(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 710 431**

(51) Int. CI.:

G06F 21/62 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **15.11.2012 PCT/EP2012/072781**

(87) Fecha y número de publicación internacional: **23.05.2013 WO13072433**

(96) Fecha de presentación y número de la solicitud europea: **15.11.2012 E 12797778 (3)**

(97) Fecha y número de publicación de la concesión europea: **07.11.2018 EP 2780857**

(54) Título: **Método para asegurar un dispositivo informático**

(30) Prioridad:

15.11.2011 GB 201119683

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
25.04.2019

(73) Titular/es:

ROSBERG SYSTEM AS (100.0%)
P.O. Box 26
5542 Jarnsund Norevegen, NO

(72) Inventor/es:

RAMALLO, NESTOR, MARIO;
ROSBERG, ODD, HELGE y
BRAATHEN, ALF, KENNETH

(74) Agente/Representante:

SÁEZ MAESO, Ana

DESCRIPCIÓN

Método para asegurar un dispositivo informático

Esta invención se refiere a un método para asegurar un dispositivo informático.

Antecedentes

Vivimos en una sociedad cada vez más móvil, y las personas experimentan cada vez más que sus dispositivos informáticos o una unidad que contiene dispositivos informáticos, por ejemplo, un automóvil, son robados, perdidos o desaparecidos. Cada vez más, la motivación para este robo es el robo de información en lugar del dispositivo en sí. Actualmente no hay buenas soluciones que se adapten a la necesidad de bloquear un dispositivo de ordenador o partes de él cuando no sea operacional en un grado tal que las personas que intenten robarlo u obtener acceso ilegal a él no puedan hacerlo. Esto implica que el dispositivo debe estar en un estado seguro siempre que no esté operativo, y requerirá una clave de una fuente externa para recuperar su capacidad para funcionar.

La presente invención, al menos en sus realizaciones preferidas, busca abordar esta necesidad.

"Truecrypt, Free open-source-on-the-fly encryption, user's guide, version 6.3", octubre de 2009 (2009-10-01), XP055053166, Obtenido de Internet: URL: http://www.mia-net.org/pub/pc/win/crypto/TrueCrypt/True Crypt User Guide.pdf [recuperado el 2013-02-12] se refiere a un sistema de software para establecer y mantener un volumen cifrado sobre la marcha (dispositivo de almacenamiento de datos). El documento de patente US2010266132 A1 divulga un sistema de custodia de claves basado en servicios. Los datos clave locales se pueden purgar, por ejemplo, en el momento de la hibernación.

Breve resumen de la divulgación

De acuerdo con la presente invención, se proporciona un método para asegurar un dispositivo informático como se reivindica en la reivindicación 1.

Así, de acuerdo con la invención, tan pronto como el dispositivo informático deja de estar en modo operativo, la clave de acceso se elimina de la ubicación de almacenamiento, lo que hace que el dispositivo informático sea seguro porque la clave de acceso ya no está disponible para permitir al dispositivo informático volver a entrar en el modo operativo.

El modo operativo puede ser el funcionamiento normal del dispositivo informático o el funcionamiento de una parte particular del dispositivo informático, tal como una aplicación o una máquina virtual. El modo operativo puede ser un modo en el que se otorga acceso a recursos específicos del dispositivo informático o un dispositivo externo, como un disco duro, una partición de un disco duro u otro almacenamiento de datos.

La clave de acceso puede ser una clave de cifrado u otras credenciales de acceso como se describe en este documento. La provisión de datos de identificación por parte del usuario puede ser por medio de la entrada de datos al dispositivo informático, por ejemplo, la provisión de un nombre de usuario y contraseña o datos biométricos. La provisión de datos de identificación por parte del usuario puede ser por medio de un dispositivo informático externo, por ejemplo, la comunicación desde un teléfono móvil.

El dispositivo informático externo puede ser un servidor remoto en comunicación de datos con el dispositivo informático, por ejemplo, a través de una red. El dispositivo informático externo puede ser un dispositivo informático local en comunicación de datos local con el dispositivo informático, por ejemplo, a través de Bluetooth o Zigbee. El dispositivo informático local puede estar en comunicación de datos con el dispositivo informático a través de una red, que incluye, por ejemplo, redes móviles o de satélite. El dispositivo informático local puede ser un teléfono móvil u otro dispositivo informático personal similar.

La eliminación de la clave de acceso de la ubicación de almacenamiento puede comprender sobrescribir la clave de acceso con datos alternativos. El dispositivo informático adicional puede estar, por ejemplo, en comunicación de datos locales con el primer dispositivo informático. El dispositivo informático adicional puede ser, por ejemplo, un dispositivo informático remoto. El dispositivo informático adicional puede ser, por ejemplo, un teléfono móvil. El dispositivo informático remoto puede estar en comunicación de datos con el primer dispositivo informático a través de una red. El dispositivo informático puede estar conectado a al menos un primer dispositivo informático remoto y un segundo dispositivo informático remoto a través de una red y el método puede comprender almacenar una primera parte de la clave de acceso en el primer dispositivo informático remoto y una segunda parte de la clave de acceso en el segundo dispositivo informático remoto. Esto tiene la ventaja de que ningún dispositivo informático remota almacena la clave completa. El dispositivo informático puede estar conectado a un tercer dispositivo informático remoto y el método puede comprender almacenar una de la primera parte o la segunda parte de la clave de acceso en el tercer dispositivo informático remoto. Esto tiene la ventaja de la redundancia en el almacenamiento de las partes clave. Este método puede extenderse a los dispositivos informáticos remotos cuarto, quinto, sexto y así sucesivamente. La red puede ser una red de igual a igual.

Cualquiera de los métodos anteriores para eliminar la clave de acceso se puede utilizar de forma aislada o combinada.

El dispositivo informático puede comprender una memoria volátil y el método puede comprender almacenar la clave de acceso solo en la memoria volátil durante el modo operativo, por lo que la clave de acceso se borra de la memoria volátil cuando se interrumpe el suministro de energía al dispositivo informático. Esto tiene la ventaja de que la clave de acceso se elimina en caso de una interrupción inesperada de la alimentación. El método puede incluir descargar la memoria volátil, incluida la clave de acceso, al almacenamiento cifrado durante la hibernación del dispositivo.

La etapa de eliminar la clave de acceso puede ser automática en respuesta a dicho evento y efectuarse sin la intervención del usuario. De esta manera, un usuario no autorizado no puede impedir la eliminación de la clave de acceso.

El evento puede comprender la recepción de un comando de un dispositivo informático adicional en comunicación de datos con el primer dispositivo informático. El evento puede comprender un cambio de ubicación del dispositivo informático, por ejemplo, un cambio de ubicación no autorizado. El evento puede incluir el cierre de una aplicación que se ejecuta en el dispositivo informático. El evento puede comprender la terminación de una conexión a un dispositivo informático externo. El dispositivo informático externo puede ser, por ejemplo, un servidor remoto o un dispositivo informático local tal como un teléfono móvil o similar. La conexión puede ser una conexión por cable, una conexión inalámbrica, una conexión de datos móviles, una conexión por satélite, una conexión Bluetooth u otra conexión similar.

El método puede comprender además la etapa de recuperar la clave de acceso en respuesta a la entrada de datos de identificación por parte de un usuario y almacenar la clave de acceso en la ubicación de almacenamiento. Esta etapa se puede llevar a cabo para recuperar la clave de acceso para el almacenamiento inicial en la ubicación de almacenamiento o para devolver la clave de acceso (o una nueva clave de acceso) a la ubicación de almacenamiento.

En términos generales, la presente invención se refiere a un método para mejorar la seguridad del ordenador al eliminar, retirar, mover (que incluye copiar y luego eliminar la fuente) y/o reemplazar/sobrescribir (con datos no válidos) las claves, partes de claves cualquier otro identificador utilizado para obtener acceso a ordenadores, dispositivos, depósitos o cualquier otra unidad. Esto se logra mediante un procedimiento automatizado predefinido que elimina y mueve una clave dada un conjunto de circunstancias tales como cerrar una aplicación, apagar un dispositivo de ordenador, conectar, terminar una máquina virtual o cualquier otra situación en la que sea deseable una acción de este tipo. Esta acción también puede ser manual dadas las circunstancias. La clave se restaura de forma segura mediante la identificación del usuario y/o la verificación de otras condiciones y/o credenciales requeridas (hardware o software) antes de iniciar el procedimiento de restauración.

De este modo, la clave se elimina de forma segura activada por un evento como se describe anteriormente. El evento puede ser un evento externo, como un comando externo de, por ejemplo, un servidor, un dispositivo de usuario diferente (como un teléfono móvil) u otro dispositivo asignado para dar dichos comandos. El evento puede ser un cambio en las condiciones, como ubicación, acoplamiento/desacoplamiento, cambio de red, dominio, proximidad a otros dispositivos o cualquier otra condición. El evento puede ser la terminación de una conexión, una aplicación, una máquina virtual, un subconjunto de una aplicación o cualquier otro evento que debería desencadenar esta acción.

La eliminación de una clave puede proteger un dispositivo completo, parte de un dispositivo o cualquier módulo o unidad dentro o alrededor del dispositivo, incluido el software y el hardware.

La clave de cifrado puede almacenarse en una memoria volátil, lo que garantiza que la clave se elimine (desaparezca) cuando se apaga el dispositivo.

La eliminación de la clave puede requerir que exista una copia de la clave en otro dispositivo o servidor o similar, o en varios dispositivos, ya sea como una clave completa, cifrado o como fragmentos de claves.

La clave se puede mover o eliminar de una manera segura activada por un evento como se describe anteriormente a una ubicación alternativa externamente, por ejemplo. a un servidor de claves, a un dispositivo alternativo, a un servicio en la nube o cualquier otro método de distribución de claves a otras ubicaciones.

El método puede implicar el reemplazo de la clave en lugar de eliminarla para proporcionar datos no válidos con el fin de hacer que sea más difícil leer la clave original y más difícil de ver si la clave es válida o no válida. La clave se puede sobrescribir varias veces para proporcionar suficiente seguridad.

Cuando el dispositivo a proteger está participando en una red, la clave puede fragmentarse y almacenarse en varias ubicaciones. Esto distribuye la clave en una serie de dispositivos que brindan seguridad, ya que ninguno de ellos tiene la clave completa o la conoce. Se puede crear redundancia para proporcionar una clave completa incluso si algunos dispositivos no están disponibles en el punto de recuperación.

El método puede implicar la restauración, distribución o suministro de claves para el dispositivo físico o virtual, el software, el sistema operativo o cualquier otro dispositivo, unidad o software aplicable que utilice cualquier método conocido para hacerlo, incluida cualquier medida de seguridad conocida incluida en dichos métodos para hacer que el dispositivo sea físico o dispositivo virtual, aplicación, funcionalidad o unidad disponible. Esto también se puede hacer desde un dispositivo alternativo, como un teléfono móvil, teléfono, SMS, correo electrónico o desde cualquier otro dispositivo.

El método puede usar la técnica de comunicación descrita en el documento WO 2010/039041 para restaurar claves de una manera segura. En este caso, el dispositivo cliente primero envía una solicitud al servidor utilizando cualquier método de comunicación que identifique que el cliente solicita una clave de reemplazo. Esto también se puede hacer desde un dispositivo alternativo, como un teléfono móvil, por teléfono, SMS, correo electrónico o desde cualquier otro dispositivo. Esto a su vez desencadenará un evento en el servidor utilizando las técnicas del documento WO 2010/039041 para enviar una solicitud al dispositivo que es rechazado, y el dispositivo buscará el identificador, y si lo encuentra, se conecta de nuevo utilizando cualquier medio de comunicación al servidor.

El método se puede aplicar a ordenadores, dispositivos, almacenamiento o cualquier otra unidad en una red de igual a igual, red en malla, red para compartir archivos, red tipo torrent o cualquier red similar copiando la(s) clave(s), credenciales de usuario, certificado(s), frase de contraseña(s) y otra información a una(s) ubicación(es) alternativa(s) antes de la eliminación utilizando la(s) red(s) de malla(s) y tipos de red similares. El método puede usar áreas de malla cifradas o no cifradas (o similares) para almacenar archivos de torrent que contienen bloques de claves. El dispositivo puede ser parte de una o varias redes en malla donde la clave se puede mover a otro dispositivo en la malla. Esto puede ser una malla privada, una malla corporativa o cualquier otro tipo de malla. La clave también puede distribuirse en una serie de dispositivos de malla para que ningún dispositivo mantenga la clave completa, lo que proporciona un método simple y muy seguro para imposibilitar la búsqueda de la clave sin tener acceso a varios dispositivos. Un dispositivo de malla también puede contener, por ejemplo, una clave hash que debe combinarse con una clave en otro dispositivo para generar la clave de cifrado requerida. Estos dispositivos de malla también pueden servir como un recurso para almacenar claves o parte de claves en todos estos dispositivos. También se puede crear redundancia, lo que significa que la misma clave o parte de la clave se puede almacenar en múltiples dispositivos de malla.

La invención se extiende a un dispositivo informático configurado para funcionar de acuerdo con el método de la invención. La invención también se extiende al software informático que configura un dispositivo informático para que funcione de acuerdo con el método.

Descripción detallada

En términos generales, la presente invención se refiere a un sistema para la eliminación y restauración de claves de un dispositivo informático. El dispositivo informático puede ser cualquier dispositivo que comprenda un procesador de datos de cualquier tipo. Dicho dispositivo puede ser, por ejemplo, un ordenador, un dispositivo de m2m (máquina a máquina), cualquier unidad móvil como un teléfono, un panel táctil (ordenador tipo tableta), un teléfono inteligente, un automóvil, cualquier tipo de vehículo, armas, pistolas, dispositivos personales de cualquier tipo, servicios públicos, sistemas de seguridad, en resumen, cualquier cosa con capacidad de procesamiento de datos.

La clave de acceso almacenada puede comprender credenciales de usuario (nombre de usuario, contraseña y similares), claves de licencia, claves de cifrado (para cifrar/descifrar datos en dispositivos de almacenamiento/hardware, datos enviados a través de una red privada virtual (VPN) por ejemplo, a través de dispositivos móviles redes, datos enviados a través de conexiones seguras de capa de conexión segura (SSL) y similares), certificados digitales, firmas digitales, claves biométricas, paquetes cifrados (por ejemplo, claves de cifrado hash de tiempo/biométricas o similares) u otros mecanismos de seguridad o información de seguridad de cualquier tipo.

Esta invención se refiere a un procedimiento para mejorar la seguridad de los dispositivos informáticos o una unidad que contiene dispositivos informáticos (por ejemplo, un automóvil) al eliminar, mover, retirar y/o reemplazar claves e inicializar un proceso de restauración a petición que rinda dicho dispositivo informático. en un estado seguro a menos que los procedimientos de autorización apropiados se completen con éxito. Para mejorar aún más la seguridad, la clave se puede distribuir en partes o fragmentos a varios hosts (por ejemplo, una red en malla), asegurándose de que la clave nunca se almacene en su totalidad en una única ubicación.

El método tiene la ventaja de que una clave almacenada de forma remota puede eliminarse permanentemente si el dispositivo informático es robado, en comparación con las claves almacenadas localmente que permanecen con el dispositivo robado. Además, los intentos de autenticación fraudulentos se pueden identificar y/o prevenir más efectivamente a través de un sistema centralizado o remoto. En combinación con nuestra técnica de comunicación segura anterior descrita en el documento WO 2010/039041, se puede efectuar la transferencia segura de la clave.

El método de la invención permite reglas configurables para la eliminación de claves de acuerdo con una aplicación o nivel de seguridad deseados, lo que permite un control flexible, por ejemplo, alta seguridad en comparación con la

conveniencia. El método también permite claves parciales remotas distribuidas para mayor seguridad y permite claves remotas redundantes para reducir las ocasiones en que un usuario válido está bloqueado.

El método puede usarse para proteger un dispositivo informático completo o partes de un sistema operativo, como una máquina virtual o una partición.

De acuerdo con el método de la invención, las claves o parte de las claves (por ejemplo, la clave de cifrado del disco duro) se eliminan cada vez que el dispositivo se pone en un estado diferente al estado en uso, por ejemplo, suspensión, hibernación o apagado. El retiro puede ser eliminar y mover la clave a un servidor externo, a otro dispositivo. Puede haber varios medios para eliminar la clave, ya sea manteniendo la clave en la memoria volátil o permitiendo que el dispositivo elimine la clave al colocar el dispositivo en cualquier otro estado que no sea el estado activo. Este procedimiento también puede usarse para eliminar claves mientras el dispositivo informático está en uso para permitir o impedir el acceso a partes del dispositivo y/o partes del almacenamiento del dispositivo, como una partición o un archivo cifrado, así como el acceso a cualquier Software, servicio remoto o recurso en LAN, WAN, en Internet, en un entorno de malla o en cualquier otro recurso. Una malla puede ser cualquier red privada de igual a igual a través de una red pública o privada.

La clave (o partes de la clave) se recupera leyendo desde una o varias ubicaciones diferentes que son fuentes internas y/o externas cuando el dispositivo se inicia o se retira inicialmente de cualquier estado no activo. Luego, la clave se almacena en un área de memoria volátil o en un área de memoria no volátil o ubicación de almacenamiento, con criterios predefinidos para acciones para mover, retirar, eliminar o reemplazar la clave, o al acceder a cualquier servicio, área de archivo, recurso, etc. que requiere cifrado. El método también proporcionará nuevas claves en condiciones dadas.

El proceso de eliminación implica eliminar datos del dispositivo informático, de la memoria volátil o no volátil, de dispositivos de almacenamiento tales como discos duros, discos de estado sólido (SSD), tarjetas de memoria, procesadores, chips de módulo de plataforma confiable (TPM) u otras formas de almacenamiento similares, es decir, cualquier dispositivo capaz de almacenar información. La eliminación puede ser simple (solo eliminar información) o compleja (como sobrescribir las celdas de memoria varias veces para asegurarse de que la información no se pueda restaurar). La eliminación puede ocurrir al eliminar la energía de la memoria volátil.

Una realización ejemplificada del método de la invención puede estar asegurando un ordenador portátil que contiene datos confidenciales. Cuando el ordenador portátil está apagado, en modo de suspensión o hibernación (eliminación activa de la clave de cifrado al hibernar o usar, por ejemplo, win+L en Microsoft Windows), no hay ninguna clave de cifrado dentro del dispositivo. Cuando se va a utilizar el ordenador portátil, solicita un inicio de sesión del usuario (nombre de usuario/contraseña, inicio de sesión biométrico, etc.) y luego solicita la clave de cifrado a través de un método de comunicación como VPN sobre 3G desde un servidor centralizado que valida al usuario. En función de la validación del usuario, el servidor genera un paquete cifrado que contiene la clave de cifrado que se puede marcar con una marca de tiempo o similar y se envía a el ordenador portátil, que a su vez descifrará el paquete y almacenará la clave de cifrado en la memoria volátil. El ordenador portátil utiliza la clave de cifrado para proporcionar acceso al registro de inicio maestro (MBR) y, por lo tanto, permite que el ordenador portátil inicie su procedimiento de inicio o permite el acceso al dispositivo de almacenamiento al iniciar sesión.

Otro ejemplo de uso es mientras el dispositivo informático está activo, y el usuario necesita acceso a un archivo específico, área en el disco o servicio en la nube, se puede usar el mismo método de eliminación y restauración de las claves de cifrado, ya sea utilizando Funcionalidad desde la capa de hardware o desde la capa del sistema operativo. Un ejemplo de esto puede ser una máquina virtual almacenada en el dispositivo del ordenador que da acceso a una red corporativa con altas necesidades de seguridad. La clave se almacena en la memoria volátil y se elimina activamente cada vez que la máquina virtual se cierra o se pone en otro estado que no sea el estado activo. El sistema operativo principal puede estar desprotegido por este método, o también puede estar protegido de la misma manera proporcionando una capa múltiple de seguridad, si así lo desea.

La clave de cifrado puede enviarse o recuperarse desde otras fuentes distintas de un servidor, por ejemplo, como se describe a continuación.

La clave de cifrado o partes de la clave de cifrado se pueden almacenar en otro dispositivo de usuario, como un teléfono inteligente, un panel táctil (ordenador tipo tableta), un ordenador con enchufe o cualquier otro dispositivo personal. De esta manera, el usuario no necesita confiar en el acceso al servidor central para iniciar el dispositivo, pero puede recuperar la clave a través de, por ejemplo, una conexión Bluetooth al teclado del usuario o una comunicación de campo cercano al dispositivo móvil. Esto aumenta el nivel de seguridad si el dispositivo es robado, ya que el otro dispositivo debe estar cerca del dispositivo informático que requiere la clave de cifrado. Estos dispositivos también pueden servir como un recurso para almacenar claves o parte de claves en todos estos dispositivos. También se puede crear redundancia, lo que significa que la misma clave o parte de la clave se puede almacenar en varios dispositivos.

El dispositivo informático puede ser parte de una o varias redes de malla y/o privadas (por ejemplo, redes basadas en IPv6) donde la clave puede estar en otro dispositivo en la red. Esto puede ser una red privada (interna o por Internet), una red personal, una red/malla corporativa o cualquier otro tipo de red. La clave también puede distribuirse en una serie de dispositivos para que ningún dispositivo mantenga la clave completa, lo que proporciona un método simple y muy seguro para imposibilitar la búsqueda de la clave sin tener acceso a varios dispositivos. Un dispositivo también puede contener, por ejemplo, una clave hash que debe combinarse con una clave en otro dispositivo para generar la clave de cifrado necesaria. Estos dispositivos también pueden servir como un recurso para almacenar claves o parte de claves en todos estos dispositivos. También se puede crear redundancia, lo que significa que la misma clave o parte de la clave se puede almacenar en varios dispositivos.

En el mundo de máquina a máquina (M2M) hay muchos usos para esta tecnología, especialmente en campos donde se necesita una seguridad mejorada, por ejemplo, como se describe a continuación.

El método de la invención se puede usar para aumentar la seguridad en una solución de pago móvil y para proteger la aplicación en dispositivos de tal manera que un virus u otro software malicioso no pueda obtener acceso a la información financiera del usuario y/o cuentas, por ejemplo, cuando dos dispositivos desean realizar una transacción, por ejemplo, dos teléfonos móviles, o un teléfono móvil y un cajero automático (ATM). Cada teléfono (o dispositivo) tiene una aplicación que lo conecta con la institución financiera de manera segura, pero parte de la aplicación está encriptada y protegida hasta que se identifica otro dispositivo con el cual realizar la transacción. Esta aplicación también puede ser una máquina virtual o una función similar aislada del dispositivo. El dispositivo puede ser un cajero automático, un terminal de punto de venta (POS), un terminal de tarjeta de crédito portátil, un dispositivo móvil, un ordenador de cualquier tipo o cualquier otro dispositivo adecuado. Esto se puede hacer usando NFC, una red de área personal (PAN), y LAN, WAN, redes móviles o cualquier otro medio de comunicación con cualquier forma segura de conectarse a otros dispositivos. Cuando se localiza la parte de la transacción, se envía una solicitud a la institución financiera para que proporcione claves de cifrado para los dos dispositivos que desbloquean la aplicación necesaria para realizar la transacción, pero solo a los dos dispositivos aprobados. También se pueden proporcionar certificados adicionales. Luego, la transacción se inicia mediante la combinación de claves y/o certificados y/u otros identificadores entre dispositivos. Las aplicaciones dentro de estos dispositivos y/o la institución financiera los aprueban, y completan la transacción después de la cual se le ordena al dispositivo que elimine los certificados/claves/identificadores, y se da información a la institución financiera de que se ha hecho esto. Esto garantiza que la aplicación en el dispositivo solo pueda realizar transacciones con dispositivos aprobados y, una vez completada, la aplicación se bloquea. En el caso de una conexión a un cajero automático, ATM solo el dispositivo móvil se bloquea después de completarse. En el caso de un pago de móvil a móvil, ambas aplicaciones se bloquean una vez finalizadas. Este método puede, por supuesto, combinarse con diferentes medios de autenticación, si es necesario, como contraseñas, códigos PIN, contraseñas de mensajes de texto únicos (autenticación de dos factores), huellas dactilares u otra información biométrica, o cualquier otro método de autenticación o identificación del usuario.

En los automóviles o vehículos, existen muchas formas alternativas de utilizar el método de la invención. Por ejemplo, describimos un método para cifrar la parte de gestión del vehículo para que la clave de cifrado se elimine siempre que no se use la parte de gestión. La clave de cifrado se restaura después de que se realiza la comunicación con el dispositivo, y sin la clave no hay forma de acceder a la parte de gestión del vehículo. Se pueden usar diferentes claves de cifrado para obtener acceso a diferentes niveles, por ejemplo, uno para actualizar el software y realizar el mantenimiento, otro para leer estadísticas y otro para fines de seguimiento y eliminación. Hay aplicaciones casi ilimitadas para este método.

También se puede aplicar el método de la invención como una forma segura de mover claves de cifrado a otros dispositivos, como teléfonos móviles, para obtener acceso a conducir y usar el vehículo, y también agregar funcionalidad para que un usuario tenga que: solicitar permiso para acceder a un vehículo determinado, por ejemplo, para uso militar o al alquilar un automóvil. En lugar de mover la llave, se puede eliminar la llave, lo que significa que el dispositivo tendrá una llave preinstalada que se moverá al automóvil/vehículo cuando se use. El otro dispositivo (por ejemplo, un teléfono móvil) también puede tener que solicitar la clave o parte de ella a un servidor central o similar para crear una clave con hash para enviar al vehículo.

Este método también se puede usar para dar claves de cifrado limitadas en el tiempo que expirarán después de un tiempo determinado automáticamente, ejemplificando el préstamo de un automóvil a alguien o para una empresa que alquila automóviles.

El método utilizado es, en principio, el mismo que con el pago móvil, solo que los derechos de distribución de permisos y derechos pueden pertenecer a otra persona, o a varios otros (como un garaje para mantenimiento, un seguro para informes de kilometraje, el propietario para dar permiso para utilizar el coche).

Un ejemplo adicional del uso del método de la invención es el de los dispositivos de seguridad. Este método se puede aplicar, por ejemplo, a ordenadores portátiles de tal manera que, si un ordenador portátil es robado, el propietario puede hacer que el ordenador portátil elimine las claves de cifrado y, de esa manera, inutilice el dispositivo, protegiendo los datos del dispositivo. Esto se puede hacer llamando a un centro de servicio que envía un comando al dispositivo para eliminar la clave, usando una aplicación en el teléfono inteligente de la persona, una aplicación en otro ordenador

o servicios de proximidad entre un dispositivo móvil y el ordenador o cualquier otra o similar maneras de desencadenar tal acción.

Utilizando el mismo método, también se puede activar la funcionalidad en el dispositivo para comenzar a transmitir información de ubicación o recopilar información mediante el envío de información desde el micrófono, cámara, dispositivos biométricos o similares del dispositivo.

De esta forma, se puede realizar una forma completa y muy segura de proteger un dispositivo, partes de él o rastrearlo y ubicarlo.

El método de la invención también puede aplicarse en la aplicación de máquina a máquina, por ejemplo, para dispositivos detrás de los cortafuegos del cliente. Un ejemplo de uso aquí es un escáner de tomografía computarizada (CT) en un hospital. La parte de gestión del escáner es una máquina virtual cifrada, pero conectada a 3G con un módem. El centro de servicio de confianza puede conectarse al dispositivo e ingresar la clave de cifrado, y la máquina virtual se enciende. Alternativamente, el centro de servicio necesita que el personal del cliente coloque la clave de cifrado correspondiente antes de que puedan conectarse al dispositivo por razones de seguridad. La clave de cifrado se elimina automáticamente y la máquina virtual se detiene cuando se cierra la sesión.

El método de la invención se puede usar en combinación con nuestra técnica de comunicación segura anterior divulgada en el documento WO 2010/039041. Esta técnica de comunicación se puede utilizar como un componente básico para la presente invención para proporcionar seguridad adicional a los dispositivos. La técnica de comunicación se puede realizar enviando primero una solicitud a un dispositivo que se rechaza. El dispositivo luego verifica el identificador y, si se reconoce, llama a una dirección IP designada asociada con el identificador. Después de establecer una conexión segura, la clave de cifrado al dispositivo se transfiere y el dispositivo se desbloquea y se puede utilizar.

En resumen, se describe un método para asegurar un dispositivo informático. El dispositivo informático está configurado para almacenar una clave de acceso en una ubicación de almacenamiento para que el dispositivo informático funcione en un modo operativo. El método comprende eliminar la clave de acceso de la ubicación de almacenamiento en respuesta a un evento indicativo del final del modo operativo.

A lo largo de la descripción y las reivindicaciones de esta especificación, las palabras “comprenden” y “contienen” y las variaciones de ellas significan “que incluye, pero no limitado a”, y no pretenden (y no) excluir otros componentes, enteros o pasos. A lo largo de la descripción y las reivindicaciones de esta especificación, el singular abarca el plural a menos que el contexto requiera lo contrario. En particular, cuando se usa el artículo indefinido, se debe entender que la especificación contempla la pluralidad y la singularidad, a menos que el contexto requiera lo contrario.

REIVINDICACIONES

1. Un método para asegurar un dispositivo informático, en el que el dispositivo informático está configurado para almacenar una clave de acceso en una ubicación de almacenamiento para que el dispositivo informático funcione en un modo operativo y el dispositivo informático está configurado para evitar la operación en el modo operativo sin la clave de acceso, el método comprende:

el dispositivo informático que recupera la clave de acceso de un dispositivo informático externo en respuesta a la provisión de datos de identificación por parte de un usuario y el almacenamiento de la clave de acceso en la ubicación de almacenamiento;

el dispositivo informático que funciona en dicho modo operativo en respuesta a la recepción y almacenamiento de la clave de acceso;

el dispositivo informático que elimina la clave de acceso de la ubicación de almacenamiento en respuesta a un evento indicativo del final del modo operativo, en el que la eliminación de la clave de acceso de la ubicación de almacenamiento comprende la eliminación de la clave de acceso y se caracteriza porque:

eliminar la clave de acceso la ubicación de almacenamiento comprende además almacenar la clave de acceso en un dispositivo informático adicional en comunicación de datos con el primer dispositivo informático.

2. Un método como se reivindica en la reivindicación 1, en el que el dispositivo informático externo es un servidor remoto en comunicación de datos con el dispositivo informático.

3. Un método como se reivindica en la reivindicación 1, en el que el dispositivo informático externo es un dispositivo informático local, en particular un teléfono móvil, en comunicación de datos local con el dispositivo informático.

4. Un método como se reivindica en cualquiera de las reivindicaciones anteriores, en el que la eliminación de la clave de acceso de la ubicación de almacenamiento comprende sobrescribir la clave de acceso con datos alternativos.

5. Un método como se reivindica en cualquiera de las reivindicaciones anteriores, en el que el dispositivo informático adicional está en comunicación de datos local con el primer dispositivo informático.

6. Un método según cualquier reivindicación precedente, en el que el dispositivo informático adicional es un dispositivo informático remoto en comunicación de datos con el primer dispositivo informático.

7. Un método de acuerdo con la reivindicación 6, en el que el dispositivo informático está conectado a al menos un primer dispositivo informático remoto y un segundo dispositivo informático remoto a través de una red y el método comprende almacenar una primera parte de la clave de acceso en el primer dispositivo informático remoto y una segunda parte de la clave de acceso en el segundo dispositivo informático remoto.

8. Un método como se reivindica en la reivindicación 7, en el que el dispositivo informático está conectado a un tercer dispositivo informático remoto y el método comprende almacenar una de la primera parte o la segunda parte de la clave de acceso en el tercer dispositivo informático remoto.

9. Un método como el reivindicado en cualquier reivindicación precedente, en el que el dispositivo informático comprende una memoria volátil y el método comprende almacenar la clave de acceso solo en la memoria volátil durante el modo operativo, por lo que la clave de acceso se borra de la memoria volátil cuando la fuente de alimentación al dispositivo informático se interrumpe.

10. Un método como el reivindicado en cualquier reivindicación precedente, en el que la etapa de eliminar la clave de acceso es automática en respuesta a dicho evento y se realiza sin la intervención del usuario.

11. Un método como el reivindicado en cualquier reivindicación precedente, en el que el evento comprende la recepción de un comando de un dispositivo informático adicional en comunicación de datos con el primer dispositivo informático.

12. Un método como el reivindicado en cualquier reivindicación precedente, en el que el evento comprende un cambio de ubicación del dispositivo informático.

13. Un método como el reivindicado en cualquier reivindicación precedente, en el que el evento comprende cerrar una aplicación que se ejecuta en el dispositivo informático.

14. Un dispositivo informático configurado para funcionar de acuerdo con el método de cualquier reivindicación precedente.

15. Software informático que configura un dispositivo informático para que funcione de acuerdo con el método de cualquiera de las reivindicaciones 1 a 13.