(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 703 707**

(51) Int. CI.:

H04L 29/06 (2006.01)
G07C 9/00 (2006.01)
H04L 9/00 (2006.01)
G06Q 30/00 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **16.06.2016 E 16174818 (1)**

(97) Fecha y número de publicación de la concesión europea: **03.10.2018 EP 3258660**

(54) Título: **Dispositivo de protección y llave electrónica y método para usar los mismos**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
12.03.2019

(73) Titular/es:

RIDDLE & CODE GMBH (100.0%)
ORBI Tower Thomas-Klestil-Platz 13
1030 Wien, AT

(72) Inventor/es:

FÜRSTNER, THOMAS

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Dispositivo de protección y llave electrónica y método para usar los mismos

La invención concierne a un método para suspender una protección física de un objeto lograda mediante un dispositivo de protección y un set, es decir, un grupo de dispositivos asociados, para proteger físicamente un objeto. El objeto puede ser un producto o paquete de un producto o generalmente cualquier artículo físico o colección de elementos que se pueden proteger físicamente. En particular el objeto puede ser una caja de seguridad, un recipiente, una puerta, el arranque de un coche o una válvula en cierta posición.

Cuando se comercia con productos, el vendedor usualmente tiene que asegurar a un cliente potencial que los productos en oferta son auténticos (p. ej. originarios de un cierto productor) y obtenidos legalmente. Este es especialmente el caso con productos caros y/o sensibles de otro modo. Por lo tanto los vendedores típicamente obtendrán los productos que ofrecen de fuentes en las que confían y los bloquean en un área protegida, p. ej. una caja de seguridad. Los clientes tienen que confiar en que los vendedores adopten medidas apropiadas para asegurar la autenticidad y la legalidad de los productos ofrecidos. En la práctica los clientes a menudo confiarán en la reputación de vendedores particulares. Únicamente en circunstancias excepcionales los clientes tienen medios adicionales para verificar por sí mismos la autenticidad y legalidad de los productos a mano. Por ejemplo ese puede ser el caso para productos vendidos junto con certificados de propiedad expedida por el productor original o un tercero certificador. Los propios certificados pueden contener medidas antifalsificación para seguridad y para combatir certificados falsos. Al ofrecer el producto junto con el certificado, los vendedores pueden probar que los productos son auténticos (porque el certificado es expedido por el productor original reafirmado) y obtenido legalmente (de otro modo el certificado original no estaría disponible).

Sin embargo el planteamiento tradicional que se ha descrito anteriormente tiene fallos porque los clientes a menudo no pueden verificar si el producto en oferta y el certificado están realmente asociados. A fin de probar una asociación, los productos a menudo son marcados con un número de serie o rasgo de identificación similar, que entonces se refleja en el certificado. Pero los números de serie se pueden reproducir, debilitando así la fiabilidad y así la seguridad de la asociación sugerida.

La solicitud de patente americana US2016/0036788 A1 describe un método para hacer funcionar con seguridad una cerradura electrónica por un dispositivo de usuario mediante una conexión inalámbrica. Se proporciona un identificador de cerradura a un servidor de gestión a fin de asociar la cerradura con el usuario. El servidor de gestión genera un perfil de usuario que permite más tarde que la cerradura realice autenticación de respuesta a desafío del dispositivo de usuario.

El documento "Blockchains and Smart Contracts for the Internet of Things" de Christis Konstantinos et al. describe que las cerraduras electrónicas Slock.it se pueden desbloquear con un dispositivo que lleva un símbolo apropiado, dicho símbolo se puede llevar en la cadena de bloques de Ethereum desde los propietarios de dichas cerraduras inteligentes.

Un objeto de la presente invención es proporcionar medios técnicos para establecer autenticidad y propiedad (legal) de mercancías, productos y otros objetos o elementos protegibles físicamente.

La invención resuelve esto objeto con un método de la clase enunciada al comienzo que comprende las siguientes etapas:

se establece una primera conexión de datos entre el dispositivo de protección y una llave electrónica;

se establece una segunda conexión de datos entre un dispositivo anfitrión y la llave electrónica;

se establece una tercera conexión de datos entre el dispositivo anfitrión y un directorio de transacción pública;

el dispositivo anfitrión recibe por medio de la segunda conexión de datos al menos una primera clave pública, una segunda clave pública, una tercera clave pública y un identificador combinado firmado que incorpora al menos la primera clave pública y la segunda clave pública, en donde el identificador combinado firmado se firma con una tercera clave privada, dicha tercera clave privada se asocia criptográficamente con la tercera clave pública;

el dispositivo anfitrión solicita por medio de la tercera conexión de datos una búsqueda de transacciones asociadas con el identificador combinado firmado dentro del directorio de transacción pública;

el dispositivo anfitrión autentica al menos la primera clave pública y la segunda clave pública usando una firma del identificador combinado firmado y usando la tercera clave pública;

el dispositivo anfitrión autentica el dispositivo de protección usando la primera clave pública;

el dispositivo anfitrión autentica la llave electrónica usando la segunda clave pública;

si la búsqueda del directorio de transacciones produce al menos una transacción y la primera clave pública y la segunda clave pública son auténticas y el dispositivo de protección es auténtico y la llave electrónica es auténtica, el

dispositivo anfitrión envía una petición de desbloqueo a la llave electrónica por medio de la segunda conexión de datos;

la llave electrónica recibe la petición de desbloqueo y como reacción envía una orden de desbloqueo por medio de la primera conexión de datos que controla un accionador del dispositivo de protección para suspender la protección física del objeto protegido.

La presente método suspende una protección física de un objeto lograda por un dispositivo de protección si y únicamente si se ha encontrado que el propio dispositivo de protección así como una llave electrónica separada son auténticos y están asociados entre sí. Usa claves asociadas criptográficamente o "parejas de claves", que se usan comúnmente en criptografía asimétrica (criptografía de clave pública). La asociación criptográfica entre una clave pública y una clave privada se expresa por el hecho de que un mensaje (es decir, información) encriptado usando la clave pública únicamente puede ser desencriptado usando la clave privada asociada respectiva y viceversa. A diferencia de los certificados en papel, la asociación entre la llave electrónica y el dispositivo de protección se puede establecer y verificar criptográficamente, de manera que la falsificación de la asociación es imposible para todas finalidades prácticas. Además la autenticidad del producto se establece por la autenticación de las claves públicas recibidas desde el dispositivo de protección y la llave electrónica sobre la base de la firma de un tercero de confianza, p. ej. un asegurador o un signatario muy conocidos. Correspondientemente el fallo en autenticar el dispositivo de protección y/o la llave electrónica es en efecto similar a la ausencia global del dispositivo de protección y la llave electrónica. En ambas circunstancias la autenticidad del producto no puede ser acreditada y probablemente tiene que ser denegada.

El identificador combinado firmado sirve como certificado público de la asociación del producto protegido por el dispositivo de protección con la llave electrónica y la del tercero de confianza (así como opcionalmente el productor y/o un script de contrato). Como tal se publica en un directorio de transacción pública y se le interroga sobre acceso al dispositivo de protección. Preferiblemente el directorio actúa como almacenamiento de una sola escritura, lo que significa que está protegido contra modificación y eliminación de transacciones. Sin embargo las transacciones pueden ser sustituidas por transacciones posteriores "que consumen" transacciones anteriores, en donde la transacción posterior únicamente es válida si es despejada por partes autorizadas por la transacción anterior consumida. Al buscar en el directorio de transacción pública las transacciones asociadas con el identificador combinado, se puede establecer si la asociación documentada por la correspondiente transacción ha sido revocada y/o sustituida eficazmente por una transacción posterior válida, que corresponde a una nueva asociación (p. ej. con una llave electrónica diferente). Esto tiene la ventaja adicional sobre certificados tradicionales en papel de que, p. ej., se pueden restablecer de una forma localizable certificados perdidos. Como medida de seguridad adicional, las transacciones contienen una firma producida por el signatario, que se puede usar para identificar transacciones ilegítimas además del esquema de protección proporcionado por el propio directorio de transacciones.

Correspondientemente y con las mismas ventajas, la presente invención resuelve el objeto anterior con un set de la clase enunciada al comienzo que comprende:

un dispositivo de protección que tiene un accionador controlable para acoplar y liberar protección física de un objeto y

una llave electrónica asociada con el dispositivo de protección,

en donde el dispositivo de protección comprende una memoria interna y una interfaz para establecer una primera conexión de datos a la llave electrónica, en donde la memoria interna del dispositivo de protección almacena al menos una primera clave privada,

en donde la llave electrónica comprende una memoria interna, una primera interfaz para establecer una primera conexión de datos al dispositivo de protección y una segunda interfaz para establecer una segunda conexión de datos a un dispositivo anfitrión, en donde la memoria interna de la llave electrónica almacena al menos una segunda clave privada, una tercera clave pública y un identificador combinado firmado,

en donde el identificador combinado firmado incorpora al menos una primera clave pública, que se asocia criptográficamente con la primera clave privada, y una segunda clave pública, que se asocia criptográficamente con la segunda clave privada, y

en donde el identificador combinado firmado se firma con una tercera clave privada, que se asocia criptográficamente con la tercera clave pública.

Preferiblemente las etapas para autentificar al menos la primera clave pública y la segunda clave pública mediante el dispositivo anfitrión usando la firma del identificador combinado firmado y usando la tercera clave pública son:

el dispositivo anfitrión computa un identificador combinado de al menos la primera clave pública y la segunda clave pública;

el dispositivo anfitrión compara el identificador combinado computado con el identificador combinado firmado;

el dispositivo anfitrión verifica la firma del identificador combinado firmado con la tercera clave pública;

el dispositivo anfitrión autentica al menos la primera clave pública y la segunda clave pública si los dos identificadores combinados comparados coindicen y la verificación de la firma tiene éxito. La computación del identificador combinado sigue un algoritmo predeterminado, cuyo resultado es reproducible y sigue a un formato fijado. El formato fijado del identificador combinado asegura que el identificador combinado computado de cualquier posible combinación de claves públicas válidas se pueda usar para identificar una transacción en el directorio de transacción pública. El método de computación para computar el identificador combinado se elige así para que corresponda a los requisitos formales del directorio de transacción pública. Al firmar el identificador combinado, la parte que controla la tercera clave privada (es decir, el signatario o firmante) certifica la autenticidad de ambas claves públicas, primera y segunda, así como la asociación legitima entre las dos y así entre el dispositivo de protección (que controla la primera clave privada) y la llave electrónica (que controla la segunda clave privada).

A fin de determinar si un dispositivo de protección dado es auténtico, se puede verificar si ciertamente está en posesión y control de la primera clave privada. En particular las etapas para autentificar el dispositivo de protección mediante el dispositivo anfitrión pueden ser de la siguiente manera:

el dispositivo anfitrión envía un desafío aleatorio al dispositivo de protección por medio de la segunda conexión de datos desde el dispositivo anfitrión a la llave electrónica y desde allí además por medio de la primera conexión de datos al dispositivo de protección;

el dispositivo de protección firma el desafío aleatorio usando una primera clave privada, que se asocia criptográficamente con la primera clave pública y se almacena en una memoria interna del dispositivo de protección;

el dispositivo de protección envía la firma del desafío aleatorio al dispositivo anfitrión por medio de la primera conexión de datos a la llave electrónica y desde allí por medio de la segunda conexión de datos al dispositivo anfitrión;

el dispositivo anfitrión verifica la firma con la primera clave pública y autentica el dispositivo de protección si la verificación tiene éxito. Como el contenido del desafío aleatorio es desconocido por adelantado, el dispositivo de protección únicamente puede producir una firma válida del desafío aleatorio después de su generación y únicamente si está en posesión de la primera clave privada entre la generación del desafío aleatorio y la respuesta al dispositivo anfitrión.

De manera similar y con las mismas ventajas, las etapas para autentificar la llave electrónica mediante el dispositivo anfitrión pueden ser de la siguiente manera:

el dispositivo anfitrión envía un desafío aleatorio a la llave electrónica por medio de la segunda conexión de datos;

la llave electrónica firma el desafío aleatorio usando una segunda clave privada, que se asocia criptográficamente con la segunda clave pública y se almacena en una memoria interna de la llave electrónica;

la llave electrónica envía la firma del desafío aleatorio al dispositivo anfitrión por medio de la segunda conexión de datos;

el dispositivo anfitrión verifica la firma con la segunda clave pública y autentica la llave electrónica si la verificación tiene éxito.

En una realización preferida de la invención, la llave electrónica comprende además un script de contrato almacenado que se puede usar para hacer la suspensión de la protección dependiente de condiciones previas adicionales. A este efecto el método puede incluir las etapas de que la llave electrónica recibe la petición de desbloqueo y como reacción ejecuta un script de contrato almacenado en una memoria interna de la llave electrónica, en donde el script de contrato evalúa al menos una condición para desbloquear el dispositivo de protección, en donde la llave electrónica envía la orden de desbloqueo únicamente si el script de contrato se ejecuta con éxito y se satisface la al menos una condición del script de contrato. El script de contrato puede evaluar por ejemplo una condición sobre la base de la fecha y hora actuales, p. ej. si ha trascurrido cierto término predefinido codificado en el script de contrato. También puede evaluar una condición sobre la base de la ubicación actual del dispositivo de protección conforme es adquirido por medio de un sensor de ubicación (un dispositivo GPS o similar).

Correspondientemente la memoria interna de la parte de llave electrónica del presente set puede además almacenar un script de contrato como el definido anteriormente.

Preferiblemente y a fin de proporcionar un acoplamiento del dispositivo de protección a un script de contrato específico, la memoria interna del dispositivo de protección puede además almacenar una firma de un script de contrato firmado con la segunda clave privada.

Como alternativa o adicionalmente la asociación mutua entre la llave electrónica y el dispositivo de protección se puede asegurar además si la memoria interna de la llave electrónica almacena además una firma del script de contrato firmado con la primera clave privada.

Puede ser útil evitar la reutilización del dispositivo de protección, en particular cuando el dispositivo de protección se usa para garantizar la condición o el contenido del objeto protegido. En este caso, la llave electrónica se puede configurar para permitir una y únicamente una autenticación exitosa, de manera que una parte que realiza la autenticación puede estar segura de que el objeto protegido no ha sido alterado en el tiempo después de la transacción certificada por la llave electrónica y el dispositivo de protección y antes de la presente autenticación. Para proporcionar estas ventajas e inutilizar la llave electrónica y/o el dispositivo de protección después de un uso de una vez, el presente método puede comprender además las etapas de que, después de que la llave electrónica envía la orden de desbloqueo, invalida o restablece su memoria interna y/o la memoria interna del dispositivo de protección.

Ventajosamente dentro del presente método el dispositivo de protección recibe la segunda clave pública y una copia firmada de un script de contrato (preferiblemente el script de contrato almacenado en la llave electrónica mencionado antes) por medio de la primera conexión de datos, carga una copia local almacenada del script de contrato desde una memoria interna del dispositivo de protección, firma la copia local con la primera clave privada, compara la copia autofirmada resultante del script de contrato con la copia firmada recibida del script de contrato y suspende la protección física del objeto protegido únicamente si los scripts de contrato firmados comparados son idénticos. Al autenticar la petición de desbloqueo de esta manera se puede asegurar que únicamente solicitudes de desbloqueo legitimas realmente dan como resultado la suspensión de la protección física y se ignoran solicitudes de desbloqueo falsas.

La seguridad del presente método se puede aumentar si la memoria interna del dispositivo de protección y/o de la llave electrónica es una memoria a prueba de manipulación. Al usar una memoria a prueba de manipulación, se puede evitar la manipulación y en particular la extracción de las claves privadas almacenadas dentro del dispositivo de protección y la llave electrónica. Si un atacante tuviera éxito al extraer la clave privada de la llave electrónica, en principio podría replicar la llave electrónica y de ese modo falsificar con éxito la propiedad del objeto o producto protegidos.

En una realización específica de la invención, la primera conexión de datos puede ser una conexión de datos cableada, preferiblemente usando el protocolo I2C, y/o la segunda conexión de datos puede ser una conexión de datos inalámbrica, preferiblemente una conexión Bluetooth. La conexión de datos cableada entre el dispositivo de protección y la llave electrónica tiene la ventaja de que es más fácil de implementar, menos cara y al mismo tiempo más fiable que una conexión inalámbrica. También el dispositivo de protección consume menos energía cuando está esperando un aporte únicamente mediante una conexión cableada. Además la intercepción de la conexión cableada durante la autenticación es más fácil de detectar, mejorando de ese modo la seguridad del método. Dado que la llave electrónica no se conecta al objeto o mercancías protegidos, es más fácil recargar y así puede soportar una conexión inalámbrica para una interacción más cómoda con el dispositivo anfitrión, especialmente cuando el último no tiene ninguna interfaz de datos cableada (p. ej. un teléfono inteligente).

El directorio de transacción pública es preferiblemente accesible en línea, es decir, por medio de internet. Por consiguiente la tercera conexión de datos se puede establecer por medio de internet a fin de acceder a la mayoría de datos de transacción recientes.

Beneficia a la fiabilidad y la independencia de la presente método cuando el directorio de transacción pública es un directorio público distribuido, preferiblemente la cadena de bloques de Bitcoin. Esto también promueve la trasparencia y a través de la trasparencia la confianza y en última instancia la adopción de la presente invención. La cadena de bloques de Bitcoin es particularmente muy idónea ya que proporciona estándares de seguridad ampliamente aceptados y una estructura de confianza resistente a falsificación o manipulación de las transacciones registradas.

Haciendo referencia ahora a los dibujos, en donde las figuras tienen la finalidad de ilustrar la presente invención y no a efectos de limitar la misma,

la figura 1 muestra esquemáticamente los elementos implicados para suspender una protección física de un objeto según la presente invención;

la figura 2 muestra esquemáticamente una vista más detallada de un dispositivo de protección según la figura 1;

la figura 3 muestra esquemáticamente una vista más detallada de una llave electrónica según la figura 1;

la figura 4 muestra un diagrama de flujo de las etapas generales realizadas antes de suspender la protección física según el método inventivo;

la figura 5 muestra más en detalle las etapas realizadas para autentificar las claves públicas del dispositivo de protección y la llave electrónica;

la figura 6 muestra más en detalle las etapas realizadas para autentificar el dispositivo de protección o la llave electrónica;

la figura 7 muestra más en detalle las etapas realizadas por la llave electrónica para implementar un script de contrato;

la figura 8 muestra más en detalle las etapas realizadas por el dispositivo de protección a fin de autenticar una petición de desbloqueo.

La figura 1 muestra un objeto 1, que está protegido físicamente por un dispositivo de protección 2. En la presente realización el objeto 1 es una caja, p. ej. que encierra un producto; como alternativa el objeto puede ser el propio producto. El dispositivo de protección 2 tiene un accionador controlable 3 para acoplar y liberar la protección física del objeto 1. Para lograr la protección física del objeto 1, el dispositivo de protección 2 comprende un yugo 4 para formar un candado.

En el presente ejemplo, el objeto 1 está protegido porque el yugo 4 que atraviesa montajes 5 sobre el objeto 1 está trabado en una posición de cierre por medio del dispositivo de protección 2 y específicamente el accionador 3. A fin de suspender la protección física del objeto 1, se puede controlar el accionador 3 para liberar el yugo 4 de su posición de trabado y entonces puede ser retirado de los montajes 5. Una vez liberados los montajes 5 del yugo 4, la caja que forma el objeto 1 puede ser abierta, es decir, el objeto ya no está protegido físicamente.

El dispositivo de protección 2 se conecta a una llave electrónica 6 mediante una conexión de datos cableada 7. La conexión de datos cableada 7 se forma entre un primer conector de resorte 8 del dispositivo de protección 2 y un segundo conector de resorte 9 de la llave electrónica 6. La conexión de datos cableada 7 soporta el protocolo de bus informático I2C. La llave electrónica 6 también se conecta con un dispositivo anfitrión 10, p. ej. un teléfono inteligente, tableta u ordenador personal, mediante una conexión de datos inalámbrica 11. La conexión de datos inalámbrica 11 puede ser una conexión Bluetooth; son concebibles otros protocolos o estándares de comunicación inalámbrica, p. ej. una conexión WiFi o NFC. Finalmente el dispositivo anfitrión 10 se conecta a un directorio de transacción pública en línea 12 mediante una conexión de datos mezclada 13, parcialmente inalámbrica y parcialmente cableada, establecida por medio de internet. Por simplicidad, la figura 1 muestra únicamente una primera sección de la conexión de datos mezclada 13, que se indica como conexión inalámbrica. El directorio de transacción pública 12 se indica como única base de datos. En la práctica, la base de datos se conecta a múltiples bases de datos adicionales distribuidas, que forman juntas un directorio público distribuido.

Juntos, el dispositivo de protección 2 y la llave electrónica 6 forman un set 14 para proteger físicamente el objeto 1.

La estructura y la funcionalidad del dispositivo de protección 2 se muestran más en detalle en la figura 2. Como se ha mencionado anteriormente, el dispositivo de protección 2 comprende el accionador 3 y el conector de resorte 8. El conector de resorte 8 se conecta a un microcontrolador 15. El microcontrolador 15 se conecta a un circuito integrado criptográfico (CI-Cripto) 16, p. ej. "ATECC508A" de Atmel Corporation o un dispositivo similar. El CI-Cripto 16 se conecta a un circuito integrado de comunicación inalámbrica 17, en particular a un CI-NFC, p. ej. "NT3H1201" de NXP Semiconductors. El CI-Cripto y el CI-NFC se montan sobre una placa de circuitos flexible y se configuran para comunicarse usando el protocolo de bus informático I2C. Además el CI-Cripto 16 se conecta a un relé 18 para controlar el accionador 3. El accionador 3 se puede conmutar entre un estado cerrado y un estado abierto. El accionador 3 comprende medios de impulsión, tales como un electromotor, un resorte mecánico, un elemento piezoeléctrico y/o un electroimán. Los componentes del dispositivo de protección 2 se pueden alimentar ya sea por medio de la llave electrónica 6 conectada al conector de resorte 8 o por medio de un campo de inducción de un lector NFC (no se muestra) por medio del CI-NFC 17.

El conector de resorte 8 del dispositivo de protección 2 puede ser sustituido o combinado con un conector de tarjeta inteligente o un conector inalámbrico, tal como una antena NFC y circuito integrado, para proporcionar una conexión con la llave electrónica 6 y/o el dispositivo anfitrión 10.

El CI-NFC 17 del dispositivo de protección 2 almacena una clave pública de curva elíptica asociada con la llave electrónica 6, una copia de un contrato futuro inteligente y un enlace a una aplicación de teléfono móvil para controlar el dispositivo de protección 2 y la llave electrónica 6, para ser usado con la validación, en una memoria interna a prueba de manipulación. La llave electrónica 6 se asocia así con el dispositivo de protección 2 porque el dispositivo de protección 2 dependerá de la clave pública almacenada y validará la llave electrónica 6 únicamente si puede probar su posesión de la correspondiente clave privada. El CI-NFC 17 proporciona una interfaz inalámbrica alternativa para teléfonos móviles al proceso de validación como se esboza más adelante.

La estructura y la funcionalidad de la llave electrónica 6 se muestran más en detalle en la figura 3. El conector de resorte 9 de la llave electrónica 6 se conecta a un CI-Cripto 19. El CI-Cripto 19 puede ser un "ATECC508A" de Atmel Corporation. El CI-Cripto 19 se conecta a un microcontrolador 20 (MCU), p. ej. "Atmega256rfr2" o "AtSAMD21" de Atmel Corporation. El MCU 20 puede incluir un módulo IEEE 802.15.4 (WPAN) para soportar una conexión de red con el dispositivo anfitrión 10 mediante la conexión inalámbrica 11. El MCU 20 se conecta a un módulo de comunicación inalámbrica 21, en particular un módulo Bluetooth, p. ej. "Bluetooth Low Energy breakout board" de Adafruit Industries, LLC, o un módulo NFC.

El MCU 20 se conecta al módulo de comunicación inalámbrica 21 por medio de protocolo SPI (MISO, MOSI, SCLK, SS) y al CI-Cripto 19 por medio de protocolos I2C. El MCU habla a los componentes del dispositivo protector por medio de una conexión de bus informático I2C mediante la conexión cableada 7. La llave electrónica 6 también alimenta el dispositivo de protección 2 a través de la conexión cableada 7. La llave electrónica usa Modo de Anuncio de Bluetooth

del módulo de comunicación inalámbrica 21 para conectarse a dispositivos anfitriones 10, tales como teléfonos móviles y ordenadores, para manejar los procesos de validación. Como el módulo de comunicación inalámbrica 21 se implementa como transpondedor dinámico (el MCU también puede leer/escribir en el módulo de comunicación inalámbrica 21), durante la validación o como resultado de la validación, se pueden reescribir datos en el módulo de comunicación inalámbrica 21.

El conector de resorte 9 de la llave electrónica 6 puede ser sustituido o combinado con un conector de tarjeta inteligente o un conector inalámbrico, tal como una antena NFC y circuito integrado, para proporcionar una conexión con el dispositivo de protección 2 y/o el dispositivo anfitrión 10.

El dispositivo anfitrión 10 comprende un módulo de comunicación inalámbrica (no se muestra) para establecer la conexión inalámbrica 11 y comunicarse con la llave electrónica 6. El dispositivo anfitrión 10 puede acceder y ejecutar una aplicación especializada de programa para realizar un proceso de validación junto con la llave electrónica 6 y el dispositivo de protección 2 a fin de suspender la protección física del objeto 1 y hacer accesible el objeto 1.

Las etapas de un método preferido para suspender la protección física del objeto 1 se esbozan en conexión con la figura 4. En una primera etapa 22, se establece la conexión de datos cableada 7 entre el dispositivo de protección 2 y la llave electrónica 6 cableando los conectores de resorte 8, 9. La llave electrónica 6 anuncia disponibilidad para una conexión inalámbrica ya sea permanentemente o únicamente cuando se conecta al dispositivo de protección 2. El dispositivo anfitrión 10 establece la conexión de datos inalámbrica 11 a la llave electrónica 6 (etapa 23). Entonces (etapa 24) el dispositivo anfitrión recibe de la llave electrónica 6 por medio de la conexión de datos inalámbrica 11 una clave pública del dispositivo de protección, una clave pública de la llave electrónica y una clave pública de un signatario así como identificador combinado firmado que incorpora al menos las claves públicas del dispositivo de protección 2 y la llave electrónica 6. El identificador combinado firmado se firma con una clave privada del signatario, que está asociado criptográficamente con su clave pública. La información recibida desde la llave electrónica 6 se almacena en una memoria interna de la llave electrónica 6 dentro del MCU 20. Es proporcionada por el MCU 20 al dispositivo anfitrión 10 cuando se establece la conexión de datos inalámbrica 11.

Una vez el dispositivo anfitrión 10 tiene acceso al identificador combinado, establece o usa una conexión de datos mezclada 13 preestablecida para acceder al directorio de transacción pública 12 (etapa 25). Específicamente solicita por medio de la conexión de datos mezclada 13 una búsqueda de transacciones asociadas con el identificador combinado firmado dentro del directorio de transacción pública 12. Durante esta petición el directorio de transacción pública 12 realiza la búsqueda solicitada y devuelve todas las transacciones que coinciden con el identificador proporcionado.

El dispositivo anfitrión 10 autentica (etapa 26) las claves públicas recibidas del dispositivo de protección 2 y la llave electrónica 6 evaluando la transacción recibida desde el directorio de transacción pública 12 y usando la firma del identificador combinado firmado y verificando esa firma con la clave pública del signatario. Las etapas particulares realizadas mediante el dispositivo anfitrión 10 para autenticar las dos claves públicas se muestran en la figura 5. Primero (etapa 27), el dispositivo anfitrión espera y evalúa una respuesta desde el directorio de transacción pública 12. Si no hay transacción registrada que coincida con el identificador combinado proporcionado, se encuentra que el último es inválido y falla la autenticación de las claves públicas. De otro modo (etapa 27') el dispositivo anfitrión 10 computa y de ese modo reproduce el identificador combinado a partir de las dos claves públicas. Entonces (etapa 28) compara el identificador combinado computado con el identificador combinado firmado y almacena el resultado de esta comparación. En la siguiente etapa (etapa 29), el dispositivo anfitrión verifica la firma del identificador combinado firmado proporcionado con la clave pública del signatario. Específicamente el dispositivo anfitrión 10 computa un hash del identificador combinado computado, encripta la firma proporcionada con la clave pública y compara el hash resultante de la encriptación con la hash previamente computado. Finalmente (etapa 30) el dispositivo anfitrión 10 autentica positivamente la dos claves públicas si coinciden los dos identificadores combinados comparados y coinciden los hashes comparados. De otro modo falla la autenticación y termina el procedimiento de validación (véase la figura 4).

Una vez se encuentra que las claves públicas son auténticas, el dispositivo anfitrión 10 procede (etapa 31) para autenticar el dispositivo de protección 2 usando la clave pública - autenticada - del dispositivo de protección. Las etapas particulares realizadas por el dispositivo anfitrión 10 para autenticar el dispositivo de protección 2 se muestran en la figura 6. En particular, para autentificar el dispositivo de protección 2 mediante el dispositivo anfitrión 10, el dispositivo anfitrión 10 primero (etapa 32) envía un desafío aleatorio al dispositivo de protección 2. El desafío es una cadena de bytes o letras prácticamente impredecibles generada usando un generador de número aleatorio. Tras la generación, este desafío se trasmite desde el dispositivo anfitrión 10 a la llave electrónica 6 y es reenviado por la llave electrónica 6 al dispositivo de protección 2. El dispositivo de protección 2 firma (etapa 33) el desafío aleatorio recibido desde el dispositivo anfitrión 10 usando una clave privada incrustada en el dispositivo de protección 2, es decir, almacenada en una memoria interna a prueba de manipulación del dispositivo de protección 2. Esta clave privada se asocia criptográficamente con la clave pública del dispositivo de protección 2, que el dispositivo anfitrión 10 ya ha recibido de la llave electrónica 6 y autenticado. Específicamente el dispositivo de protección 2, usando el CI-Cripto 16, encripta el desafío recibido con la clave privada y envía la firma resultante del desafío aleatorio de nuevo al dispositivo anfitrión 10, de nuevo por medio de la llave electrónica 6. El dispositivo anfitrión 10 verifica (etapa 34) la firma recibida desde el dispositivo de protección 2 con la clave pública previamente autenticada del dispositivo de protección al

desencriptar la firma recibida con la clave pública y comparar el resultado con el desafío generado inicialmente. Si (etapa 35) los desafíos coinciden, la verificación de la firma tiene éxito y el dispositivo anfitrión 10 autentica positivamente el dispositivo de protección 2.

Cuando el dispositivo de protección 2 ha sido autenticado con éxito, el dispositivo anfitrión 10 autentica la llave electrónica 6 (etapa 36 en la figura 4). La autenticación de la llave electrónica 6 es similar a la autenticación del dispositivo de protección 2. Por lo tanto se hace referencia a la descripción anterior y la figura 6, que se aplica análogamente a la autenticación de la llave electrónica 6.

Una vez se ha encontrado que tanto el dispositivo de protección 2 como la llave electrónica 6 son auténticos sobre la base de las claves públicas auténticas, el dispositivo anfitrión 10 envía (etapa 37) una petición de desbloqueo a la llave electrónica 6 por medio de la conexión de datos inalámbrica 11.

Como se muestra en la figura 7, la llave electrónica 6, tras recibir la petición de desbloqueo desde el dispositivo anfitrión 10 (etapa 38), como reacción ejecuta (etapa 39) un script de contrato. El script de contrato se almacena en una memoria interna de la llave electrónica 6, en particular una memoria interna del MCU 20, que también interpreta y ejecuta el script de contrato. El contenido del script de contrato se puede asegurar mediante firmas mutuas del dispositivo de protección 2 y la llave electrónica 6, que pueden ser intercambiadas y verificadas por la llave electrónica 6 antes de la ejecución del script de contrato. Al ejecutar el script de contrato, la llave electrónica 6 evalúa una condición para desbloquear el dispositivo de protección 2 codificado dentro del script de contrato. La llave electrónica 6 compara entonces (etapa 40) el resultado de esta evaluación con un resultado positivo esperado. Si esta comparación resulta en una coincidencia, la llave electrónica envía (etapa 41) una orden de desbloqueo por medio de la conexión de datos cableada 7 al dispositivo de protección 2. La orden de desbloqueo se firma con la clave privada de la llave electrónica 6 y se envía junto con la clave pública de la llave electrónica 6 y una copia del script de contrato almacenado firmado con la clave privada del dispositivo de protección 6 (es decir, la firma se crea durante la inicialización del dispositivo de protección y llave electrónica y se almacena dentro de la llave electrónica).

Opcionalmente, se indica mediante la etapa 42 en la figura 7, la llave electrónica 6 invalida o restablece su memoria interna y/o la memoria interna del dispositivo de protección 2 después o al mismo tiempo de enviar la orden de desbloqueo (etapa 41).

Como se muestra más en detalle en la figura 8, el dispositivo de protección 2 recibe (etapa 43) junto con la orden de desbloqueo la clave pública de la llave electrónica 6 y el script de contrato firmado por medio de la conexión de datos cableada 7. A fin de asegurar que el dispositivo de protección 2 únicamente ejecuta órdenes de desbloqueo legítimas, el dispositivo de protección 2 verifica si una orden de desbloqueo recibida procede de una llave electrónica de confianza al realizar la siguiente validación de la orden de desbloqueo recibida y script de contrato firmado. Carga (etapa 44) una copia local almacenada del script de contrato desde su memoria interna. Entonces firma (etapa 45) la copia local del script de contrato con su clave privada. Al comparar el script de contrato autofirmado resultante con el script de contrato firmado recibido, el dispositivo de protección 2 valida (etapa 46) el script de contrato firmado recibido. Si los dos son idénticos, se encuentra que el script de contrato firmado recibido es válido. De otro modo se encuentra que el script de contrato firmado recibido es inválido y se cancela el procedimiento de desbloqueo. Únicamente cuando la validación del script de contrato firmado recibido es exitosa, el dispositivo de protección 2 desencadena el procedimiento de desbloqueo y suspende la protección física del objeto protegido al controlar (etapa 47) el accionador 3 del dispositivo de protección 2 para que suspenda la protección física del objeto protegido 1.

A fin de ser usado en el proceso de validación y autenticación que se ha descrito anteriormente, el dispositivo de protección 2 y la llave electrónica 6 se inicializan durante un proceso inicialización.

Se asume que ya existen como requisitos previos de este proceso de inicialización la pareja de claves del signatario, una pareja de claves opcional de un productor y una pareja de claves opcional de un futuro propietario. Entonces en una primera etapa, se usan los CI-Cripto 16, 19 de la llave electrónica 6 y el dispositivo de protección 2 para generar una pareja de claves respectiva de los dos dispositivos 2, 6. Tras la generación, las claves privadas se almacenan con seguridad en una memoria interna a prueba de manipulación y las claves públicas son accesibles. Entonces, usando todas las claves públicas implicadas, el identificador combinado es computado y firmado por el signatario para obtener el identificador combinado firmado. Este identificador combinado firmado es trasmitido entonces a la llave electrónica 6 y almacenado en su memoria interna. Adicionalmente se envía una transacción al directorio de transacción pública, por ejemplo la cadena de bloques de Bitcoin. Esta transacción puede trasferir por ejemplo una pequeña cantidad de Bitcoins desde una dirección controlada por el signatario a una dirección derivada del identificador combinado, certificando de ese modo la legitimidad del último. En este caso el identificador combinado puede ser una dirección multifirma computada a partir de las claves públicas del dispositivo de protección, de la llave electrónica, del signatario, opcionalmente del productor original de un producto y opcionalmente de un hash de script de contrato. Como medida de seguridad adicional, en la transacción se puede incrustar una firma del identificador combinado generada por el signatario. La llave electrónica 6 y el dispositivo de protección 2 almacenan ambos la clave pública del signatario en una zona de datos protegida para validación futura. Adicionalmente también pueden almacenar la clave pública del productor original. Si se usa un script de contrato, se pueden intercambiar versiones firmadas del script de contrato entre la llave electrónica 6 y el dispositivo de protección 2 para seguridad adicional. Específicamente, el script de contrato puede ser modificado con hash y firmado dos veces. Un script de contrato firmado con hash con la clave

privada de la llave electrónica se escribe a la memoria del dispositivo de protección y un script de contrato firmado con hash con la clave privada del dispositivo de protección se escribe a la memoria de la llave electrónica. Entontes se bloquean los CI-Cripto 16, 19 de la llave electrónica 6 y el dispositivo de protección 2, lo que significa que ya no se pueden sobrescribir las claves y firmas almacenadas. Dicha llave electrónica 6 y dispositivo de protección 2 preparados son entregados entontes al productor, que puede aplicar el dispositivo de protección 2 a un objeto 1 para protegerlo y activar/bloquear el dispositivo de protección 2 sobre el objeto 1 antes de distribuir el objeto protegido a vendedores o consumidores.

REIVINDICACIONES

1. Método para suspender una protección física de un objeto (1) lograda por un dispositivo de protección (2), que comprende las siguientes etapas:

se establece una primera conexión de datos entre el dispositivo de protección (2) y una llave electrónica (6);

se establece una segunda conexión de datos entre un dispositivo anfitrión (10) y la llave electrónica (6);

se establece una tercera conexión de datos entre el dispositivo anfitrión (10) y un directorio de transacción pública (12);

el dispositivo anfitrión (10) recibe por medio de la segunda conexión de datos al menos una primera clave pública, una segunda clave pública, una tercera clave pública y un identificador combinado firmado que incorpora al menos la primera clave pública y la segunda clave pública, en donde el identificador combinado firmado se firma con una tercera clave privada, dicha tercera clave privada se asocia criptográficamente con la tercera clave pública;

el dispositivo anfitrión (10) solicita por medio de la tercera conexión de datos una búsqueda de transacciones asociadas con el identificador combinado firmado dentro del directorio de transacción pública (12);

el dispositivo anfitrión (10) autentica al menos la primera clave pública y la segunda clave pública usando una firma del identificador combinado firmado y usando la tercera clave pública;

el dispositivo anfitrión (10) autentica el dispositivo de protección (2) usando la primera clave pública;

el dispositivo anfitrión (10) autentica la llave electrónica (6) usando la segunda clave pública;

si la búsqueda del directorio de transacciones (12) produce al menos una transacción y la primera clave pública y la segunda clave pública son auténticas y el dispositivo de protección (2) es auténtico y la llave electrónica (6) es auténtica, el dispositivo anfitrión (10) envía una petición de desbloqueo a la llave electrónica (6) por medio de la segunda conexión de datos;

la llave electrónica (6) recibe la petición de desbloqueo y como reacción envía una orden de desbloqueo por medio de la primera conexión de datos que controla un accionador (3) del dispositivo de protección (2) para suspender la protección física del objeto protegido (1).

2. Método según la reivindicación 1, caracterizado por que las etapas para autentificar al menos la primera clave pública y la segunda clave pública mediante el dispositivo anfitrión (10) usando la firma del identificador combinado firmado y usando la tercera clave pública son:

el dispositivo anfitrión (10) computa un identificador combinado de al menos la primera clave pública y la segunda clave pública;

el dispositivo anfitrión (10) compara el identificador combinado computado con el identificador combinado firmado;

el dispositivo anfitrión (10) verifica la firma del identificador combinado firmado con la tercera clave pública;

el dispositivo anfitrión (10) autentica al menos la primera clave pública y la segunda clave pública si los dos identificadores combinados comparados coindicen y la verificación de la firma tiene éxito.

3. Método según la reivindicación 1 o 2, caracterizado por que las etapas para autentificar el dispositivo de protección (2) mediante el dispositivo anfitrión (10) son:

el dispositivo anfitrión (10) envía un desafío aleatorio al dispositivo de protección (2) por medio de la segunda conexión de datos desde el dispositivo anfitrión a la llave electrónica (6) y desde allí además por medio de la primera conexión de datos al dispositivo de protección (2);

el dispositivo de protección (2) firma el desafío aleatorio usando una primera clave privada, que se asocia criptográficamente con la primera clave pública y se almacena en una memoria interna del dispositivo de protección (2);

el dispositivo de protección (2) envía la firma del desafío aleatorio al dispositivo anfitrión (10) por medio de la primera conexión de datos a la llave electrónica (6) y desde allí por medio de la segunda conexión de datos al dispositivo anfitrión (10);

el dispositivo anfitrión (10) verifica la firma con la primera clave pública y autentica el dispositivo de protección (2) si la verificación tiene éxito.

4. Método según una de las reivindicaciones anteriores, caracterizado por que las etapas para autentificar la llave electrónica (6) mediante el dispositivo anfitrión (10) son:

el dispositivo anfitrión (10) envía un desafío aleatorio a la llave electrónica (6) por medio de la segunda conexión de datos;

la llave electrónica (6) firma el desafío aleatorio usando una segunda clave privada, que se asocia criptográficamente con la segunda clave pública y se almacena en una memoria interna de la llave electrónica (6);

la llave electrónica (6) envía la firma del desafío aleatorio al dispositivo anfitrión (10) por medio de la segunda conexión de datos;

el dispositivo anfitrión (10) verifica la firma con la segunda clave pública y autentica la llave electrónica si la verificación tiene éxito.

5. Método según una de las reivindicaciones anteriores, caracterizado por que la llave electrónica (6) recibe la petición de desbloqueo y como reacción ejecuta un script de contrato almacenado en una memoria interna de la llave electrónica (6), en donde el script de contrato evalúa al menos una condición para desbloquear el dispositivo de protección (2), en donde la llave electrónica (6) envía la orden de desbloqueo únicamente si el script de contrato se ejecuta con éxito y se satisface la al menos una condición del script de contrato.

6. Método según una de las reivindicaciones anteriores, caracterizado por que después de que la llave electrónica (6) envía la orden de desbloqueo, invalida o restablece su memoria interna y/o la memoria interna del dispositivo de protección (2).

7. Método según una de las reivindicaciones anteriores, caracterizado por que el dispositivo de protección (2):

recibe la segunda clave pública y una copia firmada de un script de contrato por medio de la primera conexión de datos,

carga una copia local almacenada del script de contrato desde una memoria interna del dispositivo de protección (2),

firma la copia local con la primera clave privada,

compara la copia autofirmada resultante del script de contrato con la copia firmada recibida del script de contrato y

suspende la protección física del objeto protegido (1) únicamente si los scripts de contrato firmados comparados son idénticos.

8. Método según una de las reivindicaciones 3 a 7, caracterizado por que la memoria interna del dispositivo de protección (2) y/o de la llave electrónica (6) es una memoria a prueba de manipulación.

9. Método según una de las reivindicaciones anteriores, caracterizado por que la primera conexión de datos es una conexión de datos cableada, preferiblemente usando el protocolo I2C, y/o la segunda conexión de datos es una conexión de datos inalámbrica, preferiblemente una conexión Bluetooth.

10. Método según una de las reivindicaciones anteriores, caracterizado por que la tercera conexión de datos se establece por medio de internet.

11. Método según una de las reivindicaciones anteriores, caracterizado por que el directorio de transacción pública (12) es un directorio público distribuido, preferiblemente la cadena de bloques de Bitcoin.

12. Set (14) para proteger físicamente un objeto (1) que comprende:

un dispositivo de protección (2) que tiene un accionador controlable (3) para acoplar y liberar protección física de un objeto (1) y

una llave electrónica (6) asociada con el dispositivo de protección (2),

en donde el dispositivo de protección (2) comprende una memoria interna y una interfaz para establecer una primera conexión de datos a la llave electrónica (6), en donde la memoria interna del dispositivo de protección (2) almacena al menos una primera clave privada,

en donde la llave electrónica (6) comprende una memoria interna, una primera interfaz para establecer una primera conexión de datos al dispositivo de protección (2) y una segunda interfaz para establecer una segunda conexión de datos a un dispositivo anfitrión (10), en donde la memoria interna de la llave electrónica (6) almacena al menos una segunda clave privada, una tercera clave pública y un identificador combinado firmado,

en donde el identificador combinado firmado incorpora al menos una primera clave pública, que se asocia criptográficamente con la primera clave privada, y una segunda clave pública, que se asocia criptográficamente con la segunda clave privada, y

en donde el identificador combinado firmado se firma con una tercera clave privada, que se asocia criptográficamente

con la tercera clave pública.

13. El set (14) según la reivindicación 12, caracterizado por que la memoria interna de la llave electrónica (6) almacena además un script de contrato.

14. El set (14) según la reivindicación 13, caracterizado por que la memoria interna del dispositivo de protección (2) almacena además una firma de un script de contrato firmado con la segunda clave privada.

15. El set (14) según la reivindicación 13 o 14, caracterizado por que la memoria interna de la llave electrónica (6) almacena además una firma del script de contrato firmado con la primera clave privada.

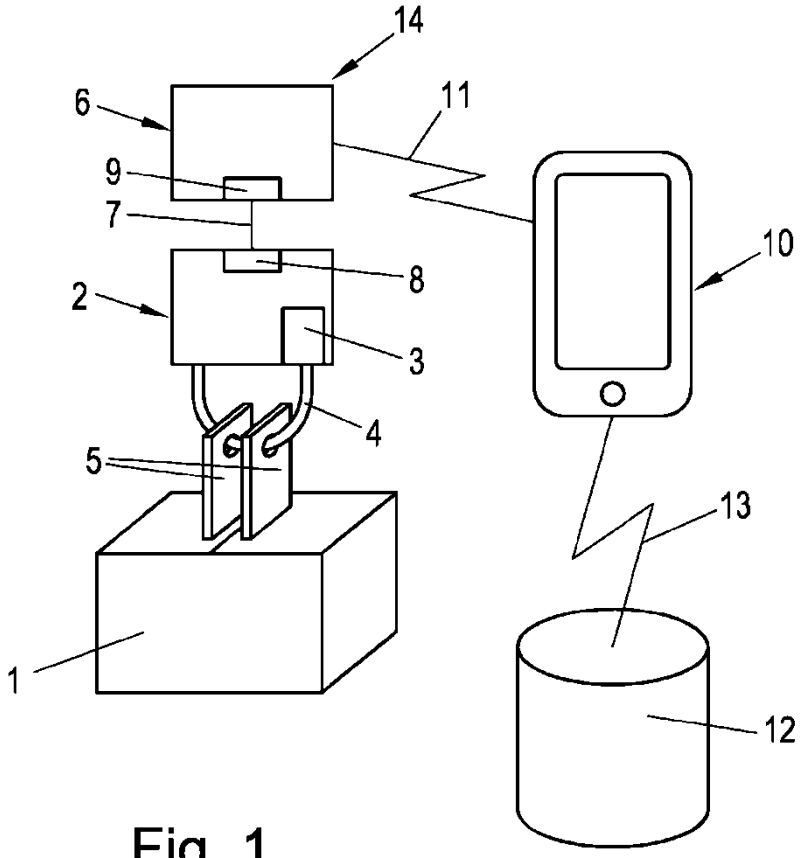

Fig. 1

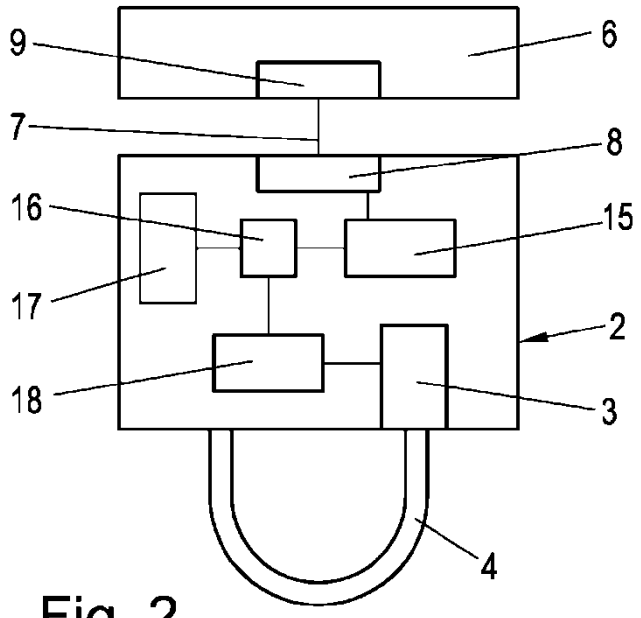

Fig. 2

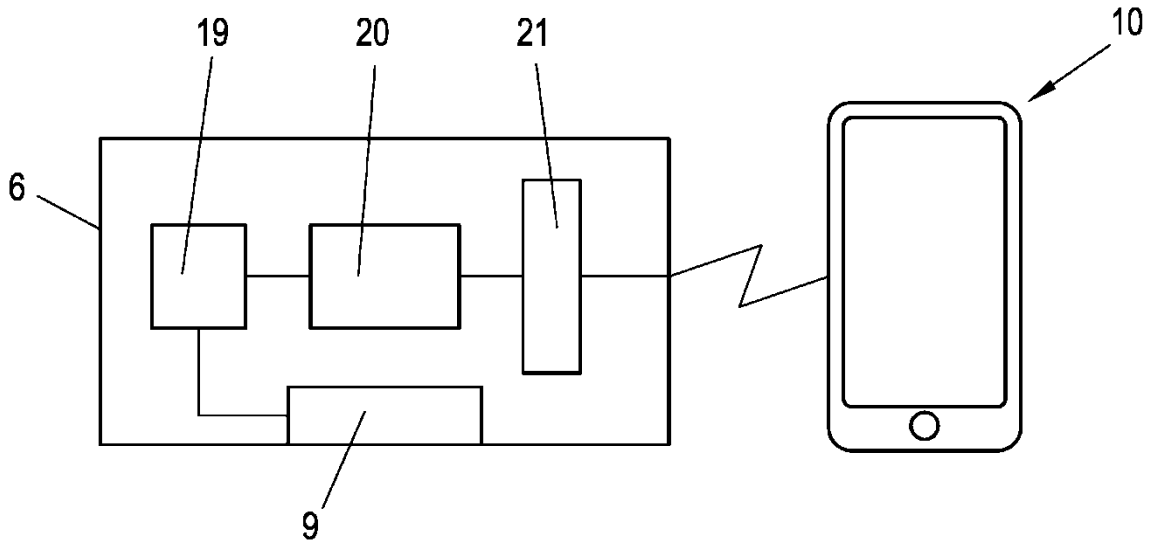
19
20
21
10
6
9

Fig. 3

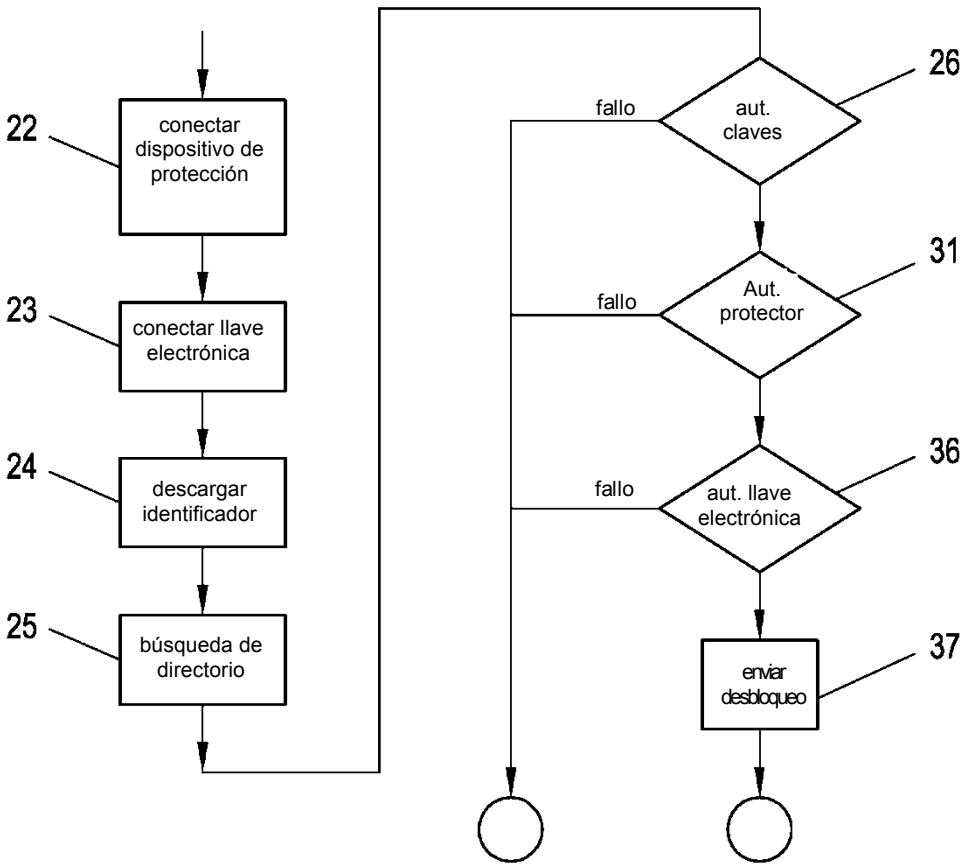
22
conectar dispositivo de protección
23
conectar llave electrónica
24
descargar identificador
25
búsqueda de directorio
fallo
aut. claves
26
fallo
Aut. protector
31
fallo
aut. llave electrónica
36
enviar desbloqueo
37

Fig. 4

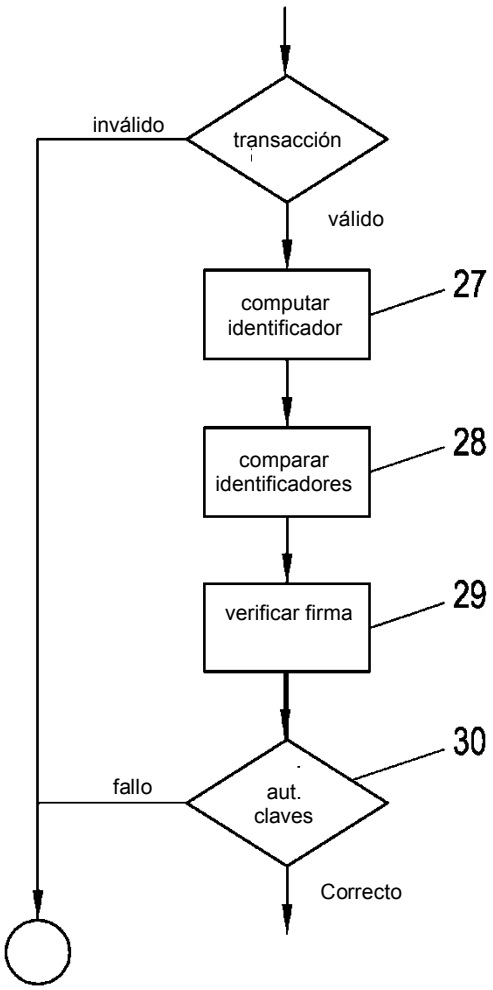
transacción
inválido
válido
computar identificador
27
comparar identificadores
28
verificar firma
29
aut. claves
30
fallo
Correcto

Fig. 5

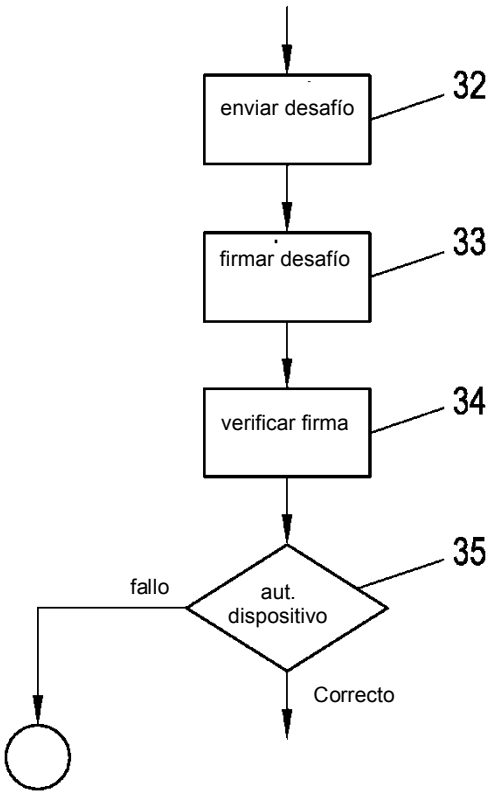
enviar desafío
32
firmar desafío
33
verificar firma
34
aut. dispositivo
35
fallo
Correcto

Fig. 6

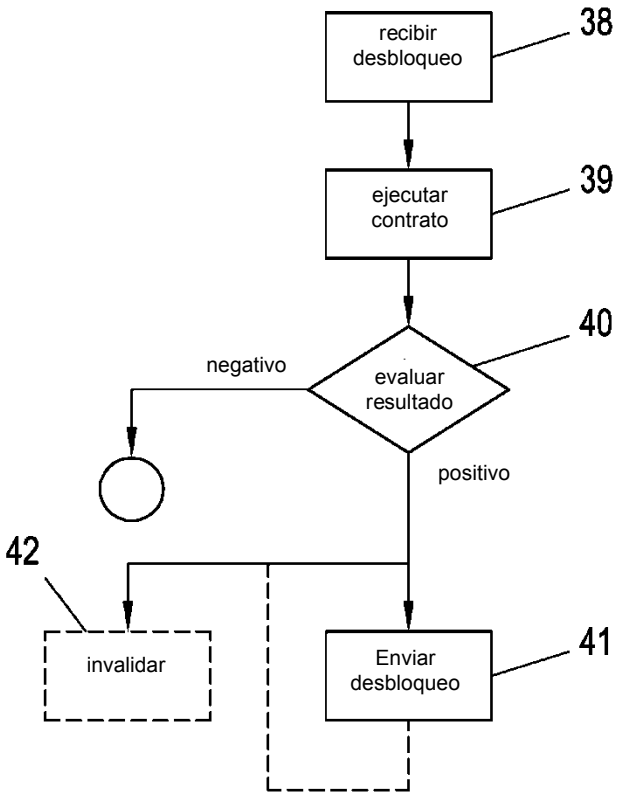
recibir desbloqueo
38
ejecutar contrato
39
evaluar resultado
40
negativo
positivo
42
invalidar
Enviar desbloqueo
41

Fig. 7

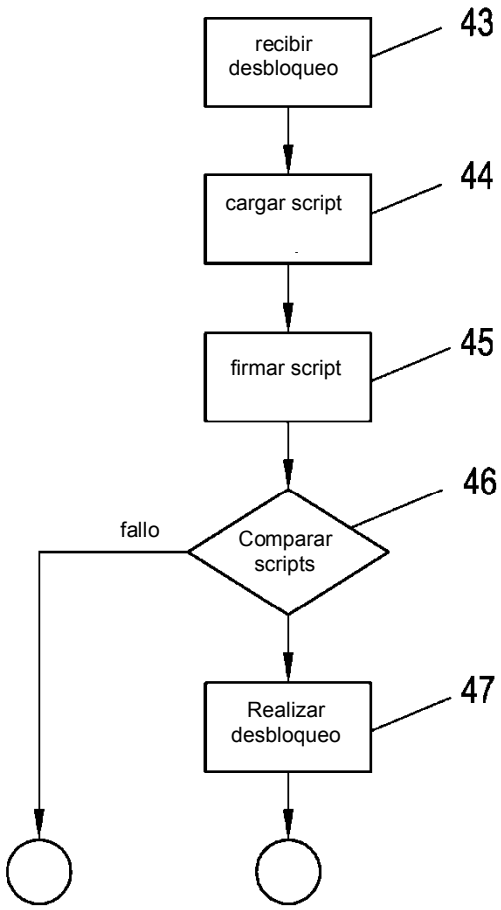
recibir desbloqueo
43
cargar script
44
firmar script
45
Comparar scripts
46
fallo
Realizar desbloqueo
47

Fig. 8