(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 986 651**

(51) Int. Cl.:

G07C 9/00 (2010.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **20.12.2018 E 18214679 (5)**

(97) Fecha y número de publicación de la concesión europea: **03.07.2024 EP 3671663**

(54) Título: **Delegaciones de cofirma**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
12.11.2024

(73) Titular/es:

ASSA ABLOY AB (100.0%)
P.O. Box 70340
107 23 Stockholm, SE

(72) Inventor/es:

LUNDBERG, FRANS

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Delegaciones de cofirma

Campo técnico

La presente descripción se refiere al campo de controlar el acceso al espacio físico usando un acceso delegado que incluye una delegación de cofirma, de manera que al menos una delegación en una cadena de delegación necesita ser cofirmada por un controlador de acceso.

Antecedentes

Las cerraduras y las llaves están evolucionando con respecto a las cerraduras puramente mecánicas tradicionales. Actualmente, las cerraduras electrónicas se están haciendo cada vez más comunes. Para cerraduras electrónicas, no se necesita ningún perfil de llave mecánica para la autenticación de un usuario. Las cerraduras electrónicas pueden, por ejemplo, abrirse usando una llave electrónica almacenada en un portador especial (llavero, tarjeta, etc.) o en un teléfono inteligente. La llave electrónica y la cerradura electrónica pueden, por ejemplo, comunicarse a través de una interfaz inalámbrica. Dichas cerraduras electrónicas proporcionan una serie de beneficios, incluyendo flexibilidad mejorada en la gestión de derechos de acceso, registros de auditoría, gestión de llaves, etc.

De vez en cuando, el propietario de la cerradura que controla el dispositivo de cerradura necesita dar acceso a proveedores de servicios para la entrega de un servicio. El servicio puede ser cualquier servicio donde la persona que realiza el servicio necesita que la cerradura electrónica se abra. Por ejemplo, el servicio puede ser un servicio de atención domiciliaria, una entrega de un producto, un servicio de limpieza, un constructor/fontanero/electricista, etc. Para poder consumir el servicio, el propietario de la cerradura necesita, por lo tanto, proporcionar acceso a un proveedor de servicios que usa la cerradura electrónica.

Simplifica enormemente la instalación de la cerradura si el dispositivo de cerradura no necesita estar conectado a una red, es decir, una instalación fuera de línea. Sin embargo, un problema en la implementación fuera de línea es cómo controlar el acceso a la cerradura. Los documentos WO2018/154058A1 y la publicación de "Distributed Authorization in Vanadium" de Ankur Taly et al., describen métodos de delegación de acceso según la técnica anterior.

Compendio

Es un objeto de la presente descripción permitir que un propietario de una cerradura revoque el acceso a los proveedores de servicios para una cerradura fuera de línea, cuando el propietario de la cerradura no conoce la identidad exacta del agente de proveedor de servicios asignado para entregar el servicio.

Según un primer aspecto, se proporciona un método para controlar el acceso a un espacio físico usando una delegación de cofirma según la reivindicación independiente 1.

El método puede comprender además el paso de: evaluar una restricción de tiempo del controlador de acceso aplicada por el controlador de acceso en una delegación de la cadena de delegaciones, y en donde el paso de conceder acceso solo se realiza cuando no se viola la restricción de tiempo del controlador de acceso.

La restricción de tiempo del controlador de acceso puede ser de 24 horas o menos.

El método puede comprender además el paso de: evaluar una restricción de tiempo del delegante aplicada por un delegante en una delegación de la cadena de delegaciones, y en donde el paso de conceder acceso solo se realiza cuando no se viola la restricción de tiempo del delegante.

El paso de obtención de una pluralidad de delegaciones puede comprender recibir al menos parte de la cadena de delegaciones de la llave electrónica.

En la delegación de cofirma, el controlador de acceso puede especificarse mediante una clave pública del controlador de acceso.

Según un segundo aspecto, se proporciona un dispositivo de cerradura para controlar el acceso a un espacio físico usando una delegación de cofirma según la reivindicación 6.

El dispositivo de cerradura puede comprender además instrucciones que, cuando son ejecutadas por el procesador, hacen que el dispositivo de cerradura: evalúe una restricción de tiempo del controlador de acceso aplicada por el controlador de acceso en una delegación de la cadena de delegaciones, y en donde las instrucciones para conceder acceso solo se realizan cuando no se viola la restricción de tiempo del controlador de acceso.

La restricción de tiempo del controlador de acceso puede ser de 24 horas o menos.

El dispositivo de cerradura puede comprender además instrucciones que, cuando son ejecutadas por el procesador, hacen que el dispositivo de cerradura: evalúe una restricción de tiempo del delegante aplicada por un delegante en una delegación de la cadena de delegaciones, y en donde las instrucciones para conceder acceso solo se realizan cuando no se viola la restricción de tiempo del delegante.

Las instrucciones para obtener una pluralidad de delegaciones pueden comprender instrucciones que, cuando son ejecutadas por el procesador, hacen que el dispositivo de cerradura reciba al menos parte de la cadena de delegaciones de la llave electrónica.

En la delegación de cofirma, el controlador de acceso puede especificarse mediante una clave pública del controlador de acceso.

Según un tercer aspecto, se proporciona un programa informático para controlar el acceso a un espacio físico usando una delegación de cofirma según la reivindicación 11.

Según un cuarto aspecto, se proporciona un producto de programa informático según la reivindicación 12 que comprende un programa informático según el tercer aspecto y un medio legible por ordenador en el que se almacena el programa informático.

Generalmente, todos los términos usados en las reivindicaciones deben interpretarse según su significado ordinario en el campo técnico, a menos que se defina explícitamente lo contrario en la presente memoria. Todas las referencias a "un/una/el elemento, aparato, componente, medio, paso, etc." deben interpretarse abiertamente como referidos a al menos una instancia del elemento, aparato, componente, medio, paso, etc., a menos que se indique explícitamente lo contrario. Los pasos de cualquier método descrito en la presente memoria no tienen que realizarse en el orden exacto descrito, a menos que se indique explícitamente.

Breve descripción de los dibujos

Los aspectos y realizaciones se describen ahora, a modo de ejemplo, con referencia a los dibujos adjuntos, en los que:

La Figura 1 es un diagrama esquemático que muestra un entorno en el que pueden aplicarse las realizaciones presentadas en la presente memoria;

La Figura 2 es un diagrama de flujo que ilustra un método para controlar el acceso a un espacio físico;

La Figura 3 es un diagrama esquemático que ilustra componentes del dispositivo de cerradura de la Figura 1; y

La Figura 4 muestra un ejemplo de un producto de programa informático 90 que comprende medios legibles por ordenador.

Descripción detallada

Los aspectos de la presente descripción se describirán ahora con mayor detalle a continuación con referencia a los dibujos adjuntos, en los que se muestran ciertas realizaciones de la invención. Sin embargo, estos aspectos pueden realizarse de muchas formas diferentes y no deben interpretarse como limitativos; más bien, estas realizaciones se proporcionan a modo de ejemplo de modo que esta descripción sea exhaustiva y completa, y para transmitir completamente el alcance de todos los aspectos de la invención a los expertos en la técnica. Los números similares se refieren a elementos similares a lo largo de la descripción.

Las realizaciones presentadas en la presente memoria se basan en cadenas de delegación de un propietario del dispositivo de cerradura, a través de uno o más nodos intermedios al agente de proveedor de servicios. La cadena de delegación permite que el dispositivo de cerradura esté fuera de línea. Además, la cadena de delegación requiere cofirma por parte de un controlador de acceso. De esta manera, el propietario de la cerradura puede interactuar con el controlador de acceso para controlar cuándo el controlador de acceso debe cofirmar delegaciones y cuándo no. Esto proporciona una solución que está fuera de línea para el dispositivo de cerradura, mientras que el propietario de la cerradura todavía puede controlar a quien se le permite obtener acceso a un espacio físico restringido. Al mismo tiempo, al controlador de acceso no se le da acceso per se, solo la capacidad de aprobar el acceso para otras entidades.

La Figura 1 es un diagrama esquemático que muestra un entorno en el que pueden aplicarse las realizaciones presentadas en la presente memoria. El acceso a un espacio físico 16 está restringido por una barrera física 15 que puede desbloquearse de manera selectiva usando un dispositivo de cerradura 10. La barrera 15 puede ser una puerta, portón, escotilla, puerta de armario, cajón, ventana, etc. La barrera física 15 se proporciona en una estructura física circundante (siendo una pared, valla, techo, suelo, etc.) y se encuentra entre el espacio físico restringido 16 y un espacio físico accesible 14. Cabe señalar que el espacio físico accesible 14 puede ser un espacio físico restringido en sí mismo, pero en relación con esta barrera física 15, el espacio físico accesible 14 es accesible.

El propietario L o usuario del dispositivo de cerradura 10 se denomina aquí propietario de cerradura L. El propietario de cerradura L puede portar un dispositivo de propietario de cerradura, que es cualquier dispositivo electrónico adecuado, por ejemplo, un teléfono inteligente, teléfono móvil, tableta, ordenador portátil, ordenador de escritorio, televisión inteligente, decodificador, etc.

El dispositivo de cerradura 10 puede comunicarse con llaves electrónicas. Dichas llaves electrónicas pueden implementarse como parte de un teléfono móvil, un teléfono inteligente, un llavero, un dispositivo para llevar puesto, una carcasa de teléfono inteligente, una tarjeta de acceso, una llave física electrónica, etc. La llave electrónica puede comunicarse con el dispositivo de cerradura 10 a través de una interfaz cableada o inalámbrica, por ejemplo, usando Bluetooth, Bluetooth de baja energía (BLE), cualquiera de los estándares IEEE 802.15, identificación por radiofrecuencia (RFID), comunicación de campo cercano (NFC), una interfaz en serie (por ejemplo, RS485, RS232), bus serie universal (USB) o incluso una conexión eléctrica simple con un protocolo de comunicación personalizado.

También hay un proveedor de servicios S. El proveedor de servicios S puede ser, por ejemplo, una empresa de atención domiciliaria, una empresa de entrega, una empresa de limpieza, una empresa de construcción, un fontanero, un electricista, etc. El proveedor de servicios S también puede ser proporcionado por una tercera parte, en nombre del proveedor de servicios.

Como se explica con más detalle a continuación, el propietario de la cerradura L desea que el proveedor de servicios S preste un servicio, lo que requiere acceso al espacio físico restringido 16. El proveedor de servicios S usa un agente de proveedor de servicios A para entregar el servicio. El agente de proveedor de servicios A es una persona física y puede ser un empleado o un subcontratista del proveedor de servicios. El agente de proveedor de servicios A porta un dispositivo de agente de proveedor de servicios 7, que es un dispositivo electrónico portátil, por ejemplo, un teléfono inteligente, teléfono móvil, tableta, ordenador portátil, etc. Las funciones descritas en la presente memoria como realizadas por el agente de proveedor de servicios pueden, por ejemplo, realizarse en una aplicación de software (también conocida como app) que se ejecuta en el dispositivo de agente de proveedor de servicios 7.

Un controlador de acceso AC es una entidad de control para la delegación de acceso. Cuando se usa como se describe en las realizaciones de la presente memoria, el controlador de acceso AC permite o deniega la delegación de derechos de acceso pero no se le otorga el propio derecho de acceso. Por lo tanto, el controlador de acceso AC puede usarse para invalidar dispositivos de llave sin que el propio controlador de acceso AC obtenga derechos de acceso para abrir un dispositivo de cerradura. El propietario de la cerradura L puede interactuar con el controlador de acceso AC, por ejemplo, a través de una interfaz web para controlar las acciones del controlador de acceso AC con respecto a los derechos de acceso que posee el propietario de la cerradura L.

La comunicación entre los diferentes nodos en la Figura 1 puede producirse usando comunicación local, por ejemplo usando Bluetooth, Bluetooth de baja energía (BLE), cualquiera de los estándares IEEE 802.15, cualquiera de los estándares IEEE 802.11, USB inalámbrico (bus serie universal), USB, Ethernet, conexión en serie (por ejemplo RS-485), etc. y/o comunicación de área amplia tal como redes celulares e Internet. En una capa superior, podría usarse el Protocolo de Internet (IP) para la comunicación, interna y/o externamente.

Ahora se explicará el concepto de delegación de derechos de acceso y cómo se emplea esto en las realizaciones presentadas en la presente memoria. Cada delegación es una delegación de un delegante a una delegado. La pluralidad de delegaciones forma colectivamente una cadena de delegaciones. Para cada enlace en la cadena, cuando dos delegaciones se encadenan juntas, el delegado de una delegación es el delegante la siguiente delegación. Cada entidad en la cadena de delegación, es decir, todos los delegantes y delegados usan dispositivos físicos tales como dispositivos portátiles u ordenadores/servidores en las operaciones que usan delegaciones. En otras palabras, siempre que se mencione que una parte es delegante o delegado en este documento, esto se implementa en un dispositivo físico de este tipo.

La pluralidad de delegaciones puede formar una cadena. Por ejemplo, considérese el siguiente ejemplo de una cadena de delegación:

L-->C-->S -->A

Usando los signos de referencia usados anteriormente, L denota el propietario de la cerradura, C denota el coordinador, S denota el proveedor de servicios y A denota el agente de proveedor de servicios. Por lo tanto, esta cadena de delegaciones comienza en el propietario de la cerradura, y procede desde el propietario de la cerradura, al coordinador, al proveedor de servicios y al agente de proveedor de servicios. Cuando esta delegación es válida, se le delega el acceso al proveedor de servicios, indirectamente, por parte del propietario de la cerradura.

Cada flecha es una delegación y cada delegación es un elemento de datos que puede comunicarse a través de un canal de comunicación digital y puede almacenarse en memoria. Cada delegación contiene (referencias a) un delegante y un delegado. Todas las delegaciones pueden usar el mismo formato de datos, lo que simplifica las extensiones a la cadena de delegación o estructura de delegaciones, mejorando así la flexibilidad en la cadena de delegación. Además, al emplear el mismo formato de datos para todas las delegaciones, es más fácil y más consistente

para el dispositivo de cerradura, que eventualmente comprueba la validez de la cadena de delegación, comprobar las delegaciones en la cadena de delegación.

La delegación es firmada criptográficamente por el delegante, usando cualquier algoritmo de firma adecuado y una clave privada del delegante. La firma puede verificarse usando una clave pública (correspondiente a la clave privada) del delegante. La firma criptográfica puede anexarse a la delegación.

A continuación, se indica una delegación firmada mediante una delegación de doble línea. Por ejemplo, lo siguiente denota una delegación del coordinador al proveedor de servicios, donde la delegación es firmada criptográficamente por el coordinador.

C = = => S

Cuando el agente de proveedor de servicios llega y necesita que el dispositivo de cerradura se desbloquee, el agente de proveedor de servicios (o más específicamente, el dispositivo de agente de proveedor de servicios 7) transmite al menos la última delegación en la cadena de delegaciones al dispositivo de cerradura. En una realización, solo la primera delegación (del dispositivo de cerradura) se almacena en el dispositivo de cerradura. Todas las delegaciones posteriores en la cadena de delegaciones se transmiten desde el agente de proveedor de servicios.

Según las realizaciones de la presente memoria, una delegación también puede contener un requisito, establecido por el delegante, de que las delegaciones adicionales necesitan ser firmadas criptográficamente por un controlador de acceso. Dicha delegación se denota aquí (co:AC), donde 'AC' denota el controlador de acceso del que se requiere la firma. El controlador de acceso puede, por ejemplo, identificarse por su clave pública.

El siguiente ejemplo denota una delegación del propietario de la cerradura al coordinador, con un requisito de cofirma de que las delegaciones posteriores, en la cadena de delegaciones, necesitan ser firmadas por el controlador de acceso AC.

L–(co:AC)–->C

Un ejemplo más detallado de una cadena de delegación con requisitos de cofirma se describirá ahora en el contexto de la atención domiciliaria:

L–(co:AC)-> C ==(co:AC)==> S ==(co:AC)==> A

El propietario de la cerradura usa aquí un coordinador para seleccionar su proveedor de atención domiciliaria. El coordinador en este caso puede ser un municipio o ciudad, por ejemplo, la ciudad de Estocolmo. El propietario de la cerradura puede seleccionar un proveedor de atención domiciliaria, es decir, una empresa de proveedor de atención domiciliaria, para su uso. En este ejemplo, el proveedor de atención domiciliaria se denota por S. El propietario de la cerradura informa al coordinador de la selección.

El propietario de la cerradura L crea una delegación al coordinador C que es una delegación de cofirma, lo que requiere que el controlador de acceso AC cofirme cualquier delegación adicional en la cadena de delegación. El coordinador C crea una delegación de cofirma (que también requiere que el controlador de acceso AC cofirme cualquier delegación adicional) al proveedor de atención domiciliaria S. La delegación de cofirma por parte del coordinador C se envía al controlador de acceso AC para ser firmada. Una vez que la delegación de cofirma del coordinador C es firmada por el controlador de acceso AC, la delegación de cofirma se transmite al delegado, es decir, al proveedor de atención domiciliaria S.

El proveedor de atención domiciliaria S crea una delegación de cofirma (que también requiere que el AC cofirme cualquier delegación adicional) a un agente de proveedor de servicios A (es decir, un empleado de atención domiciliaria). La delegación de cofirma por parte del proveedor de atención domiciliaria S se envía al controlador de acceso AC para ser firmada. Una vez que la delegación de cofirma del proveedor de atención domiciliaria S es firmada por el controlador de acceso AC, esto se transmite al agente del proveedor de servicios A, así como a la delegación de cofirma delegada por el coordinador C.

Cuando el agente de proveedor de servicios A llega al dispositivo de cerradura, el agente de proveedor de servicios A envía una solicitud de acceso al dispositivo de cerradura 10. El agente de proveedor de servicios A también proporciona, a partir de la cadena de delegaciones, la delegación por parte del coordinador C al proveedor de servicios S y la delegación por parte del proveedor de atención domiciliaria S al agente de proveedor de servicios A. Ambas de estas delegaciones contienen una firma por parte del controlador de acceso AC.

El dispositivo de cerradura 10 también obtiene la primera delegación, del propietario de la cerradura L al coordinador, por ejemplo, de la memoria local.

El uso de la cadena de delegaciones permite que el dispositivo de cerradura 10 verifique la autoridad de cualquier agente de proveedor de servicios A, para determinar así si el dispositivo de cerradura 10 debe establecerse en un

estado desbloqueado para permitir el acceso al espacio restringido 16. Esta verificación se basa en las delegaciones de la cadena de delegación, es decir, los datos proporcionados por el agente de proveedor de servicios A y los datos almacenados localmente. Por lo tanto, el dispositivo de cerradura 10 no necesita tener acceso a la red para realizar esta verificación.

También pueden aplicarse restricciones de tiempo para permitir una revocación más flexible de los derechos de acceso. Por ejemplo, puede haber una restricción de tiempo del controlador de acceso, donde el controlador de acceso limita un tiempo de validez de su firma de una delegación particular. De esta manera, cualquier delegación que necesite ser firmada por el controlador de acceso necesita ser firmada de nuevo después de que expire la restricción de tiempo del controlador de acceso. En una realización, la restricción de tiempo del controlador de acceso es de 24 horas o menos, lo que implica que el controlador de acceso necesita firmar las delegaciones pertinentes diariamente. Además, la delegación del propietario de la cerradura al coordinador puede establecerse de manera segura con un tiempo de validez largo, del orden de meses o incluso años, ya que la restricción de tiempo del controlador de acceso es más corta y puede ser controlada por el propietario de la cerradura usando una interfaz, por ejemplo, una interfaz web, con el controlador de acceso.

Usando las realizaciones presentadas en la presente memoria, pueden aplicarse reglas de redelegación avanzadas usando el controlador de acceso AC. Por ejemplo, considérese una regla donde el proveedor de servicios S puede volver a delegar la delegación del coordinador (procedente del propietario de la cerradura), pero solo a cinco delegados a la vez. Dado que cada delegación por parte del proveedor de servicios necesita ser firmada por el controlador de acceso AC, cuando se intenta una sexta delegación por parte del proveedor de servicios S, el controlador de acceso AC puede rechazar firmarla. Otro ejemplo es que el controlador de acceso AC puede imponer una regla de que una delegación solo puede volver a delegarse a un miembro de un grupo particular de delegados válidos.

Si es necesario revocar una delegación, el propietario de la cerradura L puede ordenar al controlador de acceso que no aplique ninguna nueva firma para las delegaciones del derecho de acceso delegado por el propietario de la cerradura. Esto permite que un derecho de acceso sea revocado incluso aunque el dispositivo de cerradura 10 pueda proporcionarse sin conectividad de red. Cabe señalar que la revocación no es inmediata, sino que se efectúa cuando expira la restricción de tiempo del controlador de acceso. Por lo tanto, las duraciones de la restricción de tiempo del controlador de acceso determinan con qué rapidez tiene efecto una revocación.

Usando la delegación de cofirma, el cofirmante (controlador de acceso AC) puede controlar delegaciones adicionales, usando opcionalmente restricciones de tiempo para forzar a cualquier delegado a obtener una nueva firma regularmente.

Significativamente, usando las realizaciones presentadas en la presente memoria, el controlador de acceso AC no tiene acceso a las cerraduras; el controlador de acceso no puede acceder a cerraduras usando sus propias credenciales, ni delegar el acceso a nadie más. Aun así, el controlador de acceso puede proporcionar una interfaz, por ejemplo, una interfaz web, para permitir que los propietarios de cerraduras controlen a qué entidades (empresas o individuos) se les podría conceder acceso al espacio físico restringido.

La Figura 2 es un diagrama de flujo que ilustra un método para controlar el acceso a un espacio físico. El método se realiza en un dispositivo de cerradura.

En un paso de recibir solicitud de acceso 40, el dispositivo de cerradura recibe una solicitud de acceso de una llave electrónica. La llave electrónica puede, por ejemplo, pertenecer al agente de proveedor de servicios A de la Figura 1.

En el paso de obtener delegaciones 42, el dispositivo de cerradura obtiene una pluralidad de delegaciones. Como se explicó anteriormente, cada delegación es una delegación de un delegante a un delegado. La pluralidad de delegaciones forma colectivamente una cadena de delegaciones. Para cada enlace en la cadena, cuando dos delegaciones se encadenan juntas, el delegado de una delegación es el delegante de la siguiente delegación.

Al menos parte de las delegaciones en la cadena de delegaciones puede recibirse desde la llave electrónica. En una realización, todas las delegaciones (en la cadena de delegaciones), excepto la primera delegación (por parte del propietario de la cerradura) se reciben de la llave electrónica.

En un paso de determinar la delegación de cofirma 44, el dispositivo de cerradura determina que una delegación en la cadena de delegaciones es una delegación de cofirma. La delegación de cofirma indica que todas las delegaciones adicionales necesitan ser firmadas criptográficamente tanto por el delegante de la delegación respectiva como por un controlador de acceso. El controlador de acceso se especifica en la delegación de cofirma. El controlador de acceso puede especificarse mediante una clave pública del controlador de acceso. Alternativamente, el controlador de acceso se especifica mediante un identificador que puede estar asociado a una clave pública.

En un paso opcional de evaluar la restricción de tiempo del controlador de acceso 46, el dispositivo de cerradura evalúa una restricción de tiempo del controlador de acceso aplicada por el controlador de acceso en una delegación de la cadena de delegaciones. En una realización, la restricción de tiempo del controlador de acceso es de 24 horas o menos.

En un paso opcional de evaluar la restricción de tiempo del delegante 47, el dispositivo de cerradura evalúa una restricción de tiempo del delegante aplicada por una delegante en una delegación de la cadena de delegaciones.

En un paso de conceder acceso cuando esté autorizado 48, el dispositivo de cerradura concede acceso al espacio físico cuando la cadena de delegaciones comienza en el propietario del dispositivo de cerradura y termina en la llave electrónica y cuando todas las delegaciones en la cadena de delegaciones después de la delegación de cofirma están firmadas criptográficamente tanto por el delegante de la delegación respectiva como por el controlador de acceso. Adicionalmente, cuando se aplica una restricción de tiempo del controlador de acceso (véase el paso 46 anterior), el acceso sólo se concede cuando no se viola la restricción de tiempo del controlador de acceso. Adicionalmente, cuando se aplica una restricción de tiempo del delegante (véase el paso 47 anterior), el acceso sólo se concede cuando no se viola la restricción de tiempo del delegante.

La Figura 3 es un diagrama esquemático que ilustra los componentes del dispositivo de cerradura 10 de la Figura 1. Se proporciona un procesador 60 usando cualquier combinación de una o más de una unidad central de procesamiento (CPU) multiprocesador, microcontrolador, procesador de señales digitales (DSP), etc., adecuados capaces de ejecutar instrucciones de software 67 almacenadas en una memoria 64, que puede ser, por lo tanto, un producto de programa informático. El procesador 60 podría implementarse alternativamente usando un circuito integrado de aplicación específica (ASIC), una matriz de puertas programables por campo (FPGA), etc. El procesador 60 puede configurarse para ejecutar el método descrito con referencia a la Figura 2 anterior.

La memoria 64 puede ser cualquier combinación de memoria de acceso aleatorio (RAM) y/o memoria de sólo lectura (ROM). La memoria 64 comprende también almacenamiento persistente, que, por ejemplo, puede ser cualquier única o una combinación de memoria magnética, memoria óptica, memoria de estado sólido o incluso memoria montada de forma remota.

También se proporciona una memoria de datos 66 para leer y/o almacenar datos durante la ejecución de instrucciones de software en el procesador 60. La memoria de datos 66 puede ser cualquier combinación de RAM y/o ROM.

El dispositivo de cerradura comprende además una interfaz de E/S 62 para comunicarse con entidades externas, tales como un dispositivo de llave. Opcionalmente, la interfaz de E/S 62 también incluye una interfaz de usuario.

Otros componentes del dispositivo de cerradura 10 se omiten para no oscurecer los conceptos presentados en la presente memoria.

La Figura 4 muestra un ejemplo de un producto de programa informático 90 que comprende medios legibles por ordenador. En estos medios legibles por ordenador, puede almacenarse un programa informático 91, cuyo programa informático puede hacer que un procesador ejecute un método según las realizaciones descritas en la presente memoria. En este ejemplo, el producto de programa informático es un disco óptico, tal como un CD (disco compacto) o un DVD (disco versátil digital) o un disco Blu-Ray. Como se explicó anteriormente, el producto de programa informático también podría incorporarse en una memoria de un dispositivo, tal como el producto de programa informático 64 de la Figura 3. Aunque el programa informático 91 se muestra aquí esquemáticamente como una pista en el disco óptico representado, el programa informático puede almacenarse de cualquier manera que sea adecuada para el producto de programa informático, tal como una memoria de estado sólido extraíble, por ejemplo, una unidad de bus serie universal (USB).

Los aspectos de la presente descripción se han descrito principalmente anteriormente con referencia a unas pocas realizaciones. Sin embargo, como es fácilmente apreciado por un experto en la técnica, otras realizaciones distintas de las descritas anteriormente son igualmente posibles dentro del alcance de la invención, como se define en las reivindicaciones de patente adjuntas.

REIVINDICACIONES

1. Un método para controlar el acceso a un espacio físico (16) usando una delegación de cofirma, siendo realizado el método en un dispositivo de cerradura (10) y comprendiendo los pasos de:

recibir (40), usando una interfaz cableada o inalámbrica, una solicitud de acceso de una llave electrónica (7);

obtener (42) una pluralidad de delegaciones, en donde cada delegación es un elemento de datos que indica un delegante y un delegado, formando la pluralidad de delegaciones colectivamente una cadena de delegaciones en donde, cuando dos delegaciones están encadenadas entre sí, el delegado de una delegación es el delegante de la siguiente delegación, en donde una primera delegación en la cadena de delegaciones se recibe de una memoria local del dispositivo de cerradura, y en donde todas las delegaciones adicionales en la cadena de delegaciones se reciben de la llave electrónica;

determinar (44) que la primera delegación en la cadena de delegaciones es una delegación de cofirma, indicando la delegación de cofirma que todas las delegaciones adicionales en la cadena de delegaciones necesitan ser firmadas criptográficamente tanto por el delegante de la delegación respectiva como por un controlador de acceso (AC); y

conceder (48) acceso al espacio físico (16) cuando la cadena de delegaciones comienza en un delegante de la primera delegación y termina en la llave electrónica (7); y cuando todas las delegaciones en la cadena de delegaciones después de la delegación de cofirma están firmadas criptográficamente tanto por el delegante de la delegación respectiva como por el controlador de acceso (AC).

2. El método según la reivindicación 1, que comprende además el paso de:

evaluar (46) una restricción de tiempo del controlador de acceso aplicada por el controlador de acceso (AC) a una delegación de la cadena de delegaciones, y en donde el paso de conceder (48) acceso solo se realiza cuando no se viola la restricción de tiempo del controlador de acceso.

3. El método según la reivindicación 2, en donde la restricción de tiempo del controlador de acceso es de 24 horas o menos.

4. El método según una cualquiera de las reivindicaciones precedentes, que comprende además el paso de:

evaluar (47) una restricción de tiempo del delegante aplicada por un delegante en una delegación de la cadena de delegaciones, y en donde el paso de conceder (48) acceso solo se realiza cuando no se viola la restricción de tiempo del delegante.

5. El método según cualquiera de las reivindicaciones precedentes, en donde, en la delegación de cofirma, el controlador de acceso (AC) está especificado por una clave pública del controlador de acceso (AC).

6. Un dispositivo de cerradura (10) para controlar el acceso a un espacio físico (16) usando una delegación de cofirma, comprendiendo el dispositivo de cerradura (10):

un procesador (60); y

una memoria (64) que almacena instrucciones (67) que están configuradas para, cuando son ejecutadas por el procesador, hacer que el dispositivo de cerradura (10):

reciba, usando una interfaz cableada o inalámbrica, una solicitud de acceso de una llave electrónica (7);

obtenga una pluralidad de delegaciones, en donde cada delegación es un elemento de datos que indica un delegante y de un delegado, formando la pluralidad de delegaciones colectivamente una cadena de delegaciones en donde cuando dos delegaciones están encadenadas juntas, el delegado de una delegación es el delegante de la siguiente delegación, en donde una primera delegación en la cadena de delegaciones se recibe de una memoria local del dispositivo de cerradura, y en donde todas las delegaciones adicionales en la cadena de delegaciones se reciben de la llave electrónica;

determine que una primera delegación en la cadena de delegaciones es una delegación de cofirma, indicando la delegación de cofirma que todas las delegaciones adicionales en la cadena de delegaciones necesitan ser firmadas criptográficamente tanto por el delegante de la delegación respectiva como por un controlador de acceso; (AC) y

conceda acceso al espacio físico (16) cuando la cadena de delegaciones comienza en delegante de la primera delegación y termina en la llave electrónica (7); y cuando todas las delegaciones en la cadena de delegaciones después de la delegación de cofirma están firmadas criptográficamente tanto por el delegante de la delegación respectiva como por el controlador de acceso (AC).

7. El dispositivo de cerradura (10) según la reivindicación 6, que comprende además instrucciones (67) que, cuando son ejecutadas por el procesador, hacen que el dispositivo de cerradura (10):

evalúe una restricción de tiempo del controlador de acceso aplicada por el controlador de acceso (AC) en una delegación de la cadena de delegaciones, y en donde las instrucciones para conceder acceso solo se realizan cuando no se viola la restricción de tiempo del controlador de acceso.

8. El dispositivo de cerradura (10) según la reivindicación 7, en donde la restricción de tiempo del controlador de acceso es de 24 horas o menos.

9. El dispositivo de cerradura (10) según una cualquiera de 6 a 8, que comprende además instrucciones (67) que, cuando son ejecutadas por el procesador, hacen que el dispositivo de cerradura (10):

evalúe una restricción de tiempo del delegante aplicada por un delegante en una delegación de la cadena de delegaciones, y en donde las instrucciones para conceder acceso solo se realizan cuando no se viola la restricción de tiempo del delegante.

10. El dispositivo de cerradura (10) según una cualquiera de las reivindicaciones 6 a 9, en donde, en la delegación de cofirma, el controlador de acceso (AC) está especificado por una clave pública del controlador de acceso (AC).

11. Un programa informático (67, 91) para controlar el acceso a un espacio físico (16) usando una delegación de cofirma, comprendiendo el programa informático código de programa informático que está configurado para hacer que, cuando se ejecuta en un procesador de un dispositivo de cerradura (10), el dispositivo de cerradura (10):

reciba una solicitud de acceso de una llave electrónica (7) usando una interfaz cableada o inalámbrica;

obtenga una pluralidad de delegaciones, en donde cada delegación es un elemento de datos que indica un delegante y de un delegado, formando la pluralidad de delegaciones colectivamente una cadena de delegaciones en donde cuando dos delegaciones están encadenadas juntas, el delegado de una delegación es el delegante de la siguiente delegación, en donde una primera delegación en la cadena de delegaciones se recibe de una memoria local del dispositivo de cerradura, y en donde todas las delegaciones adicionales en la cadena de delegaciones se reciben de la llave electrónica;

determine que una primera delegación en la cadena de delegaciones es una delegación de cofirma, indicando la delegación de cofirma que todas las delegaciones adicionales en la cadena de delegaciones necesitan ser firmadas criptográficamente tanto por el delegante de la delegación respectiva como por un controlador de acceso (AC); y

conceda acceso al espacio físico (16) cuando la cadena de delegaciones comienza en un delegante de la primera delegación y termina en la llave electrónica (7); y cuando todas las delegaciones en la cadena de delegaciones después de la delegación de cofirma están firmadas criptográficamente tanto por el delegante de la delegación respectiva como por el controlador de acceso (AC).

12. Un producto de programa informático (64, 90) que comprende un programa informático según la reivindicación 11 y un medio legible por ordenador en donde se almacena el programa informático.

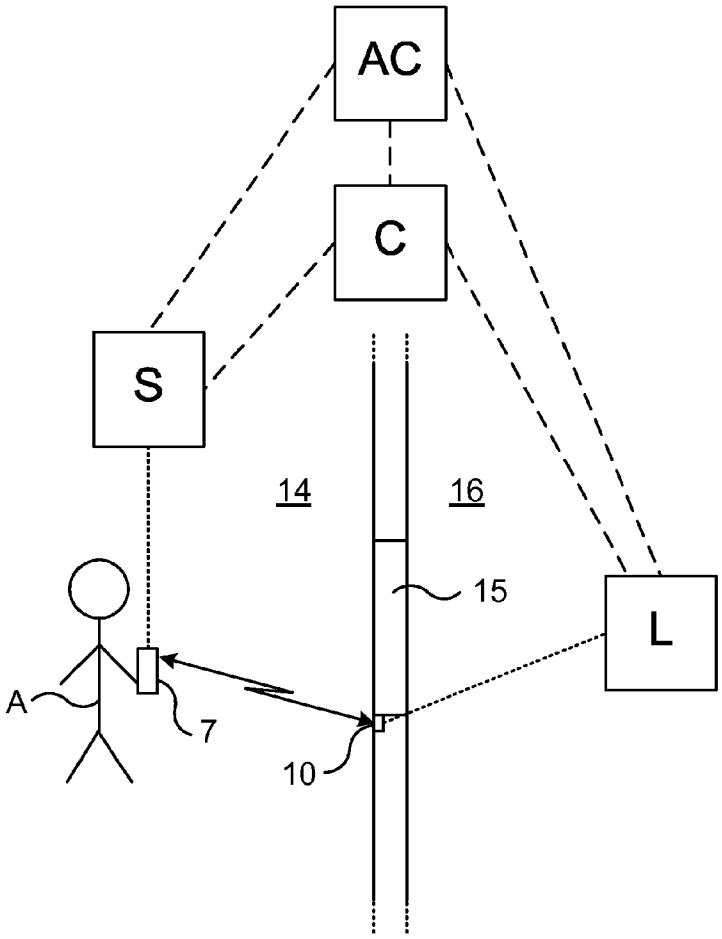

Fig. 1

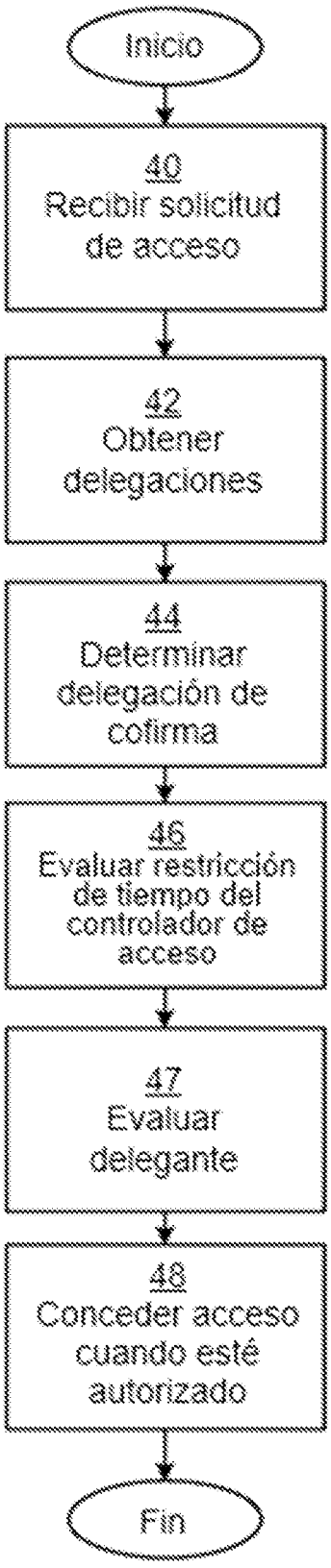

Fig. 2

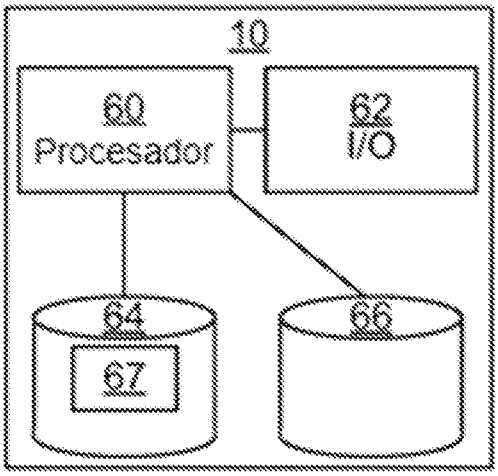

Fig. 3

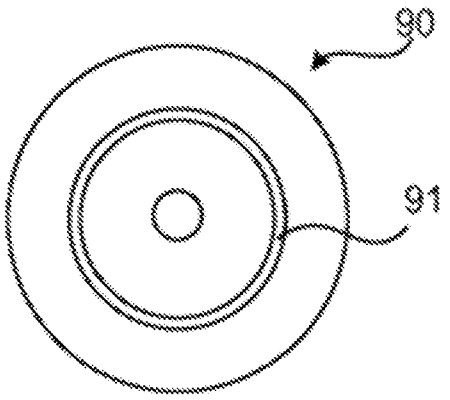

Fig. 4