(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 610 387**

(51) Int. CI.:

G07C 9/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **03.06.2011 PCT/NL2011/050395**

(87) Fecha y número de publicación internacional: **08.12.2011 WO11152729**

(96) Fecha de presentación y número de la solicitud europea: **03.06.2011 E 11725218 (9)**

(97) Fecha y número de publicación de la concesión europea: **26.10.2016 EP 2577616**

(54) Título: **Un método de autorización de una persona, una arquitectura de autorización y un programa informático para ordenador**

(30) Prioridad:

04.06.2010 NL 2004825

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.04.2017

(73) Titular/es:

UBIQU B.V. (100.0%)
Kerstant van den Bergelaan 13b
3054 EM Rotterdam, NL

(72) Inventor/es:

GORANOV, BORIS PETROV DOKOV

(74) Agente/Representante:

SÁEZ MAESO, Ana

DESCRIPCIÓN

Un método de autorización de una persona, una arquitectura de autorización y un programa informático para ordenador

La presente invención se refiere a un método para autorizar a una persona, que comprende la etapa de recibir datos de autenticación de un dispositivo de autenticación personal que transmite dichos datos a un lector asociado con un sistema de autorización central.

Los sistemas de autorización centrales son conocidos por autorizar a los usuarios de un dispositivo de autenticación personal, tal como una tarjeta inteligente, para tener acceso a un edificio o para retirar dinero de un banco, por ejemplo. Generalmente, los lectores asociados con un sistema de autorización central incluyen un procesador y una memoria para verificar si el usuario del dispositivo de autenticación personal está autorizado a tener acceso al sistema.

Sin embargo, la aplicación de lectores inteligentes es relativamente costosa. Por otra parte, se conocen sistemas lectores que incluyen un número limitado de lectores individuales, por ejemplo, cuatro lectores, que están conectados a una unidad de control. La unidad de control incluye un procesador y una memoria para llevar a cabo el proceso de verificación. La unidad de control está conectada a un sistema de autorización central.

Se observa que las publicaciones de patentes Estadounidenses US 2007/0200665 y US 2006/0170533 describen cada una un sistema de control de acceso que incluye un sistema de autorización central que está dispuesto para verificar datos telefónicos con una lista precargada de teléfonos autorizados.

Dicho sistema cerrado son menos flexibles para la aplicación de dispositivos de autenticación personal que son desconocidos para el sistema de autorización central.

Es un objeto de la invención proporcionar un método para autorizar a una persona en el que se reduce uno de los inconvenientes identificados anteriormente. En particular, un objeto de la invención es proporcionar un método en el que se pueden aplicar lectores relativamente simples y en los que se puede conceder autorización a usuarios de dispositivos de autenticación personal que son desconocidos para el sistema de autorización central. De acuerdo a lo anterior, se provee un procedimiento según la invención como se define en la reivindicación 1.

Simplemente incluyendo, en el lector, los datos de autenticación recibidos en un mensaje de petición, el lector no está obligado a llevar a cabo ningún proceso de identificación en los datos. Como consecuencia, el lector puede implementarse de una manera de bajo rendimiento y bajo coste. Además, debido a la estructura de lector simple, el proceso de autorización es flexible en términos de transmisión de datos desde dispositivos de autenticación personal que están asociados con un sistema de autenticación desconocido para el sistema de autorización central. Los usuarios de un dispositivo de autenticación personal que no está incluido en una lista del sistema de autorización central, pero es conocido en el sistema de autenticación, tienen acceso, proporcionando así un esquema de autorización elegante y flexible.

Preferentemente, la etapa de llevar a cabo un proceso de autenticación incluye los pasos de generar un mensaje de petición que incluye los datos de autenticación y transmitir el mensaje de petición a un sistema de autenticación central asociado con el dispositivo de autenticación de persona, verificando el mensaje de petición en el sistema de autenticación central comprobando datos de autenticación en el mensaje de petición y generar un mensaje de respuesta a la petición que contiene datos asociados con el dispositivo de autenticación personal y transmitir el mensaje de respuesta a la petición al sistema de autorización central.

De manera similar, la etapa de ejecutar un proceso de autorización puede incluir las etapas de verificar el mensaje de respuesta a la petición en el sistema de autorización central comprobando los datos asociados con el dispositivo de autenticación personal, generar un mensaje de autorización si la verificación de la respuesta a la petición fue exitosa y transmitir el mensaje de autorización a un accionador asociado con el sistema de autorización central.

Al proporcionar un camino de comunicación transparente, también denominado "túnel", entre el dispositivo de autenticación personal y el sistema de autenticación central, por una parte, y un camino de comunicación transparente, también denominado "túnel", entre el lector y el sistema de autorización central por otra parte, el sistema de autorización central puede dedicarse a comunicarse con el lector y el accionador, mientras que el sistema de autenticación central se comunica con el dispositivo de autenticación personal. En este contexto, cabe señalar que el concepto de "comunicación" significa en este contexto un intercambio de información significativo, y no simplemente una transmisión de datos. Sin embargo, en las implementaciones prácticas del método de acuerdo con la invención, un mensaje comunicado entre el lector y el sistema de autorización central puede ser enviado a través de un componente de la red de autenticación, tal como el dispositivo de autenticación personal.

De acuerdo con un aspecto de la invención, el proceso de identificación de un usuario (identidad o capacidad) se realiza en un sistema central de autenticación, mientras que un proceso de verificar si dicho usuario (identidad o capacidad) está autorizado a tener acceso a un el espacio físico y/o la información se realiza por separado en un sistema de autorización. Como resultado, los lectores pueden implementarse con una funcionalidad mínima, reduciendo así los costes, mejorando la fiabilidad y facilitando la puesta a punto de una infraestructura de lectores. Ventajosamente, al almacenar centralmente la información del dispositivo de autenticación personal, el almacenamiento, la protección y el manejo de dicha información se hacen más sencillos. Además, utilizando la estructura de mensajes especificada entre el dispositivo de autenticación central y el dispositivo de autorización central, se obtiene una interacción eficiente deseada que proporciona un método flexible de autorizar a una persona.

La invención también se refiere a una arquitectura de autorización según se define en la reivindicación 11.

Además, la invención se refiere a un producto de programa de ordenador como se define en la reivindicación 13. Un producto de programa informático puede comprender un conjunto de instrucciones ejecutables por ordenador almacenadas en un soporte de datos, tal como un CD o un DVD. El conjunto de instrucciones ejecutables por ordenador, que permiten a un ordenador programable llevar a cabo el procedimiento definido anteriormente, también puede estar disponible para descargar desde un servidor remoto, por ejemplo a través de Internet.

Otras realizaciones ventajosas de acuerdo con la invención se describen en las siguientes reivindicaciones.

A modo de ejemplo solamente, las realizaciones de la presente invención se describirán ahora con referencia a las figuras adjuntas en las que la figura 1 muestra un diagrama de flujo de datos correspondiente a una primera realización de un método de acuerdo con la invención;

la figura 2 muestra un diagrama de flujo de datos correspondiente a una segunda realización de un método según la invención;

la figura 3 muestra un diagrama de flujo de datos parcial correspondiente a una tercera realización de un método según la invención;

la figura 4 muestra una vista esquemática de una arquitectura de autorización de acuerdo con la invención; y

la figura 5 muestra un diagrama de flujo de una realización de un método de acuerdo con la invención.

Se observa que las figuras muestran simplemente una realización preferida de acuerdo con la invención. En las figuras, los mismos números de referencia se refieren a partes iguales o correspondientes.

La figura 1 muestra un diagrama de flujo de datos correspondiente a una primera realización de un método de acuerdo con la invención. El diagrama de flujo de datos muestra una serie de componentes de procesamiento de datos que forman una arquitectura de autorización. La arquitectura 9 incluye un sistema 10 de autorización central para autorizar a una persona y un sistema 11 central de autenticación de forma comunicativa conectado al sistema 10 de autorización central. Además, la arquitectura 9 incluye un lector 12 y un accionador 13 asociados con el sistema 10 de autorización central.

El sistema 10 de autorización central proporciona acceso a un espacio físico, tal como un edificio o una habitación, y/o a información, tal como datos relacionados con cuentas bancarias. A través del lector 12, la información se transmite al sistema 10 de autorización central. Después de haber realizado un proceso de autorización, como se explica con más detalle a continuación, el sistema 10 de autorización central puede permitir que el accionador 13 accione, por ejemplo abriendo una puerta y/o proporcionando información en una pantalla.

El sistema 11 central de autenticación realiza una verificación de la identidad y/o capacidad de un dispositivo 14 de autenticación personal que comunica con el lector 12. Según un aspecto de la invención, las actividades del sistema 10 de autorización central y del sistema 11 central de autenticación están coordinadas para proporcionar un proceso de autorización altamente eficiente.

Durante el uso de la arquitectura de autorización 9, el dispositivo 14 de autenticación personal, por ejemplo un teléfono móvil, una PDA, una tarjeta inteligente, una clave física o electrónica o una clave electrónica, transmite datos de autenticación 20 al lector 12. Los datos 20 pueden incluir datos personales, tales como el nombre del usuario del dispositivo 14 de autenticación personal. Los datos de autenticación incluyen datos de identidad y/o datos de capacidad. El lector 12 recibe dichos datos 20. Entonces, el lector 12 genera un mensaje 21 de petición mediante la inclusión de dichos datos de autenticación recibidos en un mensaje y transmite el mensaje 21 de petición al sistema 10 de autorización central. El proceso de generación del mensaje 21 de petición puede incluir la adición de datos de localización o información ambiental adicionales a los datos de autenticación recibidos 20. A modo de ejemplo, se puede añadir la ubicación de la habitación en la que está situado el lector 12 o un número de

identificación de lector en el mensaje 21 de petición. Sin embargo, el mensaje 21 de petición puede, como una alternativa, incluir explícitamente datos de localización o información ambiental adicional, incluir también información relativa al lector de manera implícita, por ejemplo si solamente un lector 12 está asociado al sistema 10 de autorización central o si se aplica un protocolo específico de lector para el mensaje 21 de petición. El mensaje 21 de petición puede transmitirse al sistema 10 de autorización central, por ejemplo, a través de una línea de comunicación física que interconecta el lector 12 y el sistema 10 de autorización, o a través de una conexión inalámbrica. Con el fin de proteger los datos, especialmente durante la transmisión inalámbrica, la etapa de generar un mensaje de petición puede incluir una etapa de protección de datos, por ejemplo con el fin de determinar la integridad del mensaje, para encriptar datos para contrarrestar que las partes no autorizadas obtengan conocimiento de los datos incluidos en el mensaje y/o para validar el transmisor del mensaje.

Como paso siguiente, el mensaje 21 de petición se recibe en el sistema 10 de autorización central. A partir del mensaje 21 de petición, se recuperan los datos de autenticación, para identificar al menos parcialmente el dispositivo 14 de autenticación personal que interactúa con el lector 12. En la recuperación de los datos de autenticación está indicada por un primer disco 30 en el sistema 10 de autorización central. En el proceso de recuperación, el mensaje 21 de petición se somete a un proceso de desencriptación y/o verificación en el sistema 10 de autorización central, si el mensaje 21 de petición ha sido protegido. A continuación, se realiza un proceso de autenticación. El proceso de autenticación incluye que el sistema 10 de autorización central genere un mensaje 22 de petición que incluye los datos de autenticación. El mensaje 22 de petición se transmite al sistema 11 central de autenticación para su posterior procesamiento. Después de la recepción, el sistema 11 central de autenticación verifica el mensaje 22 de petición comprobando los datos de autenticación incluidos en el mensaje 22 de petición. La verificación del mensaje de petición se indica mediante un disco 31 en el sistema 11 central de autenticación. Para llevar a cabo la verificación, los datos de autenticación se pueden comparar con los datos correspondientes en una base de datos de autenticación central proporcionada en el sistema 11 central de autenticación. Como ejemplo, la base de datos puede incluir una lista de claves que corresponden con datos de autenticación únicos y una identificación específica o capacidad asignadas al usuario de dichas claves físicas.

Además, en este proceso, puesto que se establece una ruta de transferencia de datos entre la clave física y el sistema de autenticación central, el sistema de autenticación central puede comunicar otros datos con la clave física, por ejemplo sobre la actualización de la información sobre la clave física, etc.

Si se ha encontrado una coincidencia positiva entre los datos de autenticación y un dispositivo de autenticación personal identificado en el sistema 11 central de autenticación, se genera un mensaje de respuesta a la petición 23 que contiene datos asociados con el dispositivo 14 de autenticación personal. El mensaje de respuesta a la petición 23 es transmitido de vuelta al sistema 10 central de autorización, poniendo así fin al proceso de autenticación.

En la autorización 10 central, se ejecuta un proceso de autorización, incluyendo que el mensaje de respuesta a la petición 23 se verifica comprobando los datos asociados con el dispositivo 14 de autenticación personal. La verificación del mensaje de respuesta a la petición se indica mediante un segundo disco 32 en el sistema 10 de autorización. De manera similar, el proceso de verificación de datos puede incluir una etapa de comparación de dichos datos con datos correspondientes en una base de datos de autorización central proporcionada en el sistema 10 de autorización central.

Si la verificación ha sido exitosa, se genera un mensaje 24 de autorización y se transmite al accionador 13, finalizando así el proceso de autorización. Entonces, el accionador 13 está autorizado para iniciar un acto autorizado. Como ejemplo, el accionador está dispuesto para accionar una cerradura, un interruptor, una luz o una puerta, para dispensar un bien, para hacer una transacción o pagar, y/o hacer un sonido. Como un ejemplo adicional, el accionador puede proporcionar acceso a sistemas de transporte, por ejemplo un sistema para arrancar el motor de un automóvil, barco, avión, etc.

La figura 2 muestra un diagrama de flujo de datos correspondiente a una segunda realización de un método según la invención. En este caso, el mensaje 21 de petición se transmite al sistema 10 de autorización central a través de una ruta que incluye el dispositivo 14 de autenticación personal y el sistema 11 central de autenticación. En la configuración mostrada, la línea de comunicación directa entre el lector 12 y el sistema 10 de autorización central asociado con el lector 12 es reemplazada por la conexión virtual usando el dispositivo 14 de autenticación personal y el sistema 11 central de autenticación. El lector 12 puede colocarse de forma independiente. De forma similar, el mensaje 24 de autorización se transmite desde el sistema 10 de autorización central a través del sistema 11 central de autenticación y el dispositivo 14 de autenticación personal al accionador (no mostrado). El accionador puede conectarse al lector 12 o está dispuesto para recibir directamente el mensaje de autorización a través del dispositivo 14 de autenticación personal. Se observa que la ruta física a lo largo del cual se transmite el mensaje 24 puede incluir otros puntos de comunicación y/o secciones de ruta.

La figura 3 muestra un diagrama de flujo de datos parcial que corresponde a una tercera realización de un método según la invención. Aquí, la arquitectura 9 de autorización comprende un sistema de separación 15, por ejemplo para llevar a cabo una verificación de fraude y/o garantía. En el ejemplo mostrado, se transmiten al sistema 15 de

autorización, tanto por el sistema 10 de autorización como por el sistema 11 de autenticación, mensajes 22A, 23A de petición de verificación adicionales antes de generar y transmitir el mensaje de respuesta a la petición 23 y el mensaje 24 de autorización, respectivamente. El mensaje respectivo se genera y transmite después de recibir un mensaje 22B, 23B de autorización positiva.

La figura 4 muestra una vista esquemática de una arquitectura 9 de autorización de acuerdo con la invención. La arquitectura 9 comprende dos lectores 12a, 12b, un sistema 10 de autorización central, también denominado centro de seguridad, y un sistema 11 de autenticación, también denominado sistema de gestión de claves. Además, la arquitectura 9 incluye una interfaz 70 de usuario web y un servidor 71 para llevar a cabo la funcionalidad que se ofrece en la interfaz de usuario web, también llamada portal. Como ejemplo, el portal 70 incluye una serie de sitios para ofrecer servicios, a saber, un sitio 70a de venta, un sitio 70b de cliente para gestión privilegiada por clientes de la arquitectura, un sitio 70c de supervisor para gestionar los servicios que se ofrecen en el portal 70 y un sitio 70d de activación para activar claves físicas, tal como un teléfono móvil, por ejemplo a través de un mensaje SMS. Se observa que el portal 70 puede incluir también más, menos y/u otros sitios para ofrecer servicios. El sistema de gestión de claves 11 proporciona y gestiona información clave que está asociada con los testigos 14a, 14b proporcionados. De forma similar, el centro 10 de seguridad comunica con los lectores 12a, 12b, accionadores y un servidor 72 de respaldo. El servidor 72 de respaldo es un componente de memoria caché para soportar la transferencia de datos a nivel local cuando la comunicación entre los lectores 14 y el centro 10 de seguridad ha sido interrumpida.

Una red 80, por ejemplo una intranet local o una Internet global, interconecta los lectores 12, el centro 10 de seguridad y el servidor 72 de respaldo. Con ello, los lectores 12 y el centro 10 de seguridad están provistos de una interfaz 51a, b; 52a. Opcionalmente, un testigo 14a está también provisto de una interfaz 54d para comunicación con la red 80. El lector 12a y la clave 14a física se comunican a través de una línea 81 de comunicación específica, por ejemplo Blueetooth o infrarrojo. Debido a ello, el lector y la clave física están provistos de una interfaz 51c, d; 54a, b, respectivamente. Opcionalmente, la clave 14a también incluye una interfaz para comunicar, a través de una red 82 separada, preferiblemente segura, con el portal 70. Debido a ello, también, el portal 70 está provisto de una interfaz 56a. Además, el centro 10 de seguridad, el sistema de gestión de claves 11 y el servidor 71 están provistos de interfaces 52b, 53a, 55a correspondientes para la comunicación mutua utilizando una red preferiblemente 83a, b, c. La clave física es implementada por ejemplo como un teléfono móvil, teléfono inteligente j2me o tarjeta ISO 14443. Aparentemente, la clave física puede incluir otras interfaces para la comunicación.

En este contexto se observa que el lector puede estar provisto de un único o múltiples números de interfaces para la comunicación con tipos de claves físicas específicos o diferentes. Aunque la figura 4 muestra dos lectores, también se puede aplicar otro número de lectores, por ejemplo alrededor de diez lectores o alrededor de cien lectores. Además, se puede aplicar un único o un número múltiple de accionadores, por ejemplo para abrir una puerta o controlar una unidad de visualización. En principio, la arquitectura puede incluir un número múltiple de sistemas de autorización centrales. Además, puede aplicarse un número múltiple de sistemas de autenticación central, por ejemplo para soportar un número múltiple de proveedores que soportan una autorización basada en claves físicas. Además, pueden aplicarse otros sistemas de testigos heredados y/u otros sistemas de accionadores.

Cuando un testigo comunica con un lector, los datos de autenticación se transmiten al lector. La transmisión puede ser iniciada por la clave física o el lector. Los datos de autenticación inicial pueden ser suficientes para la autorización. Sin embargo, el sistema 10 de autorización puede solicitar información adicional, ya sea iniciada por el sistema 10 o por otros sistemas, tal como un sistema 11 de autenticación. Como consecuencia, se pueden transmitir al lector múltiples mensajes que incluyen datos de autenticación para su procesamiento. Como una opción adicional, el lector incluye un sistema de posicionamiento, por ejemplo utilizando un número de antenas de radio, para determinar si el lector está situado en una ubicación predeterminada. El lector puede estar dispuesto para establecer una conexión o aceptar una conexión con la clave física sólo si la posición determinada del lector coincide con la ubicación predeterminada cerca de la clave física.

Según un aspecto de la invención, el lector no interpreta datos de autenticación que son transmitidos por la clave física al lector. Como tal, el lector no identifica un tipo de clave física, una configuración de tipo de clave física o una clave física por sí mismo. El lector incluye dicha información en un mensaje de petición -sin llevar a cabo ninguna identificación- para su transmisión al sistema de autorización. Como se ha descrito anteriormente, el lector opcionalmente puede enriquecer el mensaje de petición incluyendo además información adicional, tal como tipo de interfaz de clave física, ubicación, tiempo y/o características de cifrado.

La figura 5 muestra un diagrama de flujo de una realización del método según la invención. Se utiliza un método para autorizar a una persona. El método comprende una etapa (100) de recepción de datos de autenticación desde un dispositivo de autenticación personal que transmite dichos datos a un lector asociado con un sistema de autorización central, una etapa (110) de incluir los datos de autenticación recibidos en un mensaje de petición y transmitir el mensaje de petición al sistema de autorización central, una etapa (120) de recepción del mensaje de petición en el sistema de autorización central y recuperación de los datos de autenticación del mensaje de petición, una etapa (130) de llevar a cabo un proceso de autenticación en un sistema de autenticación central que utiliza

dicha datos de autenticación del lector, y una etapa (140) de ejecución de un proceso de autorización en el sistema de autorización central basado en el resultado del proceso de autenticación.

El método de autorización de una persona puede ser llevado a cabo utilizando estructuras de hardware dedicadas, tales como componentes FPGA y/o ASIC. De lo contrario, el método también llevarse a cabo al menos parcialmente utilizando un producto de programa informático que comprende instrucciones para hacer que un procesador del sistema informático realice las etapas descritas anteriormente del método según la invención. En principio, todas las etapas pueden realizarse en un solo procesador. Sin embargo, se observa que en realizaciones ventajosas de acuerdo con la invención, se realizan grupos de etapas en procesadores separados. Como un ejemplo, la etapa (120) de recepción el mensaje de petición y recuperar los datos de autenticación del mensaje, y la etapa de ejecución (140) se puede llevar a cabo un proceso de autorización en un procesador asociado con el sistema de autorización central.

Se entenderá que las realizaciones descritas anteriormente de la invención son sólo ejemplos y que son posibles otras realizaciones sin apartarse del alcance de la presente invención. Se entenderá que son posibles muchas variantes.

Dichas variantes serán evidentes para el experto en la materia y se consideran que están dentro del alcance de la invención como se define en las siguientes reivindicaciones.

Reivindicaciones

1. Un método para autorizar a una persona, que comprende las etapas de:

recibir, por un lector asociado con un sistema de autorización central, datos de autenticación transmitidos desde un dispositivo de autenticación personal;

incluir, por el lector, los datos de autenticación recibidos en un mensaje de petición y transmitir, por el lector, el mensaje de petición al sistema de autorización central;

recibir el mensaje de petición en el sistema de autorización central y recuperar los datos de autenticación del mensaje de petición;

llevar a cabo un proceso de autenticación en un sistema de autenticación central que utiliza dichos datos de autenticación; y

ejecutar un proceso de autorización en el sistema de autorización central basado en el resultado del proceso de autenticación,

en el que la etapa de llevar a cabo un proceso de autenticación incluye las etapas de:

generar un mensaje de petición que incluye los datos de autenticación y de transmitir el mensaje de petición al sistema de autenticación central asociado con el dispositivo de autenticación de personas;

verificar el mensaje de petición en el sistema de autenticación central comprobando los datos de autenticación en el mensaje de petición; y

generar un mensaje de respuesta a la petición que contiene datos asociados con el dispositivo de autenticación personal y transmitir el mensaje de respuesta a la petición al sistema de autorización central y

en el que la etapa de ejecución de un proceso de autorización incluye las etapas de:

verificar el mensaje de respuesta a la petición en el sistema de autorización central comprobando los datos asociados con el dispositivo de autenticación personal;

generar un mensaje de autorización si la verificación de la respuesta a la petición ha sido satisfactoria;

y

transmitir el mensaje de autorización a un accionador asociado con el sistema de autorización central.

2. Un método de acuerdo con la reivindicación 1, que comprende transmitir el mensaje de petición al sistema de autorización central a través del dispositivo de autenticación personal y el sistema de autenticación central.

3. Un método según la reivindicación 1 ó 2, en el que el proceso de autenticación incluye la identificación de una identidad o capacidad.

4. Un método de acuerdo con cualquiera de las reivindicaciones precedentes, en el que el proceso de autorización incluye comprobar si la identidad o capacidad identificada está autorizada para tener acceso a un espacio físico y/o a información.

5. Un método de acuerdo con cualquiera de las reivindicaciones precedentes, en el que la etapa de generar el mensaje de petición incluye añadir datos de localización o información ambiental adicional a los datos de autenticación recibidos.

6. Un método de acuerdo con cualquiera de las reivindicaciones precedentes, en el que la etapa de generación de un mensaje de petición incluye una etapa de protección de datos.

7. Un método de acuerdo con cualquiera de las reivindicaciones precedentes, en el que la etapa de verificación de datos de autenticación en el mensaje de petición comprende una etapa de comparación de los datos de autenticación con los datos correspondientes en una base de datos de autenticación central.

8. Un método de acuerdo con cualquiera de las reivindicaciones anteriores, en el que la etapa de verificación, en el mensaje de respuesta de petición delos datos asociados con el dispositivo de autenticación personal comprende una etapa de comparación de dichos datos con los datos correspondientes en una base de datos de autorización central.

9. Un método de acuerdo con cualquiera de las reivindicaciones precedentes 1, 3-8, que comprende transmitir el mensaje de petición al sistema de autorización central a través del lector.

10. Un método de acuerdo con cualquiera de las reivindicaciones precedentes, que incluye un número múltiple de sistemas centrales de autenticación.

11. Una arquitectura de autorización, que comprende un sistema de autorización central para autorizar a una persona, al menos un lector y al menos un accionador, estando asociado el lector y el accionador con el sistema de autorización central, que comprende además un sistema central de autenticación comunicativamente conectado con el sistema de autorización central en el que la arquitectura está dispuesta para llevar a cabo las etapas de:

recibir, por el lector asociado con un sistema de autorización central, datos de autenticación transmitidos desde un dispositivo de autenticación personal;

incluir, por el lector, los datos de autenticación recibidos en un mensaje de petición y transmitir, por el lector, el mensaje de petición al sistema de autorización central;

recibir el mensaje de petición en el sistema de autorización central y recuperar los datos de autenticación del mensaje de petición;

llevar a cabo un proceso de autenticación en un sistema de autenticación central que utiliza dichos datos de autenticación; y

ejecutar un proceso de autorización en el sistema de autorización central con base en el resultado del proceso de autenticación,

en el que la etapa de llevar a cabo un proceso de autenticación incluye las etapas de:

generar un mensaje de petición que incluye los datos de autenticación y transmitir el mensaje de petición al sistema de autenticación central asociado con el dispositivo de autenticación de personas;

verificar el mensaje de petición en el sistema de autenticación central comprobando los datos de autenticación en el mensaje de petición; y

generar un mensaje de respuesta a la petición que contiene datos asociados con el dispositivo de autenticación personal y transmitir el mensaje de respuesta a la petición al sistema de autorización central, y

en el que la etapa de ejecutar un proceso de autorización incluye las etapas de:

verificar el mensaje de respuesta a la petición en el sistema de autorización central comprobando los datos asociados con el dispositivo de autenticación personal;

generar un mensaje de autorización si la verificación de la respuesta a la petición ha sido satisfactoria;

y

transmitir el mensaje de autorización a un accionador asociado con el sistema de autorización central.

12. Una arquitectura de autorización de acuerdo con la reivindicación 11, en la que al menos un lector incluye un sistema de posicionamiento para determinar si el lector está situado en un lugar predeterminado.

13. Un producto de programa informático para autorizar a una persona, comprendiendo el producto de programa informático un código legible por ordenador para hacer que un procesador realice los pasos de:

recibir, por un lector asociado con un sistema de autorización central, datos de autenticación transmitidos desde un dispositivo de autenticación personal;

incluir, por el lector, los datos de autenticación recibidos en un mensaje de petición y transmitir, por el lector, el

mensaje de petición al sistema de autorización central;

recibir el mensaje de petición en el sistema de autorización central y recuperar los datos de autenticación del mensaje de petición;

llevar a cabo un proceso de autenticación en un sistema de autenticación central que utiliza dichos datos de autenticación; y

ejecutar un proceso de autorización en el sistema de autorización central con base en el resultado del proceso de autenticación

en el que la etapa de llevar a cabo un proceso de autenticación incluye las etapas de:

generar un mensaje de petición que incluye la autenticación de datos y transmitir el mensaje de petición al sistema de autenticación central asociado con el dispositivo de autenticación de personas;

verificar el mensaje de petición en el sistema de autenticación central comprobando los datos de autenticación en el mensaje de petición; y

generar un mensaje de respuesta a petición que contiene datos asociados con el dispositivo de autenticación personal y transmitir el mensaje de respuesta a la petición al sistema de autorización central y

en el que la etapa de ejecutar un proceso de autorización incluye las etapas de:

verificar el mensaje de respuesta a la petición en el sistema de autorización central comprobando los datos asociados con el dispositivo de autenticación personal;

generar un mensaje de autorización si la verificación de la respuesta a la petición ha sido satisfactoria;

y

transmitir el mensaje de autorización a un accionador asociado con el sistema de autorización central.

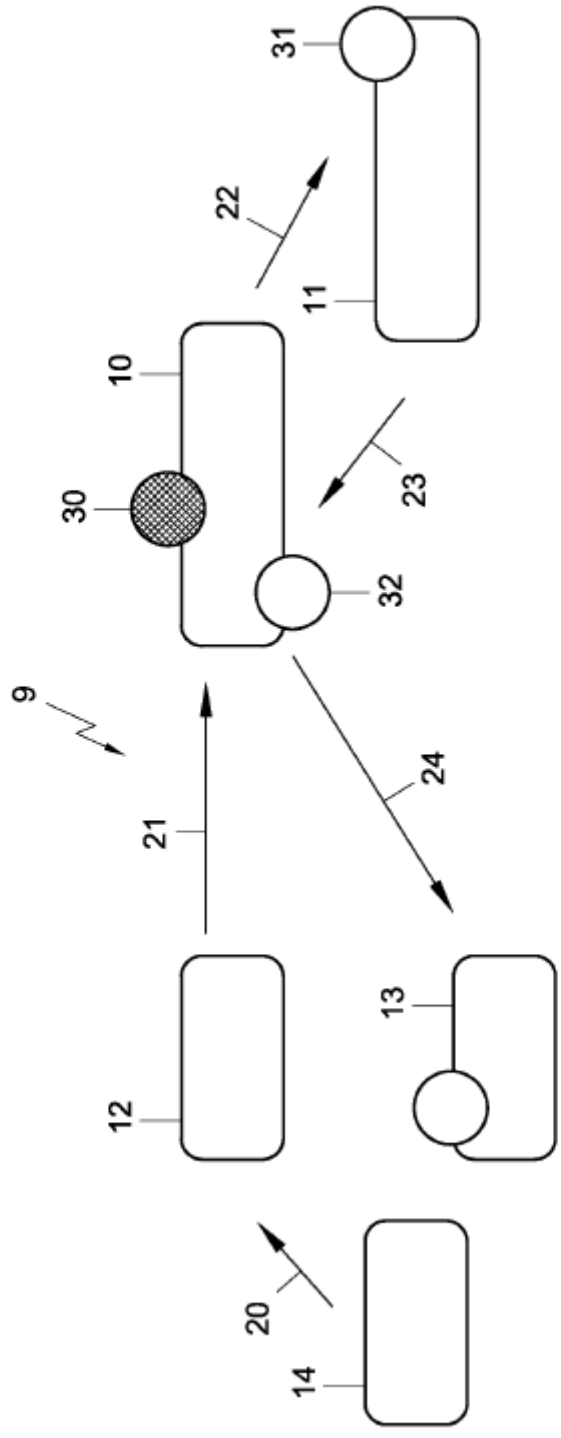

Fig. 1

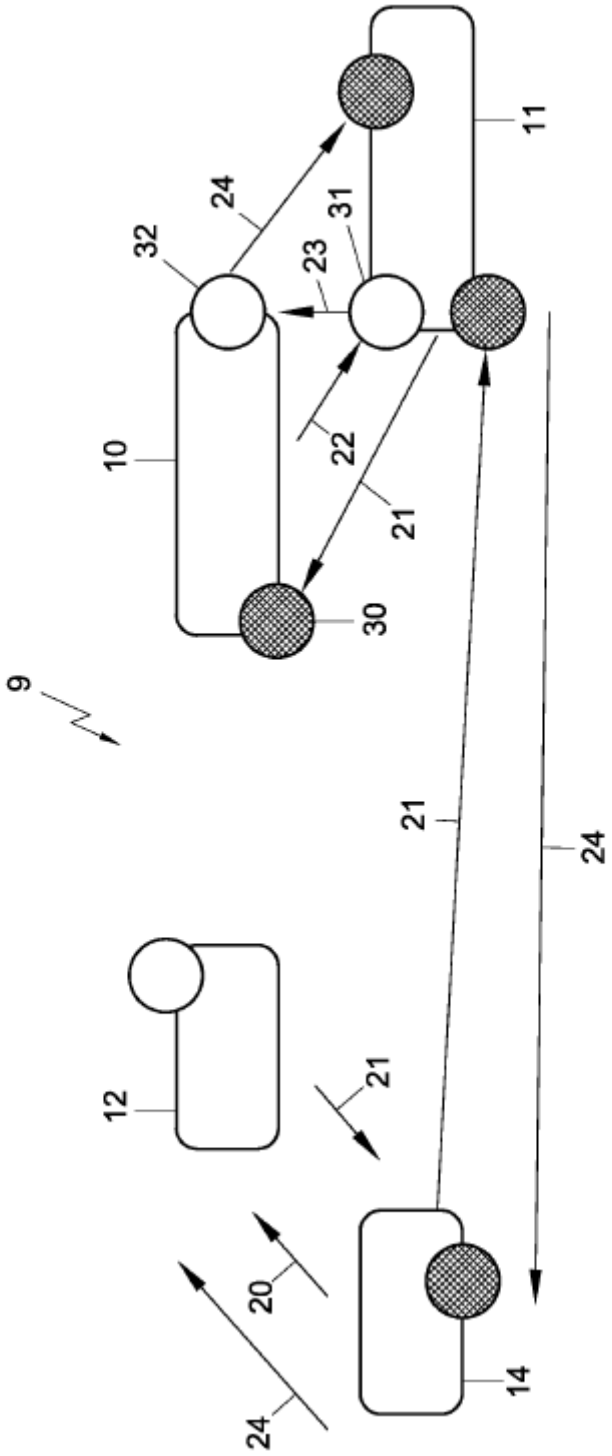

Fig. 2

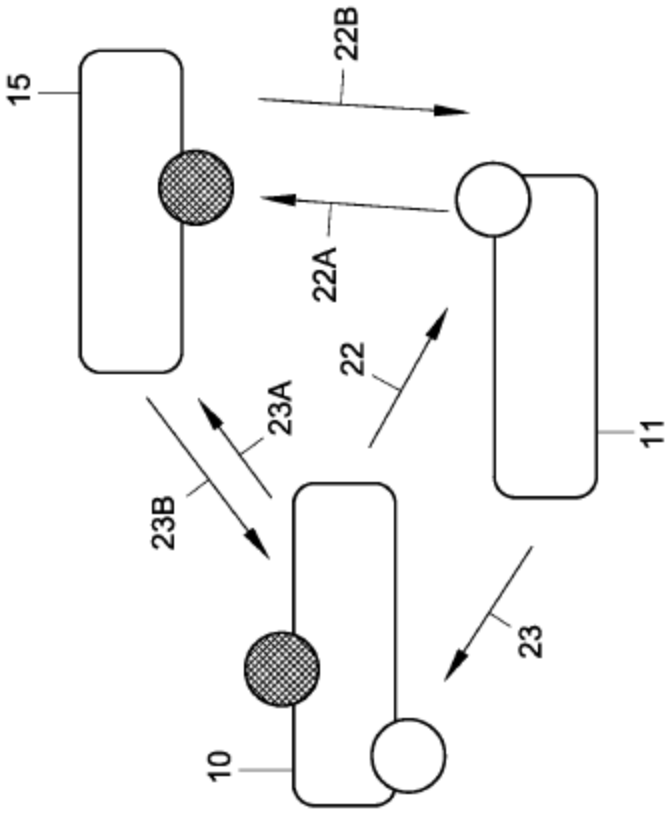

Fig. 3

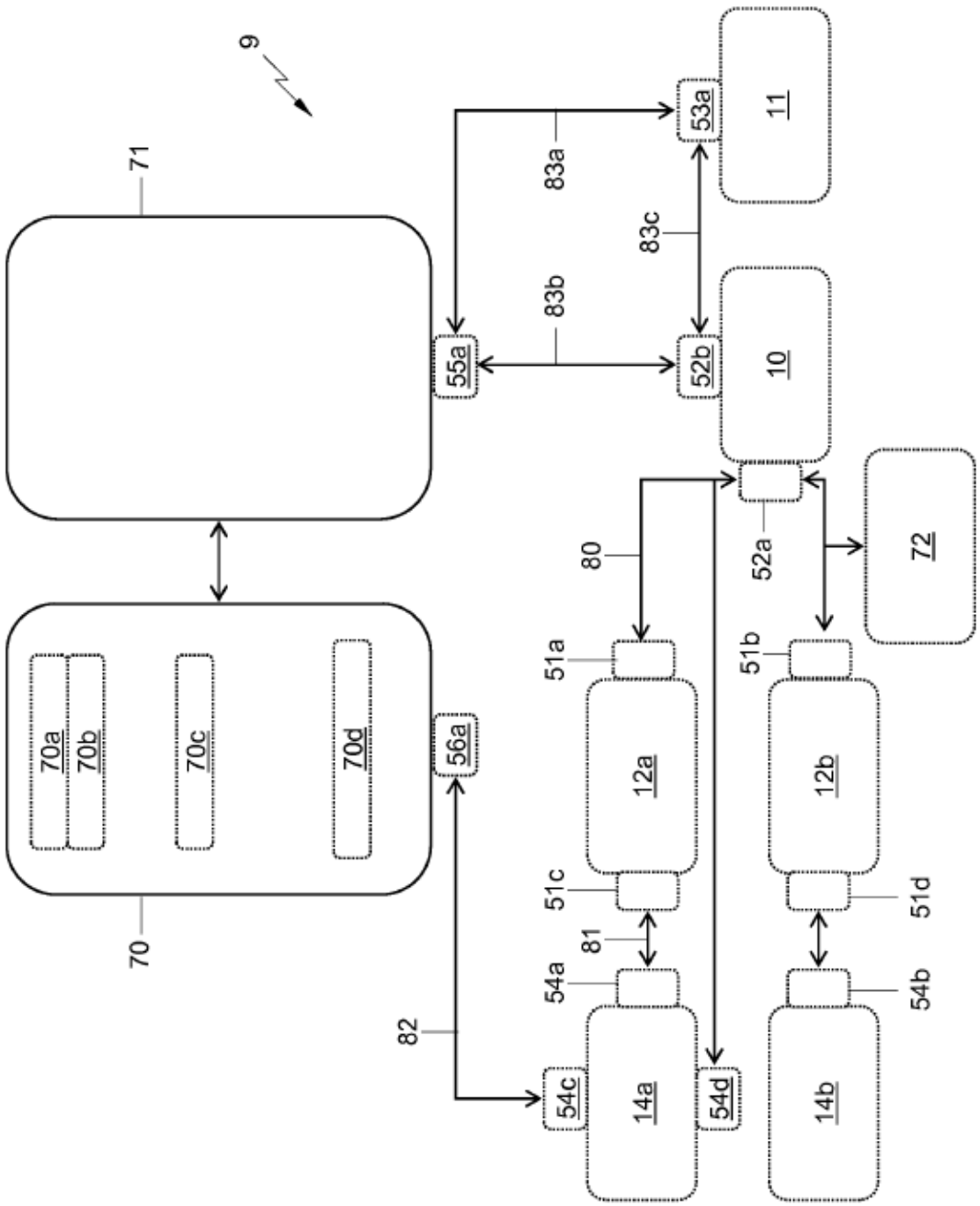
9
71
70
70a
70b
70c
70d
56a
55a
83a
83b
83c
53a
11
52b
10
52a
72
80
51a
12a
51c
81
54a
54c
14a
54d
82
51b
12b
51d
54b
14b

Fig.4

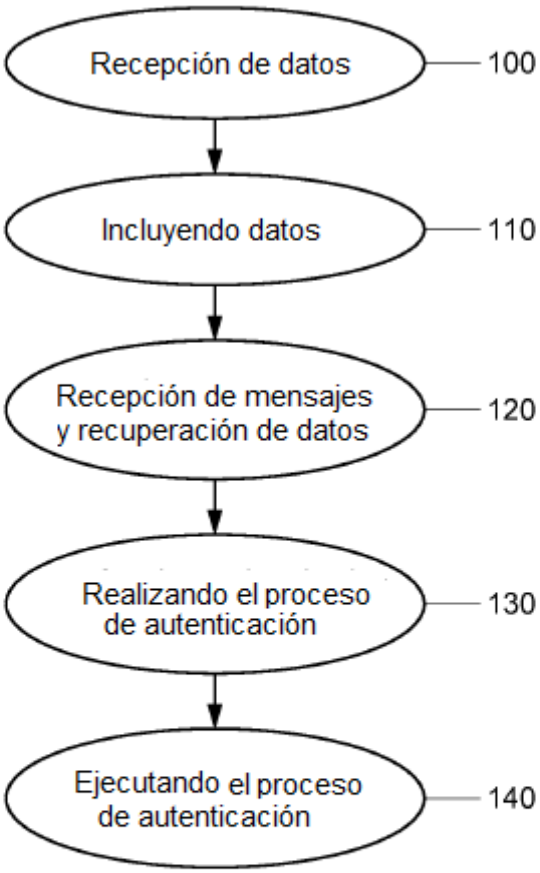
Recepción de datos
100
Incluyendo datos
110
Recepción de mensajes y recuperación de datos
120
Realizando el proceso de autenticación
130
Ejecutando el proceso de autenticación
140

Fig. 5