(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 659 835**

(51) Int. CI.:

G07C 9/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **17.10.2014 PCT/EP2014/072311**

(87) Fecha y número de publicación internacional: **23.04.2015 WO15055812**

(96) Fecha de presentación y número de la solicitud europea: **17.10.2014 E 14784491 (4)**

(97) Fecha y número de publicación de la concesión europea: **22.11.2017 EP 3058554**

(54) Título: **Comunicación y procesamiento de datos de credenciales**

(30) Prioridad:

18.10.2013 US 201314057271

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
19.03.2018

(73) Titular/es:

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

(72) Inventor/es:

SINGH, SONA

(74) Agente/Representante:

ISERN JARA, Jorge

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Comunicación y procesamiento de datos de credenciales

Antecedentes de la invención y estado de la técnica

La presente invención se refiere, en general, a soluciones para el manejo de datos de credenciales de una manera eficaz, por ejemplo, en relación con el control de acceso. Más específicamente, la invención se refiere a una unidad de lectura de acuerdo con el preámbulo de la reivindicación 1, un sistema de comunicación de datos de acuerdo con el preámbulo de la reivindicación 2 y un método de acuerdo con el preámbulo de la reivindicación 8. La invención también se refiere a un producto de programa informático de acuerdo con reivindicación 13 y un medio legible por ordenador de acuerdo con la reivindicación 14.

En los edificios modernos, especialmente en los locales comerciales, a menudo se utilizan sistemas de control de acceso electrónico (CAO) para controlar las entradas y las salidas de las diversas instalaciones. En este caso, los llamados datos de credenciales personales se usan normalmente como una base para definir qué sujetos están autorizados a entrar en una zona determinada durante un intervalo de tiempo dado. Los datos de credenciales pueden estar incorporados en un llavero de control remoto, una tarjeta inteligente, una tarjeta de proximidad u otro soporte apropiado, por ejemplo, una tarjeta de módulo de identidad de abonado (SIM) de un teléfono móvil o un asistente digital personal (PDA).

Una unidad de lectura, por ejemplo, del tipo de comunicación de radio de corto alcance, puede emplearse para registrar los datos de credenciales y reenviar los datos a un nodo de control de acceso. En este contexto, se entiende que el tipo de interfaz de comunicación de radio de corto alcance se adhiere a un protocolo inalámbrico conocido, por ejemplo, el protocolo NFC (comunicación de campo cercano), Bluetooth, ZigBee o WiFi. Siempre que se encuentren los datos de credenciales para representar a un sujeto autorizado, el nodo de control de acceso hace que se envíe un mensaje de acceso a un mecanismo de control de una puerta asociada al lector, por ejemplo a través de un protocolo UART (UART = receptor/transmisor asíncrono universal), lo que resulta en que la puerta se abre.

El documento US 2008/0163361 describe una solución, para proporcionar una red de acceso seguro. En este caso, las decisiones de acceso se toman mediante una credencial portátil usando datos y algoritmos almacenados en la credencial. Ya que las decisiones de acceso se toman por la credencial portátil, pueden emplearse hosts no conectados en red o hosts locales que no necesitan necesariamente conectarse a un controlador de acceso central o base de datos, reduciendo de este modo el coste de construcción y mantenimiento de la red de acceso seguro.

El documento US 2011/0187493 desvela un sistema, en el que el acceso se controla dentro de una instalación de múltiples habitaciones. Un invitado de la instalación de múltiples habitaciones se le permite en este caso confirmar remotamente las reservas a la instalación, así como eludir la recepción de la instalación de múltiples habitaciones con el fin de registrarse. En una localización dentro de la instalación, a los invitados se les permite confirmar su llegada, registrarse y tener su credencial de acceso escrita con datos de acceso personalizados que pueden usarse durante la estancia del invitado.

El documento 2012/278901 A1 presenta un sistema para la gestión de los derechos de acceso a los datos de funcionamiento y/o a los datos de control de edificios o complejos de edificios que incluyen un servicio de liberación de comunicaciones que se ejecuta en un servidor principal. Este servicio de liberación libera una comunicación de un usuario, que está registrado con una identidad, con los edificios o los complejos de edificios presentados para él en una lista cuando su identidad se corresponde con una identidad presentada en la lista.

El documento US 2013/093563 A1 presenta un método y aparato para controlar el acceso desde una primera zona a una segunda zona que incluye recibir una señal de identificación desde un dispositivo de entrada de identificador, y comprobar los datos almacenados que indican que la identidad representada por la señal de identificación está registrada como presente en la primera zona. Si se cumple un requisito de acceso predeterminado, entonces se genera una señal de paso en el primer controlador de acceso. Para controlar el acceso desde la segunda zona a una tercera zona, se envía un mensaje de entrada a un segundo controlador con al menos la identidad y los datos que indican que la identidad está presente en una zona de acceso del segundo controlador. Se envía un mensaje de salida a un tercer controlador que controla el acceso a la primera zona, que incluye al menos la identidad y los datos que indican que la identidad no está presente en una zona de acceso del tercer controlador.

Problemas asociados con el estado de la técnica

En consecuencia, se conocen soluciones de acceso flexibles. Sin embargo, aún no existe un sistema eficaz que permita a diferentes empresas/organizaciones compartir una o más puertas automáticas (u otros componentes relacionados con el acceso) de un edificio sin requerir una función de control central para dichas una o más puertas/componentes, que sea común para todas las organizaciones.

Sumario de la invención

El objeto de la presente invención es por lo tanto resolver el problema anterior, y ofrecer de este modo una solución flexible y eficaz que permita a diferentes empresas/organizaciones compartir convenientemente una o más puertas automáticas (u otros componentes relacionados con el acceso).

De acuerdo con un aspecto de la invención, el objetivo se consigue mediante la unidad de lectura descrita inicialmente, en la que la unidad de lectura, que está asociada con una puerta, está configurada para comunicarse con al menos un segundo receptor de datos de credenciales para provocar al menos una decisión de acceso con respecto al espacio bien definido a efectuar. La unidad de lectura está configurada además para reenviar cada pieza registrada de datos de credenciales al primer receptor de datos de credenciales controlado por una primera organización o a uno específico del al menos un segundo receptor de datos de credenciales controlado por una organización respectiva diferente de la primera organización basándose en una dirección vinculada a la pieza de datos de credenciales. La dirección vinculada identifica al primer receptor de datos de credenciales o al uno específico del al menos un segundo receptor de datos de credenciales. La dirección vinculada (preferiblemente del tipo protocolo de internet), a su vez, se almacena o en un módulo de memoria asociado con la unidad de lectura; o en un soporte (por ejemplo, una tarjeta) que contiene la pieza de datos de credenciales, dicho soporte está configurado para presentarse a la unidad de lectura para registrar la pieza de datos de credenciales.

Esta unidad de lectura es ventajosa debido a que hace posible que diferentes empresas y organizaciones controlen diversos componentes relacionados con el acceso, independientemente entre sí mientras que comparten una unidad de lectura común.

De acuerdo con otro aspecto de la invención, el objetivo se consigue mediante el sistema de comunicación de datos descrito inicialmente, en el que el sistema de comunicación de datos incluye al menos un segundo receptor de datos de credenciales configurado para recibir datos de credenciales registrados por la unidad de lectura, y en respuesta a lo mismo provocar al menos una decisión de acceso con respecto al espacio bien definido a efectuar. Además, la unidad de lectura está conectada de manera comunicativa con el primer receptor de datos de credenciales y a el al menos un segundo receptor de datos de credenciales. La unidad de lectura está configurada además para reenviar una pieza registrada de datos de credenciales al primer receptor de datos de credenciales o al uno específico del al menos un segundo receptor de datos de credenciales basándose en una dirección vinculada a la pieza de datos de credenciales, dirección que identifica el primer receptor de datos de credenciales o uno específico del al menos un segundo receptor de datos de credenciales. La dirección vinculada, a su vez, se almacena en un módulo de memoria asociado con la unidad de lectura, o en un soporte que contiene la pieza de datos de credenciales, soporte que está configurado para presentarse a la unidad de lectura para registrar la pieza de datos de credenciales. Las ventajas de este sistema son las mismas que las asociadas con la unidad de lectura propuesta anteriormente.

De acuerdo con la invención, la al menos una decisión de acceso implica conceder o denegar el acceso al espacio bien definido. En este caso, el componente de construcción relacionado con el control de acceso incluye un mecanismo de bloqueo configurado para habilitar o evitar selectivamente el acceso al espacio bien definido a través de una puerta asociada con la unidad de lectura. En respuesta a una pieza de datos de credenciales recibida, cada uno del primer y al menos un segundo receptor de datos de credenciales está configurado para comprobar la pieza de datos de credenciales contra una base de datos que define un conjunto de derechos de acceso de los usuarios al espacio bien definido. Si se encuentra que la pieza de datos de credenciales designa un usuario autorizado, los receptores de datos de credenciales se configuran para hacer que se envíe un mensaje de concesión de acceso al mecanismo de bloqueo, mensaje de concesión de acceso que ordena al mecanismo de bloqueo abrir la puerta. De lo contrario, es decir, si se encuentra que el usuario no está autorizado, los receptores de datos de credenciales están configurados para evitar que el mensaje de concesión de acceso se envíe al mecanismo de bloqueo. Por lo tanto, el acceso a un edificio, o a parte del mismo, puede controlarse de una manera muy conveniente y eficaz.

De acuerdo con otra realización preferida de este aspecto de la invención, la al menos una decisión de acceso implica registrar una entrada a o una salida del espacio bien definido. En este caso, en respuesta a una pieza recibida de datos de credenciales, cada uno del primer y al menos un segundo receptor de datos de credenciales está configurado para: registrar una entrada si se recibe la pieza de datos de credenciales a través de un primer escáner de la unidad de lectura, y registrar una salida si se recibe la pieza de datos de credenciales a través de un segundo escáner de la unidad de lectura. Por lo tanto, puede implementarse convenientemente una perforadora digital/un reloj de fichar.

De acuerdo con una realización preferida adicional de este aspecto de la invención, el sistema de comunicación de datos incluye un nodo de control que está conectado de manera comunicativa con la unidad de lectura y a cada uno del primer y al menos un segundo receptor de datos de credenciales. El nodo de control está configurado para recibir datos de credenciales desde la unidad de lectura y reenviar los datos de credenciales recibidos a un receptor de datos de credenciales identificado por la dirección vinculada a los datos de credenciales. El nodo de control también está configurado para recibir mensajes de concesión de acceso desde el primero y el al menos un segundo receptor de datos de credenciales; y para reenviar los mensajes de concesión de acceso recibidos al mecanismo de bloqueo. Cada mensaje de concesión de acceso está configurado en este caso para ordenar que se abra el

mecanismo de bloqueo durante un intervalo predeterminado, por ejemplo, para permitir que una persona pase a través de una puerta. Esto permite una implementación altamente eficaz de una puerta automática o función similar.

De acuerdo con otra realización preferida más de este aspecto de la invención, el nodo de control está conectado de manera comunicativa con al menos una unidad de lectura, además de a dicha unidad de lectura. El nodo de control está configurado además para recibir datos de credenciales de la unidad de lectura adicional, reenviar los datos de credenciales recibidos a un receptor de datos de credenciales identificado por la dirección vinculada a los datos de credenciales, recibir mensajes de concesión de acceso desde el primer y al menos un segundo receptor de datos de credenciales, y reenviar los mensajes de concesión de acceso recibidos a un mecanismo de bloqueo además de a dicho mecanismo de bloqueo. También en este caso cada mensaje de concesión de acceso está configurado para ordenar que se abra el mecanismo de bloqueo adicional durante un intervalo predeterminado. Por lo tanto, el nodo de control puede controlar múltiples mecanismos de bloqueo de una manera directa y eficaz.

Preferentemente, las direcciones de enlaces que identifican al primer y a el al menos un segundo receptor de datos de credenciales son direcciones del protocolo de internet.

De acuerdo con otro aspecto de la invención, el objeto se consigue por el método descrito inicialmente, en el que se presume que la red incluye un primer receptor de datos de credenciales y al menos un segundo receptor de datos de credenciales. El método implica reenviar cada pieza registrada de datos de credenciales o al primer receptor de datos de credenciales, o a uno específico del al menos un segundo receptor de datos de credenciales basándose en una dirección vinculada a la pieza de datos de credenciales, dirección que identifica el primer receptor de datos de credenciales o el específico del al menos un segundo receptor de datos de credenciales. La dirección vinculada, a su vez, está almacenada en un módulo de memoria asociado con la unidad de lectura, o en un soporte que contiene la pieza de datos de credenciales, soporte que está configurado para presentarse a la unidad de lectura para registrar la pieza de datos de credenciales. Las ventajas de este método, así como las realizaciones preferidas de las mismas, son evidentes a partir de la exposición anterior haciendo referencia a la unidad de lectura y al sistema de comunicación de datos propuestos.

De acuerdo con un aspecto adicional de la invención, el objeto se consigue mediante un producto de programa informático, que puede cargarse en la memoria de un ordenador, que incluye un software para realizar las etapas del método propuesto anteriormente cuando se ejecuta en un ordenador.

De acuerdo con otro aspecto de la invención, el objeto se consigue mediante un medio legible por ordenador, que tiene un programa grabado en el mismo, donde el programa hace que un ordenador realice el método propuesto anteriormente cuando el programa se carga en el ordenador.

Otras ventajas, características beneficiosas y aplicaciones de la presente invención serán evidentes a partir de la siguiente descripción y de las reivindicaciones dependientes.

Breve descripción de los dibujos

La invención se explicará más detalladamente a continuación por medio de las realizaciones preferidas, que se desvelan como ejemplos, y haciendo referencia a los dibujos adjuntos.

La figura 1 muestra un diagrama de bloques sobre un sistema de control de acceso de la técnica anterior;

las figuras 2 a 6 muestran diagramas de bloques sobre unos sistemas de comunicación de datos de acuerdo con diversas realizaciones de la invención; y

la figura 7 ilustra, por medio de un diagrama de flujo, el método general de acuerdo con la invención.

Descripción de las realizaciones preferidas de la invención

Inicialmente, se hace referencia a la figura 1 que muestra un diagrama de bloques sobre un sistema de control de acceso de la técnica anterior. En este caso, los lectores primero y segundo, 110 y 120, están conectados a un panel de control primero y segundo 130 y 160, respectivamente. Cada lector 110 y 120 está dispuesto para controlar las entradas a través de una puerta 115 basándose en la comunicación con los paneles de control 130 y 160.

El primer panel de control 130, a su vez, está controlado por un primer nodo EAC 140 y se basa en las entradas de una primera base de datos 150 asociada con el primer panel de control 130. Más precisamente, cuando un primer usuario se aproxima a la puerta 115 y presenta una credencial de datos C (por ejemplo, en la forma de una tarjeta de proximidad, llavero de control remoto, tarjeta inteligente u otro soporte apropiado, tal como una tarjeta de módulo de identidad de abonado (SIM) de un teléfono móvil o un asistente digital personal (PDA)) para un lector dado, dicho un primer lector 110, este lector 110 lee los datos de credenciales CD del soporte de datos C y envía los datos de credenciales CD al primer panel de control 130. A continuación, el primer panel de control 130 comprueba la primera base de datos 150 para cualquier entrada que coincida con los datos de credenciales CD. Si se encuentra una

coincidencia, el primer panel de control 130 consulta el primer nodo EAC 140 para determinar si el primer usuario (es decir, la persona asociada con los datos de credenciales CD) puede o no entrar a través de la puerta 115. Ya que se encuentra que el primer usuario está autorizado, el primer panel de control 130 envía un primer mensaje de concesión de acceso AG1 (por ejemplo, a través de un protocolo UART) a un mecanismo de control de bloqueo 105 en la puerta 115. En respuesta al primer mensaje de concesión de acceso AG1, el mecanismo de control de bloqueo 105 desbloquea la puerta 115, de tal manera que el primer usuario pueda entrar.

Puede suponerse que cada una de una organización primera y segunda controla la puerta 115, y que el primer usuario mencionado anteriormente pertenece a la primera organización. Cuando un segundo usuario que pertenece a la segunda organización se acerca a la puerta 115 con el fin de entrar, presenta su soporte de datos de credenciales C al segundo lector 120. El segundo lector 120 lee los datos de credenciales CD del soporte de datos C y reenvía estos datos al segundo panel de control 160. A continuación, el segundo panel de control 160 comprueba una segunda base de datos 180 para cualquier entrada que coincida con los datos de credenciales CD del segundo usuario. Si se encuentra una coincidencia, el segundo panel de control 160 consulta un segundo nodo EAC 170 para determinar si el segundo usuario puede o no entrar a través de la puerta 115. Ya que se encuentra que el segundo usuario está autorizado, el segundo panel de control 160 envía un segundo mensaje de concesión de acceso AG2 al mecanismo de control de bloqueo 105, que en respuesta al mismo, desbloquea la puerta 115, de tal manera que el segundo usuario puede entrar.

Como puede verse en la figura 1, cada organización que desee controlar entradas (y/o salidas) a través de una puerta dada necesita disponer de una unidad de lectura correspondiente en esta puerta y construir una estructura de comunicación entera de su propio para controlar el mecanismo de bloqueo de la puerta. En consecuencia, si se involucran muchas organizaciones, se requiere una gran cantidad de hardware, por ejemplo, en forma de unidades de lectura en la puerta. Además, por muchas razones, no se desea compartir paneles de control, nodos EAC y/o bases de datos entre organizaciones, por ejemplo, en referencia a riesgos de seguridad/integridad y administración.

Este tipo de problemas, sin embargo, pueden evitarse mediante la presente invención. La figura 2 muestra un diagrama de bloques sobre un sistema de comunicación de datos de acuerdo con una primera realización de la invención.

En este caso, una unidad de lectura R está asociada con una puerta D a través de la que los usuarios pueden obtener acceso a un espacio bien definido. La unidad de lectura R está configurada para registrar los datos de credenciales de usuario CD, que pueden almacenarse en un soporte personal C incorporado en un llavero de control remoto, una tarjeta inteligente, una tarjeta de proximidad o cualquier otro soporte apropiado, por ejemplo, una tarjeta SIM de un teléfono móvil o una PDA.

El sistema incluye un primer receptor de datos de credenciales EAC1 y al menos un segundo receptor de datos de credenciales EAC2, donde el primer receptor de datos de credenciales EAC1 está controlado por una primera organización y el al menos un segundo receptor de datos de credenciales EAC2 está controlado por un organización respectiva diferente de la primera organización. Por razones de claridad, sin embargo, en la siguiente descripción, solo se hace referencia a un segundo receptor de datos de credenciales EAC2.

De manera análoga al ejemplo anterior, se espera que un usuario que busca el acceso al espacio bien definido presente su soporte C a la unidad de lectura R, y en respuesta a lo mismo, la unidad de lectura R se configura para registrar los datos de credenciales CD en el soporte C. En este caso, ya que hay más de un nodo de control, la unidad de lectura R está configurada para comunicarse tanto con el primer como con el segundo receptor de datos de credenciales EAC1 y EAC2, preferentemente a través de una red de comunicación general NW, tal como Internet. Sin embargo, en cada caso individual, la unidad de lectura R está configurada para reenviar los datos de credenciales CD registrados a exactamente uno del primer receptor de datos de credenciales EAC1 o del segundo receptor de datos de credenciales EAC2.

De acuerdo con la invención, cada pieza de datos de credenciales CD está vinculada a una dirección A, que identifica, o al primer receptor de datos de credenciales EAC1 o al segundo receptor de datos de credenciales EAC2 (o en el caso general, uno específico del al menos un segundo receptor de datos de credenciales EAC2). La dirección vinculada A, preferentemente una dirección del protocolo de internet, se almacena en un módulo de memoria M asociado con la unidad de lectura R (como se muestra en la figura 1) o en el soporte C que contiene la pieza de datos de credenciales CD (como se describirá a continuación haciendo referencia a las figuras 3a, 3b y 6).

En el ejemplo ilustrado en la figura 2, se supone que las decisiones de acceso generadas por el sistema implican la concesión o denegación de acceso al espacio bien definido, es decir, que un componente de construcción relacionado con el control de acceso comprende un mecanismo de bloqueo L configurado para habilitar o evitar selectivamente el acceso a un espacio bien definido a través de una puerta D que está asociada con una unidad de lectura R. En el ejemplo específico mostrado en la figura 2, se supone además que la dirección A vinculada a los datos de credenciales CD identifica al primer receptor de datos de credenciales EAC1. Por lo tanto, los datos de credenciales CD se envían, a través de la red de comunicación NW, al primer receptor de datos de credenciales EAC1. En este caso, los datos de credenciales CD se comprueban con una primera base de datos DB1 para

determinar si el usuario asociado con los datos de credenciales CD está autorizado o no a entrar por la puerta D en el momento actual. Si es de este modo, el primer receptor de datos de credenciales EAC1 reenvía un mensaje de concesión de acceso AG a un mecanismo de control de bloqueo L, que en respuesta al mismo, desbloquea la puerta D, de tal manera que el usuario puede entrar por la puerta D.

Del mismo modo, si se presenta un soporte C a la unidad de lectura R, el soporte C que contiene datos de credenciales CD vinculados a una dirección A que identifican al segundo receptor de datos de credenciales EAC2, los datos de credenciales CD se reenvían al segundo receptor de datos de credenciales EAC2 para su comprobación contra una segunda base de datos DB2.

La figura 3a muestra un diagrama de bloques sobre un sistema de comunicación de datos de acuerdo con una segunda realización de la invención. En este caso, todas las unidades, componentes, señales y mensajes que también aparecen en la figura 2 representan las mismas unidades, componentes, señales y mensajes que los descritos anteriormente haciendo referencia a la figura 2. Como puede verse, en la figura 3a, no hay ningún módulo de memoria M asociado con la unidad de lectura R. En su lugar, cada soporte C contiene la dirección A que está vinculada a los datos de credenciales CD. De este modo, tras la presentación del soporte C a la unidad de lectura R, la unidad de lectura R está configurada para leer los datos de credenciales CD así como la dirección A vinculada a los mismos. Basándose en esta dirección A, a su vez, la unidad de lectura R se configura para enviar los datos de credenciales CD al receptor de datos de credenciales identificado por la dirección A, que en este ejemplo es así mismo el primer receptor de credenciales EAC1. A continuación, el primer receptor de credenciales EAC1 ejecuta el procedimiento de verificación descrito anteriormente, y si se encuentra que los datos de credenciales CD corresponden a un usuario autorizado, se emite un mensaje de concesión de acceso AG en respuesta al cual se hace que se desbloquee el bloqueo L. De lo contrario, es decir, si no se encuentra que la pieza de datos de credenciales CD designa un usuario autorizado, el primer receptor de credenciales EAC1 se abstiene de hacer que se envíe el mensaje de concesión de acceso AG al mecanismo de bloqueo L, y el mecanismo de bloqueo L permanece bloqueado.

La figura 3b muestra un ejemplo de cómo el contenido de datos del soporte C en la figura 3a puede estar organizado de acuerdo con una realización de la invención. En este caso, una zona de almacenamiento 310 contiene una clave de cifrado general K, que se requiere en la unidad de lectura R para obtener un acceso al contenido del soporte C. La dirección A, a su vez, contiene un primer campo de dirección 310, que incluye una dirección Adr_{EAC} para el primer receptor de credenciales EAC1; y un segundo campo de dirección 320 que incluye otra dirección Adr_x. Esta dirección puede especificar que un receptor de credencial diferente sea responsable de controlar otra puerta. Sin embargo, el segundo campo de dirección 320 puede usarse igualmente también para fines no relacionados completamente con el bloqueo/desbloqueo de una puerta, por ejemplo, registrar la presencia de un usuario. Cada uno de la dirección general A y los campos de direcciones individuales 310 y 320 están preferentemente protegidos por una clave de cifrado respectiva, de tal manera que solo las entidades autorizadas pueden obtener acceso a los datos en los mismos.

La figura 4 muestra un diagrama de bloques de un sistema de comunicación de datos de acuerdo con una tercera realización de la invención. En este caso, todas las unidades, componentes, señales y mensajes que también aparecen en cualquiera de las figuras 2 o 3 representan las mismas unidades, componentes, señales y mensajes que los descritos anteriormente haciendo referencia a la figura 2 o 3.

En el sistema de comunicación de datos de la figura 4, las decisiones de acceso implican registrar entradas o salidas de un espacio bien definido. Es decir, el sistema puede implementar una perforadora digital/un reloj de fichar. Con este fin, la unidad de lectura R contiene un primer escáner R-ENTRADA y un segundo escáner R-SALIDA, que están dispuestos en el interior y en el exterior, respectivamente, de la puerta D.

Por otra parte, cada uno de los receptores de datos de credenciales primero y segundo EAC1 y EAC2 está configurado para registrar una entrada en el espacio bien definido con respecto a un usuario asociado con una pieza dada de datos de credenciales CD si se recibe la pieza de datos de credenciales CD a través de un primer escáner R-ENTRADA de la unidad de lectura R, y registra una salida del espacio bien definido con respecto al usuario si se recibe la pieza de datos de credenciales CD a través de un segundo escáner R-SALIDA. Análogamente a lo anterior, en respuesta a una pieza recibida de datos de credenciales CD, la unidad de lectura R está configurada para enviar la pieza de datos de credenciales CD al primer receptor de datos de credenciales EAC1 si la dirección A vinculada al mismo identifica al primer receptor de datos de credenciales EAC1, y al segundo receptor de datos de credenciales EAC2 si la dirección A vinculada identifica al segundo receptor de datos de credenciales EAC2.

Las figuras 5 y 6 muestran unos diagramas de bloques sobre los sistemas de comunicación de datos de acuerdo con una cuarta y quinta realización, respectivamente, de la invención, en las que las decisiones de acceso implican tanto la concesión o la denegación de acceso a los espacios bien definidos a través de las puertas D1 y D2 controlables a través de los mecanismos de bloqueo L1 y L2 a los que está asociada una unidad de lectura respectiva R1 y R2.

Una vez más, todas las unidades, componentes, señales y mensajes que también aparecen en cualquiera de las figuras 2 a 4 representan las mismas unidades, componentes, señales y mensajes como ha descrito anteriormente haciendo referencia a la figura 2 a 4.

En el sistema de la figura 5, las direcciones A vinculadas a los datos de credenciales CD se almacenan en un módulo de memoria M (análogo a las figuras 2 y 4), mientras que en el sistema de la figura 6 las direcciones vinculadas se almacenan en los soportes C (análogos a la figura 3); de otro modo, los sistemas en las figuras 5 y 6 son idénticos.

Entre otros, ambos sistemas contienen un nodo de control N, que está conectado de manera comunicativa con una primera unidad de lectura R1 asociada con una primera puerta D1. El nodo de control N también está conectado de manera comunicativa con una segunda unidad de lectura R2 asociada con una segunda puerta D2 y, a través de una red de comunicación NW, conectada de manera comunicativa con cada uno de un receptor de datos de credenciales primero y segundo EAC1 y EAC2, respectivamente. El nodo de control N está configurado para recibir datos de credenciales CD desde las unidades de lectura R1 y R2, y para reenviar los datos de credenciales CD recibidos al receptor de datos de credenciales EAC1 o EAC2 identificado por la dirección A vinculada a los datos de credenciales CD.

El nodo de control N está configurado además para recibir mensajes de concesión de acceso AG desde el receptor de datos de credenciales primero y segundo EAC1 y EAC2, y reenviar los mensajes de concesión de acceso recibidos AG, o a un primer mecanismo de bloqueo L1 asociado con la primera puerta D1 o a un segundo mecanismo de bloqueo L2 asociado con la segunda puerta D2, en función de en qué unidad de lectura R1 o R2 se originen los datos de credenciales CD. Como se ha mencionado anteriormente, cada mensaje de concesión de acceso AG está configurado para ordenar que se abra el mecanismo de bloqueo L1 o L2 durante un intervalo predeterminado.

Naturalmente, de acuerdo con la invención, el nodo de control N puede estar configurado para manejar cualquier otro número de espacios bien definidos y receptores de datos de credenciales mayores que dos, es decir, desde uno y en adelante. También debería observarse que la cantidad de espacios bien definidos (puertas) y la cantidad de receptores de datos de credenciales no necesitan ser idénticos. Por el contrario, podría ser muy bien el caso que la cantidad de espacios bien definidos (puertas) sea relativamente grande, mientras que la cantidad de receptores de datos de credenciales sea relativamente pequeño, digamos dos; o viceversa, que la cantidad de receptores de datos de credenciales sea relativamente grande, mientras que la cantidad de espacios bien definidos sea solo uno o dos.

En cualquier caso, tras la presentación de una pieza de datos de credenciales CD a una de las unidades de lectura R1 o R2, esta unidad de lectura se configura para reenviar la pieza de datos de credenciales CD al receptor de datos de credenciales EAC1 o EAC2 identificado por el dirección A vinculada a los datos de credenciales CD. A continuación, en respuesta a una pieza recibida de datos de credenciales CD, cada uno del primer y el al menos un segundo receptor de datos de credenciales EAC1 y EAC2 está configurado para comprobar la pieza de datos de credenciales CD contra una base de datos DB1 o DB2 respectivamente definiendo un conjunto de derechos de acceso de los usuarios al espacio bien definido detrás de la puerta D1 o D2 a la que está asociada la unidad de lectura R1 o R2 por la que se registró la pieza de datos de credenciales CD. Si la pieza de datos de credenciales CD designa un usuario autorizado, el receptor de datos de credenciales EAC1 o EAC2 se configura para provocar un mensaje de concesión de acceso AG a enviar al mecanismo de bloqueo L1 o L2 que ordena al mecanismo de bloqueo L1 o L2 que abra la puerta D1 o D2.

Si, sin embargo, no se encuentra la pieza de datos de credenciales CD para designar un usuario autorizado, el receptor de datos de credenciales EAC1 o EAC2 se configura para abstenerse de provocar un mensaje de concesión de acceso AG a enviar a cualquiera de los mecanismos de bloqueo L1 o L2.

Preferentemente, las unidades de lectura R, R1 y R2, los receptores de datos de credenciales EAC, EAC1 y EAC2 y el nodo de control N incluyen, o están en conexión comunicativa con al menos una unidad de memoria que almacena al menos un producto de programa informático, que contiene un software para realizar las acciones descritas anteriormente cuando el producto de programa informático se ejecuta en un procesador de las unidades de lectura R, R1 y R2, los receptores de datos de credenciales EAC, EAC1 y EAC2 y el nodo de control N respectivamente.

Con el fin de resumir, a continuación se describe el método general ejecutado por la unidad de lectura propuesta de acuerdo con la invención haciendo referencia al diagrama de flujo de la figura 7.

Una primera etapa 710 comprueba si se han recibido los datos de credenciales, y si es de este modo sigue a la etapa 720. De lo contrario, el procedimiento vuelve atrás y permanece en la etapa 710.

La etapa 720 lee la dirección vinculada a los datos de credenciales, desde o un módulo de memoria asociada con la unidad de lectura o desde un soporte para los datos de credenciales. Preferentemente, para mantener una

seguridad adecuada y reducir el riesgo de manipulación fraudulenta, la lectura de los datos de credenciales desde el soporte requiere un acceso a una primera clave de cifrado en la unidad de lectura.

Después de haber leído los datos de credenciales, una etapa 730 reenvía los datos de credenciales registrados al receptor de datos de credenciales identificado por la dirección vinculada a los datos de credenciales registrados. Nuevamente, por razones de seguridad y para reducir el riesgo de manipulación fraudulenta, se requiere preferentemente el acceso a una segunda clave de cifrado (idéntica o diferente de la primera clave) en la unidad de lectura para permitir esta transmisión.

Una etapa posterior 740 determina si el usuario asociado con los datos de credenciales está autorizado o no. Desde el punto de vista de la unidad de lectura esto significa esperar una decisión de acceso del receptor de datos de credenciales. Si tal decisión llega dentro de un tiempo predefinido, por ejemplo, en forma de un mensaje de concesión de acceso, sigue a una etapa 750. Análogo a lo anterior, el envío de la decisión de acceso, preferentemente, requiere también el acceso a una tercera clave de cifrado, de tal manera que la unidad de lectura puede estar segura de que una decisión de acceso recibida fue emitida por una fuente autorizada, por ejemplo, uno de sus receptores de datos de credenciales asociados.

Si la decisión de acceso no llega dentro del tiempo predefinido, el procedimiento vuelve a la etapa 710.

En la etapa 750, se efectúa al menos una decisión de acceso en respuesta a la decisión de acceso con respecto a un espacio bien definido y al usuario que está asociado con los datos de credenciales registrados. La decisión de acceso puede implicar la concesión de acceso al espacio bien definido, registrando una entrada al espacio bien definido o registrando una salida del espacio bien definido.

Después de la etapa 750, el procedimiento vuelve a la etapa 710.

Cabe señalar que, a pesar de las etapas 710, 720 y 730 toda mención a “los datos de credenciales”, esto no significa que debe recibirse, leerse y enviarse respectivamente una copia exacta de estos datos específicos. En su lugar, las diversas formas de los datos obtenidos a partir de los datos de credenciales pueden recibirse, leerse y enviarse en y desde la unidad de lectura. Por lo tanto, la expresión “datos de credenciales” debería considerarse en este caso como un testigo que se pasa desde el soporte.

Todas las etapas de proceso, así como cualquier subsecuencia de las etapas, descritas haciendo referencia a la figura 7 anterior, pueden controlarse por medio de un aparato informático programado. Además, aunque las realizaciones de la invención descritas anteriormente haciendo referencia a los dibujos comprenden un aparato informático y unos procesos realizados en un aparato informático, la invención por lo tanto también se extiende a los programas informáticos, específicamente a los programas de ordenador en un soporte, adaptados para poner la invención en práctica. El programa puede estar en la forma de código fuente, código objeto, una fuente intermedia de código y un código objeto tal como en una forma parcialmente compilada, o en cualquier otra forma adecuada para su uso en la implementación del procedimiento de acuerdo con la invención. El programa puede ser o bien una parte de un sistema operativo, o ser una aplicación separada. El soporte puede ser cualquier entidad o dispositivo capaz de transportar el programa. Por ejemplo, el soporte puede comprender un medio de almacenamiento, tal como una memoria flash, una ROM (memoria de solo lectura), por ejemplo, un DVD (vídeo digital/disco versátil), un CD (disco compacto) o una ROM de semiconductores, una EPROM (memoria de solo lectura programable y borrable), una EEPROM (memoria de solo lectura eléctricamente programable y borrable), o un medio de registro magnético, por ejemplo un disco flexible o un disco duro. Además, el soporte puede ser un soporte transmisible tal como una señal eléctrica u óptica que puede transmitirse a través de cable eléctrico u óptico o por radio o por otros medios. Cuando el programa está incorporado en una señal que puede transportarse directamente por un cable u otro dispositivo o medio, el soporte puede estar constituido por tal cable o dispositivo o medio. Como alternativa, el soporte puede ser un circuito integrado en el que está incrustado el programa, estando el circuito integrado adaptado para realizar, o para su uso en la realización de los procesos relevantes.

El término “comprende/comprendiendo” cuando se usa en esta memoria descriptiva se toma para especificar la presencia de características, enteros, etapas o componentes establecidos. Sin embargo, el término no excluye la presencia o adición de una o más características, enteros, etapas o componentes o grupos de los mismos.

La invención no se limita a las realizaciones descritas en las figuras, sino que puede variarse libremente dentro del alcance de las reivindicaciones.

REIVINDICACIONES

1. Una unidad de lectura (R, R1, R2) asociada con una puerta (D), estando la unidad de lectura configurada para:

registrar datos de credenciales (CD) con respecto a los usuarios que buscan acceder a un espacio bien definido,
comunicarse con un componente de construcción relacionado con el control de acceso (L, L1, L2) asociado con el espacio bien definido, y
comunicarse con un primer receptor de datos de credenciales (EAC1) controlado por una primera organización para hacer que al menos se efectúe una decisión de acceso (AG) con respecto al espacio bien definido,
estando la unidad de lectura (R, R1, R2) caracterizada por que está configurada además para:

comunicarse con al menos un segundo receptor de datos de credenciales (EAC2) controlado por una organización respectiva diferente de la primera organización en la que se basa para hacer que al menos se efectúe una decisión de acceso (AG) con respecto al espacio bien definido, y
reenviar cada pieza registrada de datos de credenciales (CD), o al primer receptor de datos de credenciales (EAC1) o a uno específico del al menos un segundo receptor de datos de credenciales (EAC2) basándose en una dirección (A) vinculada a la pieza de datos de credenciales (CD), dirección (A) que identifica el primer receptor de datos de credenciales (EAC1) o el específico del al menos un segundo receptor de datos de credenciales (EAC2), almacenándose la dirección vinculada (A) en:

un módulo de memoria (M, M1, M2) asociado con la unidad de lectura (R, R1, R2) o en un soporte (C) que contiene la pieza de datos de credenciales (CD), soporte (C) que está configurado para presentarse a la unidad de lectura (R, R1, R2) para registrar la pieza de datos de credenciales (CD); en la que la al menos una decisión de acceso (AG) implica conceder o denegar el acceso al espacio bien definido, el componente de construcción relacionado con el control de acceso comprende un mecanismo de bloqueo (L, L1, L2) configurado para habilitar o evitar de manera selectiva el acceso al espacio bien definido a través de la puerta (D) asociada con la unidad de lectura (R, R1, R2), y en respuesta a una pieza recibida de datos de credenciales (CD), cada uno del primer y el al menos un segundo receptor de datos de credenciales (EAC1; EAC2) está configurado para:

comprobar la pieza de datos de credenciales (CD) contra una base de datos (DB1; DB2) que define un conjunto de derechos de acceso de los usuarios al espacio bien definido,
si se encuentra la parte de datos de credenciales (CD) para designar un usuario autorizado, provocar un mensaje de concesión de acceso (AG) a enviar al mecanismo de bloqueo (L, L1, L2) ordenando al mecanismo de bloqueo (L, L1, L2) que abra la puerta (D), y de otro modo
abstenerse de provocar el mensaje de concesión de acceso (AG) a enviar al mecanismo de bloqueo (L, L1, L2).

2. Un sistema de comunicación de datos que comprende:

una unidad de lectura (R, R1, R2) asociada con una puerta (D), estando la unidad de lectura configurada para registrar datos de credenciales (CD) con respecto a los usuarios que buscan acceso a un espacio bien definido,
un componente de construcción relacionado con el control de acceso (L, L1, L2) asociado con la unidad de lectura (R, R1, R2) y el espacio bien definido, y
un primer receptor de datos de credenciales (EAC1) controlado por una primera organización configurada para recibir datos de credenciales (CD) registrados por la unidad de lectura (R, R1, R2) y en respuesta a lo mismo provocar al menos una decisión de acceso (AG) con respecto al espacio bien definido a efectuar,
estando el sistema de comunicación de datos caracterizado por que comprende al menos un segundo receptor de datos de credenciales (EAC2) controlado por una organización respectiva diferente de la primera organización en la que se basa configurada para recibir datos de credenciales (CD) registrados por la unidad de lectura (R, R1, R2) y en respuesta a lo mismo provocar al menos una decisión de acceso (AG) con respecto al espacio bien definido a efectuar, estando la unidad de lectura (R, R1, R2) conectada de manera comunicativa con el primer receptor de datos de credenciales (EAC1) y a el al menos un segundo receptor de datos de credenciales (EAC2), y estando la unidad de lectura (R, R1, R2) configurada además para reenviar una pieza registrada de datos de credenciales (CD) o al primer receptor de datos de credenciales (EAC1) o a uno específico del al menos un segundo receptor de datos de credenciales (EAC2) basándose en una dirección (A) vinculada a la pieza de datos de credenciales (CD), dirección (A) que identifica el primer receptor de datos de credenciales (EAC1) o el específico del al menos un segundo receptor de datos de credenciales (EAC2), estando la dirección vinculada (A) almacenada en:

un módulo de memoria (M, M1, M2) asociado con la unidad de lectura (R, R1, R2) o
en un soporte (C) que contiene la pieza de datos de credenciales (CD), soporte (C) que está configurado para presentarse a la unidad de lectura (R, R1, R2) para registrar la pieza de datos de credenciales (CD);
en el que la al menos una decisión de acceso (AG) implica conceder o denegar el acceso al espacio bien definido, el componente de construcción relacionado con el control de acceso comprende un mecanismo de bloqueo (L, L1, L2) configurado para habilitar o evitar de manera selectiva el acceso al espacio bien definido a

través de la puerta (D) asociada con la unidad de lectura (R, R1, R2), y en respuesta a una pieza recibida de datos de credenciales (CD), cada uno del primer y el al menos un segundo receptor de datos de credenciales (EAC1; EAC2) está configurado para:

comprobar la pieza de datos de credenciales (CD) contra una base de datos (DB1; DB2) que define un conjunto de derechos de acceso de los usuarios al espacio bien definido,
si se encuentra la pieza de datos de credenciales (CD) para designar un usuario autorizado, provocar un mensaje de concesión de acceso (AG) a enviar al mecanismo de bloqueo (L, L1, L2) ordenando al mecanismo de bloqueo (L, L1, L2) que abra la puerta (D), y de otro modo
abstenerse de provocar el mensaje de concesión de acceso (AG) a enviar al mecanismo de bloqueo (L, L1, L2).

3. La unidad de lectura (R) de acuerdo con la reivindicación 1 o el sistema de comunicación de datos de acuerdo con la reivindicación 2, en el que la al menos una decisión de acceso implica registrar una entrada o salida del espacio bien definido, y en respuesta a una pieza recibida de datos de credenciales (CD), cada uno del primer y el al menos un segundo receptor de datos de credenciales (EAC1; EAC2) está configurado para:

registrar una entrada si se recibe la pieza de datos de credenciales (CD) a través de un primer escáner (R-ENTRADA) de la unidad de lectura (R), y
registrar una salida si se recibe la pieza de datos de credenciales (CD) a través de un segundo escáner (R-SALIDA) de la unidad de lectura (R).

4. El sistema de comunicación de datos de acuerdo con la reivindicación 3, que comprende un nodo de control (N) conectado de manera comunicativa con la unidad de lectura (R1) y cada uno del primer y el al menos un segundo receptor de datos de credenciales (EAC1; EAC2), estando el nodo de control (N) configurado para:

recibir datos de credenciales (CD) de la unidad de lectura (R1),
reenviar los datos de credenciales recibidos (CD) a un receptor de datos de credenciales (EAC1; EAC2) identificado por la dirección (A) vinculada a los datos de credenciales (CD),
recibir los mensajes de concesión de acceso (AG) del primer y el al menos un segundo receptor de datos de credenciales (EAC1; EAC2), y
reenviar los mensajes de concesión de acceso recibidos (AG) al mecanismo de bloqueo (L1), estando cada mensaje de concesión de acceso (AG) configurado para ordenar al mecanismo de bloqueo (L1) que se abra durante un intervalo predeterminado.

5. El sistema de comunicación de datos de acuerdo con la reivindicación 3, en el que el nodo de control (N) está conectado de manera comunicativa con al menos una unidad de lectura (R2) además de a dicha unidad de lectura (R1), estando el nodo de control (N) configurado además para

recibir datos de credenciales (CD) de dicha unidad de lectura adicional (R2),
reenviar los datos de credenciales recibidos (CD) a un receptor de datos de credenciales (EAC1; EAC2) identificado por la dirección (A) vinculada a los datos de credenciales (CD),
recibir los mensajes de concesión de acceso (AG) del primer y el al menos un segundo receptor de datos de credenciales (EAC1; EAC2), y
reenviar los mensajes de concesión de acceso recibidos (AG) a un mecanismo de bloqueo (L2) además de a dicho mecanismo de bloqueo (L1), estando cada mensaje de concesión de acceso (AG) configurado para ordenar al mecanismo de bloqueo adicional (L2) que se abra durante un intervalo predeterminado.

6. El sistema de comunicación de datos de acuerdo con una cualquiera de las reivindicaciones 4 o 5, en el que las direcciones de enlaces (A) que identifican el primer y el al menos un segundo receptor de datos de credenciales (EAC1; EAC2) son direcciones del protocolo de internet.

7. Un método para comunicar datos en una red que comprende:

registrar datos de credenciales (CD) en una unidad de lectura (R, R1, R2) asociada con una puerta (D), representando los datos de credenciales (CD) a los usuarios que buscan acceso a un espacio bien definido asociado a la unidad de lectura (R, R1, R2),
reenviar uno cualquiera de los datos de credenciales registrados (CD) a un receptor de datos de credenciales (EAC1; EAC2) y en respuesta a lo mismo
efectuar al menos una decisión de acceso (AG) con respecto al espacio bien definido,
caracterizado por la red que comprende un primer receptor de datos de credenciales (EAC1) controlado por una primera organización y al menos un segundo receptor de datos de credenciales (EAC2) controlado por una organización respectiva diferente de la primera organización en la que se basa y comprendiendo el método
reenviar cada pieza registrada de datos de credenciales (CD) o al primer receptor de datos de credenciales (EAC1) o a uno específico del al menos un segundo receptor de datos de credenciales (EAC2) basándose en una dirección (A) vinculada a la pieza de datos de credenciales (CD), dirección (A) que identifica al primer

receptor de datos de credenciales (EAC1) o a uno específico del al menos un segundo receptor de datos de credenciales (EAC2), almacenándose la dirección vinculada (A) en:

un módulo de memoria (M, M1, M2) asociado con la unidad de lectura (R, R1, R2) o
en un soporte (C) que contiene la pieza de datos de credenciales (CD), soporte (C) que está configurado para presentarse a la unidad de lectura (R, R1, R2) para registrar la pieza de datos de credenciales (CD);
en el que en respuesta a una pieza recibida de datos de credenciales (CD), en cada uno del primer y el al menos un segundo receptor de datos de credenciales (EAC1; EAC2), el método comprende:

comprobar la pieza de datos de credenciales (CD) contra una base de datos (DB1; DB2) que define un conjunto de derechos de acceso de los usuarios al espacio bien definido, si se encuentra la pieza de datos de credenciales (CD) para designar un usuario autorizado,
provocar un mensaje de concesión de acceso (AG) a enviar al mecanismo de bloqueo (L, L1, L2) configurado para habilitar o evitar de manera selectiva el acceso al espacio bien definido a través de la puerta (D, D1, D2) asociada con la unidad de lectura (R, R1, R2), estando el mensaje de concesión de acceso (AG) configurado para ordenar al mecanismo de bloqueo (L, L1, L2) que abra la puerta (D, D1, D2), y de otro modo
abstenerse de provocar el mensaje de concesión de acceso (AG) a enviar al mecanismo de bloqueo (L, L1, L2).

8. El método de acuerdo con la reivindicación 7, en el que en respuesta a una pieza recibida de datos de credenciales (CD), en cada uno del primer y el al menos un segundo receptor de datos de credenciales (EAC1; EAC2), el método comprende:

registrar una entrada al espacio bien definido si se recibe la pieza de datos de credenciales (CD) a través de un primer escáner (R-ENTRADA) de la unidad de lectura (R), y
registrar una salida del espacio bien definido si se recibe la pieza de datos de credenciales (CD) a través de un segundo escáner (R-SALIDA) de la unidad de lectura (R).

9. El método de acuerdo con una cualquiera de las reivindicaciones 7 a 8, que comprende:

recibir los datos de credenciales (CD) de la unidad de lectura (R1) en un nodo de control (N),
reenviar los datos de credenciales recibidos (CD) desde el nodo de control a un receptor de datos de credenciales (EAC1; EAC2) identificado por la dirección (A) vinculada a los datos de credenciales (CD),
recibir, en el nodo de control, los mensajes de concesión de acceso (AG) del primer y el al menos un segundo receptor de datos de credenciales (EAC1; EAC2), y
reenviar los mensajes de concesión de acceso recibidos (AG) desde el nodo de control (N) al mecanismo de bloqueo (L1), ordenando cada mensaje de concesión de acceso (AG) al mecanismo de bloqueo (L1) que se abra durante un intervalo predeterminado.

10. El método de acuerdo con una cualquiera de las reivindicaciones 7 a 9, en el que las direcciones vinculadas (A) que identifican los receptores de datos de credenciales primero y segundo (EAC1; EAC2) son direcciones del protocolo de internet.

11. Un producto de programa informático que puede cargarse en la memoria de un ordenador, comprendiendo el producto de programa informático un software, que cuando se ejecuta en un ordenador:

registra datos de credenciales (CD) en una unidad de lectura (R, R1, R2) asociada con una puerta (D), representando los datos de credenciales unos usuarios que buscan acceso a un espacio bien definido asociado con la unidad de lectura,
reenvía cada pieza registrada de datos de credenciales o a un primer receptor de datos de credenciales (EAC1) controlado por una primera organización o a uno específico del al menos un segundo receptor de datos de credenciales (EAC2) controlado por una organización respectiva diferente de la primera organización basándose en una dirección (A) vinculada a la pieza de datos de credenciales, dirección que identifica el primer receptor de datos de credenciales o el específico del al menos un segundo receptor de datos de credenciales, almacenándose la dirección vinculada en un módulo de memoria (M, M1, M2) asociado con la unidad de lectura o en un soporte (C) que contiene la pieza de datos de credenciales, soporte que está configurado para presentarse a la unidad de lectura para registrar la pieza de datos de credenciales,
en el que cada uno de dichos receptores de datos de credenciales está configurado para, en respuesta a una pieza de datos de credenciales, efectuar al menos una decisión de acceso (AG) con respecto al espacio bien definido,
en el que el producto de programa informático comprende un software, el cual, en respuesta a una pieza recibida de datos de credenciales (CD), en cada uno del primer y el al menos un segundo receptor de datos de credenciales (EAC1; EAC2), cuando se ejecuta en un ordenador:

comprueba la pieza de datos de credenciales (CD) contra una base de datos (DB1; DB2) que define un conjunto de derechos de acceso de los usuarios al espacio bien definido, si se encuentra la pieza de datos de credenciales (CD) para designar un usuario autorizado,
provoca un mensaje de concesión de acceso (AG) a enviar al mecanismo de bloqueo (L, L1, L2) configurado para habilitar o evitar de manera selectiva el acceso al espacio bien definido a través de la puerta (D, D1, D2) asociada con la unidad de lectura (R, R1, R2), estando el mensaje de concesión de acceso (AG) configurado para ordenar al mecanismo de bloqueo (L, L1, L2) que abra la puerta (D, D1, D2), y de otro modo
abstenerse de provocar el mensaje de concesión de acceso (AG) a enviar al mecanismo de bloqueo (L, L1, L2).

12. Un medio legible por ordenador, que contiene el producto de programa informático de acuerdo con la reivindicación 11.

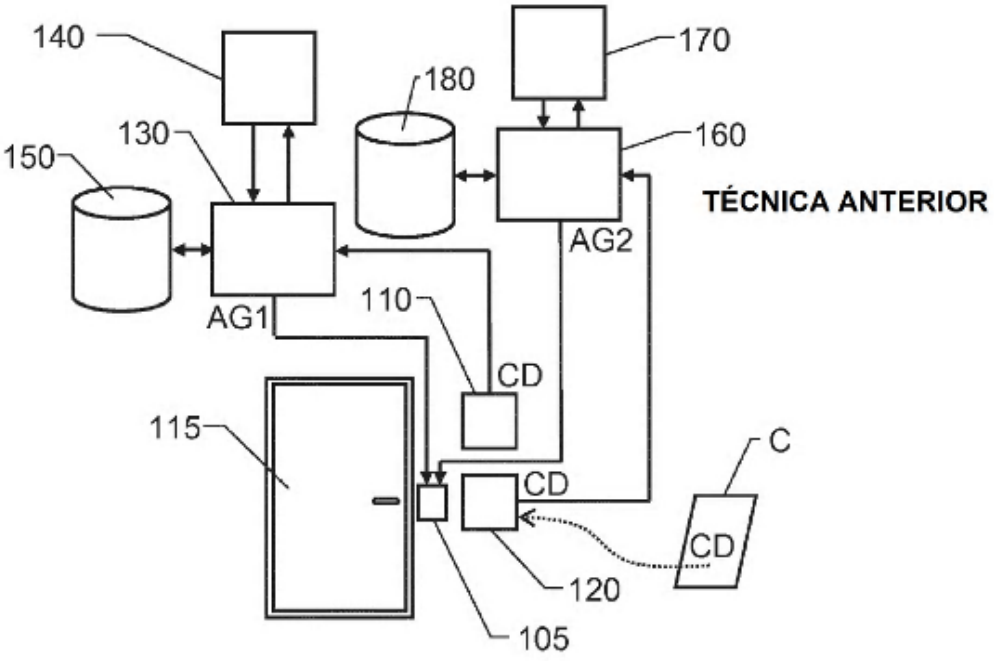
140
170
180
130
160
150
TÉCNICA ANTERIOR
AG2
AG1
110
CD
115
C
CD
CD
120
105

Fig. 1

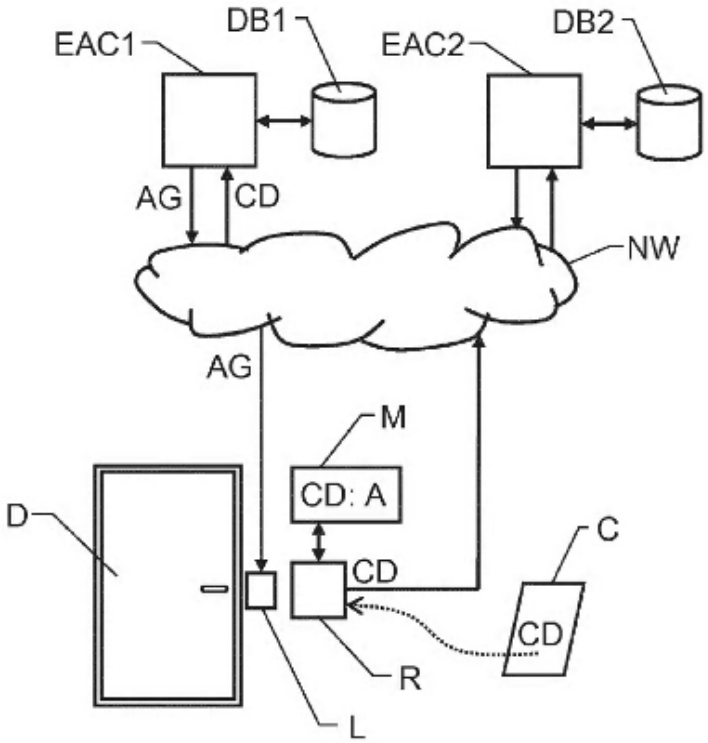
EAC1
DB1
EAC2
DB2
AG
CD
NW
AG
M
CD: A
D
C
CD
CD
R
L

Fig. 2

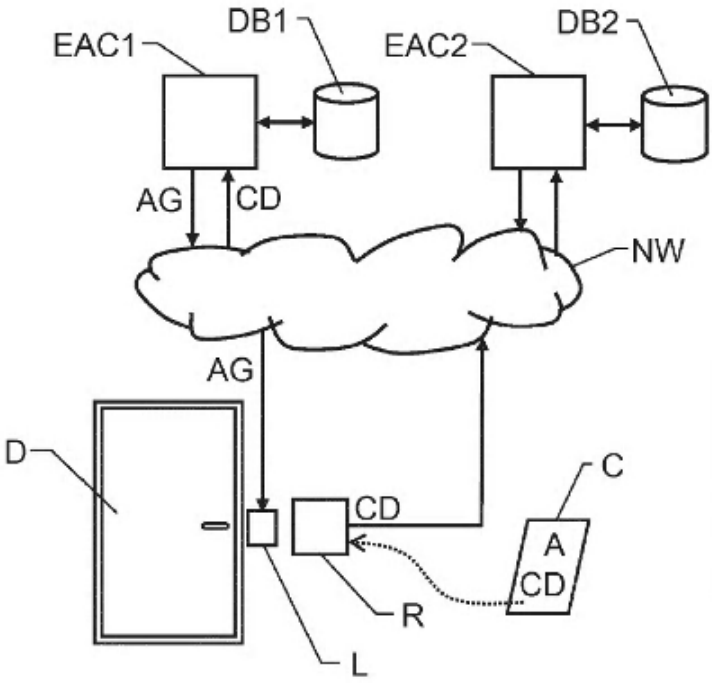

Fig. 3a

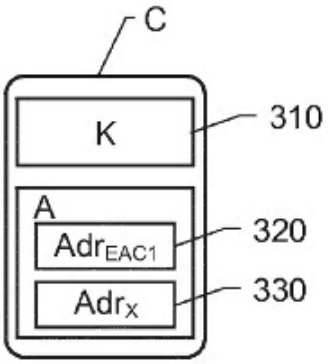

Fig. 3b

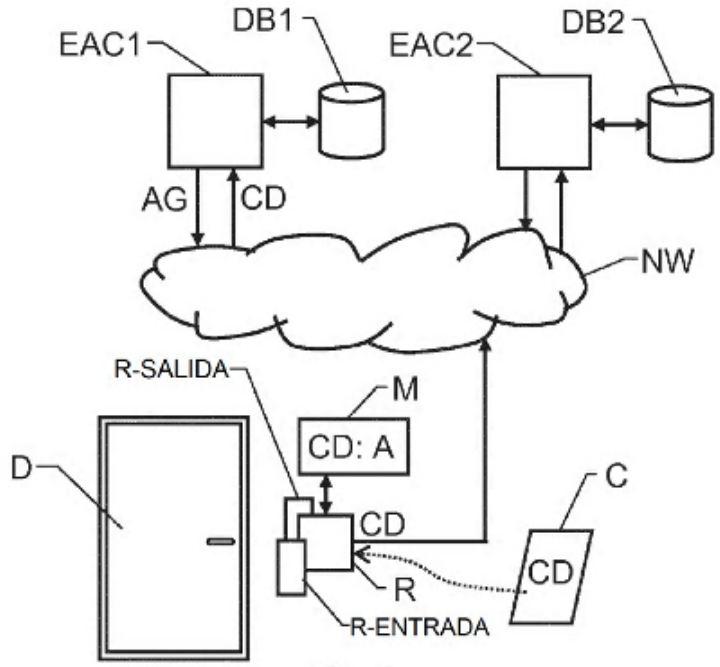

Fig. 4

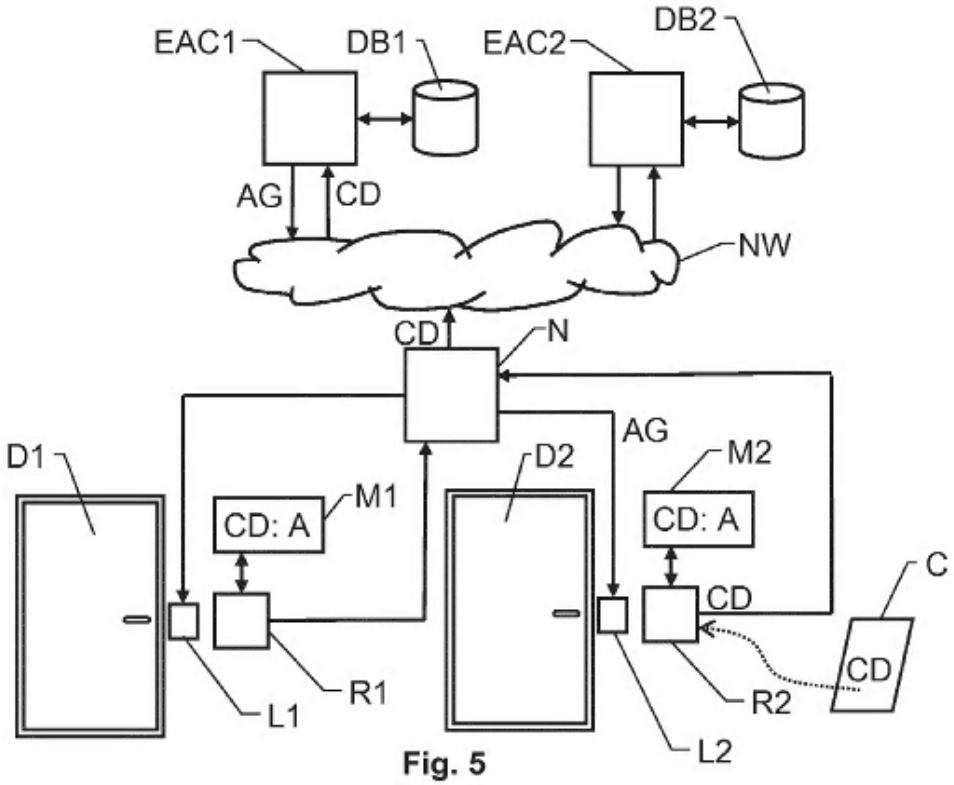
EAC1
DB1
EAC2
DB2
AG
CD
NW
CD
N
AG
D1
D2
M2
M1
CD: A
CD: A
C
CD
CD
R1
R2
L1
L2

Fig. 5

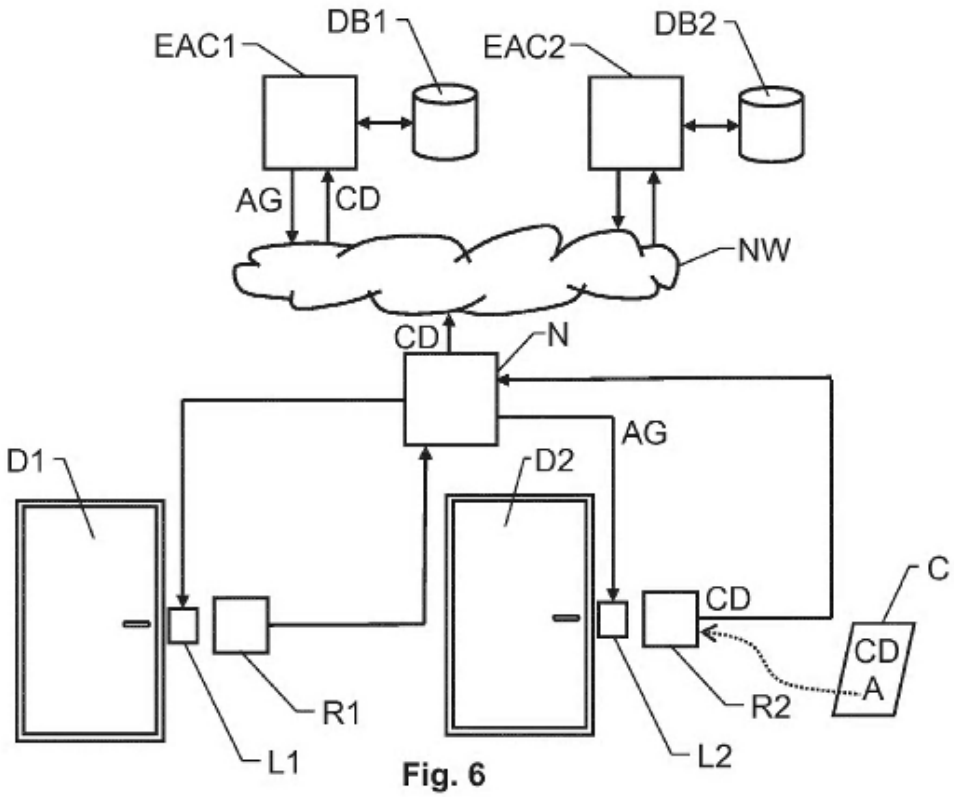
EAC1
DB1
EAC2
DB2
AG
CD
NW
CD
N
AG
D1
D2
C
CD
CD
A
R1
R2
L1
L2

Fig. 6

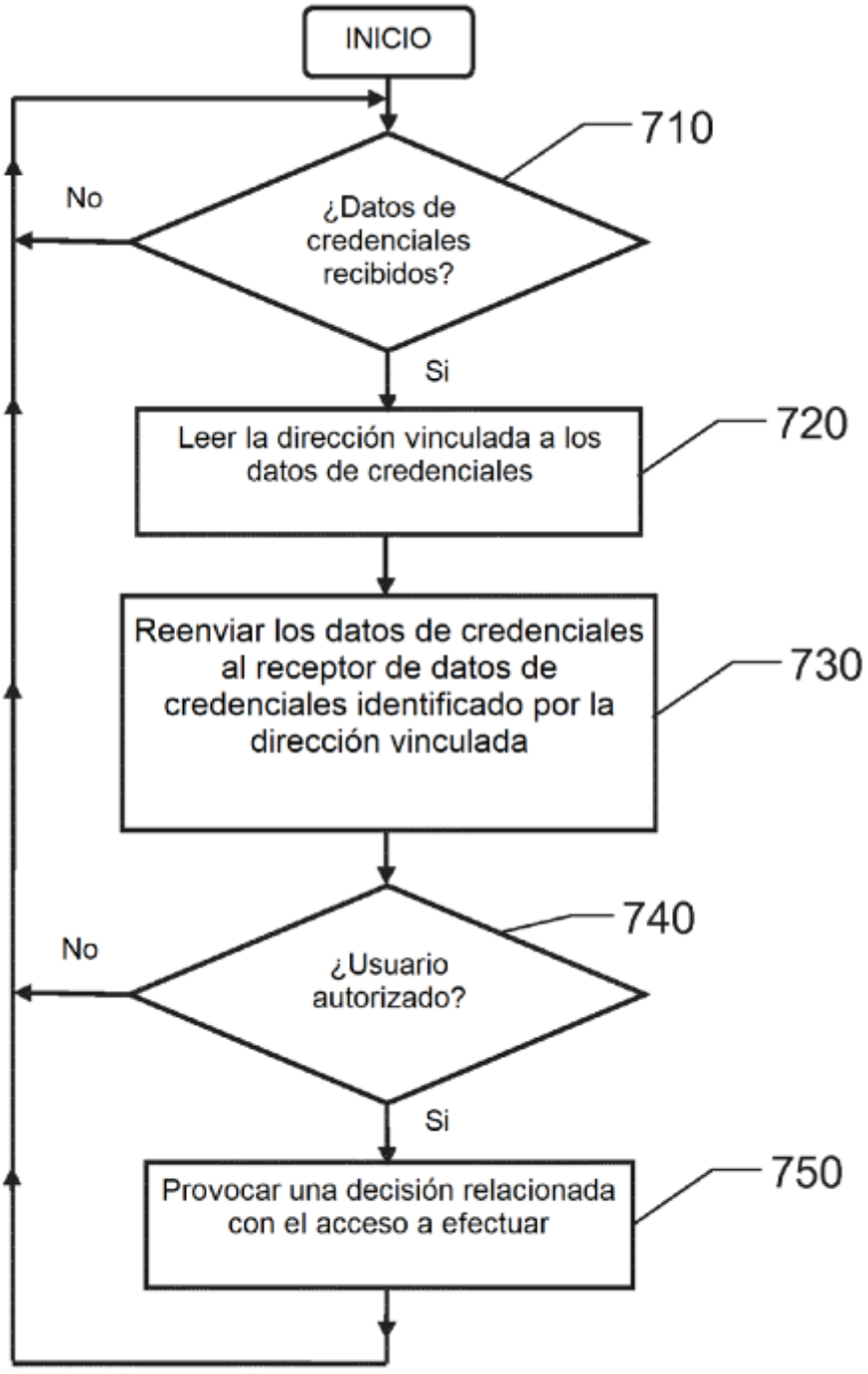
INICIO
710
¿Datos de credenciales recibidos?
No
Si
720
Leer la dirección vinculada a los datos de credenciales
730
Reenviar los datos de credenciales al receptor de datos de credenciales identificado por la dirección vinculada
740
¿Usuario autorizado?
No
Si
750
Provocar una decisión relacionada con el acceso a efectuar

Fig. 7