(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 893 655**

(51) Int. CI.:

G06F 21/57 (2013.01)
H04W 12/043 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **27.05.2016 E 16171815 (0)**

(97) Fecha y número de publicación de la concesión europea: **21.07.2021 EP 3098745**

(54) Título: **Seguridad de clave de dispositivo**

(30) Prioridad:

28.05.2015 GB 201509181

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
09.02.2022

(73) Titular/es:

VODAFONE IP LICENSING LIMITED (100.0%)
Vodafone House The Connection
Newbury, Berkshire RG14 2FN, GB

(72) Inventor/es:

BOURNE, SOPHIE NICOLE y
SNAPE, TIM

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Seguridad de clave de dispositivo

Campo de la invención

La presente invención se refiere a un método y sistema para mejorar la seguridad de clave en un dispositivo y, en particular, en dispositivos de máquina a máquina y otro equipo de las instalaciones del cliente.

Antecedentes de la invención

Los dispositivos que generan, almacenan, usan, procesan o son sensibles a la comunicación o a los datos privados requieren medidas de seguridad particulares. Por ejemplo, la comunicación con el dispositivo puede necesitar encriptarse y/o autenticarse tanto en el dispositivo como en un servidor o estación remotos que interactúan con el dispositivo. Esto puede ser particularmente importante para dispositivos desatendidos o aquellos que típicamente no tienen interacción con los usuarios. Tales dispositivos pueden incluir dispositivos de Equipo de las Instalaciones del Cliente (CPE) y de máquina a máquina (M2M), por ejemplo.

Los datos manejados por tales dispositivos pueden incluir contraseñas, ID de usuario, claves de seguridad y datos privados o sensibles, tales como la ubicación, datos médicos, datos de conductor de vehículo (para casos de automóviles, usos de seguros, etc.) Adicionalmente, partes de una base de código que se ejecuta en el dispositivo pueden considerarse también muy sensibles y requerir protección. Este código puede incluir secretos industriales (tales como detalles acerca de lo que está haciendo el dispositivo y cómo funciona) y también información personal sensible (un dispositivo puede tener diferentes bibliotecas instaladas que cubren diversas clases de condiciones médicas, características de conductor para vehículos, edad, género, estado de conductor aprendiz y otra información).

Cualquiera o todas las partes de estos datos sensibles pueden necesitar usarse localmente en el dispositivo y/o comunicarse de manera segura con partes externas (tal como un servidor de gestión). En particular, el código sensible necesita protegerse cuando se está ejecutando localmente y también se comunica a través del aire durante actualizaciones de código o de firmware. En otras palabras, necesitan protegerse los datos sensibles tanto en tránsito como en reposo.

La sensibilidad (para tanto datos como código) puede abarcar tanto la confidencialidad de la información, pero también (y en ocasiones de manera más importante) la integridad de la información. Es importante que los dispositivos ejecuten el código o las bibliotecas correctas y que haya confianza en que estos no hayan sido manipulados. La manipulación puede conducir a vulnerabilidades de seguridad y al secuestro del dispositivo para fines no intencionados o maliciosos.

Proteger datos en reposo (es decir, cuando no se están usando por el dispositivo o mientras que el dispositivo no se encuentra en operación) encriptándolos en el dispositivo es una técnica conocida. Sin embargo, esto viene con problemas de gestión de clave. Adicionalmente, puede ser difícil usar una única clave para proteger los datos o el código tanto en reposo como en tránsito (p. ej. en uso o con el dispositivo operacional), lo que puede requerir a su vez la encriptación de los mismos datos varias veces. Esto tiene unas sobrecargas de procesamiento, potencia y energía significativas. La integridad del código en los dispositivos a menudo se gestiona por procesos de arranque seguro. Sin embargo, esto también puede tener sus propias limitaciones.

La encriptación de datos y/o código puede llevarse a cabo en un dispositivo. Esto puede ser para frustrar la manipulación local o para proteger la privacidad de un usuario legítimo en el caso de que el dispositivo sea robado, por ejemplo.

Una dificultad con esto es que puede ser necesario que la clave para desencriptar los datos (y/o el código) se almacene en el dispositivo. Como alternativa, un usuario humano puede introducir la clave, o alguna información a partir de la que se derive la clave (PIN, contraseña o huella dactilar, por ejemplo). La clave puede almacenarse también en el dispositivo, pero de una manera "ofuscada" (p. ej., dividida en varias porciones o mantenida en ubicaciones no esperadas). La clave puede almacenarse en el dispositivo en hardware seguro (p. ej., un Entorno de Ejecución Confiable, un Elemento Seguro, Tarjeta Inteligente, una UICC con SIM/USIM/ISIM, etc.)

De manera similar, estas técnicas pueden usarse para almacenar una clave secreta usada para verificar la integridad de los datos o código en el dispositivo.

La integridad del código puede conseguirse de manera alternativa por métodos asimétricos. La imagen de código legítimo puede firmarse con una clave privada (una clave privada de raíz, o una clave privada de entidad final, que tiene un certificado firmado bajo una clave privada de raíz) y verificarse en el dispositivo usando una clave pública (clave pública de raíz o clave pública de entidad final). Esto tiene un uso restringido sobre dispositivos de gama baja (requiere soporte de operaciones de clave pública), problemas de rendimiento (el arranque puede ser lento) y un número de limitaciones significativas en la seguridad conseguible.

Las soluciones existentes para el almacenamiento de clave segura son particularmente inadecuadas para el uso de M2M. Muchos dispositivos de M2M no tienen interfaz de usuario y ni capacidad de introducir los PIN o contraseñas.

Incluso, si esto fuera posible, entonces la seguridad que puede obtenerse de un PIN o contraseña memorizable por los humanos está limitada y es vulnerable a fuerza bruta y al reseteo de cualquier contador de reintentos. Las técnicas de ofuscación no son adecuadas para piratas informáticos determinados que pueden des-ofuscar las claves.

El hardware seguro es aplicable en algunos casos específicamente cuando el dispositivo tiene una tarjeta de SIM/UICC, pero para usarlo de manera eficaz requiere imponer lógica y aplicaciones específicas en la tarjeta SIM/UICC (tales como, un almacén de claves de Javacard y otra lógica de manejo de claves). Tal lógica típicamente no se despliega en tarjetas SIM producidas en masa. Por lo tanto, una solución de este tipo añade una gran cantidad al coste y complejidad a los dispositivos que están fabricados con funcionalidad y rendimiento limitados. El hardware seguro también puede ser vulnerable al robo y cualquier instrucción de limpieza (por ejemplo) puede nunca alcanzar el dispositivo o puede bloquearse para que tenga su efecto pretendido en el dispositivo.

La situación para la integridad del código y los datos es incluso más difícil. Las operaciones de clave pública pueden no estar disponibles o pueden no ser lo suficientemente rápidas en hardware limitado. La clave pública de raíz puede ser vulnerable a la manipulación. Si la clave pública de raíz se almacena en memoria, entonces la memoria puede reprogramarse. Si se almacena en fusibles, entonces estos fusibles pueden reconectarse. Si se usa almacenamiento de ROM, entonces el chip de ROM puede desoldarse y remplazarse por una alternativa. Si la clave se almacena en una tarjeta inteligente, entonces la tarjeta inteligente puede retirarse y remplazarse, por ejemplo. Los métodos de clave pública también son inadecuados para proteger imágenes de arranque específicas de dispositivo, bibliotecas específicas de dispositivo o datos específicos de dispositivo ya que permiten que se muevan los datos entre diferentes dispositivos con la misma clave pública de raíz.

Puede también haber riesgos relacionados con la reversión de la versión (donde se instala una imagen de código firmada antigua, con vulnerabilidades, en lugar de la última imagen de código). La protección contra esta vulnerabilidad puede requerir almacenamiento seguro adicional (y parcialmente reprogramable) para registrar la última versión (tal como fusibles adicionales). El arranque seguro puede no ayudar si el dispositivo se enciende durante mucho tiempo después del arranque ya que esto puede proporcionar muchas oportunidades para la manipulación durante ese tiempo.

Adicionalmente, estas soluciones pueden tener dificultad cuando usan la misma clave (o conjunto de claves) para proteger datos y código en tránsito (para entrega al dispositivo) como el usado para los datos en reposo. Esto puede requerir desencriptación y re-encriptación compleja. Un problema adicional es que puede ser difícil hacer disponible la clave almacenada localmente en el dispositivo (para propósitos de datos en reposo) a partes autorizadas fuera del dispositivo.

GEMPLUS ET AL: "Deletion of GBA keys when UICC is not inserted in the ME", 3GPP DRAFT; C6-060324, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE; 650, ROUTE DES LUCIOLES; F-06921 SOPHIA-ANTIPOLIS CEDEX; FRANCIA, vol. CT WG6, n.° Lisboa, Portugal; 20060511, 11 de mayo de 2006 describe el borrado de claves de GBA establecidas si una aplicación intenta usarlas y la UICC no está insertada en el ME.

ERICSSON: "Deletion of Ks in ME in GBA_ME", 3GPP DRAFT; S3-131064, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE; 650, ROUTE DES LUCIOLES; F-06921 SOPHIA-ANTIPOLIS CEDEX; FRANCIA, vol. SA WG3, n.° San Francisco, US; 20131111 - 20131115 4 de noviembre de 2013 (04-11-2013), XP050765958, recuperado de Internet: URL:http://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_73_SanFrancisco/Docs / describe el borrado de unas K de un ME cuando se privan las K de un GPI tan pronto como tiene K NAF derivadas y entregadas a una aplicación en el ME.

Ghader Ebrahimpour ET AL: "Introducing the GBA Covert Channel in IP Multimedia Subsystem (IMS)" In "Communications in computer and information science", 1 de enero de 2014 (01-01-2014), Springer, DE, XP055305131, ISSN: 1865-0929 vol. 428, páginas 13-22, DOI: 10.1007/978-3-319-10903-9_2 describe la introducción de un canal encubierto de GBA en subsistemas de medios de IP.

El documento GB 2518254 describe la distribución de clave de sesión de GBA a un UE.

El documento US 2009/0110195 describe proporcionar un sello lógico que monitoriza el acceso a una máquina.

El documento US 2007/0240205 describe el borrado de una credencial de una entidad de aplicación tras la recepción de un comando de borrado de credencial.

El documento US 2011/0185186 describe una clave secreta usada para encriptar datos en un dispositivo, que, a continuación, se borra.

Por lo tanto, se requiere un sistema y método que superen estos problemas.

Compendio de la invención

Un dispositivo, tal como un dispositivo de máquina a máquina (M2M), puede requerir una o más claves para que alguna o todas sus funciones operen. El dispositivo puede tener dos estados. En un primer estado, la una o más claves de dispositivo está o están disponibles y/o pueden accederse de modo que la función o funciones pueden operar. En otro estado, la una o más claves de dispositivo está o están no disponibles o no presentes en el dispositivo. Pueden implementarse diferentes mecanismos para evitar o posibilitar el acceso a la clave o claves de dispositivo. Por ejemplo, la clave puede borrarse del dispositivo para hacerla no disponible. La clave puede enviarse al dispositivo para hacerla disponible. En un ejemplo, la clave de dispositivo puede encriptarse por otra clave (p. ej. una clave simétrica) pero mantenerse en el dispositivo en forma encriptada. Para evitar la desencriptación de la clave de dispositivo, la otra clave puede borrarse del dispositivo (parcial o completamente). Proporcionar acceso al dispositivo puede implicar la recuperación de la otra clave para posibilitar la desencriptación de la clave de dispositivo. Por lo tanto, la clave de dispositivo puede almacenarse en una forma que no puede usarse hasta que se reciba la otra clave (es decir, material criptográfico) del servidor. Por lo tanto, aunque las funciones requieren que se ejecute la clave de dispositivo, esto se consigue indirectamente recibiendo material criptográfico, que "desbloquea" o hace disponible la clave de dispositivo. Las funciones pueden "conectarse" o "desconectarse" recibiendo y borrando el material criptográfico en este ejemplo, en lugar de recibiendo o borrando la clave de dispositivo real.

La clave de dispositivo o material criptográfico puede hacerse no disponible cuando el dispositivo se apaga, desconecta o pasa a modo de baja energía u otro cambio de modo, por ejemplo. Puede conseguirse seguridad adicional almacenando la clave de dispositivo (o material criptográfico requerido para acceder a la clave de dispositivo) en memoria activa que requiere potencia para almacenar datos. El apagado, por lo tanto, borra los contenidos de la memoria y cualquier clave o material criptográfico requerido. Cuando se enciende (o cambia de modo) entonces la clave de dispositivo puede hacerse disponible de nuevo. La clave de dispositivo puede enviarse al dispositivo usando un proceso o algoritmo de arranque, tal como GBA, por ejemplo. Adicionalmente, un fabricante de dispositivo no necesita aprovisionar a cada dispositivo con un dispositivo de clave con antelación. Sin embargo, el dispositivo puede estar asociado con un dispositivo de clave que puede almacenarse en una base de datos de claves de dispositivo e identificadores de dispositivo (p. ej. números de serie, IMSI, IMEA u otro identificador). Por lo tanto, esto simplifica el proceso de fabricación y distribución.

Según un primer aspecto, se proporciona un dispositivo como se describe en la reivindicación 1.

Por lo tanto, puede mejorarse la seguridad del dispositivo. Borrar el material criptográfico y comunicarse con el servidor para recibir el material criptográfico puede llevarse a cabo automáticamente y/o sin intervención del usuario. Por ejemplo, el material criptográfico (p. ej. un dispositivo de clave) únicamente necesita estar disponible durante algún tiempo. Cuando se apaga el dispositivo (o cambia de modo, de desbloqueado a bloqueado, por ejemplo) el material criptográfico puede borrarse automáticamente. Ciertas funciones o datos pueden encriptarse con el material criptográfico (o con una parte de un par de claves) pero este material criptográfico (o la clave de desencriptación del par) puede no estar disponible o borrarse. Esto puede evitar la manipulación con la clave de dispositivo o el material criptográfico o evitar que se recupere sin permiso. El material criptográfico puede ser una clave simétrica, clave asimétrica (par de claves o una parte de un par de claves) u otra clave. Preferiblemente, el dispositivo puede ser un dispositivo que puede comunicarse con una red celular, pero puede usar también DSL, cable, fibra, Wi-Fi u otra red. El borrado del material criptográfico puede conseguirse de un número de maneras. Por ejemplo, el material criptográfico puede borrarse del dispositivo completamente y almacenarse únicamente fuera del dispositivo. El material criptográfico puede suprimirse de una ubicación en el dispositivo y almacenarse en otra ubicación que no es accesible para funciones particulares del dispositivo. El material criptográfico puede ofuscarse (borrarse de una ubicación y almacenarse en otra en su totalidad o en parte) o borrarse y almacenarse de una manera modificada para evitar su acceso. El material criptográfico y una o más funciones de dispositivo pueden almacenarse juntos en una porción de memoria o almacenarse en chips o áreas de memoria separadas (o en más de una ubicación de memoria).

Opcionalmente, el material criptográfico es un dispositivo de clave. En otras palabras, el material criptográfico se usa directamente por las funciones de dispositivo para ejecutarse, sin etapas criptográficas adicionales (p. ej., desencriptación de una clave con otra). Por lo tanto, es una clave de dispositivo de este tipo la que recibe el servidor, en lugar del material criptográfico para desencriptar o acceder a un dispositivo de clave que está encriptado en el dispositivo (de manera que las funciones de dispositivo requieren indirectamente el material criptográfico).

Ventajosamente, la lógica puede configurarse para evitar el acceso al dispositivo borrando la clave de dispositivo (o parte de un dispositivo de clave o par de claves) de la memoria. Esto puede tomar varias formas. Esto puede mejorar adicionalmente la seguridad ya que la clave de dispositivo puede estar ausente durante cualquier intento no autorizado para recuperarla. La clave de dispositivo o material criptográfico puede borrarse de tal manera para hacer difícil o imposible recuperarlos (p. ej. la ubicación de almacenamiento puede sobrescribirse una o más veces).

Preferiblemente, la lógica configurada para recibir desde el servidor a través de la interfaz de comunicaciones el material criptográfico requerido para ejecutar la una o más funciones de dispositivo puede estar protegida, encriptada, autenticada o asegurada de otra manera.

Opcionalmente, la lógica puede estar configurada adicionalmente para ejecutar un protocolo de Arquitectura de Arranque Genérico, GBA, y, adicionalmente, en donde el material criptográfico se recibe desde el servidor protegido usando el protocolo GBA. Pueden usarse otros protocolos, pero GBA tiene ventajas particulares cuando se usa con dispositivos M2M. Pueden hallarse detalles adicionales del protocolo GBA que se usa en http://www.3gpp.org/DynaReport/33220.htm (3GPP TS 33.220 Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)). Variantes de GBA pueden incluir, pero sin limitación, GBA-push y 2G-GBA (con SIM en lugar de USIM), por ejemplo.

Opcionalmente, la lógica puede estar configurada adicionalmente para borrar el material criptográfico de la memoria. Esto puede ser una manera (activa) de que el dispositivo está configurado para borrar el material criptográfico. Pueden usarse también métodos pasivos.

Opcionalmente, el dispositivo puede estar configurado adicionalmente para borrar el material criptográfico activado por uno cualquiera o más de:

recibir un comando a través de la interfaz de comunicaciones; apagar el aparato;

una pérdida de potencia a una porción de la memoria que almacena el material criptográfico;

entrar en un modo de baja potencia del aparato;

después del agotamiento de un tiempo predeterminado;

detección de movimiento o cambio de ubicación; y/o

detección de un evento de manipulación. Por lo tanto, el dispositivo puede asegurarse automáticamente sin la intervención del usuario.

Pueden usarse otros activadores.

Opcionalmente, la una o más funciones pueden incluir uno o más de:

encriptación de contenido o comunicaciones, desencriptación de contenido o comunicaciones, validación, autenticación, validación de un nuevo módulo de identidad de abonado, SIM, y actualización de firmware. Pueden incluirse otras funciones.

Preferiblemente, la interfaz de comunicaciones puede ser una interfaz celular. Pueden usarse otros tipos de interfaz. Esta puede ser inalámbrica (p. ej. Wi-Fi) o alámbrica (p. ej. Ethernet).

Opcionalmente, la lógica puede estar configurada adicionalmente para recibir desde el servidor a través de la interfaz de comunicaciones el material criptográfico durante un proceso de arranque del dispositivo. Por lo tanto, cuando se arranca o inicia (o el estado cambia) el dispositivo, a continuación, el servidor puede proporcionar acceso al dispositivo. Por ejemplo, el servidor puede enviar la clave de dispositivo al dispositivo. Preferiblemente, esta puede estar en una forma encriptada y/o se envía de una manera que permite que se autentique o valide la clave de dispositivo. El servidor puede enviar otro material al dispositivo, lo que posibilita el acceso a la clave de dispositivo. Por ejemplo, esta puede ser una clave de desencriptación que permite que se desencripte una clave de dispositivo encriptada almacenada el dispositivo.

Opcionalmente, el dispositivo puede comprender adicionalmente memoria que almacena una o más funciones de dispositivo que no requieren que se ejecute el material criptográfico. En otras palabras, el dispositivo puede contener algunas funciones que pueden operar sin la clave de dispositivo (p. ej. arranque, conexión de la interfaz a una red, protocolo GBA para obtener la clave de dispositivo, etc.) y otras funciones pueden requerir acceso a la clave de dispositivo (p. ej. desencriptar o encriptar datos específicos de usuario, enviar una lectura de contador a un servidor externo, recibir y ejecutar comandos de operación, etc.)

Opcionalmente, la una o más funciones de dispositivo que no requieren que se ejecute el material criptográfico pueden incluir uno cualquiera o más de:

un cargador de arranque, comunicación a través de la interfaz de comunicaciones, y establecimiento de una comunicación segura a través de la interfaz de comunicaciones.

Según una implementación de ejemplo, se proporciona un servidor que comprende:

una interfaz de comunicaciones para comunicarse con uno o más dispositivos a través de una red;

un almacén de datos configurado para almacenar material criptográfico requerido por los dispositivos para ejecutar una o más funciones en los dispositivos; y

lógica configurada para:

proporcionar el material criptográfico a los dispositivos a través de la interfaz de comunicaciones. El material criptográfico puede ser las mismas claves de desencriptación u otras claves que posibilitan el acceso (en los dispositivos) a las claves de desencriptación. El servidor puede usarse para proporcionar acceso a la clave de dispositivo de un dispositivo anteriormente mencionado proporcionado el material criptográfico. El almacén de datos o base de datos puede ser un almacén de datos asegurado. El almacén de datos puede contener claves de dispositivo (o material criptográfico que posibilita el acceso a las claves de dispositivo) asociadas con identificadores para cada dispositivo (p. ej. un número de serie, IMSI, IMEA, etc.) o con un módulo de identificación de abonado en cada dispositivo o suministrado de manera separada a usuarios finales para adaptarse en sus dispositivos, por ejemplo.

Opcionalmente, el almacén de datos puede estar configurado para almacenar uno o más materiales criptográficos (p. ej. claves de dispositivo o claves de desencriptación para las claves de desencriptación) para cada dispositivo. El dispositivo puede tener más de una clave de dispositivo de modo que el acceso a las claves de dispositivo puede proporcionarse independientemente (p. ej. algunas funciones pueden estar permitidas y otras evitadas restringiendo o permitiendo el acceso a una o más claves de dispositivo). Un elemento de material criptográfico puede posibilitar el acceso (o ser) una clave de dispositivo (o un grupo de claves de dispositivo) en un dispositivo mientras que un segundo o tercer (o más) elementos de material criptográfico pueden posibilitar el acceso (o ser) una clave adicional de dispositivo (o grupo de claves de dispositivo adicional) en el dispositivo.

Preferiblemente, el almacén de datos puede contener material criptográfico (p. ej. claves de dispositivo o claves para desencriptar claves de dispositivo) previamente borradas de los dispositivos. En otras palabras, el material criptográfico (p. ej. la clave de dispositivo) puede ser el mismo pero borrado repetitivamente y a continuación proporcionado por el servidor bajo ciertas circunstancias (p. ej. a intervalos, después de activarse por un evento, encendido, etc.)

Según un aspecto adicional, se proporciona un método como se describe en la reivindicación 6.

Opcionalmente, el servidor puede proporcionar el material criptográfico a la clave de dispositivo recuperando el material criptográfico de un almacén de material criptográfico y enviando el material criptográfico al dispositivo a través de la red de comunicaciones.

Preferiblemente, el método puede comprender adicionalmente la etapa de usar el material criptográfico para ejecutar una de las funciones del dispositivo. Por ejemplo, la función ejecutada puede usar el material criptográfico para desencriptar datos en el dispositivo o la misma función ejecutada puede necesitar ser desencriptada por el material criptográfico antes de que se ejecute. La función ejecutada puede requerir que una clave de dispositivo se ejecute de estas maneras después de que se desencripte la misma clave de dispositivo por el material criptográfico, por ejemplo.

Ventajosamente, el material criptográfico puede borrarse de la memoria en el dispositivo después de un evento seleccionado del grupo de eventos que consiste en:

recibir un comando a través de la interfaz de comunicaciones desde el servidor;

apagar el dispositivo;

una pérdida de potencia a una porción de la memoria que almacena el material criptográfico (es decir, borrado pasivo);

entrar en un modo de baja potencia del dispositivo; después del agotamiento de un tiempo predeterminado;

detección de movimiento o cambio de ubicación del dispositivo; y/o la detección de un evento de manipulación en o dentro del dispositivo.

Opcionalmente, el método puede comprender adicionalmente las etapas de:

desencriptar un dispositivo de clave usando el material criptográfico; y

ejecutar una de las funciones del dispositivo usando la clave de dispositivo.

El dispositivo y el servidor (y cualquiera otra de sus variaciones descritas en la presente memoria) pueden formar un sistema. El sistema puede incluir también una pluralidad de dispositivos (uno o más) y/o servidores.

El dispositivo puede ser un dispositivo de M2M, equipo de las instalaciones del cliente (CPE), módem de DSL o de cable, encaminador de Wi-Fi, femtocélula, decodificador de salón (para TV, etc.) u otro equipo doméstico o comercial, por ejemplo.

Los métodos anteriormente descritos pueden implementarse como un programa informático que comprende instrucciones de programa para operar un ordenador. El programa informático puede almacenarse en un medio legible por ordenador.

El sistema informático puede incluir un procesador tal como una unidad de procesamiento central (CPU). El procesador puede ejecutar lógica en forma de un programa de software. El sistema informático puede incluir una memoria que

incluye un medio de almacenamiento volátil y no volátil. Un medio legible por ordenador puede incluirse para almacenar las instrucciones lógicas o de programa. Las diferentes partes del sistema pueden conectarse usando una red (p. ej. redes inalámbricas y redes alámbricas). El sistema informático puede incluir una o más interfaces. El sistema informático puede contener un sistema operativo adecuado, tal como UNIX, Windows (RTM) o Linux, por ejemplo.

Debería observarse que, cualquier característica anteriormente descrita puede usarse con cualquier aspecto o realización particular de la invención.

Breve descripción de las figuras

La presente invención puede ponerse en práctica en un número de maneras y se describirán ahora las realizaciones a modo de ejemplo únicamente y con referencia a los dibujos adjuntos, en los que:

La Figura 1 muestra un diagrama esquemático de un dispositivo que incluye un dispositivo de clave, dado a modo de ejemplo únicamente;

La Figura 2 muestra un diagrama esquemático de un servidor usado para proporcionar el dispositivo de la figura 1 con acceso a la clave de dispositivo;

La Figura 3 muestra un diagrama esquemático de un sistema que incluye el dispositivo de la figura 1 y el servidor de la figura 2;

La Figura 4 muestra un diagrama de flujo de un método para operar el sistema de la figura 3, dado a modo de ejemplo únicamente; y

La Figura 5 muestra un diagrama esquemático de un sistema de ejemplo adicional.

Debería observarse que las figuras se ilustran por simplicidad y no están dibujadas necesariamente a escala. Se proporcionan características similares con los mismos números de referencia.

Descripción detallada de las realizaciones preferidas

La Arquitectura de Arranque Genérico (GBA) del 3GPP permite que un dispositivo cliente y servidor acuerden un secreto compartido fuerte y único "arrancando" a partir de la clave compartida entre una tarjeta de SIM (UICC) y HLR/HSS. Ventajosamente, puede acordarse una nueva clave de este tipo de manera regular o cada vez que sea necesario (por ejemplo, en el cambio de propietario u operaciones de reseteo). Las transformaciones basadas en el secreto compartido permiten que se deriven o se vuelvan a derivar otras claves según se requiera.

La conectividad celular no se requiere necesariamente para este arranque ya que el protocolo funciona a través de otros tipos de conectividad (p. ej. DSL, cable, fibra y Wi-Fi). Por lo tanto, el método y sistema descritos pueden usarse para diferentes tipos de equipo de las instalaciones del cliente (CPE) y dispositivos de M2M.

La Figura 1 muestra un diagrama esquemático de un dispositivo 10 usado para almacenar y/o generar datos sensibles o confidenciales. El dispositivo 10 incluye uno o más almacenes 20 de memoria. El almacén 20 de memoria está configurado para almacenar un dispositivo 30 de clave y una o más funciones 40 que requieren el uso de la clave 30 de dispositivo para operar.

El dispositivo 10 también incluye una interfaz 50 de comunicaciones e instrucciones o lógica 60 de programa para operar el dispositivo 10. La lógica 60 también controla el acceso a la clave 30 de dispositivo almacenada en el almacén 20 de memoria. Esta lógica 60 puede evitar el acceso a la clave 30 de dispositivo en ciertas circunstancias. Por ejemplo, la lógica 60 puede borrar la clave de dispositivo del dispositivo 10 cuando tiene lugar cierto activador. Estos activadores pueden incluir desconectar o mover el dispositivo 10 en un nuevo estado de baja potencia (o de un estado a otro), manipular el dispositivo, mover físicamente el dispositivo o comunicaciones inusuales, por ejemplo.

La lógica 60 puede proporcionar o posibilitar el acceso también a la clave 30 de dispositivo. Esto puede conseguirse recibiendo una nueva o la misma clave 30 de dispositivo de una fuente externa tal como un servidor 100, por ejemplo.

La Figura 2 muestra un diagrama esquemático del servidor 100 usado para posibilitar el acceso a la clave 30 de dispositivo en el dispositivo 10. En una implementación de ejemplo, el servidor 100 proporciona al dispositivo 10 con una nueva o la misma clave de dispositivo que se borra por la lógica 60. El servidor 100 contiene una base de datos 110 de claves 30 de dispositivo específica a una pluralidad de dispositivos 10. El servidor 100 también incluye una interfaz 120 de comunicaciones para comunicarse con los dispositivos 10 (p. ej. a las interfaces 50 de comunicaciones de los dispositivos). El servidor 100 también incluye instrucciones de programa 130 usadas para proporcionar acceso a las claves 30 de desencriptación y/o envía la clave 30 de dispositivo a los correspondientes dispositivos 10.

La Figura 3 muestra un diagrama esquemático de un sistema 200 formado de una pluralidad de los dispositivos 10 descritos con referencia a la figura 1 y el servidor 100 descrito con referencia a la figura 2. El sistema 200 puede comprender muchos más dispositivos 10 del mismo o diferentes tipos y también múltiples servidores 100 que pueden incluirse para propósitos de equilibrado de carga, por ejemplo.

La Figura 3 muestra los dispositivos 10 y el servidor 100 que forman una red. En este ejemplo, el servidor envía el material criptográfico (u otro) de los dispositivos para posibilitar el acceso a la clave 30 de dispositivo en cada dispositivo 10 de modo que las funciones que requieren las claves 30 de desencriptación pueden realizarse en los dispositivos 10. El material criptográfico puede ser las mismas claves de desencriptación, claves o porciones de claves que posibilitan el acceso a las claves 30 de desencriptación (p. ej. desencriptándolas en el dispositivo) u otros datos que posibilitan el acceso. En el ejemplo mostrado en la figura 3, la red es una red celular y los dispositivos están en comunicación con una estación 210 base de la red celular y el servidor 100 también mantiene una conexión con la red celular (o puede ser parte de la red celular, por ejemplo). Pueden usarse otras redes, tanto inalámbricas como alámbricas.

La Figura 4 muestra un diagrama de flujo de un método 300 para operar el sistema 200 descrito con referencia a la figura 3. En particular, este método 300 describe los diversos estados de cada dispositivo 10 y las interacciones de cada dispositivo 10 con el servidor o el servidor 100 de gestión.

En la etapa 310 la clave 30 de dispositivo está disponible para el dispositivo 10 y así las funciones 40 son operables. En la etapa 320, el dispositivo se apaga (o tiene lugar otro activador o acción para hacer que la clave 30 de dispositivo se vuelva no disponible). En este método de ejemplo, la clave de dispositivo se borra en la etapa 330, pero esto podría ser un proceso de encriptación y otra manera para hacer a la clave 30 de dispositivo no disponible. En la etapa 340 se arranca el dispositivo 10. Pueden quedar disponibles ciertas funciones para permitir que el dispositivo arranque y se conecte a la red, así como funciones que no se basan en seguridad mejorada, mientras que otras funciones y datos pueden estar no disponibles (es decir, funciones para desencriptar datos almacenados en el dispositivo 10). Después o como parte del procedimiento de arranque del dispositivo, el dispositivo 10 se comunica a través de una red con un servidor 100. En este ejemplo, el servidor 100 envía al dispositivo 10 su clave 30 de dispositivo particular (etapa 350), aunque esta podría ser otro material criptográfico que posibilita el acceso a la clave de dispositivo y que permite por lo tanto que las funciones operen de nuevo (es decir, el método vuelve a la etapa 310).

La Figura 5 muestra un diagrama esquemático de una implementación 400 de ejemplo del método de la figura 4. En este ejemplo, el dispositivo 410, 410' pasa de un primer estado donde la clave 30 de dispositivo no está disponible (o no está presente) y los datos pueden ser ininteligibles (puesto que están encriptados y falta la clave de desencriptación o no está disponible de otra manera) a un segundo estado donde la clave 30 de dispositivo está disponible y los datos se vuelven inteligibles (es decir, pueden desencriptarse puesto que la clave de desencriptación está presente).

En este ejemplo, la clave 30 de dispositivo es una clave simétrica y puede usarse para propósitos de encriptación, desencriptación e integridad. Sin embargo, pueden usarse claves asimétricas y puede usarse una clave separada para integridad y autenticación.

En este ejemplo sencillo, la clave 30 de dispositivo puede ser una única "clave de encriptación específica de dispositivo" (DSEK). Sin embargo, en este ejemplo, la DSEK puede remplazarse por cualquier clave 30 de dispositivo.

Los números encerrados en círculo mostrados en la figura 5 corresponden con las siguientes etapas numeradas.

1. Mientras está apagado y en un estado de baja potencia o de inactividad (primer estado), el dispositivo 410 no tiene una copia local de su DSEK 30. Si es robado o se manipula el dispositivo en este estado, entonces será difícil o imposible para el atacante desencriptar cualquier cosa en el dispositivo. También puede evitarse la carga de código o datos falsos en el dispositivo en este estado. Los datos 420 en el dispositivo 410 están sombreados en esta figura para ilustrar que están encriptados y que la función de desencriptación no puede realizarse ya que falta la DSEK 30.

2. En el primer estado del dispositivo 410, pueden realizarse algunas funciones que no requieren acceso a la DSEK 30 que falta. Estas funciones principales pueden almacenarse (o grabarse en) una ROM 430 u otro almacenamiento permanente, por ejemplo. Las funciones principales del dispositivo 410 que no necesitan la DSEK 30 pueden incluir un cargador de arranque inicial y algún código de base para permitir la conectividad (p. ej. a una red celular u otra red), que puede ser código de función fija. En algunas implementaciones de ejemplo, la ROM puede fabricarse para que sea demasiado grande para retirarse sin dañar o destruir el dispositivo 10).

3. En este ejemplo, las funciones principales incluyen la capacidad (hacia el final del proceso de arranque) para ejecutar el protocolo Arquitectura de Arranque Genérico (GBA) y establecer una sesión segura (encriptada y protegida en integridad) con un servidor 100 de gestión. Obsérvese que una sesión de este tipo puede protegerse mediante claves de sesión recientes cada vez que se establezca. Puede usarse TLS o DTLS, por ejemplo.

4. El servidor 100 de gestión almacena una copia de la DSEK 30 del dispositivo en su propia base de datos 100 (preferiblemente un área de memoria protegida). El servidor 100 de gestión puede almacenar las DSEK 30 de una pluralidad de dispositivos 410. Después de que se ha completado el proceso de arranque y configuración de GBA, el servidor 100 de gestión entrega la DSEK 30 al dispositivo 410' a través de la sesión segura. El dispositivo 410' ahora está en su segundo estado.

5. El dispositivo 410' puede ejecutar ahora las funciones que requieren el acceso a la clave 30 de dispositivo. Por ejemplo, el dispositivo 410' puede llevar a cabo las funciones de desencriptación y/o verificación (para determinar la integridad de datos) en sus datos y código 420 específicos de dispositivo. Esto se ilustra en la figura 5 por los datos

no sombreados 420 en el dispositivo 410' (es decir ahora disponibles y accesibles). El dispositivo 410' puede crear datos o código adicionales (todos encriptados/protegidos en integridad usando la DSEK 30). Adicionalmente, el dispositivo 410' puede intercambiar fácilmente datos y código adicionales con el servidor 100 de gestión, que puede usar también la DSEK 30 para generar o verificar dicho código. No se requieren operaciones de desencriptación/re-encriptación para esto.

6. En el apagado o al retornar a un estado de inactividad (transición del segundo estado al primer estado del dispositivo 410, 410') el dispositivo borrará su DSEK 30 y volverá a la etapa 1. Este proceso de borrado (o, de otra manera, que haga a la DSEK 30 no disponible) puede activarse también por uno o más eventos adicionales tales como detectar diversas condiciones de manipulación mientras se enciende o recibe una instrucción del servidor 100 de gestión.

Las variaciones pueden incluir cambiar la DSEK 30 en diversos intervalos y después de diversos activadores. Esto puede requerir una reinstalación de correspondiente código y datos re-encriptados por el servidor 100 de gestión. Una actualización completa de firmware puede ser un momento adecuado para hacer esto. La migración entre las DSEK 30 p. ej., desencriptación y re-encriptación, puede llevarse a cabo en un bloque en un momento para suavizar el proceso.

Si el dispositivo 10, 410, 410' no puede conectarse al servidor 100 de gestión, entonces no puede recuperar su DSEK 30 (o hacerla de otra manera disponible al dispositivo). Esto puede mitigarse mediante una distribución cuidadosa de funciones entre el código principal (en la ROM 430) y otro código o funciones 40 que requieren el acceso a la DSEK 30. Sin embargo, ya que el dispositivo 10, 410, 410' se pretende normalmente que sea un dispositivo conectado entonces su funcionalidad puede ya estar limitada cuando está desconectado.

Este sistema 200 y método 300 mejoran la encriptación de datos en reposo y en movimiento y de la integridad de datos en reposo y en movimiento. La capacidad para cambiar una DSEK 30 protege adicionalmente contra la reversión de la versión.

Como se apreciará por el experto en la técnica, los detalles de la realización anterior pueden variarse sin alejarse del alcance de la presente invención, según se define por las reivindicaciones adjuntas.

Por ejemplo, aunque se ha descrito una única DSEK o clave 30 de dispositivo para cada dispositivo 10, 410, 410', puede haber diferentes (es decir, múltiples) DSEK o claves 30 de dispositivo para diferentes tipos de código y datos. Estas pueden gestionarse de manera central o por diferentes partes y servicios.

Una mejora adicional al sistema puede requerir que el servidor 100 de gestión incluya una copia de respaldo de las DSEK 30 (o usar un servidor de respaldo, servidor distribuido, agrupación, almacenamiento RAID u otro mecanismo) para evitar la pérdida de datos a través de múltiples dispositivos 10, 410, 410'.

Puede desarrollarse un número de contramedidas contra formas indirectas de ataque, tales como intentar comprometer el servidor 100 de gestión (o servidor de respaldo). Esto puede incluir proteger las DSEK 30 en el servidor de gestión usando un módulo de seguridad de hardware (HSM) o usando mecanismos de almacenamiento de "m de n" distribuido y recuperación de clave, por ejemplo.

Preferiblemente, la seguridad puede estar basada en una tarjeta/UICC de SIM del dispositivo. Si la UICC se mueve en un dispositivo 10, 410, 410' diferente entonces esto puede permitir también que se transfieran los datos específicos de dispositivo. Esto puede ser una ventaja en algunos casos, pero puede representar también una amenaza de seguridad, que puede mitigarse por una SIM soldada o embebida, o "bloqueando" criptográficamente la tarjeta SIM a un dispositivo específico.

Los dispositivos 10, 410, 410' que se sabe que han sido robados o están comprometidos pueden simplemente tener sus SIM prohibidas, por lo que ya no se puede ejecutar más el protocolo GBA. El servidor 10 de gestión puede marcar adicionalmente o como alternativa la DSEK 30 como que no está distribuida. Las formas temporales de prohibición o suspensión pueden usarse también donde hay una sospecha de robo o compromiso. La monitorización del entorno (por el dispositivo 10, 410, 410' o el servidor o una combinación de estos) puede proporcionar indicios para comportamiento sospechoso y puede activar una alerta a un usuario legítimo del dispositivo 10, 410, 410' (por ejemplo, en la siguiente solicitud de la DSEK 30). Un usuario puede a continuación aprobar o rechazar la liberación de la DSEK 30.

El dispositivo 10, 410, 410' puede protegerse de robo o compromiso cada vez que no tenga su DSEK (clave 30 de dispositivo). El flujo puede estar dispuesto de modo que la DSEK 30 esté disponible para el dispositivo únicamente cuando sea necesario, y en esa ventana el dispositivo puede tener también medidas activas (encendidas) para detectar la manipulación. Por ejemplo, el dispositivo 10, 410, 410' puede usar la detección de ubicación para comprobar si se ha movido sin advertencia. Pueden usarse otras formas de monitorización ambiental, como comprobar el estado de otro equipo en un entorno dentro del vehículo. Para implementaciones particularmente de alto riesgo o de alto valor (p. ej. seguridad de vehículo), puede haber dos dispositivos de rastreo de ubicación donde uno puede ser inamovible del vehículo. Si estos dispositivos de ubicación proporcionan lecturas inconsistentes, entonces puede indicarse la retirada del dispositivo 10, 410, 410' protegido por DSEK del vehículo.

Una clave para desbloquear la clave de dispositivo puede considerarse como otra clave de dispositivo (es decir, material criptográfico requerido para ejecutar una o más funciones de dispositivo) aunque no necesariamente una DSEK, puesto que no se usa directamente para encriptar o desencriptar cualquier cosa en el dispositivo. La clave de dispositivo puede describirse, por lo tanto, como una clave para encriptar o desencriptar datos o código en el dispositivo (p. ej., la DSEK). El material criptográfico puede ser la clave de dispositivo (p. ej., la DSEK), o cualquier clave que se use para proteger o desbloquear la clave de dispositivo o DSEK.

Serán fácilmente evidentes muchas combinaciones, modificaciones o alteraciones a las características de las realizaciones anteriores para el experto en la técnica y se pretende que formen parte de la invención. Cualquiera de las características descritas específicamente relacionadas con una realización o ejemplo puede usarse en cualquier otra realización haciendo los cambios apropiados. La invención se especifica en las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un dispositivo (10) que comprende:

memoria (20) activa que requiere potencia para almacenar datos configurados para almacenar material criptográfico requerido para ejecutar una o más funciones de dispositivo;

una interfaz (50) de comunicaciones para comunicarse a través de una red; y

lógica (60) configurada para:

cuando se enciende el dispositivo, recibir de un servidor (100) a través de la interfaz (50) de comunicaciones el material criptográfico requerido para ejecutar la una o más funciones de dispositivo; y

almacenar el material criptográfico en la memoria (20) activa,

en donde el dispositivo (10) está configurado para borrar el material criptográfico del dispositivo (10) cuando se apaga el dispositivo 10 retirando la potencia de la memoria (20) activa, y

en donde el dispositivo está configurado adicionalmente para acceder al material criptográfico almacenado en la memoria (20) activa desencriptando una clave (30) de dispositivo encriptada almacenada en el dispositivo usando el material criptográfico y ejecutar la una o más funciones de dispositivo usando la clave (30) de dispositivo desencriptada.

2. El dispositivo (10) de la reivindicación 1, en donde la lógica está configurada adicionalmente para ejecutar un protocolo de Arquitectura de Arranque Genérico, GBA, y adicionalmente en donde el material criptográfico se recibe desde el servidor (100) protegido usando dicho protocolo GBA.

3. El dispositivo (10) según cualquier reivindicación anterior, en donde la una o más funciones incluyen uno cualquiera o más de:

encriptación de contenido o comunicaciones, desencriptación de contenido o comunicaciones, validación, autenticación, validación de un nuevo módulo de identidad de abonado, SIM, y actualización de firmware.

4. El dispositivo (10) según cualquier reivindicación anterior, en donde la interfaz (50) de comunicaciones es una interfaz celular.

5. Un método realizado por un dispositivo, comprendiendo el método las etapas ordenadas de:

(i) borrar del dispositivo (10), material criptográfico requerido para ejecutar una o más funciones de dispositivo almacenadas en el dispositivo (10), apagando el dispositivo (10) para retirar potencia de memoria (20) activa en el dispositivo (10) que almacena el material criptográfico;

(ii) encender el dispositivo;

(iii) recibir de un servidor (100) a través de una red de comunicaciones el material criptográfico;

(iv) almacenar el material criptográfico en la memoria (20) activa;

(v) acceder al material criptográfico almacenado en la memoria (20) activa desencriptando una clave (30) de dispositivo encriptada almacenada en el dispositivo (10) usando el material criptográfico; y

(vi) ejecutar la una o más de las funciones del dispositivo usando la clave (30) de dispositivo desencriptada.

6. El método de la reivindicación 5, en donde el servidor (100) proporciona el material criptográfico al dispositivo (10) recuperando el material criptográfico de un almacén (110) de material criptográfico y enviando el material criptográfico al dispositivo (10) a través de la red de comunicaciones.

Figura 1

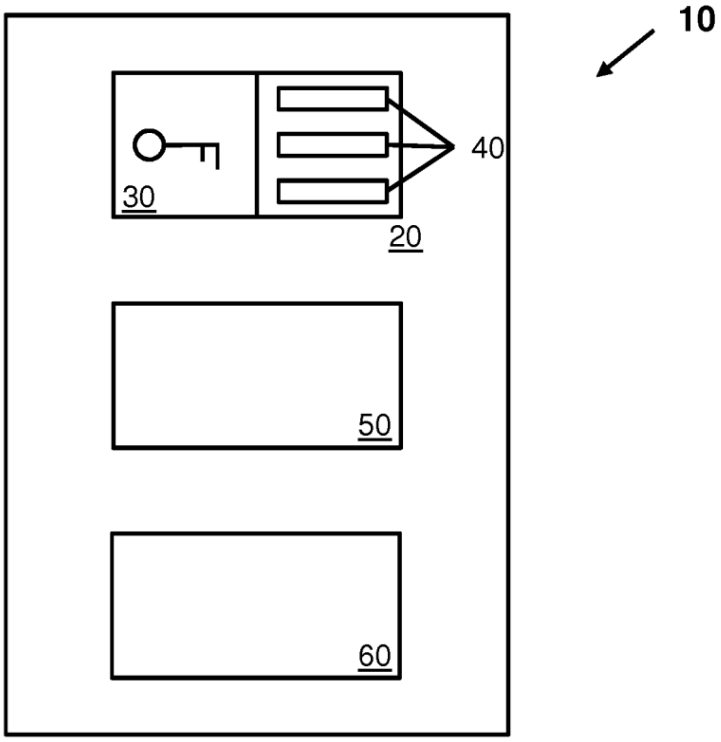

Figura 2

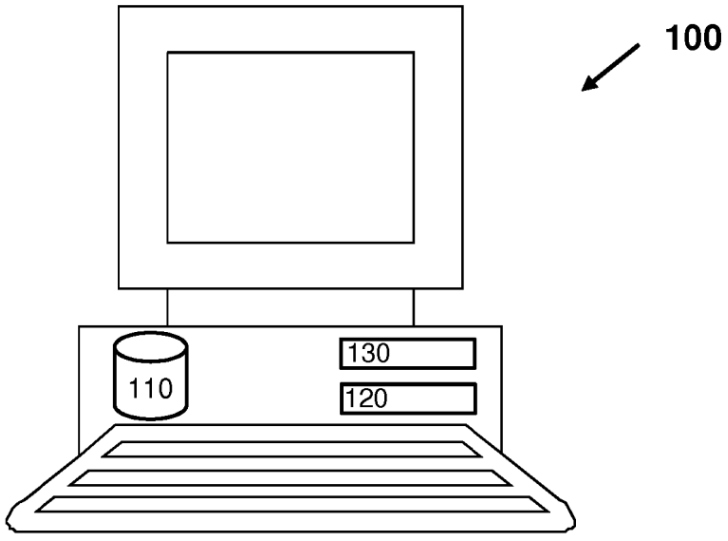

Figura 3

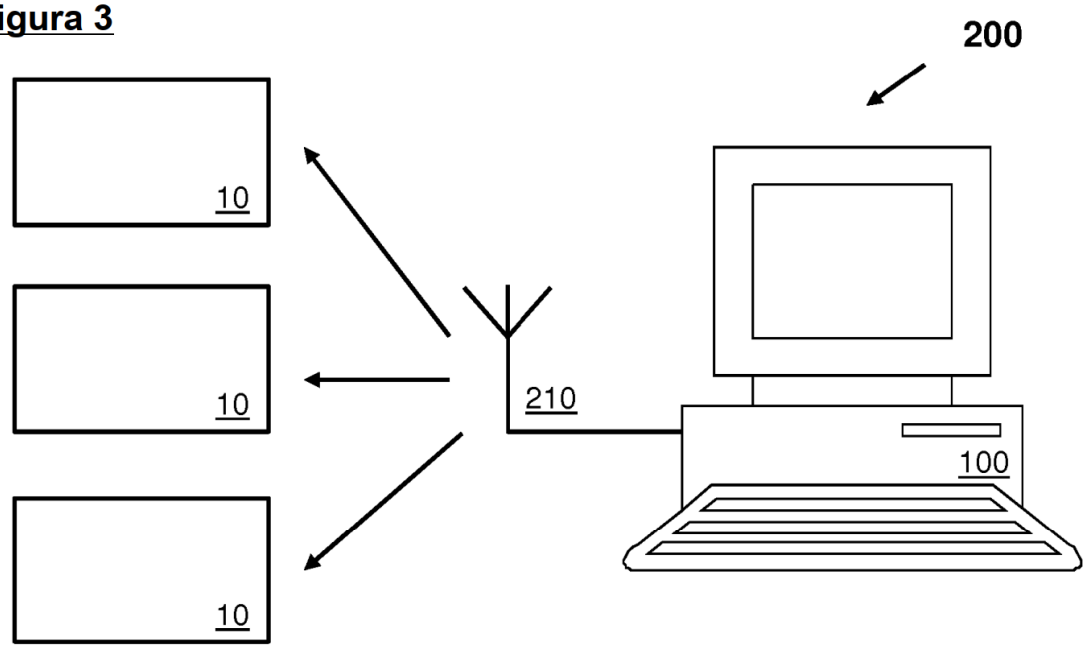

Figura 4

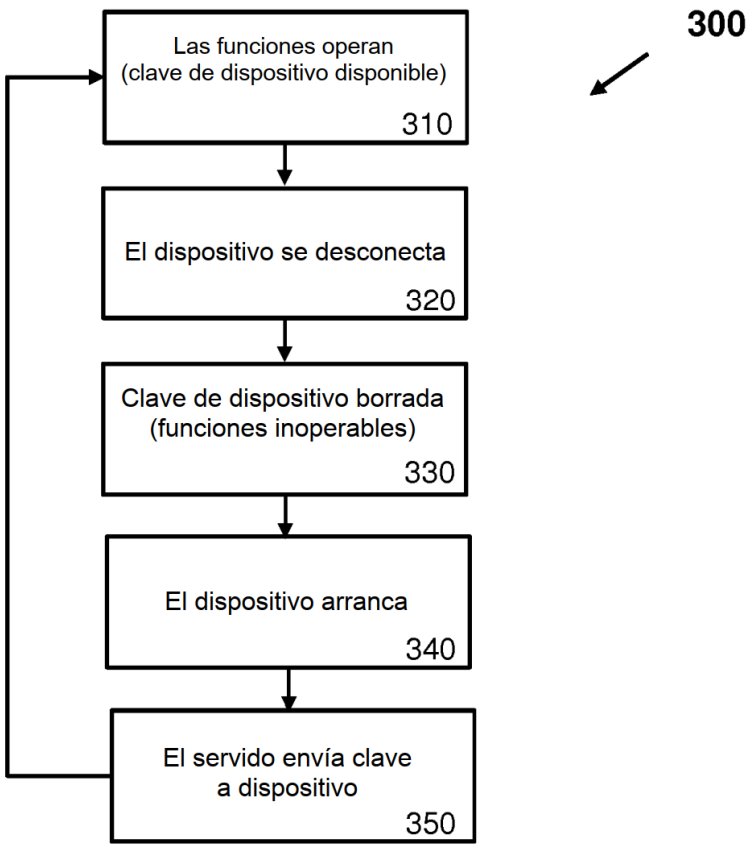

Figura 5