(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 922 812**

(51) Int. CI.:

G06F 21/35 (2013.01)
G06F 21/79 (2013.01)
G06F 21/81 (2013.01)
G06F 21/88 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **24.01.2017 PCT/FR2017/050139**

(87) Fecha y número de publicación internacional: **03.08.2017 WO17129887**

(96) Fecha de presentación y número de la solicitud europea: **24.01.2017 E 17706283 (3)**

(97) Fecha y número de publicación de la concesión europea: **11.05.2022 EP 3408777**

(54) Título: **Sistema de control de acceso**

(30) Prioridad:

25.01.2016 FR 1650570

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
20.09.2022

(73) Titular/es:

GASCUEL, JACQUES, CLAUDE, GUY (100.0%)
Edifici Santa Maria de Coll de Caldes Escala A
Planta Cinquena Crta d'Engolasters
AD700 Escaldes-Engordany, AD

(72) Inventor/es:

GASCUEL, JACQUES, CLAUDE, GUY

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Sistema de control de acceso

1. Campo técnico de la invención

La invención se refiere a un sistema de control de acceso. En particular, la invención se refiere a un sistema para controlar el acceso a un dispositivo protegido, por ejemplo el acceso a una o más memorias protegidas de un componente electrónico.

2. Antecedentes de tecnología

Los sistemas de control de acceso permiten restringir el acceso a un dispositivo protegido solo a las personas que tienen los permisos necesarios para acceder al dispositivo protegido. Este dispositivo protegido puede ser, por ejemplo, una memoria que contenga datos digitales a los que se deba restringir el acceso, o un equipo físico bloqueado cuyo uso esté sujeto a autorización de acceso. La solicitud de patente US2008098134 A1 divulga por ejemplo un dispositivo de protección de una memoria que realiza una comparación entre una clave contenida en un registro del dispositivo y una clave almacenada en un transpondedor y que se obtiene por medio de una interfaz inalámbrica. En caso de correspondencia, se cierra un interruptor que ofrece acceso a la memoria.

Los sistemas de control de acceso actuales normalmente implementan uno o más factores de autenticación antes de emitir la autorización de acceso. Cada factor de autenticación define uno o más criterios de validez para una clave que se le presenta, una clave válida que permite colocar el factor de autenticación en un estado llamado desbloqueado. Cuando todos los factores de autenticación están desbloqueados, se otorga acceso. Puede ser, por ejemplo, una contraseña que se compara con una lista de contraseñas autorizadas.

La verificación de la correspondencia de los factores de autenticación con al menos una clave y la configuración de los factores de autenticación se realizan a menudo mediante una conexión a un servidor externo, en particular a través de Internet. Esta solución presenta riesgos de interceptación de datos sobre la marcha por parte de un operador malintencionado, lo que permite obtener información sobre el factor de autenticación implementado o sobre la clave sujeta al factor de autenticación.

Además, los sistemas de control de acceso actuales son poco modulares, y los factores de autenticación son fácilmente identificables por cualquier persona malintencionada que desee acceder al dispositivo protegido sin autorización. Por lo tanto, los ataques para obtener acceso se centran en estos factores.

3. Objetivos de la invención

La invención pretende superar al menos algunos de los inconvenientes de los sistemas de control de acceso conocidos.

En particular, la invención tiene como objetivo proporcionar, en al menos un modo de realización de la invención, un sistema de control de acceso autónomo, que no requiere una conexión con un servidor externo.

La invención también tiene como objetivo proporcionar, en al menos un modo de realización, un sistema de control de acceso que permita una parametrización personalizable de los factores de autenticación.

4. Divulgación de la invención

Para ello, la invención se refiere a un sistema de control de acceso a un dispositivo protegido por al menos un factor de autenticación previamente parametrizado, definiendo cada factor de autenticación al menos un criterio de validez de una clave y encontrándose en un estado denominado desbloqueado si una clave que se le presenta cumple los criterios de validez, y un estado llamado bloqueado si ninguna clave que se le presenta cumple los criterios de validez, que comprende:

- una unidad de control de acceso que comprende:
    - un dispositivo de comunicación inalámbrica de corto alcance, que comprende un módulo de transmisión de datos inalámbrico y un módulo de recolección de energía eléctrica,
    - un módulo de recepción de claves, adaptado para recibir al menos una clave,
    - un módulo de verificación de factores, adaptado para verificar la validez de cada factor de autenticación previamente parametrizado con al menos una clave recibida por el módulo de recepción de claves y proporcionar autorización de acceso si el conjunto de factores de autenticación está en estado desbloqueado,
    - al menos una ruta de acceso, adaptada para permitir el acceso al dispositivo protegido,

- al menos un interruptor controlable, configurado para abrir o cerrar la ruta de acceso al dispositivo protegido, estando la ruta de acceso cerrada por defecto y abierta en caso de recibir una autorización de acceso del módulo de verificación,

- una unidad de administración, adaptada para permitir la preconfiguración de cada factor de autenticación por interacción con el módulo de transmisión inalámbrica de datos del dispositivo de conexión de la unidad de control de acceso,

- una unidad de usuario, distinta de la unidad de administración, configurada para transmitir al menos una clave al módulo de recepción de claves, a través del módulo de transmisión inalámbrica de datos.

Por lo tanto, un sistema de control de acceso según la invención permite gestionar el acceso a un dispositivo protegido de forma autónoma, sin conexión a un servidor externo, la configuración de los factores de uso y la verificación de los factores de uso se realizan solo en la unidad de control o en la proximidad de esta, las interacciones con la unidad de control de acceso solo se realizan únicamente a través de una conexión inalámbrica de corto alcance (menos de 100 m). Por lo tanto, el sistema de acceso es más resistente a los ataques por interceptación de tramas, porque las interacciones críticas (en particular, la parametrización previa de los factores de autenticación por parte del administrador gracias a la unidad de administración y los intentos de acceso por parte de un usuario gracias a una unidad de usuario) se realizan solo localmente a corta distancia.

Además, los factores de autenticación pueden configurarse completamente de antemano por un administrador humano, a través de la unidad de administración.

La unidad de administración y la unidad de usuario son equipos que permiten la transmisión inalámbrica de datos y cada uno de ellos está controlado por un operador humano, denominados respectivamente administrador y usuario. Por lo tanto, la unidad de administración y la unidad de usuario están separadas, es decir, son piezas de equipo separadas utilizadas por operadores humanos separados. El equipo es por ejemplo un terminal de comunicación como un teléfono inteligente (comúnmente llamado smartphone en inglés). El administrador establece los factores de autenticación mediante la unidad de administración y el usuario intenta desbloquear el acceso al dispositivo protegido con la unidad de usuario. Las claves pueden ser proporcionadas manualmente por el administrador al usuario, por ejemplo mediante validación en una aplicación o software instalado en la unidad de administración y transmisión a la unidad de usuario.

El sistema también es autónomo gracias a la recolección de energía realizada por el módulo de recolección de energía eléctrica. Esta recolección de energía es por ejemplo una producción de energía fotovoltaica, cinética, termoeléctrica, etc., y se elige en función del dispositivo a proteger, su ubicación, su función, etc. La recolección de energía permite que el sistema no dependa únicamente de una batería, que tiene una vida útil limitada. Sin embargo, el sistema puede comprender un dispositivo de almacenamiento de energía, recargado gracias a la recolección de energía (permitiendo, por ejemplo, almacenar energía fotovoltaica durante el día para uso del sistema durante la noche).

El dispositivo protegido, cuyo acceso y/o uso está controlado por el sistema, puede ser de diferentes tipos, por ejemplo, un medio de almacenamiento legible por computadora (memoria tipo llave USB, disco duro externo o interno, etc.), un vehículo (coche autoservicio protegido, bicicleta o scooter, etc.), una puerta de acceso, etc.

La ruta de acceso que permite el acceso al dispositivo protegido es, por ejemplo, un bus de transmisión de datos. El interruptor controlable permite controlar físicamente este bus de transmisión. La vía de acceso está abierta (es decir, se puede acceder al dispositivo protegido) cuando el interruptor está eléctricamente cerrado y, a la inversa, la vía de acceso está cerrada cuando el interruptor está eléctricamente abierto.

Así, por ejemplo, cuando el dispositivo protegido es un medio de almacenamiento, si el medio de almacenamiento está conectado a una computadora y la ruta de acceso está cerrada, la computadora no detecta la presencia del medio de almacenamiento y, por lo tanto, no es detectable por un operador malicioso no autorizado.

Ventajosamente y según la invención, cada factor de autenticación define al menos un criterio de validez para una clave elegida del grupo que comprende las siguientes claves:

- contraseña,
- clave transmitida por la unidad de administración,
- datos de geolocalización del dispositivo protegido y/o de la unidad de usuario,
- valores medidos por uno o más sensores electrónicos,
- datos de tiempo,
- clave de una baliza de proximidad.

De acuerdo con este aspecto de la invención, los factores de autenticación pueden ser de diferentes tipos y pueden combinarse para ofrecer la mejor seguridad posible, dependiendo del contexto de uso del dispositivo protegido.

Por lo tanto, un dispositivo protegido por el sistema de control es accesible solo si todos los factores de autenticación están desbloqueados: por ejemplo, el acceso de un usuario a un disco duro que contiene información de carácter profesional solo puede autorizarse si el disco duro está en las instalaciones comerciales (geolocalización factor o baliza de proximidad), durante el horario laboral autorizado (factor tiempo), si el usuario tiene su teléfono consigo y si el usuario ha ingresado su contraseña.

Ventajosamente y de acuerdo con la invención, el dispositivo de comunicación inalámbrica de corto alcance es un dispositivo de comunicación inalámbrica de campo cercano, y la unidad de administración y la unidad de usuario están adaptadas para suministrar energía eléctrica al módulo de recolección de energía eléctrica del dispositivo de comunicación inalámbrica de campo cercano para alimentar la unidad de control de acceso.

Según este aspecto de la invención, la comunicación inalámbrica entre la unidad de administración y el dispositivo de comunicación inalámbrica o entre la unidad de usuario y el dispositivo de comunicación inalámbrica son comunicaciones de campo cercano, tipo NFC (por *Near Field Communication* en inglés). Las comunicaciones de campo cercano permiten aumentar la seguridad del sistema de control de acceso, debiendo realizarse la pre-parametrización por parte de la unidad de administración y el intento de conexión por parte de la unidad de usuario en proximidad directa, a menos de 20cm. Además, la unidad de administración y la unidad de usuario proporcionan la energía eléctrica necesaria para alimentar la unidad de control de acceso cuando se utilizan. Así, la unidad de control puede no estar alimentada cuando no está en uso, haciéndola en particular invisible en términos de radiación electromagnética. De este modo, la unidad de control puede estar oculta y, por lo tanto, menos fácilmente detectable por los usuarios que no están informados de su ubicación.

Ventajosamente y según la invención, la unidad de control de acceso comprende al menos un interruptor controlable configurado para abrir o cerrar una fuente de alimentación eléctrica del dispositivo protegido, independiente de la unidad de control, estando cerrada la fuente de alimentación por defecto y abriéndose cuando se recibe una autorización de acceso desde el módulo de verificación.

Según este aspecto de la invención, el sistema de control de acceso también controla el suministro de energía eléctrica del dispositivo protegido. Si el acceso no está autorizado, se corta la alimentación y, por lo tanto, el dispositivo protegido es menos visible y el acceso a los contenidos del dispositivo sin autorización es más difícil.

Ventajosamente, un sistema según la invención comprende una baliza de proximidad, externa a la unidad de control, que comprende un generador de claves aleatorias adecuado para generar periódicamente una clave de proximidad y transmitir la clave de proximidad a la unidad de control mediante un protocolo de comunicación inalámbrica, dicha baliza de proximidad y dicha unidad de control están previamente emparejadas por la unidad de administración.

Según este aspecto de la invención, la baliza de proximidad permite saber si el dispositivo protegido se encuentra en una zona concreta (dentro del alcance de la baliza de proximidad) o fuera de esta zona (fuera del alcance de la baliza de proximidad). La ubicación del dispositivo protegido por la baliza de proximidad permite no depender de la información de geolocalización proporcionada por un usuario, que puede ser falsificada. La baliza de proximidad también se puede ocultar, dependiendo así el acceso al dispositivo protegido de la baliza de proximidad, pero sin que el usuario sea consciente de la necesidad de esta baliza de proximidad.

La clave de proximidad transmitida a la unidad de control de acceso es una de las claves cuyos criterios de validez se comprueban. La presencia (o ausencia) de esta clave de proximidad puede ser entonces un factor de autenticación verificado por el módulo de verificación de factores de la unidad de control de acceso.

La invención también se refiere a un medio de almacenamiento de datos, que comprende al menos dos memorias protegidas separadas, caracterizado por que el acceso a cada memoria protegida está controlado por un sistema de control de acceso según la invención.

Un medio de almacenamiento según la invención permite que en un mismo equipo cohabiten memorias independientes y se les apliquen diferentes factores de autenticación, posibilitando así tener memorias que pueden contener información que no está destinada a ser utilizada simultáneamente, o sólo puede ser utilizada bajo ciertas condiciones.

La invención también se refiere a un método para controlar el acceso a un dispositivo protegido por un sistema de control de acceso según la invención, caracterizado por que comprende:

- una etapa de pre-parametrización de los factores de autenticación por parte de un administrador utilizando la unidad de administración,
- una etapa de transmisión de al menos una clave por parte de un usuario que utiliza la unidad de usuario,
- una etapa de apertura de la ruta de acceso al dispositivo protegido si todos los factores de autenticación están desbloqueados.

Ventajosamente, un procedimiento según la invención comprende:

- una etapa de envío de una solicitud por parte del usuario a través de la unidad de usuario, a la unidad de administración,
- una etapa de validación manual por parte del administrador de la solicitud a través de la unidad de administración,
- una etapa de transmisión de una clave de validación por parte de la unidad de administración a la unidad de usuario, si la solicitud es validada por el administrador.

Según este aspecto de la invención, el administrador realiza una validación manual de la solicitud del usuario, sin procesamiento automático, lo que permite acentuar la seguridad del sistema al autorizar el acceso al dispositivo protegido únicamente a los usuarios aprobados por el administrador.

La invención también se refiere a un sistema de control de acceso, un medio de almacenamiento y un procedimiento de control de acceso caracterizados en combinación por todas o algunas de las características mencionadas anteriormente o a continuación.

5. Lista de Figuras

Otros objetivos, características y ventajas de la invención aparecerán con la lectura de la siguiente descripción dada a título no limitativo y que se refiere a las figuras anexas en las que:

- la figura 1 es una vista esquemática de un sistema de control de acceso a un dispositivo protegido según un modo de realización de la invención.
- la figura 2 es una vista esquemática de un medio de almacenamiento protegido por un sistema de control de acceso según un modo de realización de la invención.

6. Descripción detallada de una realización de la invención.

Las siguientes realizaciones son ejemplos. Aunque la descripción se refiere a una o más realizaciones, esto no significa necesariamente que cada referencia sea al mismo modo de realización, o que las características se apliquen solo a un único modo de realización. Las características simples de diferentes modos de realización también se pueden combinar para proporcionar otras realizaciones. En las figuras, las escalas y proporciones no se cumplen estrictamente, con fines ilustrativos y de claridad.

La figura 1 representa esquemáticamente un sistema de control de acceso 10 según un modo de realización de la invención.

El sistema de control 10 comprende una unidad de control de acceso 12, una unidad de administración 14 y una unidad de usuario 16.

El sistema de control de acceso tiene como objetivo controlar el acceso a un dispositivo protegido 18, por ejemplo un medio de almacenamiento, una memoria de un medio de almacenamiento, un vehículo de autoservicio sujeto a autorización previa, una puerta de acceso, etc.

El dispositivo 18 está protegido por al menos un factor de autenticación previamente parametrizado. El sistema 10 permite comprobar la validez de las claves que se le presentan en función de cada factor de autenticación: un factor de autenticación está en estado desbloqueado si una clave que se le presenta cumple los criterios de validez, y en un estado llamado bloqueado si no se le presenta ninguna clave que cumpla los criterios de validez. Por ejemplo, un factor de autenticación puede ser que una contraseña presentada coincida con una contraseña definida. Si la contraseña presentada es idéntica a la contraseña definida, el factor de autenticación está en estado desbloqueado.

El dispositivo 18 está generalmente protegido por una pluralidad de factores de autenticación previamente parametrizados, y el acceso al dispositivo protegido 18 solo se permite en caso de desbloqueo de todos los factores de autenticación.

Para ello, la unidad de control de acceso 12 comprende:

- un dispositivo de comunicación inalámbrico de corto alcance 20, que comprende un módulo de transmisión de datos inalámbrico 22 y un módulo de recolección de energía eléctrica 24,
- un módulo 26 para recibir claves,
- un módulo de verificación de factores 28,
- al menos una ruta de acceso 30 al dispositivo protegido,

- al menos un interruptor controlable, aquí un primer interruptor controlable 32a y un segundo interruptor controlable 32b, combinados en un módulo de conmutación 34.

A lo largo del texto, módulo significa un elemento de software, un subconjunto de un programa de software, que se puede compilar por separado, ya sea para uso independiente o para ensamblarse con otros módulos de un programa, o un elemento de hardware, o una combinación de un elemento de hardware y una rutina de software. Tal elemento de hardware puede incluir un circuito integrado específico para una aplicación (más conocido por las siglas ASIC por la denominación en inglés *Application-Specific Integrated Cicuit*) o un circuito lógico programable (más conocido por las siglas FPGA por el nombre en inglés *Field-Programmable Gate Array)* o un circuito de microprocesadores especializados (más conocido por las siglas DSP por el nombre en inglés *Digital Signal Procesor*) o cualquier material equivalente. En general, un módulo es por tanto un elemento (software y/o hardware) que proporciona una función.

El módulo de recepción de claves 26 permite la recepción de una o varias claves transmitidas por diferentes elementos, por ejemplo la unidad de usuario 16, uno o varios sensores externos 36, una baliza de proximidad 38 a través de un módulo de recepción inalámbrico 40, etc.

Todas las claves recibidas son transmitidas al módulo de verificación de factores 28, el cual verifica la validez de cada factor de autenticación, es decir verifica si al menos una clave transmitida valida los criterios de cada factor de autenticación. Para esta verificación, el módulo de verificación 28 tiene acceso a una memoria segura 42 que contiene los factores de autenticación previamente parametrizados y los criterios asociados.

Las transmisiones de las claves al módulo de verificación de factores 28 se realizan de forma cifrada, realizándose el descifrado de las claves únicamente en el módulo de verificación de claves 28 (mediante un firmware de descifrado), para mayor seguridad. El módulo de verificación de claves 28 y la memoria segura 42 se combinan preferiblemente en el mismo componente seguro, de modo que las claves descifradas no sean accesibles fuera de este componente.

Si todos los factores de autenticación se desbloquean después de su verificación, el módulo de verificación de claves 28 proporciona una autorización de acceso, transmitida al módulo de conmutación 34.

La autorización de acceso al dispositivo protegido 18 provoca la conmutación de los interruptores vinculados al dispositivo protegido 18: el primer interruptor controlable 32a se cierra eléctricamente para abrir la vía de acceso 30 al dispositivo protegido 18 en caso de recepción de una autorización de acceso, o abrir eléctricamente para cerrar la ruta de acceso 30 si no se recibe autorización (por lo tanto, por defecto). Además, el segundo interruptor controlable 32b también puede activarse al mismo tiempo que el primer interruptor controlable 32a, estando conectado este segundo interruptor 32b a una fuente de alimentación 44 del dispositivo protegido 18: de manera similar, el segundo interruptor 32b es cerrado eléctricamente para alimentar el dispositivo protegido 18 en caso de recibir una autorización de acceso, o eléctricamente abierto para bloquear la alimentación 44 del dispositivo protegido 18 si no se recibe autorización de acceso.

Así, sin autorización de acceso, el dispositivo protegido 18 no es accesible ni está alimentado. Si este dispositivo protegido 18 es una memoria, es imposible intercambiar datos con esta memoria, ni acceder a los datos, y la memoria no es visible.

El acceso al dispositivo protegido 18 está regulado por un administrador, lo que permite determinar quién tiene acceso al dispositivo protegido 18 y en qué condiciones. El usuario desea acceder al dispositivo protegido 18, por lo que debe cumplir las condiciones establecidas por el administrador.

El administrador preparametriza los factores de autenticación del dispositivo 18 protegido mediante la unidad de administración 14. La unidad de administración 14 es por ejemplo un teléfono inteligente que comprende un software (o aplicación) que permite la elección de factores de autenticación y la preconfiguración de estos factores. La unidad de administración 14 permite la transmisión de los factores de autenticación elegidos en la memoria segura, a través del dispositivo 20 de comunicación inalámbrica de corto alcance. Los datos que contienen los factores de autenticación (transmitidos en forma encriptada) se transmiten a través del módulo de transmisión inalámbrica 22.

El dispositivo de comunicación inalámbrica 20 también comprende un módulo de recolección de energía 24, que permite recolectar energía de diferentes fuentes (fotovoltaica, cinética, termoeléctrica), en particular proveniente de la unidad de administración 14 (por inducción electromagnética). El módulo de recolección de energía 24 permite alimentar la unidad de control de acceso 12, en particular todos los módulos de la unidad de control de acceso 12.

En esta realización, el dispositivo de comunicación inalámbrica 20 es un dispositivo de comunicación inalámbrica de campo cercano, del tipo NFC. El módulo de recolección de energía 24 está así adaptado para recolectar energía de la unidad de administración 14, con el fin de alimentar a la unidad de control 12 durante el tiempo para realizar la preconfiguración de los factores de autenticación.

Una vez pre-parametrizados los factores, el dispositivo 18 queda protegido por los factores de autenticación. En particular, la ruta de acceso 30 al dispositivo protegido 18 está cerrada por defecto (y eventualmente el dispositivo protegido 18 no esté alimentado eléctricamente).

Cuando un usuario desea acceder al dispositivo protegido 18, debe abrir la ruta de acceso 30 (y eventualmente la

fuente de alimentación eléctrica 44) del dispositivo protegido 18. Para ello, debe cumplir con los criterios definidos por todos los factores de autenticación. Las claves son recibidas por el módulo de recepción de claves 26, transmitidas al módulo de verificación de claves 28 y verificadas, como se explicó anteriormente. El usuario utiliza la unidad de usuario 16 para acceder al dispositivo protegido 18. La unidad de usuario 16 es, por ejemplo, un teléfono inteligente que comprende un software (o aplicación) que permite intentar acceder al dispositivo protegido 18 y la transmisión de al menos una clave. La unidad de usuario 16 se comunica con el módulo de transmisión inalámbrica 22 del dispositivo de comunicación inalámbrica de corto alcance 20 mediante un protocolo de comunicación inalámbrica de corto alcance como por ejemplo IEEE 802.15.1 (en particular Bluetooth), IEEE 802.15.11 (en particular Wi-fi), etc. Preferentemente, la comunicación tiene lugar en campo cercano (distancia generalmente inferior a 20 cm, preferentemente inferior a 10 cm) a través de una tecnología como NFC.

Al igual que la unidad de administración 14, la unidad de usuario 16 puede proporcionar la energía eléctrica necesaria para el funcionamiento de la unidad de control 12 por inducción electromagnética. En determinadas realizaciones, la unidad de control 12 solo puede ser funcional cuando una unidad de administración 14 o una unidad de usuario 16 está suministrando energía, y está apagada el resto del tiempo, para ocultar su presencia reduciendo las emisiones electromagnéticas.

Al menos una clave recibida es transmitida por la unidad de usuario 16. Esta clave puede ser una clave que verifique un factor simple, por ejemplo, solo el hecho de que la unidad de usuario 16 está presente y que un usuario desea acceder al dispositivo protegido 18, o un factor más complejo, como una contraseña ingresada por el usuario en la aplicación de la unidad de usuario 16. La unidad de usuario 16 también puede transmitir varias claves, algunas de las cuales independientemente de la voluntad del usuario, para desbloquear o bloquear ciertos factores de autenticación: por ejemplo, las claves pueden ser valores registrados por sensores de la unidad de usuario 16 (sensor de temperatura, giroscopio, geolocalización, reloj, etc.), o un número de identificación del teléfono. Por ejemplo, sólo se puede autorizar el acceso al dispositivo protegido 18 si el usuario utiliza un teléfono autorizado, si el teléfono está dispuesto en una determinada configuración (colocado sobre un mueble, por lo tanto, horizontalmente por ejemplo), si la temperatura está dentro de un rango determinado, etc.

De manera similar, durante un intento de acceso al dispositivo protegido 18 por parte de un usuario, el módulo de recepción de claves 26 puede recibir claves de los sensores externos 36. Las claves pueden ser valores registrados por los sensores externos 36 (sensor de temperatura, giroscopio, geolocalización, reloj, sensor de humo, sensor químico, etc.). Por ejemplo, se puede prohibir el acceso al dispositivo protegido 18 fuera de los intervalos de tiempo predeterminados, si el usuario ha excedido un tiempo máximo de conexión, si el dispositivo protegido 18 no está en una disposición particular; una puerta de acceso no puede desbloquearse si un sensor químico detecta una presencia anormal de un componente químico en la habitación a la que da acceso la puerta, etc.

Una clave proporcionada por la unidad de usuario 16 también puede ser proporcionada por un administrador, a través de la unidad de administración 14. Para obtener esta clave, el usuario envía una solicitud a través de la unidad de usuario 16 a la unidad de administración 14. Esta solicitud se envía, por ejemplo, por SMS (por *Servicio de mensajería corta* en inglés) desde la aplicación del usuario de la unidad 16. El administrador recibe la solicitud en la unidad de administración 14 y valida (o no valida) manualmente la solicitud. Los criterios de validación son elegidos por el administrador: por ejemplo, si un identificador de la unidad de usuario 16 (su número de teléfono por ejemplo) pertenece a una lista aprobada por el administrador, puede optar por validar la solicitud. Si el administrador carece de información sobre el usuario, puede llamarlo por conexión telefónica entre la unidad de administración 14 y la unidad de usuario 16 antes de decidir si valida o no la solicitud. Una vez que la solicitud ha sido validada por el administrador, la unidad de administración 14 envía una clave a la unidad de usuario 16 que le permite desbloquear al menos un factor de autenticación. La clave puede configurarse, por ejemplo válida solo durante un intervalo de tiempo específico o según la geolocalización de la unidad de usuario 16 o del dispositivo 18 protegido.

En este modo de realización, el módulo receptor de claves también puede recibir claves de una baliza de proximidad 38, a través del módulo receptor inalámbrico 40 de la unidad de control 12. Esta baliza de proximidad 38 envía permanentemente una clave generada aleatoriamente (y encriptada), denominada clave de proximidad. Durante la preconfiguración, la unidad administradora 14 puede emparejar la unidad de control 12 y la baliza de proximidad 38, de modo que la unidad de control 12 considere la recepción de la clave de proximidad de la etiqueta de proximidad 38 como uno de los factores de autenticación.

La baliza de proximidad 38 se comunica a través de un protocolo de comunicación inalámbrica de corto alcance, que puede ser idéntico o diferente del protocolo de comunicación entre la unidad de usuario 16 y el dispositivo de comunicación inalámbrica 20. Si los dos protocolos de comunicación son diferentes, la interceptación de la clave o claves proporcionadas por el usuario y de la clave de proximidad emitida por la baliza de proximidad 38 es complicada, porque es necesario recuperar tramas de dos protocolos diferentes.

Además, la baliza de proximidad 38 está generalmente oculta al usuario, y permite asegurar la presencia del usuario cerca de esta baliza 38 (dentro de la distancia permitida por la comunicación inalámbrica de corto alcance). Por ejemplo, una baliza de proximidad 38 oculta en un local profesional permite garantizar que el acceso al dispositivo protegido 18, por ejemplo un medio de almacenamiento, sólo sea posible cuando el medio de almacenamiento está cerca de la baliza 38 de proximidad, y por tanto en el local comercial. El usuario puede no saber que su proximidad a

la baliza de proximidad 38 es una condición para desbloquear el medio de almacenamiento, lo que permite aumentar la protección contra intrusiones.

El factor de autenticación también puede ser exclusivo, es decir que se autoriza el acceso al dispositivo si una clave no está en un valor preciso o si no se recibe una clave. En particular, en el ejemplo de la baliza de proximidad 38 en un local profesional, el acceso a un dispositivo protegido 18, por ejemplo un medio de almacenamiento que comprende datos personales, puede bloquearse si el dispositivo protegido 18 está cerca de la baliza de proximidad 38 y por lo tanto en el local profesional. El criterio así definido por el factor de autenticación es la no recepción de una clave de la baliza de proximidad 38.

Una aplicación de este ejemplo se presenta con más detalle con referencia a la figura 2, que representa esquemáticamente un medio de almacenamiento 45 protegido por un sistema de control de acceso según un modo de realización de la invención.

En particular, el medio de almacenamiento 45 comprende dos memorias protegidas, distintas, independientes y separadas (en diferentes componentes), una primera memoria protegida 46a y una segunda memoria protegida 46b.

El medio de almacenamiento 45 comprende un conector, aquí un conector USB 48 (por Universal Serial Bus en inglés), que permite, gracias a una pluralidad de pines (no mostrados), transmitir datos a través de un bus de transmisión de datos 50 y alimentar el medio de almacenamiento 45 con una fuente de alimentación eléctrica 44. El medio de almacenamiento 45 puede ser, por ejemplo, una llave USB o un disco duro externo, conectado a una computadora usando el conector USB 48. El medio de almacenamiento 45 también puede ser un disco duro interno de una computadora, conectado directamente dentro de la computadora a través de un conector específico.

El medio de almacenamiento 45 comprende una unidad de control del sistema de control de acceso 12, como se describió anteriormente con referencia a la figura 1. Las interacciones con la unidad de control 12 se realizan, como se describió anteriormente, gracias a la unidad de administración 14 (para preconfiguración) y una unidad de usuario 16 (para el intento de acceso).

La unidad de control 12 permite controlar el acceso a las dos memorias protegidas y su alimentación. Cada memoria protegida puede considerarse como un dispositivo protegido por el sistema de control de acceso. El acceso a cada memoria protegida controlada se rige por un conjunto de factores de autenticación específicos de cada memoria protegida. Para ello, la unidad de control 12 incluye interruptores controlables combinados en un módulo de conmutación 34, aquí:

- un primer interruptor controlable 32a y un segundo interruptor controlable 32b, que permiten respectivamente abrir/cerrar el acceso a los datos de la primera memoria protegida 46a y a la alimentación de la primera memoria protegida 46a,

- un tercer interruptor controlable 32c y un cuarto interruptor controlable 32d, que permiten respectivamente abrir/cerrar el acceso a los datos de la segunda memoria protegida 46b y la alimentación de la segunda memoria protegida 46b.

Los conmutadores controlables se controlan según se haya recibido o no una autorización de acceso, como se ha descrito anteriormente.

Tal medio de almacenamiento 45 es particularmente adecuado para una aplicación profesional y personal, o para ocultar datos.

En la aplicación profesional y personal, la primera memoria protegida 46a es por ejemplo una memoria dedicada a datos personales, y la segunda memoria protegida 46b está dedicada a datos profesionales. Cuando el usuario se encuentra fuera del recinto profesional, está autorizado a acceder únicamente a la primera memoria protegida 46a. Cuando el usuario se encuentra en el local profesional, una baliza de proximidad 38 como la descrita anteriormente permite autorizar el acceso a la segunda memoria protegida 46b y bloquear el acceso a la primera memoria protegida 46a, lo que permite garantizar que los datos personales nunca se accesibles en el entorno profesional y que los datos profesionales nunca son accesibles en el entorno personal. Si cada una de las memorias protegidas incluye un sistema operativo, es posible utilizar dos sistemas operativos diferentes y completamente separados (un sistema sin tener acceso a los datos del otro sistema), lo que es particularmente útil para las llamadas prácticas BYOD (*Bring Your Own Device* en inglés, ya sea “trae tu propio dispositivo personal”) o COPE (Corporate Owned, Personally Enabled en inglés, o "Propiedad corporativa, autorizada en uso privado") en el que la misma máquina se puede utilizar por motivos personales o profesionales sin aumentar los riesgos de seguridad.

En la aplicación de ocultación de datos, una primera memoria protegida 46a puede incluir cualquier dato y ser accesible por defecto. Una segunda memoria protegida 46b incluye datos confidenciales y solo es accesible y visible mediante la validación de los criterios del factor de autenticación. Así, si el medio de almacenamiento está conectado a un ordenador para comprobar su contenido, sólo la primera memoria protegida 46a será accesible y visible, lo que llama menos la atención que si no hubiera ninguna memoria accesible o visible. Por lo tanto, la segunda memoria protegida 46b no se comprueba porque no es visible.

REIVINDICACIONES

1. Sistema de control de acceso a un dispositivo (18) protegido por al menos un factor de autenticación preconfigurado, definiendo cada factor de autenticación al menos un criterio de validez para una clave y estando en un estado denominado desbloqueado si una clave que se le presenta cumple los criterios de validez, y un estado denominado bloqueado si ninguna clave que se le presenta cumple los criterios de validez, que comprende:

- una unidad de control de acceso (12) que comprende:

  - un dispositivo de comunicación inalámbrico de corto alcance (20), que comprende un módulo de transmisión de datos inalámbrico (22) y un módulo de recolección de energía eléctrica (24),

  - un módulo (26) de recepción de claves, adaptado para recibir al menos una clave,

  - un módulo (28) de verificación de factores, adaptado para verificar la validez de cada factor de autenticación preconfigurado con al menos una clave recibida por el módulo (26) de recepción de claves, y para proporcionar una autorización de acceso si todos los factores de autenticación están en el estado desbloqueado,

  - al menos un camino de acceso (30), adaptado para permitir el acceso al dispositivo protegido (18),

  - al menos un interruptor controlable (32a, 32c), configurado para abrir o cerrar la ruta (30) de acceso al dispositivo protegido (18), estando la ruta de acceso (30) por defecto cerrada y abierta en caso de recibir una autorización de acceso proveniente del módulo (28) de verificación,

- una unidad de administración (14), adaptada para permitir preconfigurar cada factor de autenticación por interacción con el módulo de transmisión inalámbrica de datos (22) del dispositivo de comunicación (20) de la unidad de control de acceso (12),

- una unidad de usuario (16), distinta de la unidad de administración (14), configurada para transmitir al menos una clave al módulo (26) de recepción de claves, a través del módulo de transmisión inalámbrica de datos (22).

2. Sistema de control según la reivindicación 1, caracterizado por que cada factor de autenticación define al menos un criterio de validez de una clave elegida del grupo que comprende las siguientes claves:

- clave,

- clave transmitida por la unidad de administración (14),

- datos de geolocalización del dispositivo protegido (18) y/o de la unidad de usuario (16),

- valores medidos por uno o más sensores electrónicos,

- datos de tiempo,

- clave procedente de una tarjeta de proximidad (38).

3. Sistema de control según una de las reivindicaciones 1 o 2, caracterizado por que el dispositivo de comunicación inalámbrico de corto alcance (20) es un dispositivo de comunicación inalámbrico de campo cercano, y por que la unidad de administración (14) y la unidad de usuario (16) están adaptadas para suministrar energía eléctrica al módulo de recolección de energía eléctrica (24) del dispositivo inalámbrico de comunicación de campo cercano (20) para alimentar la unidad de control de acceso (12).

4. Sistema de control según una de las reivindicaciones 1 a 3, caracterizado por que la unidad de control de acceso (12) comprende al menos un interruptor controlable (32b, 32d) configurado para abrir o cerrar una alimentación eléctrica (44, 44a, 44b) del dispositivo protegido (18), independiente de la unidad de control (12), estando la alimentación (44, 44a, 44b) por defecto cerrada y estando abierta en caso de recibir una autorización de acceso procedente del módulo (28) de verificación.

5. Sistema de control según una de las reivindicaciones 1 a 4, caracterizado por que comprende una baliza de proximidad (38), externa a la unidad de control (12), que comprende un generador de claves aleatorias adaptado para generar periódicamente una clave de proximidad y transmitir la clave de proximidad a la unidad de control (12) mediante un protocolo de comunicación inalámbrica, dicho baliza de proximidad (38) y dicha unidad de control (12) estando emparejada previamente por la unidad de administración (14).

6. Medio de almacenamiento de datos, que comprende al menos dos memorias protegidas separadas (46a, 46b), caracterizado por que el acceso a cada memoria protegida (46a, 46b) está controlado por un sistema de control de acceso (10) según una de las reivindicaciones 1 a 5, estando comprendido dicho sistema de control de acceso (10) en el medio de almacenamiento de datos.

7. Método para controlar el acceso a un dispositivo (18) protegido por un sistema de control de acceso (10) según una de las reivindicaciones 1 a 5, caracterizado por que comprende:

- una etapa de preconfiguración de factores de autenticación por parte de un administrador utilizando la unidad de administración (14),

- una etapa de transmisión de al menos una clave por parte de un usuario utilizando la unidad de usuario (16),

- una etapa de apertura de un camino (30) para acceder al dispositivo protegido (18) si todos los factores de autenticación están desbloqueados.

8. Método de control de acceso según la reivindicación 7, caracterizado por que comprende:

- una etapa de envío de una solicitud por parte del usuario a través de la unidad de usuario (16), a la unidad de administración (14),

- una etapa de validación manual, por parte del administrador, de la solicitud a través de la unidad de administración (14),

- una etapa de transmisión de una clave de validación por parte de la unidad de administración (14) a la unidad de usuario (16), si la solicitud es validada por el administrador.

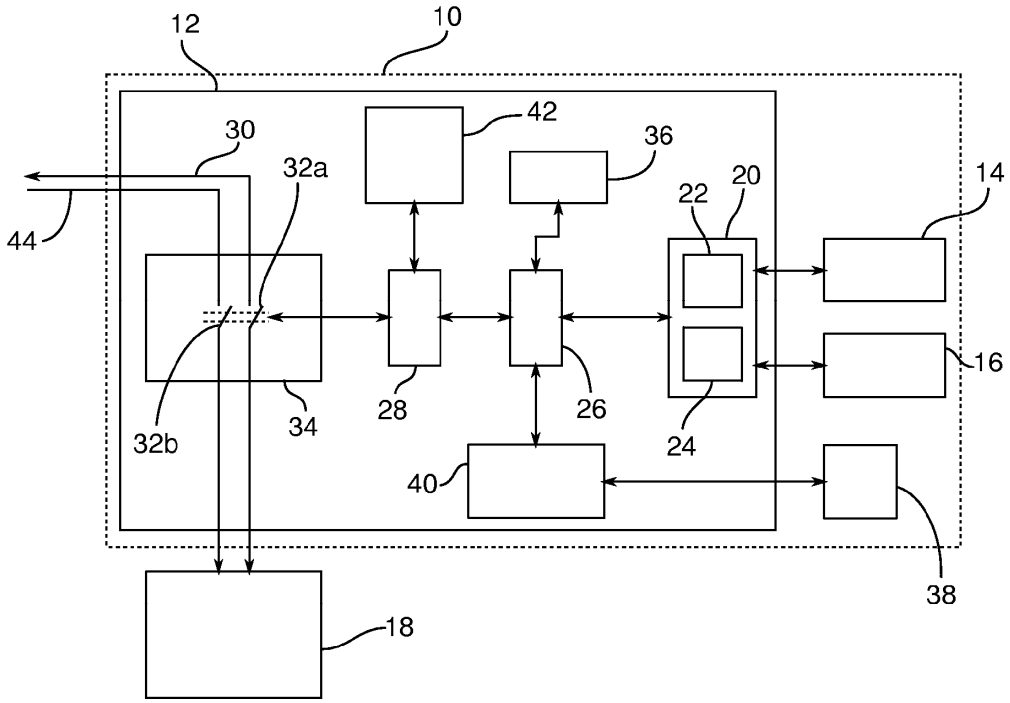
12
10
42
30
36
32a
20
22
14
44
16
32b
34
28
26
24
40
38
18

Fig. 1

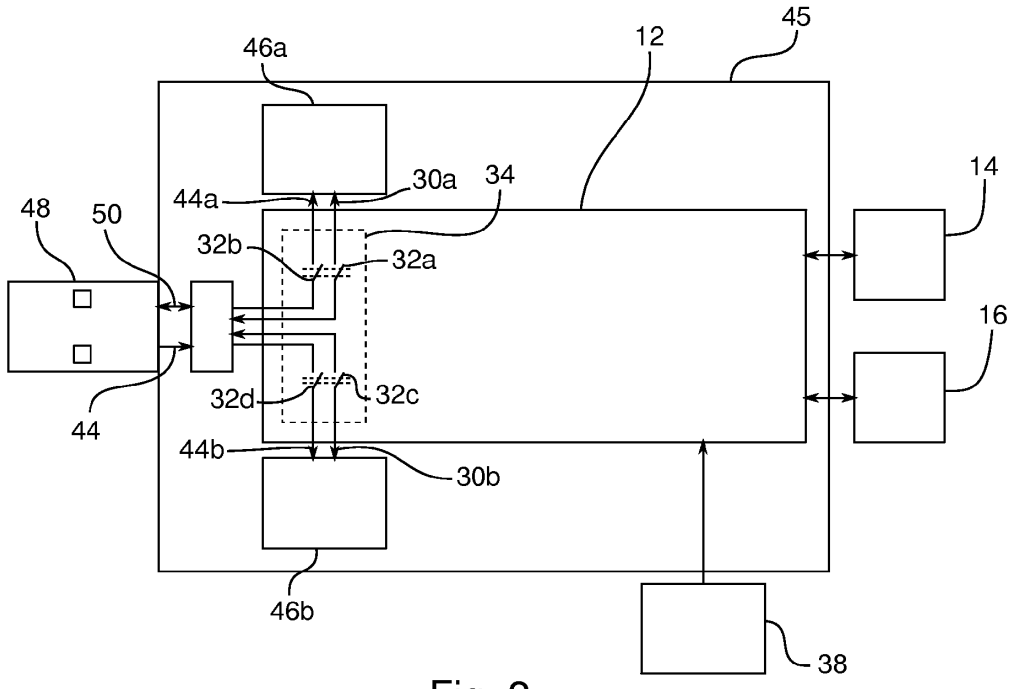
45
46a
12
14
30a
34
44a
48
50
32b
32a
16
32d
32c
44
44b
30b
46b
38

Fig. 2