en el dispositivo (202) que encripte el archivo de datos de derechos con
10 una clave de encriptado específica del dispositivo.

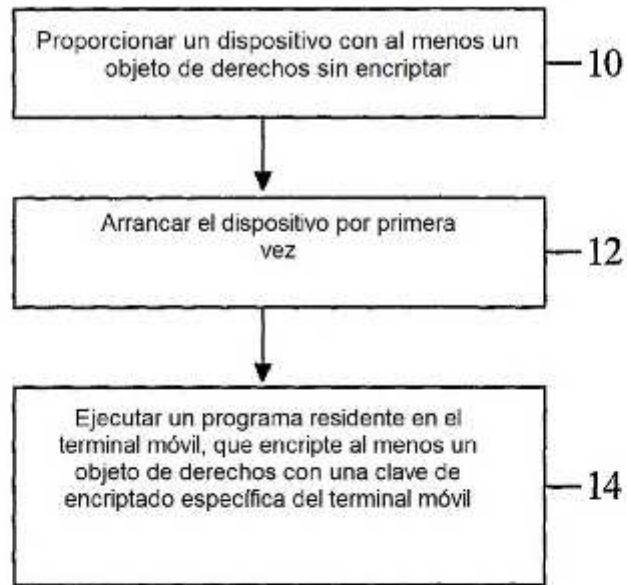


Fig. 1

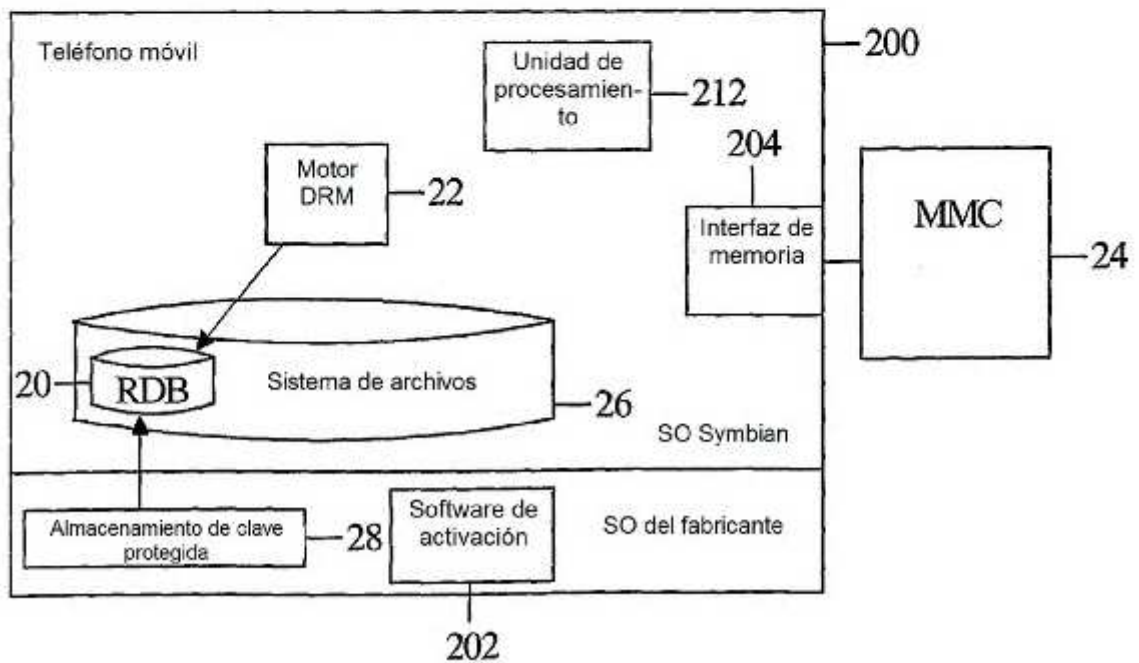


Fig. 2a

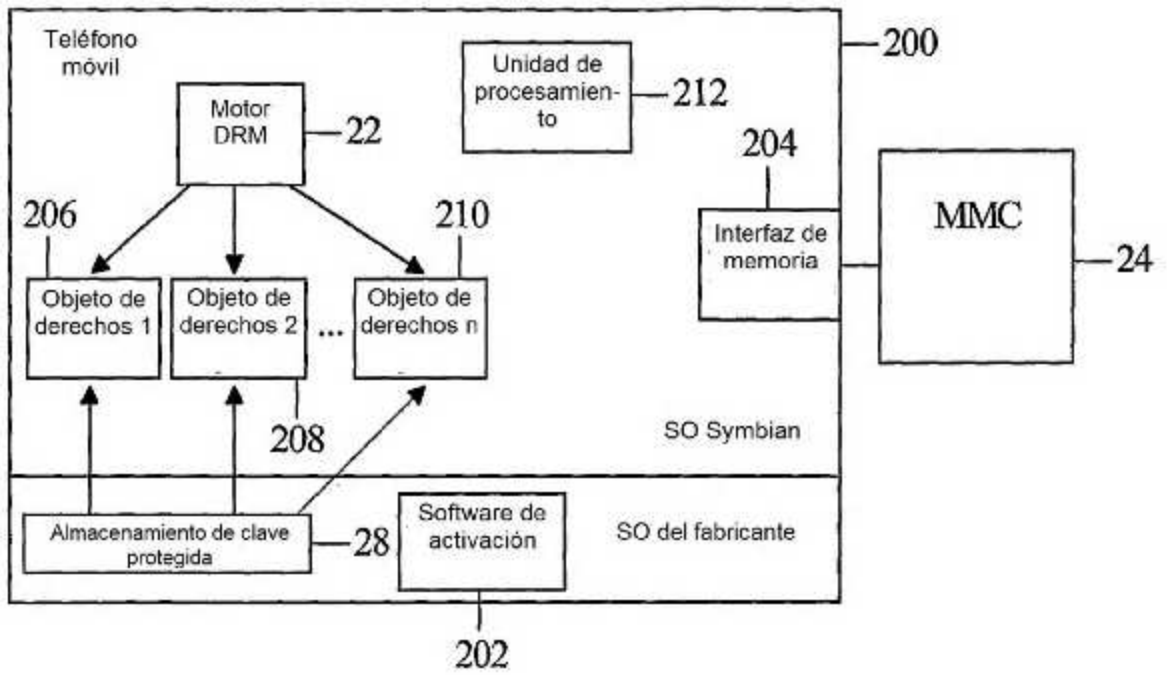


Fig. 2b

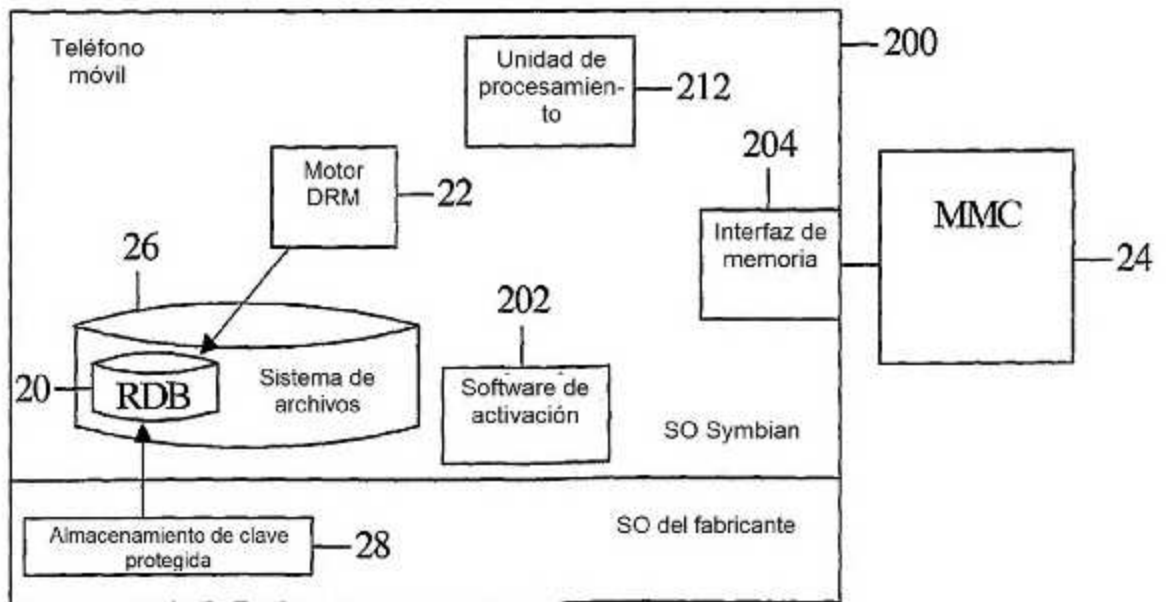


Fig. 2c

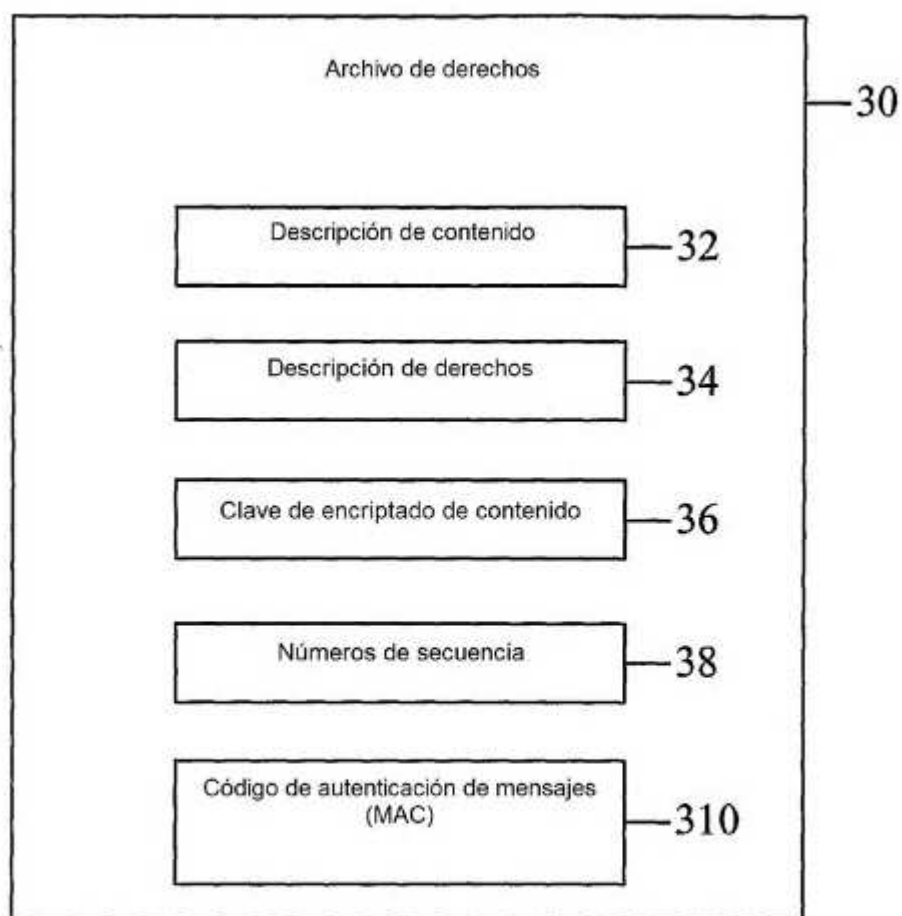


Fig. 3