(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 674 224**

(51) Int. CI.:

H04L 29/06 (2006.01)
G06F 21/31 (2013.01)
G06F 21/34 (2013.01)
H04L 29/14 (2006.01)
H04L 9/08 (2006.01)
H04L 9/32 (2006.01)
G06F 21/60 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **16.05.2014 PCT/SG2014/000215**

(87) Fecha y número de publicación internacional: **20.11.2014 WO14185865**

(96) Fecha de presentación y número de la solicitud europea: **16.05.2014 E 14727968 (1)**

(97) Fecha y número de publicación de la concesión europea: **21.03.2018 EP 2997708**

(54) Título: **Dispositivo y método de auto autenticación**

(30) Prioridad:

16.05.2013 SG 201303827

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
28.06.2018

(73) Titular/es:

FAST AND SAFE TECHNOLOGY PRIVATE LIMITED (100.0%)
9 Temasek Boulevard 09-01 Suntec Tower Two
Singapore 038989, SG

(72) Inventor/es:

HSU, HSIANG KE DESMOND

(74) Agente/Representante:

LLAGOSTERA SOTO, María Del Carmen

Descripción

DISPOSITIVO Y MÉTODO DE AUTO AUTENTICACIÓN

CAMPO DE LA INVENCIÓN

La presente invención se refiere en un sentido amplio a un sistema, dispositivo y método en el campo de la seguridad de la tecnología de la información (IT) y la seguridad electrónica.

ANTECEDENTES

En el contexto de la seguridad de IT, muchos dispositivos de usuario final, incluyendo ordenadores de escritorio, tabletas, teléfonos inteligentes, ordenadores portátiles, unidades de disco duro portátiles, unidades flash USB y varios otros dispositivos móviles, así como servidores, procesan e intercambian grandes cantidades de información en entornos cableados e inalámbricos. Parte de esta información es altamente sensible, como la información personal privada y la información de la corporación perpetrada. La información que puede beneficiar a un usuario u organización también se puede utilizar en contra del usuario o la organización si cae en manos equivocadas. Los agentes de espionaje industrial entre empresas altamente competitivas recurren a medios electrónicos para robar información corporativa.

El encriptado es la solución más generalizada para proporcionar confidencialidad de datos. La mayoría de los productos de software de encriptado de datos instalan y almacenan la clave de encriptado que se utiliza para encriptar y proteger los datos dentro del mismo dispositivo donde se almacenan los datos. Si el dispositivo se pierde o se piratea, tanto los datos encriptados como la clave de encriptado caen en las mismas manos y la seguridad de los datos se ve comprometida en consecuencia.

Utilizar un token portátil externo que esté separado físicamente del dispositivo que almacena los datos, para almacenar la clave de encriptado para encriptar y acceder a datos seguros, por ejemplo, desde un disco virtual protegido, es un planteamiento preferido para proteger datos confidenciales en un ordenador central, ya que puede separar la clave de encriptado de los datos encriptados. El enlace de comunicación entre el token y el ordenador central puede ser a través de cualquier módulo de comunicación o medios como por ejemplo canales de radiofrecuencia (RF) o conexiones cableadas. El token portátil externo puede ser cualquier dispositivo periférico, como por ejemplo una unidad flash USB, un teléfono móvil o incluso otro ordenador. El ordenador central puede ser cualquier máquina informática, como un servidor, un ordenador de escritorio, un ordenador portátil o teléfonos inteligentes. El ordenador central puede contener un administrador de seguridad de datos (DSM).

Un mecanismo de protección con contraseña se incorpora junto con el token para evitar el uso no autorizado del token. Como un ejemplo, a un usuario que solicita acceder a los datos protegidos se le pide que conecte su token y que teclee su contraseña. La exactitud de la contraseña está marcada. Si la contraseña es correcta, se permite que el token (y, por lo tanto, el usuario) acceda a los datos protegidos. Un usuario tiene permitido el acceso a los datos seguros solo si el token está conectado y la contraseña de inicio de sesión es correcta. Los datos se encriptan utilizando, por ejemplo, un algoritmo de encriptado de clave simétrica.

Si bien el planteamiento anterior puede proteger los datos confidenciales en un ordenador central, existe el problema de que un usuario minorista en un entorno de consumo puede olvidar su contraseña asociada con el token portátil. Si bien la contraseña generalmente puede ser reiniciada por el fabricante del token portátil, este planteamiento no ofrece una solución satisfactoria porque cada vez que una segunda parte está involucrada en un proceso de seguridad, la posibilidad de una fuga de seguridad se vuelve real. También existen problemas similares cuando el token está dañado, se ha perdido o ha sido robado.

Las formas de realización de la presente invención pretenden proporcionar un sistema, dispositivo y método de auto autenticación, preferiblemente un sistema, dispositivo y método de auto autenticación y recuperación, que permita al usuario o al propietario de los datos soportarlos cuando surjan dichos problemas, sin involucrar a otros.

El documento US 2008/0263656 describe permitir operaciones administrativas en un token de usuario bajo el control de un token de administrador “Large Scale Password Management With Hitachi ID Password Manager”, 1 de abril de 2013, https://web.archive.org/web/2012102505/http//hitachi-id.com/password-manager/docs/large-sclae-password-management-with-hid-pw-manager.pdf, describe un usuario que se

autentifica a sí mismo utilizando un navegador de web o a través de una llamada de teléfono para reiniciar su contraseña.

RESUMEN

La presente invención se define en las reivindicaciones independientes. Las formas de realización preferentes se definen en las reivindicaciones dependientes.

De acuerdo con un primer aspecto de la presente invención, se proporciona un dispositivo de auto autenticación para el usuario o propietario de un dispositivo de seguridad electrónico, en que el dispositivo de auto autenticación está separado del dispositivo de seguridad y está configurado para conectarse a un ordenador a través de un primer enlace de comunicación para el proceso de auto autenticación, preferiblemente para la auto autenticación y el proceso de recuperación.

De acuerdo con un segundo aspecto de la presente invención, se proporciona un método de auto autenticación para el usuario o propietario de un dispositivo de seguridad electrónico, en que el método comprende conectar un dispositivo de auto autenticación independientemente del dispositivo de seguridad a un dispositivo informático a través de un primer enlace de comunicación para el proceso de auto autenticación, preferentemente para la auto autenticación y el proceso de recuperación.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Las formas de realización de la invención se comprenderán mejor y serán más evidentes para los expertos en la técnica a partir de la siguiente descripción escrita, solo a modo de ejemplo, y junto con los dibujos, en los que:

La Fig. 1a) muestra un diagrama esquemático que ilustra un conjunto para crear y acceder a un disco virtual protegido, de acuerdo con una forma de realización de ejemplo.

La Fig. 1b) muestra un diagrama esquemático que ilustra un ordenador central que interactúa con un token portátil externo del conjunto de la Fig. 1a, de acuerdo con una forma de realización de ejemplo.

La Fig. 2 muestra un diagrama esquemático que ilustra la configuración del token portátil externo del conjunto de la Fig. 1a, de acuerdo con una forma de realización de ejemplo.

La Fig. 3a) muestra un diagrama esquemático que ilustra el proceso de autenticación para restablecer la contraseña del token, de acuerdo con una forma de realización de ejemplo.

La Fig. 3b) muestra un diagrama de flujo que ilustra el proceso de autenticación para restablecer la contraseña del token, de acuerdo con una forma de realización de ejemplo.

La Fig. 4a) muestra un diagrama esquemático que ilustra el proceso de autenticación para crear un token duplicado para la sustitución de un token perdido, dañado o robado, de acuerdo con una forma de realización de ejemplo.

La Fig. 4b) muestra un diagrama de flujo que ilustra el proceso de autenticación para crear un token duplicado para la sustitución de un token perdido, dañado o robado, de acuerdo con una forma de realización de ejemplo.

La Fig. 5a) muestra un diagrama esquemático que ilustra el acceso de reencriptación a archivos de datos protegidos, de acuerdo con una forma de realización de ejemplo.

La Fig. 5b) muestra un diagrama de flujo que ilustra el acceso de reencriptación a archivos de datos protegidos, de acuerdo con una forma de realización de ejemplo.

La Fig. 6 muestra un diagrama esquemático que ilustra el acceso de solo lectura al disco virtual protegido, de acuerdo con una forma de realización de ejemplo.

DESCRIPCIÓN DETALLADA

Algunas partes de la descripción que sigue se presentan explícita o implícitamente en términos de algoritmos y representaciones funcionales o simbólicas de operaciones en datos dentro de una memoria de ordenador. Estas descripciones algorítmicas y representaciones funcionales o simbólicas son los medios utilizados por los expertos en la técnica de la ingeniería informática para transmitir de manera más efectiva la esencia de su trabajo a otros expertos en la materia. Aquí, y en general, un algoritmo está concebido para ser una secuencia autocontenida de pasos que conducen a un resultado deseado. Los pasos son aquellos que requieren manipulaciones físicas de cantidades físicas, como señales eléctricas, magnéticas u ópticas que pueden almacenarse, transferirse, combinarse, compararse y manipularse de otro modo.

A menos que se indique específicamente lo contrario, y tal como resulta evidente a partir de lo siguiente, se apreciará que a través de la presente especificación, las descripciones que utilizan términos tales como "escaneo", "cálculo", "determinación", "sustitución", "generación", "inicialización", "enviar", o similares, se refieren a la acción y procesos de un sistema informático o dispositivo electrónico similar que manipula y transforma datos representados como cantidades físicas dentro del sistema informático en otros datos representados de forma similar como cantidades físicas dentro del sistema informático u otros dispositivos de almacenamiento, transmisión o visualización de información.

La presente memoria descriptiva también describe un aparato para realizar las operaciones de los métodos. Dichos aparatos pueden construirse especialmente para los fines requeridos, o pueden comprender un ordenador de propósito general u otro dispositivo activado selectivamente o reconfigurado por un programa de ordenador almacenado en el ordenador. Los algoritmos y las visualizaciones presentados en este documento no están inherentemente relacionados con ningún ordenador ni otro aparato particular. Se pueden utilizar diversas máquinas de propósito general con programas de acuerdo con las enseñanzas de este documento. Alternativamente, puede resultar adecuada la construcción de un aparato más especializado para realizar los pasos de método requeridos. La estructura de un ordenador convencional de propósito general resultara aparente a partir de la descripción que se proporciona a continuación.

Además, la presente memoria descriptiva también describe implícitamente el algoritmo de un programa informático, en el sentido de que sería evidente para la persona experta en la técnica que las etapas individuales del método descrito en la presente memoria pueden ponerse en práctica mediante un código informático. El programa de ordenador no está destinado a limitarse a ningún lenguaje de programación particular ni a su implementación. Se apreciará que se puede utilizar una variedad de lenguajes de programación y codificación de los mismos para implementar las enseñanzas de la descripción contenidas en este documento. Además, el programa de ordenador no está destinado a limitarse a ningún flujo de control particular. Existen muchas otras variantes del programa de ordenador, que pueden utilizar diferentes flujos de control sin apartarse del alcance de la invención.

Además, uno o más de los pasos del programa informático pueden realizarse en paralelo en lugar de secuencialmente. Dicho programa de ordenador puede almacenarse en cualquier medio legible por ordenador. El medio legible por ordenador puede incluir dispositivos de almacenamiento tales como discos magnéticos u ópticos, chips de memoria u otros dispositivos de almacenamiento adecuados para interactuar con un ordenador de propósito general. El medio legible por ordenador también puede incluir un medio cableado tal como se ejemplifica en el sistema de Internet, o un medio inalámbrico (por ejemplo, wi-fi, dispositivo bluetooth y el sistema de teléfono móvil). Cuando se carga y ejecuta en un ordenador de propósito general, el programa de ordenador da como resultado un aparato que implementa los pasos del método preferido.

La invención también puede implementarse como módulos de hardware. Más en particular, en el sentido de hardware, un módulo es una unidad de hardware funcional diseñada para ser utilizada con otros componentes o módulos. Por ejemplo, un módulo puede implementarse utilizando componentes electrónicos discretos, o puede formar una parte de un circuito electrónico completo como por ejemplo un circuito integrado de aplicación específica (ASIC). Existen muchas otras posibilidades. Los expertos en la técnica apreciarán que el sistema también se puede implementar como una combinación de módulos de hardware y software.

Descripción General del Sistema de Encriptado de Ejemplo con el Token de Autenticación

La Fig. 1a) muestra un dibujo esquemático que ilustra un conjunto 10 para su uso en el encriptado y el acceso a datos protegidos, por ejemplo en un disco seguro virtual, de acuerdo con una forma de realización de ejemplo. El conjunto 10 comprende una ficha portátil 12 para conectarse a un ordenador central a través de un primer enlace de comunicación para encriptar y acceder a los datos protegidos en el ordenador central, y un dispositivo portátil de autenticación 14 asociado con la ficha 12. El dispositivo de autenticación

14 está configurado para conectarse a un dispositivo informático a través de un segundo enlace de comunicación para la auto autenticación y el proceso de recuperación.

La Fig. 1b) ilustra un diagrama de bloques esquemático de alto nivel de un ordenador central 100 conectado con la ficha portátil 12 utilizando el enlace de comunicación 120, de acuerdo con una forma de realización de ejemplo. El enlace de comunicación 120 representa el medio a través del cual se comunican los datos entre el token portátil 12 y el ordenador central 100 a través de la interfaz del token 140 y la interfaz del ordenador 130. El enlace de comunicación incluye, pero no se limita a, cualquier módulo de comunicación o medios tales como canales de radiofrecuencia (RF) o conexiones cableadas. El token portátil 12 podría ser cualquier dispositivo periférico, como por ejemplo una unidad flash USB, un teléfono móvil o incluso otro ordenador. El ordenador central 100 puede ser cualquier máquina informática, como un servidor, un ordenador de escritorio, un teléfono inteligente o un ordenador portátil. El ordenador central contiene un administrador de seguridad de datos (DSM) 150, que puede instalarse por separado, por ejemplo, desde un CD-ROM o puede instalarse desde el token 12 o a través de Internet.

La Fig. 2 es un diagrama de bloques esquemático de alto nivel que muestra algunos componentes importantes internos del token portátil 12 y el dispositivo de autenticación 14 de acuerdo con una forma de realización de ejemplo. El token 12 y el dispositivo de autenticación 14 contienen cada uno una memoria re-escribible no volátil 200, 201 respectivamente, un controlador integrado (EC) 210, 211 respectivamente, y la interfaz 140, 141 respectivamente con el ordenador.

La memoria no volátil 200 contiene elementos de datos como por ejemplo contraseña, valor de contador y clave de token y clave de lote de token. La contraseña se utiliza para controlar el acceso del usuario al token 12. El valor del contador puede ser un número pequeño entero positivo utilizado para controlar el número de intentos de contraseñas fallidos consecutivos. En una forma de realización, la clave de token es una clave secreta aleatoria utilizada para el encriptado y desencriptado de archivos bajo un algoritmo de encriptado de clave simétrica. La clave del lote del token es una clave secreta aleatoria que se utiliza para la clave del token o el encriptado y desencriptado de la clave de autenticación. La memoria no volátil 201 contiene elementos de datos como por ejemplo una clave de autenticación.

Volviendo a la Fig. 1b), antes de que se utilice un token 12 en un sistema informático, debe instalarse el DSM 150 y debe inicializarse el token 12. La ficha 12 está conectada al ordenador 100 y se introduce una contraseña de usuario para la ficha 12. A continuación, se genera la clave del token. Alternativamente, la clave del token se puede preinstalar de fábrica.

Claves de Emparejamiento

El dispositivo de autenticación 14 (Fig. 1a)) tiene una clave de autenticación exclusiva de emparejamiento con la clave de token. En una forma de realización, "emparejamiento" significa "igual", pero se observa que, en diferentes formas de realización, el "emparejamiento" puede incluir que una clave se puede emparejar con la otra utilizando, por ejemplo, un algoritmo para transformar una clave en la otra. La clave de autenticación exclusiva para el dispositivo de autenticación 14 se puede almacenar previamente en el dispositivo de autenticación 14 durante la producción o se puede generar y almacenar durante la instalación del usuario.

Ejemplo: Emparejamiento utilizando identificadores exclusivos separados

La asociación o emparejamiento del token 12 y el dispositivo de autenticación asociado 14 pueden implementarse utilizando identificadores exclusivos en el token 12 y en el dispositivo de autenticación 14, respectivamente. El par de identificadores exclusivos puede ser "igual", pero alternativamente puede configurarse de modo que un identificador exclusivo se pueda emparejar con el otro utilizando, por ejemplo, un algoritmo para transformar un identificador exclusivo en el otro. El par de identificadores exclusivos puede almacenarse previamente durante la producción o puede generarse y almacenarse durante la instalación del usuario.

En formas de realización de ejemplo, la asociación entre el token 12 y el dispositivo de autenticación 14 es exclusiva, es decir, se crea una asociación de uno a uno solamente entre el token 12 y el dispositivo de autenticación 14.

Ejemplo: Emparejamiento utilizando identificadores de varios a uno

En otra forma de realización de ejemplo, la asociación entre el token 12 y el dispositivo de autenticación 14 es una asociación muchos a uno entre una pluralidad de tokens 12 y el único dispositivo de autenticación 14.

Control de acceso

El DSM 150 realiza el control de acceso a datos seguros, por ejemplo, en un disco virtual seguro basado en cuatro eventos: conexión de token, extracción de token, inicio de sesión de usuario y cierre de sesión de usuario. A un usuario se le permite el acceso a los datos protegidos solamente si el token 12 está conectado y la contraseña de inicio de sesión es correcta. De lo contrario, los datos protegidos no son accesibles. Durante el acceso del usuario a los datos protegidos, el DSM 150 detecta constantemente si el token 12 está presente. Si el DSM 150 detecta que el token 12 ha sido eliminado del ordenador central, se le denegará de inmediato el acceso a los datos protegidos. La accesibilidad solo se restaura con la conexión del token 12 y el inicio de sesión satisfactorio del usuario.

Los datos se encriptan utilizando un algoritmo de encriptado de clave simétrica en una forma de realización de ejemplo.

Restablecimiento de contraseña

A continuación, se describirá cómo el dispositivo de autenticación 14 puede utilizarse ventajosamente para el proceso de autenticación antes de restablecer la contraseña en el token 12, por ejemplo para recuperar el acceso completo a los datos protegidos si el usuario ha olvidado la contraseña original, en un primer escenario

La Fig. 3a) muestra un diagrama esquemático que ilustra el proceso de autenticación utilizando el token 12 y el dispositivo de autenticación 14. En un ejemplo, el usuario presenta el token 12 junto con el dispositivo de autenticación 14 a un ordenador 300 en, por ejemplo, un centro de servicio, una estación del fabricante, una interfaz web de Internet del fabricante o un distribuidor autorizado. Este ordenador 300 también puede ser el ordenador central del usuario. El dispositivo de autenticación 14 y el token 12 están conectados al ordenador 300 a través de los respectivos enlaces de comunicación 304, 302. El token 12 y el dispositivo de autenticación 14 pueden estar conectados simultáneamente al ordenador 300, o pueden estar conectados en secuencia, por ejemplo, donde solo puede estar disponible una interfaz de comunicación para conectarse al ordenador 300. Un administrador de autenticación (AM) 306 se está ejecutando en el ordenador 300.

Ejemplo: Operación de emparejamiento antes del restablecimiento de contraseña

Tal como se ilustra en la Fig. 3b), el usuario solicita "restablecer la contraseña" en el paso 350, por ejemplo desde una lista de menú presentada en la pantalla del ordenador bajo el control del AM 306 que se ejecuta en el ordenador 300, en respuesta a la conexión del token 12 y el dispositivo de autenticación 14. Tras la confirmación de la solicitud, el dispositivo de autenticación 14 encripta su clave de autenticación en el paso 352, y envía la clave de autenticación encriptada al token 12, por ejemplo a través del AM 306, en el paso 354. Se pueden utilizar métodos tales como criptografía de clave secreta u otros métodos adecuados en formas de realización de ejemplo. Se observa que, de forma ventajosa, por lo tanto, el AM 306 en esta forma de realización de ejemplo no puede "ver" la clave de autenticación real.

A continuación, en el paso 356, el token 12 desencripta la clave de autenticación encriptada recibida desde el dispositivo de autenticación 14, para verificar la clave de autenticación en el paso 358. Si la clave de autenticación "coincide" con la clave del token almacenada en el token 12, entonces la coincidencia entre el dispositivo de autenticación 14 y el token 12 se establece de forma satosfactoria en esta forma de realización de ejemplo. El establecimiento satisfactorio del emparejamiento se comunica al AM 306. En una forma de realización alternativa, el token 12 puede realizar el encriptado de su clave de token y enviar la clave de token encriptada al dispositivo de autenticación 14 para el desencriptado y la verificación del emparejamiento. Tal como apreciará un experto en la materia, el resultado final, es decir, que el emparejamiento se verifique, puede ser ventajosamente el mismo en una forma de realización alternativa de este tipo.

A continuación, el AM 306 permitirá al usuario volver a introducir una nueva contraseña para el token 12. El AM 306 sustituirá la contraseña anterior del token con la nueva contraseña, en el paso 360 o restablecerá la contraseña a una contraseña predeterminada.

En consecuencia, solo si una persona presenta el token 12 y el dispositivo de autenticación 14 "coincidentes", se permitirá un restablecimiento de la contraseña. Esto puede superar ventajosamente los problemas asociados con las soluciones existentes descritas en la sección de antecedentes anterior. En una forma de realización alternativa, el AM 306 analiza el dispositivo de autenticación 14 y el token 12 para autenticar una asociación entre ellos. En otras palabras, el AM 306 determina automáticamente si el token 12 y el dispositivo de autenticación 14 "coinciden". Si lo hacen, esto sirve como evidencia de que la persona que presenta el token es la persona autorizada/propietaria del token 12. De lo contrario, se rechazará el restablecimiento de la contraseña.

En un ejemplo, el token 12 y el dispositivo de autenticación 14 que coinciden contienen una cadena de datos exclusiva idéntica, como la clave de token y la clave de autenticación correspondiente, respectivamente. El AM 306 comparará las cadenas de datos en el token 12 y en el dispositivo de autenticación 14. Cuando las dos cadenas son iguales, se establece una coincidencia. En otro ejemplo, las cadenas de datos en el token 12 y el dispositivo de autenticación 14 que coinciden podrían ser diferentes. En este caso, el AM 306 utilizará un algoritmo de autenticación para procesar las dos cadenas de datos para establecer si coinciden entre sí. Se pueden utilizar métodos como por ejemplo criptografía de clave secreta u otros métodos adecuados en formas de realización de ejemplo.

Si la autenticación de la asociación entre el token 12 y el dispositivo de autenticación 14 es satisfactoria, el AM 306, ya sea automáticamente o mediante la intervención del usuario, ejecuta una operación de restablecimiento de contraseña.

Tal como se ha mencionado anteriormente, los identificadores exclusivos almacenados en el token 12 y el dispositivo de autenticación 14 respectivamente se pueden utilizar en la verificación de la coincidencia entre el token 12 y el dispositivo de autenticación 14, de la misma manera que se describe para la coincidencia de claves anterior con referencia a la Fig. 3.

Duplicado del Encriptado de Token

A continuación, se describirá cómo el dispositivo de autenticación 14 puede utilizarse ventajosamente como evidencia de que la persona está "autorizada" antes de crear una ficha duplicada del token 12.

Con referencia a la Fig. 4a), en un ejemplo, el usuario presenta un token 15 "en blanco" junto con el dispositivo de autenticación 14 a un ordenador 400 en, por ejemplo, un centro de servicio, una estación del fabricante, una interfaz web de Internet del fabricante o un distribuidor autorizado. Un token 15 "en blanco" es un token que no está asociado con un token de seguridad (todavía) y, por ejemplo, no contiene la clave de token única, y que permite colocar una nueva clave de token exclusiva dentro. Se observa que un token normal también se puede convertir en un token "en blanco" eliminando la clave del token. Por ejemplo, el usuario conecta el token, introduce la contraseña para mostrar que es el propietario y a continuación elimina o sustituye la clave del token. En consecuencia, se puede utilizar un token normal en lugar de un token 15 "en blanco" en una forma de realización diferente.

El dispositivo de autenticación 14 y el token 15 están conectados al dispositivo informático 400 a través de los respectivos enlaces de comunicación 404, 402. El token 15 y el dispositivo de autenticación 14 pueden estar conectados simultáneamente al ordenador 400, o pueden estar conectados en secuencia, por ejemplo, donde solo puede estar disponible una interfaz de comunicación para conectarse al ordenador 400.

Tal como se ilustra en la Fig. 4b), el usuario elige crear una ficha duplicada en el paso 450, por ejemplo, desde una lista de menú presentada en la pantalla del ordenador bajo el control de la AM 406 que se ejecuta en el ordenador 800, en respuesta a la conexión del token en blanco 15 y el dispositivo de autenticación 14. Tras la confirmación de la solicitud, el dispositivo de autenticación 14 genera la clave de token coincidente de su clave de autenticación y encripta la clave de token en el paso 452. Se pueden utilizar métodos como por ejemplo criptografía de clave secreta u otros métodos adecuados en formas de realización de ejemplo.

La clave del token encriptada se envía al token 15 "en blanco", por ejemplo a través del AM 406, en el paso 454. El token 15 desencripta la clave de token recibida del dispositivo de autenticación 14 e instala la clave del token desencriptada, en el paso 456. En consecuencia, el token 15 "en blanco" se convierte ahora en un token que está emparejado, es decir, asociado con, el dispositivo de autenticación 14.

En una forma de realización alternativa, el AM 406 en el ordenador 400 analiza el dispositivo de autenticación 14 y genera la clave de token para el token 15. Esta clave de token se corresponde con la clave de autenticación 14 del dispositivo de autenticación, a continuación se introduce en el token 15 por parte del AM 406. El token 15 y el dispositivo de autenticación 14 ahora "coinciden", es decir, se convierten en un par asociado o emparejado. En este ejemplo, la creación de un token duplicado es para reemplazar un token dañado. En este caso, puede ser deseable que el AM 406 se aloje en un entorno autorizado.

Cuando el dispositivo de autenticación 14 también contiene un identificador exclusivo para la asociación con un token, el dispositivo de autenticación 14, o el AM 406 en la forma de realización alternativa, generan un identificador exclusivo coincidente para almacenar en el token 15 de la misma manera que la clave de token.

En los ejemplos descritos anteriormente con referencia a las Figuras 3 y 4, se supone que el usuario/propietario del token 12 mantiene de forma segura el dispositivo de autenticación 14, ya que no es necesario para un uso normal. En consecuencia, estar en posesión del dispositivo de autenticación 14 puede considerarse como evidencia de que la persona está "autorizada".

Re-Encriptar con Nueva Clave

Ejemplo: el dispositivo de autenticación vuelve a encriptar los datos

En otros casos, el usuario puede querer volver a encriptar sus datos protegidos que han sido encriptados por un token que se ha perdido. En este próximo ejemplo, el proceso para volver a encriptar los datos protegidos de modo que una ficha perdida ya no tenga acceso a estos datos se describe con referencia a las Figuras 5 a) y b), de acuerdo con una forma de realización.

Tal como se muestra en la Fig. 5a), el usuario conecta el dispositivo de autenticación 14 y el token 12 a, por ejemplo, el ordenador central 500, a través de unos enlaces de comunicación respectivos 504, 502. Este token 12 puede ser un nuevo token de sustitución de un token perdido. Tal como se ilustra en la Fig. 5b), el usuario introduce la contraseña del token en el paso 550, y se comprueba y verifica que la contraseña es correcta en el paso 552.

A continuación, el AM 506 acepta las instrucciones del usuario para cambiar la clave de autenticación y la clave de token y para volver a encriptar todos los archivos protegidos con la nueva clave de token, en el paso 554.

En el paso 556, los datos protegidos son desencriptados por el dispositivo de autenticación 14 usando la clave de autenticación actual. El dispositivo de autenticación 14 genera entonces una nueva clave de token y una clave de autenticación coincidente en el paso 558. El dispositivo de autenticación 14 vuelve a encriptar los datos utilizando la nueva clave de token en el paso 560.

El dispositivo de autenticación 14 reemplaza su antigua clave de autenticación con la clave de autenticación recién generada en el paso 562. La nueva clave del token es encriptada por el dispositivo de autenticación y enviada al token 12, por ejemplo a través del AM 506, en el paso 564. El token 12 desencripta la nueva clave de token recibida y sustituye la antigua clave de token con la nueva clave de token en el paso 566.

La clave del token y la clave de autenticación ahora han sido sustituidas por una versión más nueva y los archivos protegidos se han vuelto a encriptar con la nueva clave. Por consiguiente, la clave perdida o robada, para la cual el token 12 es la sustitución, por ejemplo, de forma ventajosa ya no podrá abrir los archivos protegidos.

Ejemplo: Nuevo token vuelve a encriptar los datos

En una forma de realización alternativa, el token 12 puede realizar las funciones de sustitución y reencriptación de claves del dispositivo de autenticación 14. Después de que los datos hayan sido desencriptados por el dispositivo de autenticación 14, el token de sustitución 12 vuelve a encriptar los datos con la nueva clave de token. Después de eso, el Token 12 encriptará su nueva clave de token y la enviará al dispositivo de autenticación 14. El dispositivo de autenticación 14 la desencripta y genera e instala una nueva clave de autenticación que coincide con la nueva clave de token. Tal como apreciará un experto en la materia, el resultado final, es decir, que la clave de token y la clave de autenticación hayan sido sustituidas por una versión más nueva y que los archivos protegidos se hayan vuelto a encriptar con la nueva clave, puede ser de forma ventajosa el mismo en una forma de realización alternativa de este tipo.

Ejemplo: el administrador de autorización vuelve a encriptar los datos

En una forma de realización alternativa, el usuario ordena al AM 506 volver a encriptar sus archivos de datos protegidos, el AM 506 generará una nueva clave de autenticación para el dispositivo de autenticación 14 y una nueva clave de token de emparejamiento para su token compatible 12, en esta forma de realización de ejemplo. Utilizando la antigua clave de autenticación, el AM 506 desencriptará los datos protegidos. A continuación volverá a encriptar los datos desencriptados utilizando la nueva clave de token. Por lo tanto, el token perdido o robado ahora no puede acceder a estos datos con su antigua clave de token. El AM 506 escribirá la nueva clave de autenticación en el dispositivo de autenticación 14 para sustituir la antigua, y la nueva clave de token en el token 12 para sustituir el antiguo token 12 ahora podrá acceder a los datos protegidos utilizando la nueva clave de token.

Acceso de solo lectura

A continuación, se describirá cómo el dispositivo de autenticación 14 se puede utilizar de forma ventajosa para el acceso de solo lectura a los datos protegidos con o sin requerir una contraseña de acuerdo con una forma de realización de ejemplo.

Con referencia a la Figura 6, si el dispositivo de autenticación 14 está conectado al ordenador central 600 a través del enlace de comunicación 604, el DSM 602 realiza un control de acceso de solo lectura a los datos protegidos en función del dispositivo de autenticación 14 y la eliminación del dispositivo de autenticación 14. Para permitir el acceso, el DSM 602 envía los datos encriptados al dispositivo de autenticación 14 para desencriptar los datos. Durante el acceso de solo lectura del usuario a los datos protegidos, el DSM 602 detecta constantemente si el dispositivo de autenticación 14 está presente. Si el DSM 602 detecta que el dispositivo de autenticación 14 ha sido eliminado del ordenador central 600, al usuario se le niega inmediatamente el acceso a los datos protegidos.

En una forma de realización alternativa, el DSM 602 lee y analiza la clave de autenticación desde el dispositivo de autenticación 14. Con la clave de autenticación, el DSM 602 puede derivar la clave del token para desencriptar los datos protegidos. En una forma de realización, la clave de autenticación del dispositivo de autenticación 14 es igual a la clave de token. A un usuario se le permite el acceso de solo lectura a los datos protegidos si el dispositivo de autenticación 14 está conectado. Durante el acceso de solo lectura del usuario a los datos protegidos, el DSM 602 detecta constantemente si el dispositivo de autenticación 14 está presente. Si el DSM 602 detecta que el dispositivo de autenticación 14 se ha eliminado del ordenador central 600, al usuario se le niega inmediatamente el acceso a los datos protegidos.

De ese modo, las formas de realización de ejemplo proporcionan ventajosamente que, en caso de que un usuario olvide la contraseña o pierda el token, el usuario todavía pueda leer los datos utilizando el dispositivo de autenticación 14.

Implementaciones y Variaciones de Ejemplo

En una forma de realización, se proporciona un dispositivo de auto autenticación para autenticar al usuario o propietario de un dispositivo de seguridad electrónico, en el que el dispositivo de recuperación de auto autenticación está separado del dispositivo de seguridad y está configurado para conectarse a un dispositivo informático a través de un primer enlace de comunicación para el proceso de autenticación, preferentemente para el proceso de autenticación y recuperación. El proceso de autenticación puede comprender la autenticación de una asociación entre el dispositivo de seguridad y el dispositivo de recuperación de auto autenticación. El proceso de autenticación puede comprender hacer coincidir una primera clave y/o un primer identificador exclusivo almacenado en el dispositivo de auto autenticación con una segunda clave y/o un segundo identificador exclusivo almacenado en el dispositivo de seguridad.

En una forma de realización, el dispositivo de auto autenticación está configurado para generar una tercera clave y / o un tercer identificador exclusivo para configurar otro dispositivo de seguridad tal como está asociado con el dispositivo de auto autenticación.

El dispositivo de auto autenticación se puede configurar para permitir el restablecimiento de una contraseña almacenada en el dispositivo de seguridad tras una autenticación satisfactoria.

El dispositivo de auto autenticación también puede configurarse para conectarse a un ordenador central a través de un segundo enlace de comunicación, para leer datos almacenados, por ejemplo, en un disco virtual protegido en el ordenador central. El dispositivo de auto autenticación también puede configurarse

para conectarse al ordenador central a través del segundo enlace de comunicación, para leer datos almacenados, por ejemplo, en el disco virtual protegido en el ordenador central con o sin necesidad de una contraseña.

En una forma de realización, el dispositivo de auto autenticación está configurado para desencriptar datos almacenados, por ejemplo, en un disco virtual protegido en un ordenador central, generando una cuarta clave y encriptando los datos utilizando la cuarta clave.

El dispositivo informático puede ser un ordenador central para el dispositivo de seguridad o un dispositivo informático que resida en uno o más de un grupo que consiste en un centro de servicio, una estación del fabricante, una interfaz web de Internet del fabricante o un distribuidor autorizado. El dispositivo de seguridad puede ser un token de encriptado de datos.

En una forma de realización, se proporciona un método de auto autenticación para autenticar al usuario o propietario de un dispositivo de seguridad electrónico, en que el método comprende conectar un dispositivo de auto autenticación independientemente del dispositivo de seguridad a un dispositivo informático a través de un primer enlace de comunicación para el proceso de autenticación, preferentemente para el proceso de autenticación y recuperación. El método puede comprender además conectar el dispositivo de seguridad al dispositivo informático a través de un segundo enlace de comunicación, para el proceso de autenticación. El proceso de autenticación puede comprender la autenticación de una asociación entre el dispositivo de seguridad y el dispositivo de auto autenticación. El proceso de autenticación puede comprender hacer coincidir una primera clave y/o un primer identificador exclusivo almacenado en el dispositivo de auto autenticación con una segunda clave y/o un segundo identificador exclusivo almacenado en el dispositivo de seguridad.

En una forma de realización, el método puede comprender además restablecer una contraseña de usuario almacenada en el dispositivo de seguridad tras la autenticación satisfactoria de la asociación entre el dispositivo de auto autenticación y el dispositivo de seguridad.

El proceso de autenticación puede comprender obtener una tercera clave y/o un tercer identificador exclusivo del dispositivo de auto autenticación para configurar un dispositivo de seguridad no asociado como asociado con el dispositivo de auto autenticación.

El método puede comprender además conectar el dispositivo de auto autenticación a un ordenador central mediante un tercer enlace de comunicación para leer datos almacenados, por ejemplo, en un disco virtual protegido en el ordenador central. La lectura de los datos almacenados, por ejemplo, en el disco virtual protegido en el ordenador central es con o sin necesidad de una contraseña.

En una forma de realización, el método comprende además desencriptar datos almacenados, por ejemplo, en un disco protegido virtual de un ordenador central; encriptar los datos desencriptados utilizando una nueva clave; y almacenar la nueva clave en el token y una clave de autenticación coincidente en el dispositivo de auto autenticación. El dispositivo de seguridad puede ser un token de encriptado de datos.

Un experto en la materia apreciará que pueden realizarse numerosas variaciones y/o modificaciones en la presente invención, tal como se muestra en las formas de realización específicas, sin apartarse del alcance de la invención tal como se describe ampliamente. Las presentes formas de realización, por lo tanto, deben considerarse en todos los aspectos como ilustrativas y no restrictivas. Además, la invención incluye cualquier combinación de características, en particular cualquier combinación de características en las reivindicaciones de la patente, incluso si la característica o combinación de características no se especifica explícitamente en las reivindicaciones de la patente o en las presentes formas de realización.

Por ejemplo, la funcionalidad del DSM y la AM descrita en las formas de realización de ejemplo puede implementarse en un Administrador de Control de Seguridad (SCM) en diferentes formas de realización.

Además, aunque las formas de realización se han descrito en el contexto de un token de seguridad para el encriptado de datos, se apreciará que la presente invención se puede aplicar a diferentes dispositivos electrónicos de seguridad tales como tarjetas de acceso de seguridad electrónicas a edificios o áreas seguras.

Como otro ejemplo, aunque que en las formas de realización descritas la ficha de seguridad se implementa como un único dispositivo portátil, se apreciará que la presente invención puede utilizarse junto con diferentes implementaciones de una ficha de seguridad. Por ejemplo, el token de seguridad se puede

implementar utilizando uno o más dispositivos que interactúan, que pueden interactuar de forma inalámbrica y / o cableada para realizar la funcionalidad de seguridad deseada. Los dispositivos pueden incluir uno o más de un dispositivo periférico como por ejemplo una unidad flash USB, un teléfono móvil o cualquier otra máquina / dispositivo informático.

Además, aunque en las formas de realización descritas la ficha de seguridad se implementa para el encriptado de datos utilizando un disco virtual, se apreciará que en diferentes formas de realización se puede implementar Encriptado de Archivo, Encriptado de Carpeta o Encriptado de Disco Completo, etc.

Reivindicaciones

1. Un dispositivo de auto autenticación (14) para el usuario o propietario de un dispositivo de seguridad electrónico (12), en que el dispositivo de auto autenticación (14) está separado del dispositivo de seguridad (12) y está configurado para conectarse a un dispositivo informático (300, 400, 500, 600) a través de un primer enlace de comunicación para el proceso de auto autenticación, y en que el dispositivo de auto autenticación (14) está configurado para permitir el restablecimiento de una contraseña de usuario almacenada en el dispositivo de seguridad (12) cuando se produce una auto autenticación satisfactoria sin requerir la introducción por parte del usuario de una contraseña de autorización.

2. El dispositivo de auto autenticación (14) tal como se reivindica en la reivindicación 1, en que el proceso de auto autenticación comprende hacer coincidir una primera clave y/o un primer identificador exclusivo almacenado en el dispositivo de auto autenticación (14) con una segunda clave y/o un segundo identificador exclusivo almacenado en el dispositivo de seguridad (12).

3. El dispositivo de auto autenticación (14) tal como se reivindica en cualquiera de las reivindicaciones 1 a 2, en que el dispositivo de auto autenticación (14) está configurado para generar una tercera clave y/o un tercer identificador exclusivo para configurar otro dispositivo de seguridad (15) tal como está asociado con el dispositivo de auto autenticación (14).

4. El dispositivo de auto autenticación (14) tal como se reivindica en cualquiera de las reivindicaciones 1 a 3, en que el dispositivo de auto autenticación (14) está configurado además para conectarse a un ordenador central (300, 400, 500, 600) a través de un segundo enlace de comunicación, para leer datos almacenados, por ejemplo, en un disco virtual protegido en el ordenador central (300, 400, 500, 600).

5. El dispositivo de auto autenticación (14) tal como se reivindica en la reivindicación 4, en que el dispositivo de auto autenticación (14) está configurado además para conectarse al ordenador central (300, 400, 500, 600) a través del segundo enlace de comunicación, para leer datos almacenados, por ejemplo, en el disco virtual protegido en el ordenador central (300, 400, 500, 600) sin requerir una contraseña.

6. El dispositivo de auto autenticación (14) tal como se reivindica en cualquiera de las reivindicaciones 1 a 5, en que el dispositivo de auto autenticación (14) está configurado para desencriptar datos almacenados, por ejemplo, en un disco virtual protegido en un ordenador central (300, 400, 500, 600), generando una cuarta clave y encriptando los datos utilizando la cuarta clave.

7. El dispositivo de auto autenticación (14) tal como se reivindica en cualquiera de las reivindicaciones 1 a 6, en que el dispositivo de seguridad (12) es un token de encriptado de datos.

8. Un método de auto autenticación para el usuario o propietario de un dispositivo de seguridad electrónico (12), en que el método comprende conectar un dispositivo de auto autenticación (14) separado del dispositivo de seguridad (12) a un dispositivo informático (300, 400, 500, 600) a través de un primer enlace de comunicación para el proceso de auto autenticación, y restaurar una contraseña de usuario almacenada en el dispositivo de seguridad (12) cuando se produce la autenticación satisfactoria de la asociación entre el dispositivo de auto autenticación (14) y el dispositivo de seguridad (12) sin requerir la introducción por parte del usuario de una contraseña autorizada.

9. El método tal como se reivindica en la reivindicación 8, en que el proceso de autenticación comprende autenticar una asociación entre el dispositivo de seguridad (12) y el dispositivo de auto autenticación (14).

10. El método tal como se reivindica en la reivindicación 9, en que el proceso de auto autenticación comprende hacer coincidir una primera clave y/o un primer identificador exclusivo almacenado en el dispositivo de auto autenticación (14) con una segunda clave y/o un segundo identificador exclusivo almacenado en el dispositivo de seguridad (12).

11. El método tal como se reivindica en cualquiera de las reivindicaciones 8 a 10, en que el proceso de auto autenticación comprende obtener una tercera clave y/o un tercer identificador exclusivo del dispositivo de auto autenticación (14) para configurar un dispositivo de seguridad no asociado (15) como asociado con el dispositivo de auto autenticación (14).

12. El método tal como se reivindica en cualquiera de las reivindicaciones 8 a 11, que comprende además conectar el dispositivo de auto autenticación (14) a un ordenador central (300, 400, 500, 600) a través de un tercer enlace de comunicación para leer datos almacenados, por ejemplo, en un disco virtual protegido en el ordenador central (300, 400, 500, 600).

13. El método tal como se reivindica en la reivindicación 12, en que la lectura de los datos almacenados, por ejemplo, en el disco virtual protegido en el ordenador central (300, 400, 500, 600) es sin la necesidad de una contraseña.

14. El método tal como se reivindica en cualquiera de las reivindicaciones 8 a 13, que comprende además:

desencriptar datos almacenados, por ejemplo, en un disco virtual protegido de un ordenador central (300, 400, 500, 600);
encriptar los datos desencriptados utilizando una nueva clave; y
almacenar la nueva clave en el dispositivo de seguridad (12) y una clave de autenticación coincidente en el dispositivo de auto autenticación (14).

15. El método tal como se reivindica en cualquiera de las reivindicaciones 8 a 14, en que el dispositivo de seguridad (12) es un token de encriptado de datos.

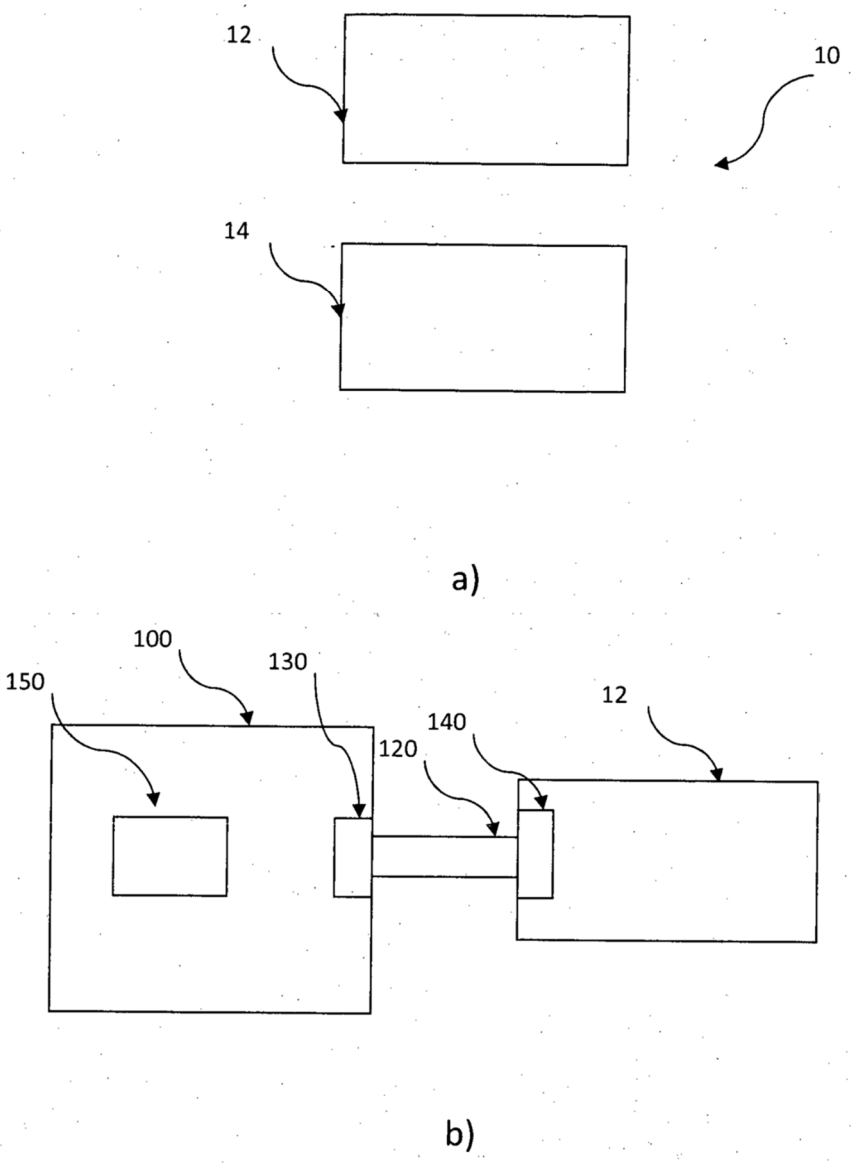


Figura 1

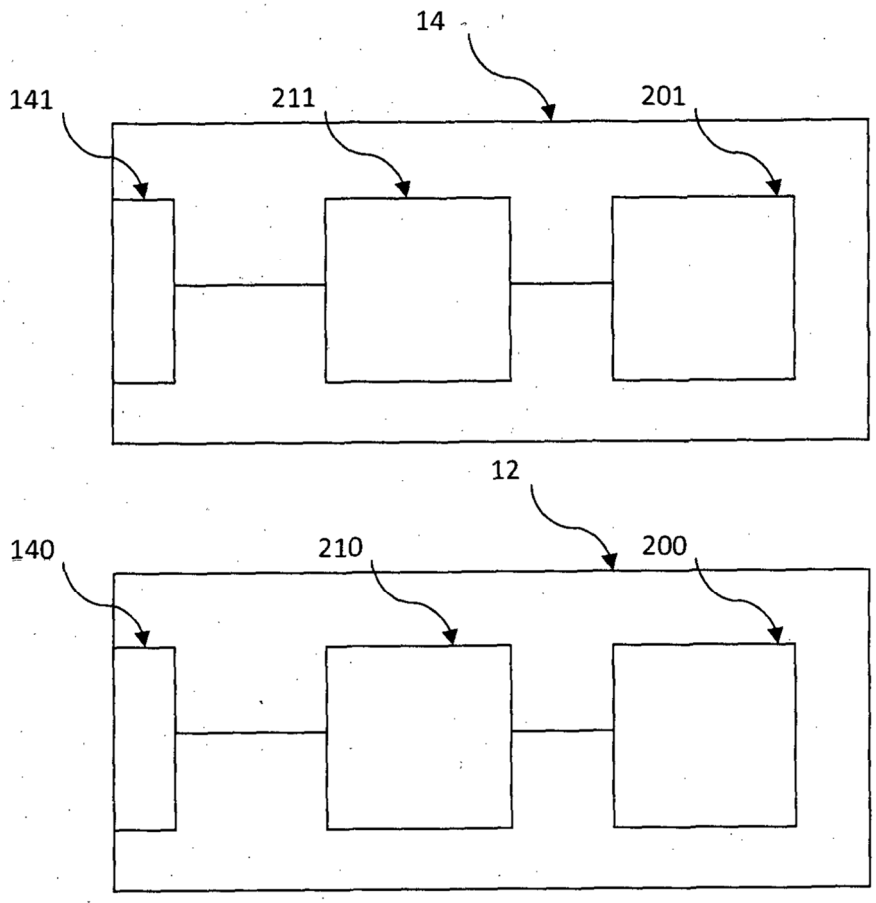
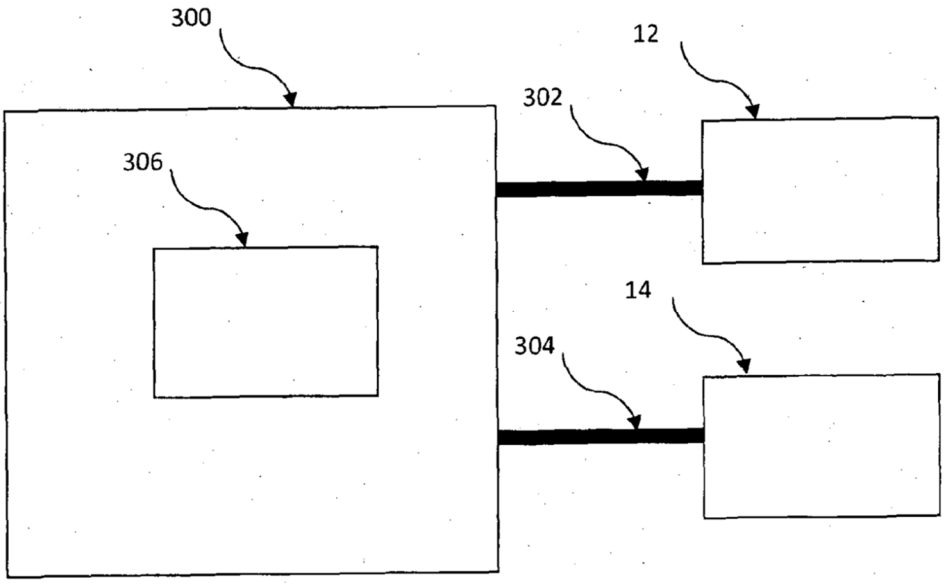
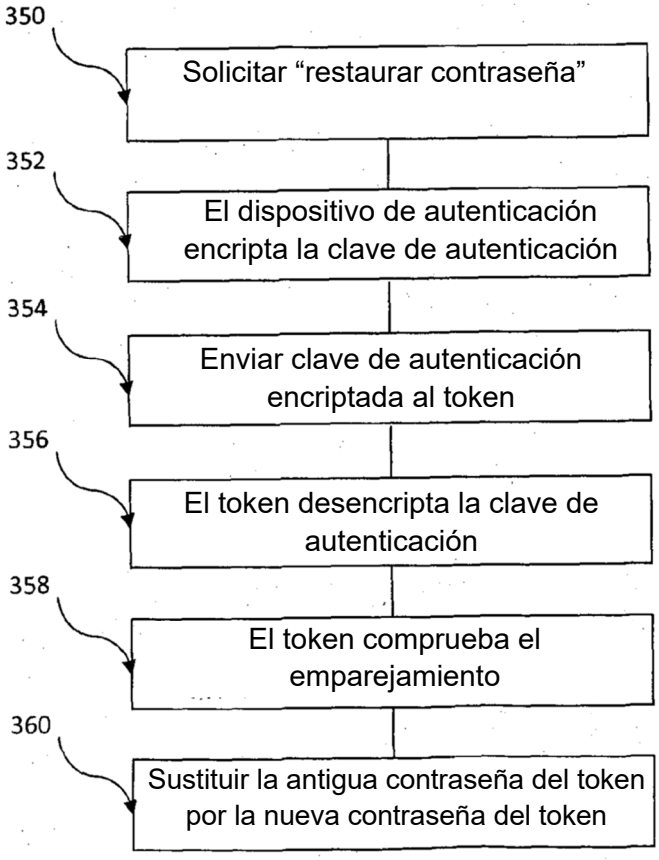


Figura 2

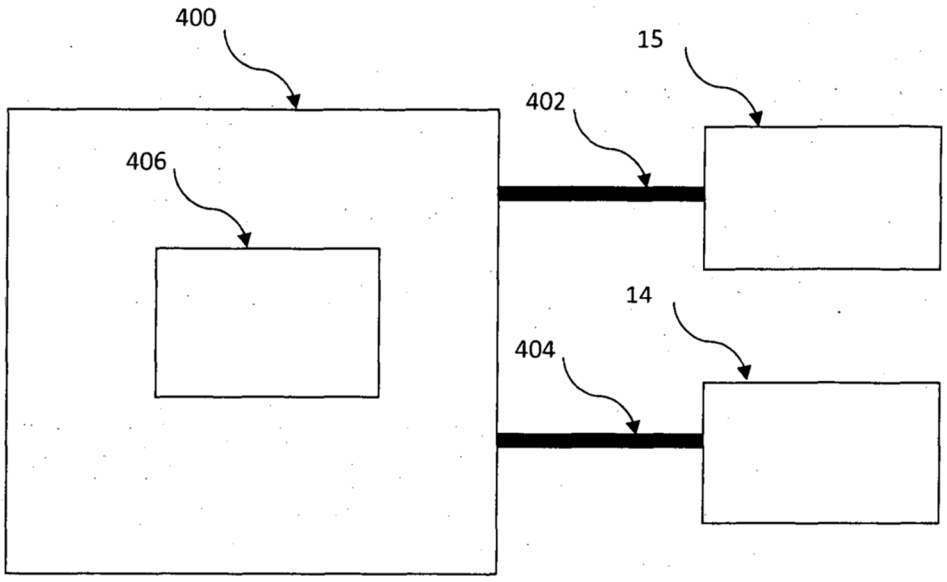

300
12
302
306
14
304

a)

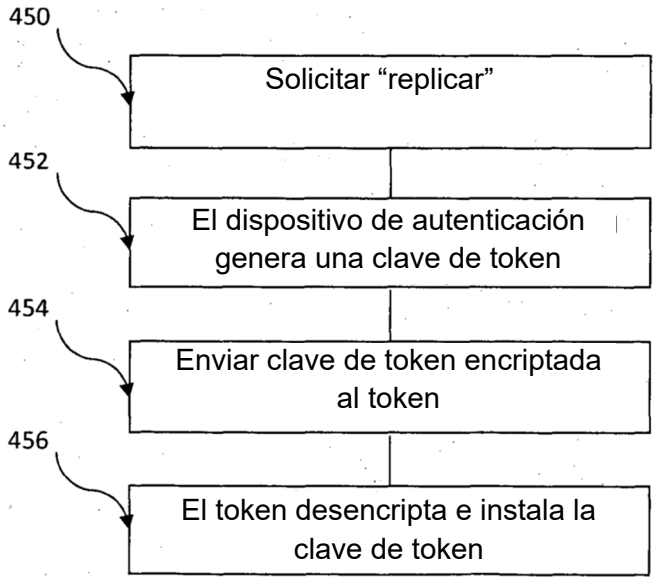

350
Solicitar “restaurar contraseña”
352
El dispositivo de autenticación encripta la clave de autenticación
354
Enviar clave de autenticación encriptada al token
356
El token desencripta la clave de autenticación
358
El token comprueba el emparejamiento
360
Sustituir la antigua contraseña del token por la nueva contraseña del token

b)

Figura 3


400
15
402
406
14
404

a)


450
Solicitar “replicar”
452
El dispositivo de autenticación genera una clave de token
454
Enviar clave de token encriptada al token
456
El token desencripta e instala la clave de token

b)

Figura 4

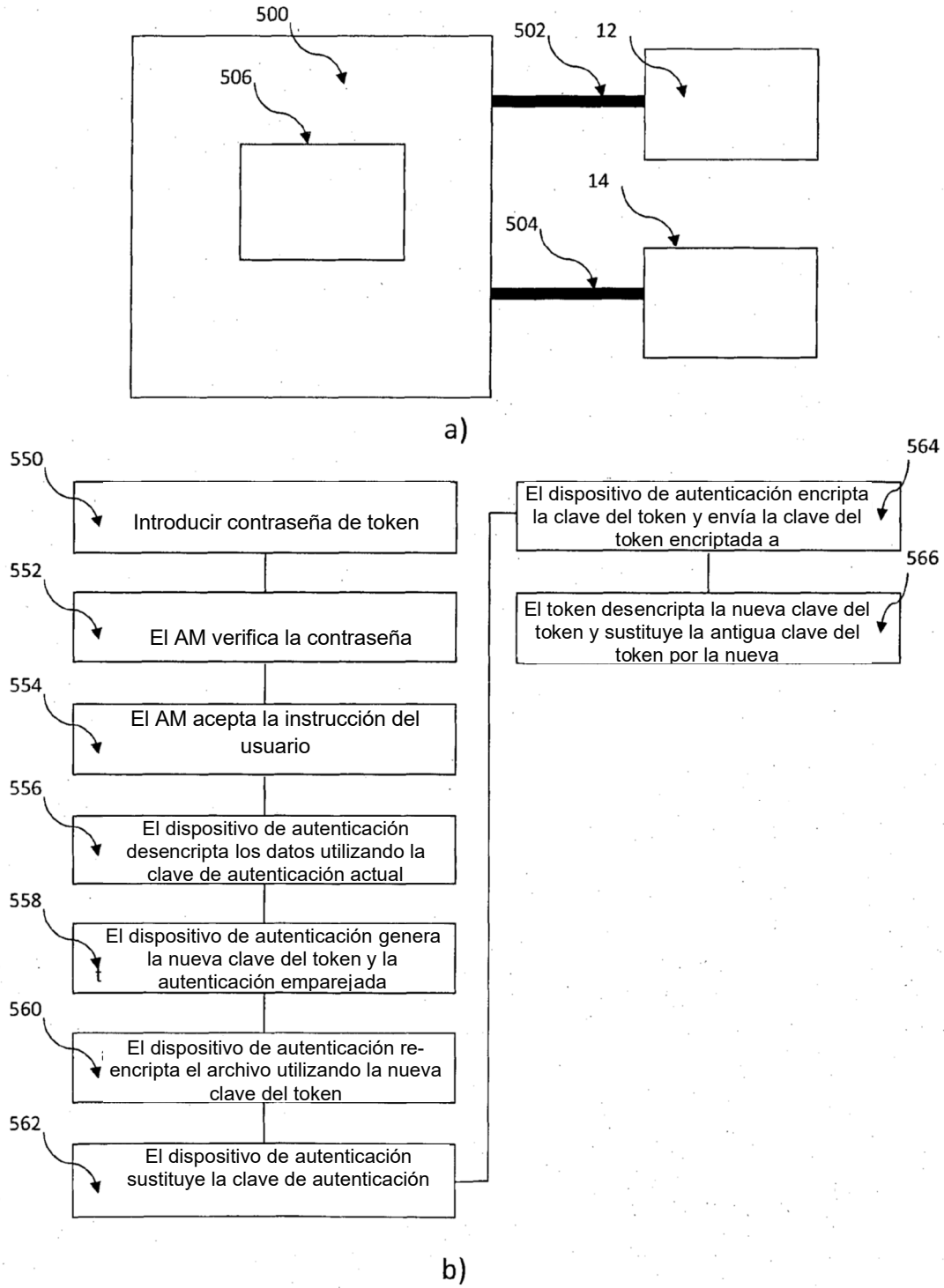

500
506
502
12
14
504
a)
550
Introducir contraseña de token
552
El AM verifica la contraseña
554
El AM acepta la instrucción del usuario
556
El dispositivo de autenticación desencripta los datos utilizando la clave de autenticación actual
558
El dispositivo de autenticación genera la nueva clave del token y la autenticación emparejada
560
El dispositivo de autenticación re-encripta el archivo utilizando la nueva clave del token
562
El dispositivo de autenticación sustituye la clave de autenticación
564
El dispositivo de autenticación encripta la clave del token y envía la clave del token encriptada a
566
El token desencripta la nueva clave del token y sustituye la antigua clave del token por la nueva
b)

Figura 5

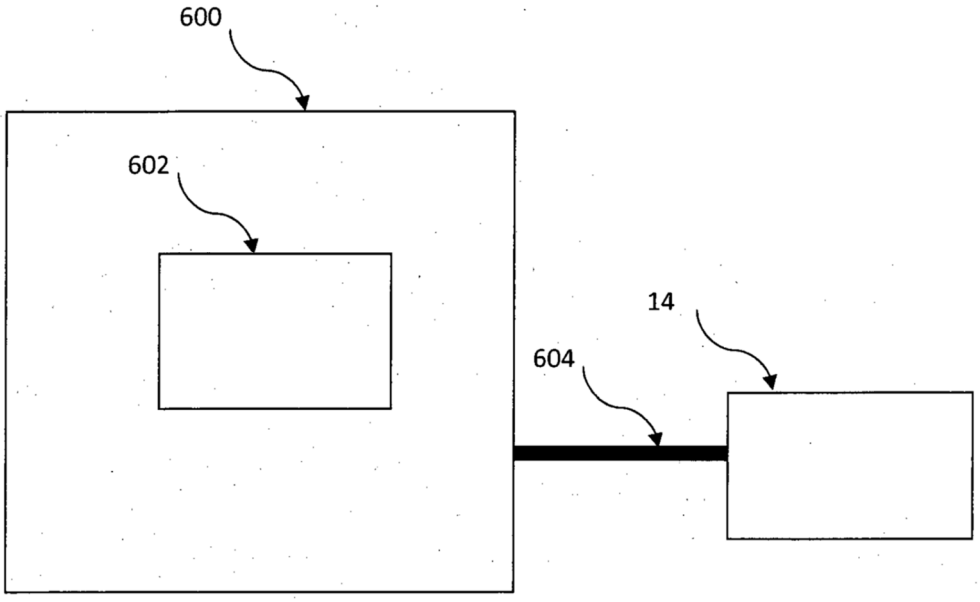


Figura 6