(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 791 600**

(51) Int. CI.:

G07C 9/00 (2010.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **28.10.2014 PCT/EP2014/073122**

(87) Fecha y número de publicación internacional: **07.05.2015 WO15063087**

(96) Fecha de presentación y número de la solicitud europea: **28.10.2014 E 14793066 (3)**

(97) Fecha y número de publicación de la concesión europea: **15.04.2020 EP 3063743**

(54) Título: **Procedimiento para la verificación de la identidad de una persona**

(30) Prioridad:

29.10.2013 DE 102013111883

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
05.11.2020

(73) Titular/es:

BUNDESDRUCKEREI GMBH (100.0%)
Kommandantenstraße 18
10969 Berlin, DE

(72) Inventor/es:

RABELER, UWE y
FISCHBECK, MATTHIAS

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Procedimiento para la verificación de la identidad de una persona

La presente invención se refiere al campo de la verificación de identidad de una persona.

La identidad de una persona puede verificarse comparando los rasgos distintivos preexistentes en un documento de identificación, por ejemplo la imagen facial, la altura del cuerpo, el color de los ojos, las huellas dactilares y/o la reproducción del iris de un ojo, con los rasgos distintivos de la persona. La identidad de la persona puede verificarse si existe una coincidencia entre los rasgos distintivos de la persona y los rasgos distintivos almacenados previamente en el documento de identificación.

Frecuentemente se utilizan estaciones de comprobación a menudo fijas para comparar los rasgos distintivos, en particular para comparar una huella dactilar y/o una reproducción del iris de un ojo con los rasgos distintivos almacenados previamente en el documento de identificación. Dentro de estas estaciones de comprobación instaladas de forma permanente se suelen utilizar dispositivos que, sin embargo, no son aptos para su uso móvil debido a sus dimensiones geométricas y su peso.

El documento WO 2010/138013 A2 se refiere a un dispositivo portátil manual para la verificación de documentos de viaje y personales, la lectura de datos biométricos y la identificación de las personas que poseen esos documentos.

El documento DE 10 2004 056 007 A 1 se refiere a un dispositivo móvil de verificación para comprobar la autenticidad de los documentos de viaje.

El documento DE 10 2006 027 253 A 1 se refiere a un lector de un documento, un procedimiento de lectura de un objeto de datos y un programa informático.

La publicación de la Oficina Federal de Seguridad de la Información: BSI TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents, 20 de marzo de 2012, páginas 1-131, Bonn, se refiere a los mecanismos de seguridad para los documentos legibles por máquina.

El documento EP 2 704 077 A1 se refiere a un sistema y un procedimiento de autenticación.

Por lo tanto, el objetivo de la presente invención es crear un concepto eficiente, rentable y móvil para verificar la identidad de una persona.

Este objetivo se logra mediante las características de las reivindicaciones independientes. Unas formas de realización ventajosas son objeto de las reivindicaciones dependientes, de la descripción y de los dibujos.

La invención se basa en la constatación de que el objetivo anterior puede resolverse mediante el uso de un equipo móvil de comunicaciones. Mediante una cámara de imágenes del equipo móvil de comunicaciones se puede capturar un rasgo biométrico de la persona. Sin embargo, mediante una interfaz de comunicación del equipo móvil de comunicaciones se puede leer de un circuito electrónico del documento de identificación un rasgo biométrico de referencia. La identidad de la persona puede verificarse comparando la característica biométrica capturada de la persona con el rasgo biométrico de referencia almacenado previamente en el circuito electrónico del documento de identificación. Por lo tanto, el uso de un equipo móvil de comunicaciones permite la verificación móvil de la identidad de una persona usando un equipo compacto y económico.

De acuerdo con un primer aspecto, la invención se refiere a un procedimiento para verificar la identidad de una persona según la reivindicación 1. Así se logra la ventaja de que se puede realizar un concepto eficiente y económico para verificar la identidad de una persona.

El documento de identificación puede ser uno de los siguientes documentos de identificación: documento de identidad, como un carné de identidad, pasaporte, tarjeta de control de acceso, tarjeta de autorización, tarjeta de identificación de la empresa, código o billete fiscal, certificado de nacimiento, permiso de conducir o documento de matrícula del vehículo, medios de pago, por ejemplo una tarjeta bancaria o una tarjeta de crédito. El documento de identificación también puede incluir un circuito de lectura electrónica, por ejemplo un chip RFID. El documento de identificación puede ser de una sola capa o bien de varias capas a base de papel y/o plástico. El documento de identificación puede estar estructurado a partir de películas a base de plástico que se unen para formar un cuerpo de tarjetas ensamblado por medio de pegado y/o laminación, teniendo las películas, preferiblemente, propiedades materiales similares.

El equipo móvil de comunicaciones puede ser un equipo manual, un teléfono móvil o un teléfono inteligente, que puede incluir una cámara de imágenes y una interfaz de comunicación.

La cámara de imágenes puede estar diseñada para tomar una imagen óptica, por ejemplo en la gama de longitudes de onda infrarrojas, visibles y/o ultravioletas, de la persona y/o del documento de identificación. La cámara de imágenes puede incluir un sensor de imágenes, una fuente de luz, por ejemplo en la gama de longitudes de onda infrarroja, visible y/o ultravioleta, para iluminar a la persona y/o el documento de identificación a registrar, y/o un objetivo de cámara.

El circuito electrónico puede ser un chip en el que se puede almacenar previamente un rasgo biométrico de referencia. El rasgo biométrico de referencia almacenado previamente en el circuito electrónico puede ser leído por medio de una interfaz de contacto o sin contacto, por ejemplo una interfaz de radio.

La captura del rasgo biométrico de la persona se realiza mediante el equipo móvil de comunicaciones tomando una imagen de la persona por medio de la cámara de imágenes, de la que se extrae el rasgo biométrico, por ejemplo mediante un reconocimiento de patrones mediante el equipo móvil de comunicaciones.

El rasgo biométrico de la persona puede ser una huella dactilar de la persona, una imagen facial de la persona o una reproducción del iris de un ojo de la persona. El rasgo biométrico de referencia es un rasgo biométrico almacenado previamente en el circuito electrónico del documento de identificación.

La lectura del rasgo biométrico de referencia puede ser realizada por medio de una interfaz de comunicación del equipo móvil de comunicaciones.

La interfaz de comunicación puede ser una interfaz basada en el contacto o una interfaz sin contacto, por ejemplo una interfaz de radiotelefonía.

La comparación del rasgo biométrico con el rasgo biométrico de referencia se realiza mediante el equipo móvil de comunicaciones, por ejemplo mediante una comparación de patrones. Si el rasgo biométrico capturado de la persona coincide con el rasgo biométrico de referencia leído, puede estar verificada la identidad de la persona.

De acuerdo con una forma de realización, en el paso de la captura se captura otra característica biométrica de la persona, y en el paso de la lectura se lee, por medio del equipo móvil de comunicaciones del circuito electrónico del documento de identificación, otro rasgo biométrico de referencia, y en el paso de la comparación, el rasgo biométrico adicional capturado se compara con el rasgo biométrico de referencia adicional. Esto tiene la ventaja de que se puede usar un rasgo biométrico adicional para verificar la identidad de la persona.

El rasgo biométrico adicional de la persona puede ser una huella dactilar de la persona, una imagen facial de la persona o una reproducción del iris de un ojo de la persona. El rasgo biométrico de referencia adicional puede ser una huella dactilar, una imagen facial o la imagen del iris de un ojo. El rasgo biométrico de referencia es un rasgo biométrico almacenado previamente en el circuito electrónico del documento de identificación.

De acuerdo con una forma de realización, la lectura del rasgo biométrico de referencia respectiva del circuito electrónico del documento de identificación se realiza utilizando la comunicación de campo cercano o la identificación por radiofrecuencia. Así se logra la ventaja de que la característica biométrica respectiva puede ser leída eficientemente.

La comunicación de campo cercano puede ser una comunicación mediante la comunicación de campo cercano (NFC, por “Near-Field-Communication”), por ejemplo según la norma ISO/IEC 14443 o ISO/IEC 18092.

La identificación por radiofrecuencia puede ser una comunicación mediante la identificación por radiofrecuencia (RFID por “Radio-Frequency-Identification”), por ejemplo según la norma ISO/CEI 14443 o ISO/CEI 18000-3.

De acuerdo con una forma de realización, el rasgo biométrico capturado respectivo es uno de los rasgos siguientes: una huella dactilar de la persona, una imagen facial de la persona o una reproducción del iris de un ojo de la persona. Así se logra la ventaja de que los rasgos biométricos que pueden ser capturados de manera eficiente pueden ser utilizados para llevar a cabo el procedimiento.

Para leer la característica biométrica de referencia, entre el equipo móvil de comunicaciones y el circuito electrónico del documento de identificación se intercambia un certificado electrónico del equipo móvil de comunicaciones del circuito electrónico del documento de identificación a fin de autorizar el equipo móvil de comunicaciones respecto del documento de identificación. Así se logra la ventaja de que los rasgos biométricos de referencia almacenados en el circuito electrónico del documento de identificación sólo se liberan si se autoriza el acceso.

El certificado electrónico del equipo móvil de comunicaciones puede ser un patrón de bits.

El certificado electrónico puede incluir una clave criptográfica.

El equipo móvil de comunicaciones se puede autorizar respecto del documento de identificación transmitiendo el certificado electrónico al circuito electrónico del documento de identificación mediante el equipo móvil de comunicaciones. El circuito electrónico del documento de identificación puede estar configurado para verificar la autenticidad del certificado electrónico.

El certificado electrónico es recuperado por medio de una red de comunicación de un servidor de certificados mediante el equipo móvil de comunicaciones. Así se logra la ventaja de que el certificado electrónico puede ser transferido eficientemente al equipo móvil de comunicaciones.

El servidor del certificado puede formar parte de una infraestructura de clave pública o de un servidor de infraestructura de clave pública (PKI, por “Public-Key-Infrastructure”).

La red de comunicación puede ser una red telefónica, una red de radiotelefonía, una red informática, por ejemplo una red de área local (LAN, por “Local Area Network”) o una red de área local inalámbrica (W-LAN, por “Wireless Local Area Network”), o Internet.

El certificado electrónico se almacena en una memoria del equipo móvil de comunicaciones y el certificado electrónico es leído de la memoria mediante el equipo móvil de comunicaciones y transmitido al circuito integrado del documento de identificación. Así se logra la ventaja de que la identidad de la persona puede verificarse sin necesidad de una conexión de comunicación con un servidor de certificados.

La memoria del equipo móvil de comunicaciones puede ser, por ejemplo, una memoria de acceso aleatorio (RAM, por “Random-Access-Memory”) del equipo móvil de comunicaciones.

La cámara de imágenes del equipo móvil de comunicaciones también se utiliza para captar datos de una zona legible por máquina del documento de identificación a fin de verificar la autenticidad del documento de identificación. Así se logra la ventaja de que la autenticidad del documento de identificación puede comprobarse mediante el equipo móvil de comunicaciones.

La zona legible por máquina puede ser un área impresa en el documento de identificación.

Los datos pueden ser en forma de una cadena de caracteres impresos dentro de una zona legible por máquina del documento de identificación. Para captar los datos de la zona legible por máquina del documento de identificación, la cámara de imágenes puede tomar una imagen de la zona legible por máquina del documento de identificación, de la que se pueden extraer los datos, por ejemplo mediante el reconocimiento de caracteres.

Los datos registrados se transmiten mediante el equipo móvil de comunicaciones a un servidor de comprobación a través de una red de comunicaciones y la autenticidad del documento de identificación se verifica por medio del servidor de comprobación, o, de acuerdo con un diseño alternativo no requerido, los datos registrados se verifican por el equipo móvil de comunicaciones mediante datos almacenados previamente en una memoria del equipo móvil de comunicaciones a fin de verificar la autenticidad del documento de identificación. Así se logra la ventaja de que la verificación de la autenticidad del documento de identificación puede ser realizada eficientemente.

El servidor de comprobación es un servidor en el que se almacenan previamente los datos para verificar la autenticidad del documento de identificación. Mediante la comparación de los datos transmitidos con los datos almacenados previamente puede comprobarse la autenticidad del documento de identificación. Si los datos transmitidos coinciden con los datos almacenados previamente, puede existir la autenticidad del documento.

Además, el equipo móvil de comunicaciones puede comprobar la autenticidad del documento de identificación comparando los datos registrados con los datos almacenados previamente. Puede existir una autenticidad del documento si los datos transmitidos coinciden con los datos almacenados previamente.

De acuerdo con una forma de realización, el equipo móvil de comunicaciones verifica el documento de identificación utilizando los datos capturados de la zona legible por máquina del documento de identificación y además determinando si integra una lista de bloqueo. Esto tiene la ventaja de que se puede reconocer un documento de identificación bloqueado.

La lista de bloqueo puede incluir una pluralidad de registros y ser almacenada en una memoria del servidor de comprobación.

El equipo móvil de comunicaciones utiliza los datos registrados de la zona legible por máquina del documento de identificación para realizar otras consultas relacionadas con la persona. Así se logra la ventaja de que se pueden proporcionar otros datos utilizables para verificar la identidad de la persona.

Las consultas posteriores relacionadas con la persona se dirigen al servidor de comprobación.

Además, las consultas relacionadas con la persona pueden incluir otros rasgos biométricos de la persona, por ejemplo la altura corporal o el peso corporal de la persona.

De acuerdo con un segundo aspecto, la invención se refiere a un equipo de comunicaciones móvil para verificar la identidad de una persona de acuerdo con la reivindicación 5. Así se logra la ventaja de que se puede poner a disposición un equipo móvil de comunicaciones para verificar la identidad de una persona.

Según una forma de realización, la interfaz de comunicación es una interfaz de comunicación de campo cercano o una interfaz de identificación por radiofrecuencia. Así se logra la ventaja de poder usar una interfaz de comunicación eficiente.

La interfaz de comunicación de campo cercano puede ser una interfaz para la comunicación a través de NFC. La interfaz de identificación por radiofrecuencia puede ser una interfaz para la comunicación a través de RFID.

De acuerdo con una forma de realización, la interfaz de comunicación está diseñada para transmitir un certificado electrónico del equipo móvil de comunicaciones al circuito electrónico del documento de identificación a fin de autorizar el equipo móvil de comunicaciones respecto del documento de identificación. Así se logra la ventaja de que los rasgos biométricos de referencia almacenados en el circuito electrónico del documento de identificación sólo se liberan si se autoriza el acceso.

De acuerdo con una forma de realización, el procesador está diseñado para comparar el rasgo biométrico capturado con el rasgo biométrico de referencia sobre la base de una comparación de patrones. Así se logra la ventaja de que el rasgo biométrico respectivo puede ser verificado eficientemente.

La comparación de patrones puede ser una comparación de las características de imagen, como esquinas, bordes, distancias relativas, posiciones y/o capas.

De acuerdo con una forma de realización, el equipo móvil de comunicaciones está configurado programáticamente para llevar a cabo el procedimiento para la verificación de la identidad de una persona. Así se logra la ventaja de que el procedimiento puede ser llevado a cabo de forma automatizada y repetible.

El equipo móvil de comunicaciones puede estar configurado para ejecutar un programa informático.

De acuerdo con una forma de realización, el equipo móvil de comunicaciones tiene un mecanismo de actualización para actualizar automáticamente los datos almacenados previamente. Así se logra la ventaja de que el equipo de comunicación puede ser aplicado eficientemente para la identificación de una persona.

El mecanismo de actualización puede ser un programa informático con un código de programa que se ejecuta en el procesador del equipo móvil de comunicaciones.

Los datos almacenados previamente pueden ser certificados electrónicos, listas de bloqueo y/o datos para verificar la autenticidad del documento de identificación.

De acuerdo con un tercer aspecto, se describe un programa informático con un código de programa para ejecutar el procedimiento de verificación de la identidad de una persona cuando el código de programa se ejecuta en un ordenador.

Así se logra la ventaja de que el procedimiento puede ser llevado a cabo de forma automatizada y repetible.

El programa informático puede incluir una secuencia de órdenes para un procesador de ordenador. El programa informático puede existir en forma de un código nativo de programa.

El ordenador puede incluir un procesador, una memoria, una interfaz de entrada y/o una interfaz de salida. El procesador del ordenador puede estar configurado para llevar a cabo el programa informático.

El programa informático puede ser ejecutado en el procesador del equipo móvil de comunicaciones.

La invención puede realizarse en hardware y/o software.

Otros ejemplos de formas de realización se explicarán con referencia a los dibujos adjuntos. Muestran:

la figura 1, un diagrama esquemático de un procedimiento para verificar la identidad de una persona mediante un documento de identificación por medio de un equipo móvil de comunicaciones;

la figura 2, un diagrama esquemático de un equipo de comunicación para verificar la identidad de una persona mediante un documento de identificación;

la figura 3, una disposición esquemática para comprobar la identidad de una persona;

la figura 4, una disposición esquemática para comprobar la identidad de una persona;

la figura 5, un diagrama esquemático de un procedimiento para verificar la identidad de una persona; y

la figura 6, un diagrama esquemático de un procedimiento para verificar la identidad de una persona.

La figura 1 muestra un diagrama esquemático de un procedimiento 100 para verificar la identidad de una persona mediante un documento de identificación por medio de un equipo móvil de comunicaciones. El documento de identificación presenta un circuito electrónico y el equipo móvil de comunicaciones presenta una cámara de imágenes.

El procedimiento 100 incluye una captura 101 de un rasgo biométrico de la persona por medio de la cámara de imágenes del equipo móvil de comunicaciones para obtener un rasgo biométrico capturado, una lectura 103 de un

rasgo biométrico de referencia del circuito electrónico del documento de identificación por medio del equipo móvil de comunicaciones, y una comparación 105 del rasgo biométrico capturado con el rasgo biométrico de referencia por medio del equipo móvil de comunicaciones para verificar la identidad de la persona.

El equipo móvil de comunicaciones puede ser un equipo manual, un teléfono móvil o un teléfono inteligente, que puede incluir una cámara de imágenes y una interfaz de comunicación.

La cámara de imágenes puede estar diseñada para tomar una imagen óptica, por ejemplo en el intervalo de longitudes de onda infrarrojo, visible y/o ultravioleta, de la persona y/o del documento de identificación. La cámara de imágenes puede incluir un sensor de imágenes, una fuente de luz, por ejemplo en el intervalo de longitudes de onda infrarrojo, visible y/o ultravioleta, para iluminar a la persona y/o el documento de identificación a capturar, y/o un objetivo de cámara.

El circuito electrónico puede ser un chip en el que se puede almacenar previamente un rasgo biométrico de referencia. El rasgo biométrico de referencia almacenado previamente en el circuito electrónico puede ser leído por medio de una interfaz de contacto o sin contacto, por ejemplo una interfaz de radiotelefonía.

La captura 101 del rasgo biométrico de la persona se puede realizar mediante el equipo móvil de comunicaciones tomando una imagen de la persona por medio de la cámara de imágenes, de la que se extrae el rasgo biométrico, por ejemplo mediante un reconocimiento de patrones por medio del equipo móvil de comunicaciones.

El rasgo biométrico de la persona puede ser una huella dactilar de la persona, una imagen facial de la persona o una reproducción del iris de un ojo de la persona. El rasgo biométrico de referencia puede ser una huella dactilar, una imagen facial o la reproducción del iris de un ojo. El rasgo biométrico de referencia es un rasgo biométrico almacenado previamente en el circuito electrónico del documento de identificación.

La lectura 103 del rasgo biométrico de referencia puede ser realizada por medio de una interfaz de comunicación del equipo móvil de comunicaciones.

La interfaz de comunicación puede ser una interfaz basada en el contacto o una interfaz sin contacto, por ejemplo una interfaz de radiotelefonía.

La comparación 105 del rasgo biométrico con el rasgo biométrico de referencia se puede realizar mediante el equipo móvil de comunicaciones, por ejemplo mediante una comparación de patrones. La identidad de la persona puede estar verificada si el rasgo biométrico capturado de la persona coincide con el rasgo biométrico de referencia leído.

El procedimiento 100 mostrado en la figura 1 para la verificación de la identidad de una persona puede llevarse a cabo mediante el equipo móvil de comunicaciones 200 mostrado en la figura 2.

La figura 2 muestra un diagrama esquemático de un equipo móvil de comunicaciones 200 para la verificación de la identidad de una persona mediante un documento de identificación, presentando el documento de identificación un circuito electrónico, con: una cámara de imágenes 201 para la captura de un rasgo biométrico de la persona por medio de la cámara de imágenes 201 del equipo móvil de comunicaciones 200 para obtener un rasgo biométrico capturado, una interfaz de comunicación 205 para la lectura de un rasgo biométrico de referencia del circuito electrónico del documento de identificación y un procesador 203 para una comparación del rasgo biométrico capturado con el rasgo biométrico de referencia por medio del equipo móvil de comunicaciones 200 para verificar la identidad de la persona.

La cámara de imágenes 201 puede estar diseñada para tomar una imagen óptica, por ejemplo en el intervalo de longitudes de onda infrarrojo, visible y/o ultravioleta, de la persona y/o del documento de identificación. La cámara de imágenes 201 puede incluir un sensor de imágenes, una fuente de luz, por ejemplo en la gama de longitudes de onda infrarroja, visible y/o ultravioleta, para iluminar a la persona y/o el documento de identificación a registrar, y/o un objetivo de cámara.

El procesador 203 puede estar configurado para la comparación del rasgo biométrico con el rasgo biométrico de referencia, por ejemplo mediante una comparación de patrón. La identidad de la persona puede estar verificada si el rasgo biométrico registrado de la persona coincide con el rasgo biométrico de referencia capturado.

La interfaz de comunicación 205 puede ser una interfaz basada en el contacto o una interfaz sin contacto, por ejemplo una interfaz de radiotelefonía.

De acuerdo con otra forma de realización, para el acceso autorizado, un dispositivo de seguridad removible o un pendrive de seguridad Universal Serial Bus (USB) puede ser, adicionalmente, conectado al equipo de comunicación 200, por ejemplo con un Trusted Platform Module (TPM).

La figura 3 muestra una disposición esquemática 300 para comprobar la identidad de una persona. La disposición 300 incluye un documento de identificación 301, el equipo móvil de comunicaciones 200, una red de comunicación 303, un servidor de certificados 305 y un servidor de comprobación 307. El equipo móvil de comunicaciones 200 está conectado al documento de identificación 301 mediante una interfaz de comunicación. Además, el equipo móvil de

comunicaciones 200 está conectado al servidor de certificados 305 y al servidor de comprobación 307 a través de la red de comunicación 303.

El documento de identificación 301 puede ser uno de los siguientes documentos de identificación: documento de identidad, como ser carné de identidad, pasaporte, tarjeta de control de acceso, tarjeta de autorización, tarjeta de identificación de la empresa, código o billete fiscal, certificado de nacimiento, permiso de conducir o documento de matrícula del vehículo, medios de pago, por ejemplo una tarjeta bancaria o una tarjeta de crédito. El documento de identificación 301 también puede incluir un circuito de lectura electrónico, por ejemplo un chip RFID. El documento de identificación 301 puede ser de una sola capa o bien de varias capas a base de papel y/o plástico. El documento de identificación 301 puede estar estructurado a partir de películas a base de plástico que se unen para formar un cuerpo de tarjetas ensamblado por medio de pegado y/o laminación, teniendo las películas, preferiblemente, propiedades materiales similares.

La red de comunicación 303 puede ser una red de telefonía, una red de radiotelefonía, una red informática, por ejemplo una red de área local (LAN) o una red de área local inalámbrica (W-LAN), o Internet.

El servidor del certificado 305 puede formar parte de una infraestructura de clave pública o de un servidor de infraestructura de clave pública (PKI).

El servidor de comprobación 307 puede ser un servidor en el que se almacenan previamente los datos para verificar la autenticidad del documento de identificación 301. Mediante la comparación de los datos transmitidos con los datos almacenados previamente puede comprobarse la autenticidad del documento de identificación 301. Si los datos transmitidos coinciden con los datos almacenados previamente, puede existir una autenticidad del documento.

La figura 4 muestra una disposición esquemática 400 para comprobar la identidad de una persona. La disposición 400 incluye un servidor de certificados 305, un servidor de comprobación 307, un servidor de radiotelefonía móvil 401, un punto de acceso de radiotelefonía móvil 403, un punto de acceso de radiotelefonía móvil 405, un equipo móvil de comunicaciones 200 y un equipo móvil de comunicaciones 407. El servidor de radiotelefonía móvil 401 está conectado al servidor de certificados 305, al servidor de comprobación 307, al punto de acceso de radiotelefonía móvil 403 y al punto de acceso de radiotelefonía móvil 405. El punto de acceso de radiotelefonía móvil 403 está conectado al equipo móvil de comunicaciones 200 y el punto de acceso de radiotelefonía móvil 405 está conectado al equipo móvil de comunicaciones 407

El servidor de radiotelefonía móvil 401 puede ser una estación de base de una red de radiotelefonía móvil

Los puntos de acceso de radiotelefonía móvil 403 y 405 pueden ser puntos de acceso a una red de radiotelefonía móvil, por ejemplo antenas conectadas a una estación de base.

El equipo móvil de comunicaciones 407 puede ser otro equipo móvil de comunicaciones configurado para llevar a cabo el procedimiento de verificación de la identidad de una persona.

La figura 5 muestra un diagrama esquemático de un procedimiento 500 para verificar la identidad de una persona 501. Además, se ilustra una persona 501, un verificador 503, un documento de identificación 301 y un equipo móvil de comunicaciones 200. El procedimiento 500 incluye los pasos de procedimiento 505 a 519 que se describen a continuación.

La persona 501 puede ser una persona cuya identidad se verifica mediante el uso del procedimiento 500, por ejemplo un ciudadano.

El verificador 503 puede ser una persona que opera el equipo móvil de comunicaciones 200, por ejemplo un oficial de policía.

Además, el equipo móvil de comunicaciones 200 también puede ser un sistema de comprobación móvil.

El paso del procedimiento 505 incluye la expresión válida de la identidad de la persona 501 por el verificador 503.

El paso de procedimiento 507 incluye la entrega del documento de identificación 301 o de un documento de identificación de la persona 501 al verificador 503.

El paso del procedimiento 509 incluye el inicio de la verificación o comprobación.

El paso de procedimiento 511 incluye una captura o registro de las huellas dactilares de la persona 501 por medio del equipo móvil de comunicaciones 200 mediante, por ejemplo, una cámara de imágenes del equipo móvil de comunicaciones 200.

El paso de procedimiento 513 incluye la captura o registro de la imagen facial de la persona 501 por medio del equipo móvil de comunicaciones 200 mediante, por ejemplo, una cámara de imágenes del equipo móvil de comunicaciones 200.

El paso de procedimiento 515 incluye la captura o registro de la reproducción del iris de un ojo de la persona 501 o del iris de la persona 501 por medio del equipo móvil de comunicaciones 200 mediante, por ejemplo, una cámara de imágenes del equipo móvil de comunicaciones 200.

El paso de procedimiento 517 incluye una entrega al verificador 503 del resultado de la comprobación por medio del equipo móvil de comunicaciones 200.

El resultado de la auditoría puede ser el resultado de una comparación de los rasgos biométricos capturados de la persona, como una huella dactilar, una imagen facial y/o una reproducción del iris de un ojo de la persona, con los rasgos biométricos almacenados previamente en el documento de identificación 301.

El paso de procedimiento 519 incluye la devolución del documento de identificación 301 o del documento de identificación del verificador 501 a la persona 503.

La figura 6 muestra un diagrama esquemático de un procedimiento 600 para verificar la identidad de una persona. El procedimiento 600 incluye los pasos de procedimiento 601 a 627.

El paso de procedimiento 601 incluye el registro de la cara de datos de un documento de identificación o del documento de identificación. Por ejemplo, una imagen de una zona legible por máquina del documento de identificación se capta por medio de una cámara de imágenes.

El paso de procedimiento 603 incluye una captura de una zona legible por máquina o una Machine-Readable-Zone (MRZ). Por ejemplo, los datos se extraen de la imagen capturada de la zona legible por máquina del documento de identificación mediante un equipo móvil de comunicaciones.

El paso de procedimiento 605 incluye una carga de un certificado o un certificado de autorización de un servidor de certificados o de un servidor PKI. Por ejemplo, un equipo móvil de comunicaciones carga un certificado de un servidor de certificados.

El paso de procedimiento 607 incluye un envío del registro de la cara de datos del documento de identificación o documento ID o el envío del registro del documento a un servidor de comprobación. Por ejemplo, un equipo móvil de comunicaciones transmite al servidor de comprobación una imagen de una zona legible por máquina del documento de identificación.

El paso de procedimiento 609 incluye una lectura de los rasgos biométricos de referencia o datos de referencia del circuito electrónico del documento de identificación a través de una interfaz de comunicación o una lectura de los datos del chip a través de NFC.

Por ejemplo, un equipo móvil de comunicaciones lee a través de una interfaz de comunicación los rasgos biométricos de referencia de un circuito electrónico del documento de identificación.

El paso de procedimiento 611 incluye una captura o un registro de las huellas dactilares con una cámara de imágenes o con una cámara incorporada. Por ejemplo, una cámara de imágenes capta una imagen de uno o más dedos de la persona.

El paso de procedimiento 613 incluye comparar o una comparación de las huellas dactilares. Por ejemplo, un equipo móvil de comunicaciones realiza una comparación de patrones de las huellas dactilares captadas de la persona con huellas dactilares almacenadas previamente.

El paso de procedimiento 615 incluye una captura o un registro de una o la imagen facial mediante la cámara de imágenes o mediante una cámara incorporada. Por ejemplo, una imagen facial de la persona se toma con una cámara de imágenes.

El paso de procedimiento 617 incluye comparar la imagen facial o una comparación de imagen facial. Por ejemplo, un equipo móvil de comunicaciones realiza una comparación de patrones de la imagen facial captada de la persona con una imagen facial almacenada previamente.

El paso de procedimiento 619 incluye capturar una reproducción de un iris de un ojo o captura del iris mediante la cámara de imágenes o mediante una cámara incorporada. Por ejemplo, la imagen del iris de un ojo de la persona se toma con una cámara de imágenes.

El paso de procedimiento 621 incluye una comparación de la reproducción del iris o una comparación de la imagen facial. Por ejemplo, un equipo móvil de comunicaciones realiza una comparación de patrones de la reproducción del iris captada con una reproducción de iris almacenada previamente.

El paso de procedimiento 623 incluye la transmisión de los resultados de la comprobación del documento mediante un servidor de comprobación o un servidor externo.

El paso de procedimiento 625 incluye una compilado o una recopilación del resultado de la auditoría. El resultado de la auditoría puede ser el resultado de las comparaciones realizadas previamente.

El paso de procedimiento 627 incluye la visualización del resultado de la auditoría o un resultado de la auditoría, por ejemplo mediante un dispositivo de visualización del equipo móvil de comunicaciones.

De acuerdo con otra forma de realización, la verificación de la identidad de una persona a partir de documentos de identidad fuera de las estaciones de comprobación instaladas de forma permanente sólo puede llevarse a cabo con equipos especiales caros y a menudo pesados.

De acuerdo con otra forma de realización, el procedimiento de verificación de la identidad de una persona puede evitar el alto costo de los equipos y las desventajas causadas por su diseño, como el peso, el tamaño y el suministro de energía.

De acuerdo con otra forma de realización, el procedimiento para la verificación de la identidad móvil se basa en el uso de un equipo móvil de comunicaciones o terminal, preferentemente un teléfono inteligente de bajo costo para usuarios privados o consumidores con función de comunicación de campo cercano o con funcionalidad NFC.

De acuerdo con otra forma de realización, el equipo móvil de comunicaciones, que puede ser un teléfono inteligente, se utiliza para captar la imagen facial o la imagen facial, así como las huellas dactilares de la persona que se va a identificar. Con la ayuda de un lector interno o externo de comunicación de campo cercano o de lectura de identificación por radiofrecuencia o un lector NFC/RFID, se lee o abre el documento de identificación o la cédula de identidad y se realiza una comprobación biométrica de las imágenes registradas respecto de las imágenes almacenadas. En la zona soberana también se pueden realizar otras consultas referidas a la persona y se pueden cargar los certificados electrónicos y/o no electrónicos necesarios para leer el documento de identificación o el carné de identidad.

De acuerdo con otra forma de realización, el procedimiento para la verificación de la identidad de una persona puede llevarse a cabo con la ayuda de un programa informático o una aplicación de software que se ejecute o funcione en el sistema operativo del equipo móvil de comunicaciones o del dispositivo móvil. Por medio de un sistema de actualización integrado o un mecanismo de actualización se puede mantener actualizado o al día el programa informático o la aplicación.

De acuerdo con otra forma de realización, los certificados electrónicos y/o no electrónicos y, cuando proceda, las listas de bloqueo podrán almacenarse o protegerse en una memoria del equipo móvil de comunicaciones o localmente con el fin de ejecutar el procedimiento para la verificación de la identidad de una persona o de operar fuera de una infraestructura de telecomunicaciones accesible.

Por ejemplo, el certificado incluye un patrón de bits y/o una clave criptográfica. El equipo móvil de comunicaciones se puede autorizar frente al documento de identificación, transmitiendo el equipo móvil de comunicaciones el certificado al circuito electrónico del documento de identificación. El circuito electrónico del documento de identificación puede estar configurado para verificar la autenticidad del certificado electrónico.

De acuerdo con otra forma de realización, para realizar el procedimiento pueden utilizarse dispositivos multifuncionales de verificación de la identidad. Debido a la alta aceptación del hardware, la verificación de la identidad puede llevarse a cabo en la calle, en la zona fronteriza o fuera de las estaciones de comprobación estacionarias existentes.

De acuerdo con otra forma de realización, para utilizar el procedimiento para la verificación de la identidad de una persona se puede conectar al equipo móvil de comunicaciones un dispositivo de seguridad extraíble.

De acuerdo con otra forma de realización, el equipo móvil de comunicaciones puede generar un informe de auditoría y mostrar un resultado de la misma.

Lista de referencias:

100 procedimiento para la verificación de la identidad de una persona.

101 captura de un rasgo biométrico de la persona

103 lectura de un rasgo biométrico de referencia

105 comparación del rasgo biométrico capturado con el rasgo biométrico de referencia

200 equipo móvil de comunicaciones

201 cámara de imágenes

203 procesador

205 interfaz de comunicación

300 disposición para la verificación de la identidad de una persona.

301 documento de identificación

303 red de comunicaciones

305 servidor de certificados

307 servidor de comprobación

400 disposición para la verificación de la identidad de una persona.

401 servidor de radiotelefonía móvil

403 punto de acceso de radiotelefonía móvil

405 punto de acceso de radiotelefonía móvil

407 equipo móvil de comunicaciones

500 procedimiento para la verificación de la identidad de una persona.

501 persona

503 verificador

505-519 pasos del procedimiento

600 procedimiento para la verificación de la identidad de una persona.

601-627 pasos del procedimiento

REIVINDICACIONES

1. Procedimiento (100) para verificar la identidad de una persona mediante un documento de identificación (301) por medio de un equipo móvil de comunicaciones (200), presentando el documento de identificación (301) un circuito electrónico, presentando el equipo móvil de comunicaciones (200) una cámara de imágenes (201) y presentando el procedimiento (100) los pasos siguientes:

captura (101) de un rasgo biométrico de la persona por medio de la cámara de imágenes (201) del equipo móvil de comunicaciones (200) para obtener un rasgo biométrico capturado;

lectura (103) de un rasgo biométrico de referencia del circuito electrónico del documento de identificación (301) por medio del equipo móvil de comunicaciones (200), y

comparación (105) del rasgo biométrico capturado con el rasgo biométrico de referencia por medio del equipo móvil de comunicaciones (200) para verificar la identidad de la persona,

en donde para la lectura (103) de la característica biométrica de referencia, entre el equipo móvil de comunicaciones (200) y el circuito electrónico del documento de identificación (301) se intercambia un certificado electrónico del equipo móvil de comunicaciones (200) desde el circuito electrónico del documento de identificación (301) a fin de autorizar el equipo móvil de comunicaciones (200) respecto del documento de identificación (301), en donde mediante el equipo móvil de comunicaciones (200), el certificado electrónico es recuperado de un servidor de certificados (305) a través de una red de comunicaciones (303),

estando el certificado electrónico almacenado en una memoria del equipo móvil de comunicaciones (200) y siendo el certificado electrónico leído de la memoria mediante el equipo móvil de comunicaciones (200) y transmitido al circuito electrónico del documento de identificación (301),

siendo la cámara de imágenes (201) del equipo móvil de comunicaciones (200) utilizado también para captar datos de una zona legible por máquina del documento de identificación (301) a fin de verificar la autenticidad del documento de identificación (301),

siendo los datos capturados transmitidos por medio del equipo móvil de comunicaciones (200) a un servidor de comprobación (307) a través de una red de comunicaciones (303), y siendo comprobada la autenticidad del documento de identificación (301) por medio del servidor de comprobación (307),

siendo el servidor de comprobación un servidor en el que se almacenan previamente los datos para verificar la autenticidad del documento de identificación, comprobando el servidor de comprobación la existencia de la autenticidad del documento de identificación mediante la comparación de los datos transmitidos con los datos almacenado previamente, en donde, al coincidir los datos transmitidos con los datos almacenados previamente, existe la autenticidad del documento de identificación.

realizando el equipo móvil de comunicaciones también otras consultas relacionadas con la persona, utilizando los datos capturados de la zona legible por máquina del documento de identificación (301) para, por lo tanto, proporcionar otros datos utilizables para verificar la identidad de la persona, siendo las demás consultas referidas a la persona dirigidas al servidor de comprobación (307).

2. Procedimiento (100) de acuerdo con la reivindación 1, en donde en el paso de la captura (101) se captura otro rasgo biométrico de la persona, y en donde en el paso de la lectura (103) se lee, por medio del equipo de comunicaciones móvil (200) del circuito electrónico del documento de identificación (301), otro rasgo biométrico de referencia, y en donde en el paso de la comparación (105), el rasgo biométrico adicional capturado se compara con el rasgo biométrico de referencia adicional.

3. Procedimiento (100) de acuerdo con las reivindicaciones 1 o 2, en donde la lectura de la característica biométrica de referencia respectiva del circuito electrónico del documento de identificación (301) se realiza utilizando la comunicación de campo cercano o la identificación por radiofrecuencia.

4. Procedimiento (100) de acuerdo con una de las reivindicaciones precedentes, en donde el rasgo biométrico capturado respectivo es uno de los rasgos siguientes:

una huella digital de la persona;

una imagen facial de la persona; o

una reproducción del iris de la persona.

una reproducción del iris de la persona.

5. Equipo móvil de comunicaciones (200) para la verificación de la identidad de una persona mediante un documento de identificación (301), presentando el documento de identificación (301) un circuito electrónico, con:

una cámara de imágenes (201) para la captura (101) de un rasgo biométrico de la persona por medio de la cámara de imágenes (201) del equipo móvil de comunicaciones (200) para obtener un rasgo biométrico capturado;

una interfaz de comunicación (205) para la lectura (103) de un rasgo biométrico de referencia del circuito electrónico del documento de identificación por medio del documento de identificación (301), y

un procesador (203) para la comparación (105) del rasgo biométrico capturado con el rasgo biométrico de referencia por medio del equipo móvil de comunicaciones (200) para verificar la identidad de la persona,

estando la interfaz de comunicación (205) diseñada para transmitir un certificado electrónico del equipo móvil de comunicaciones (200) al circuito electrónico del documento de identificación (301) a fin de autorizar el equipo móvil de comunicaciones (200) respecto del documento de identificación (301), estando el equipo móvil de comunicaciones (200) equipado para recuperar el certificado electrónico de un servidor de certificados a través de una red de comunicaciones,

estando el certificado electrónico almacenado en una memoria del equipo móvil de comunicaciones (200) y siendo el certificado electrónico leído de la memoria mediante el equipo móvil de comunicaciones (200) y transmitido al circuito electrónico del documento de identificación (301),

siendo la cámara de imágenes (201) del equipo móvil de comunicaciones (200) utilizado también para captar datos de una zona legible por máquina del documento de identificación (301) a fin de verificar la autenticidad del documento de identificación (301),

siendo los datos capturados transmitidos por medio del equipo móvil de comunicaciones (200) a un servidor de comprobación (307) a través de una red de comunicaciones (303), y siendo comprobada la autenticidad del documento de identificación (301) por medio del servidor de comprobación (307),

siendo el servidor de comprobación un servidor en el que se almacenan previamente los datos para verificar la autenticidad del documento de identificación, comprobando el servidor de comprobación la existencia de la autenticidad del documento de identificación mediante la comparación de los datos transmitidos con los datos almacenado previamente, en donde, al coincidir los datos transmitidos con los datos almacenados previamente, existe la autenticidad del documento de identificación.

realizando el equipo móvil de comunicaciones también otras consultas relacionadas con la persona, utilizando los datos capturados de la zona legible por máquina del documento de identificación (301) para, por lo tanto, proporcionar otros datos utilizables para verificar la identidad de la persona, siendo las demás consultas referidas a la persona dirigidas al servidor de comprobación (307).

6. Equipo móvil de comunicaciones (200) de acuerdo con la reivindicación 5, siendo la interfaz de comunicaciones (205) una interfaz de comunicación de campo cercano o una interfaz de identificación por radiofrecuencia.

7. Equipo móvil de comunicaciones (200) de acuerdo con las reivindicaciones 5 o 6, siendo el procesador (203) diseñado para comparar el rasgo biométrico capturado con el rasgo biométrico de referencia sobre la base de una comparación de patrones.

8. Equipo móvil de comunicaciones (200) de acuerdo con una de las reivindicaciones 5 a 7, configurado programáticamente para llevar a cabo el procedimiento (100) para la verificación de la identidad de una persona de acuerdo con una de las reivindicaciones 1 a 4.

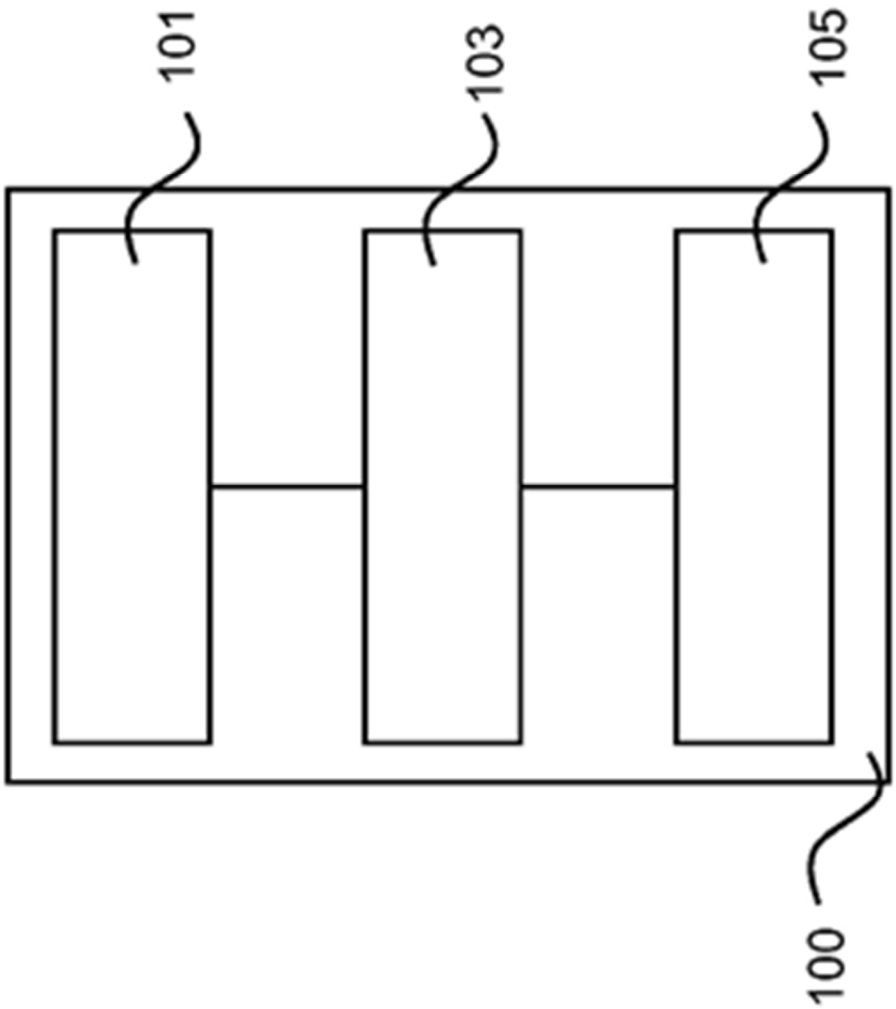

Fig. 1

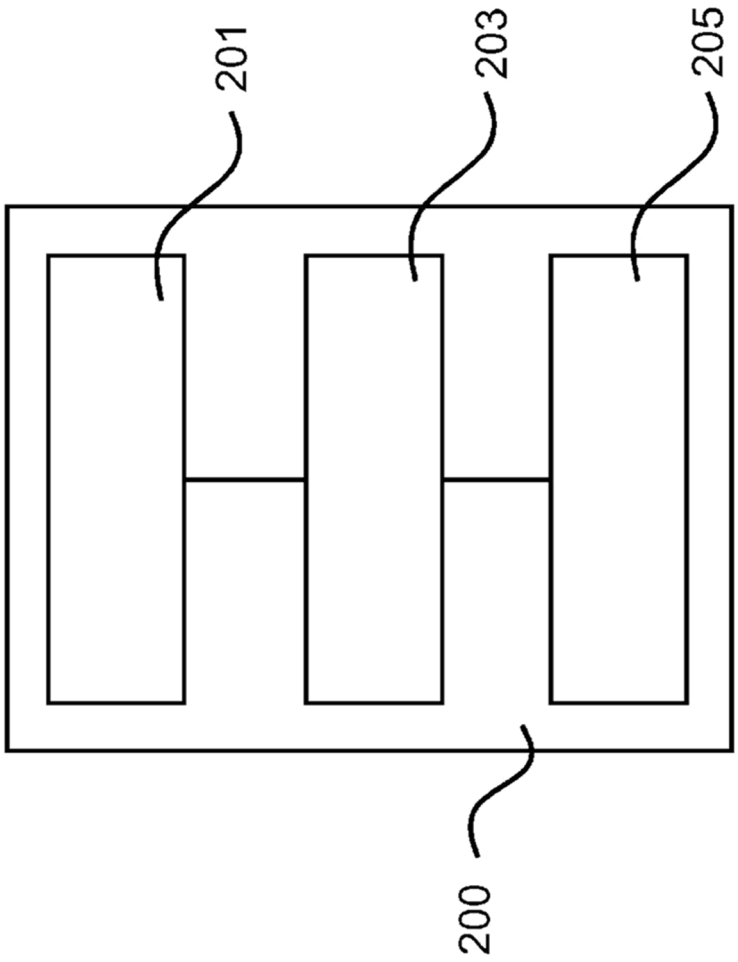

Fig. 2

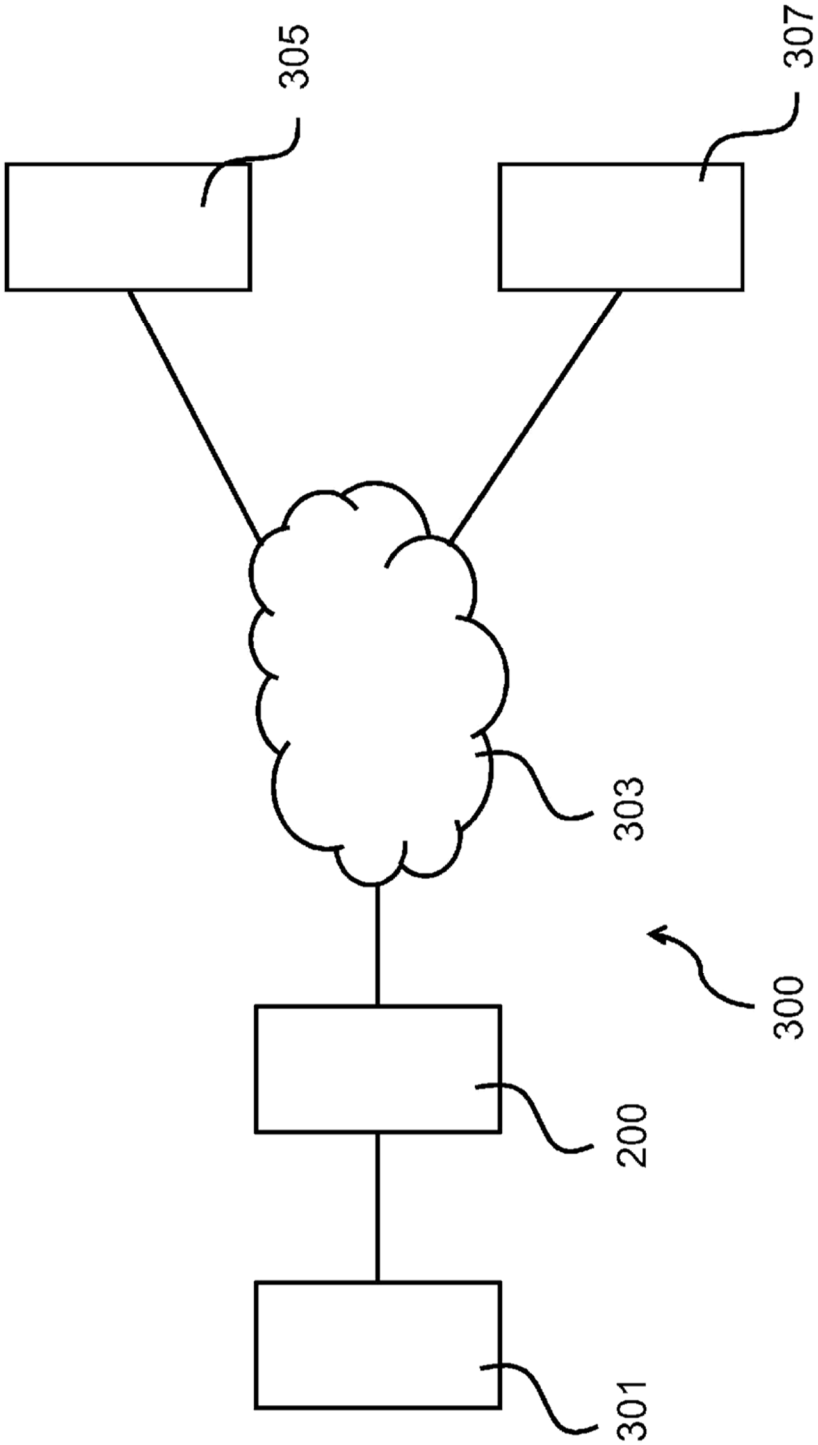

Fig. 3

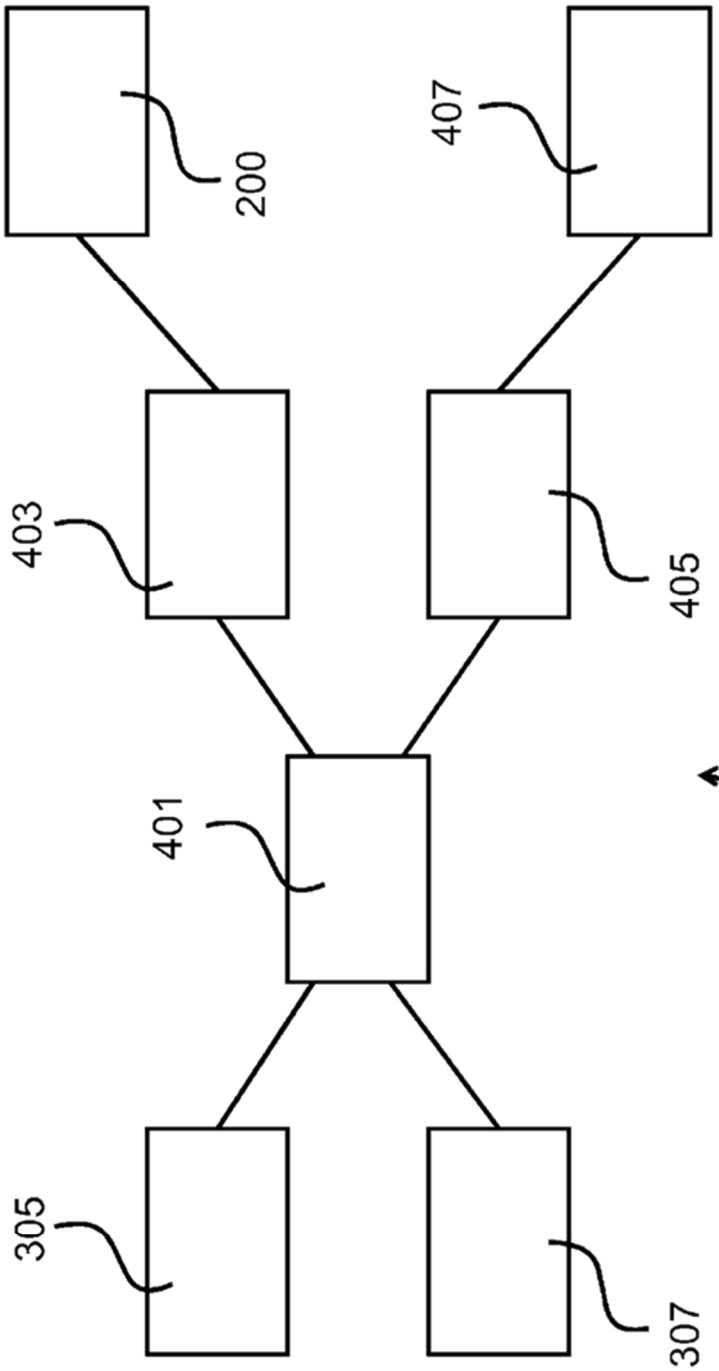

Fig. 4

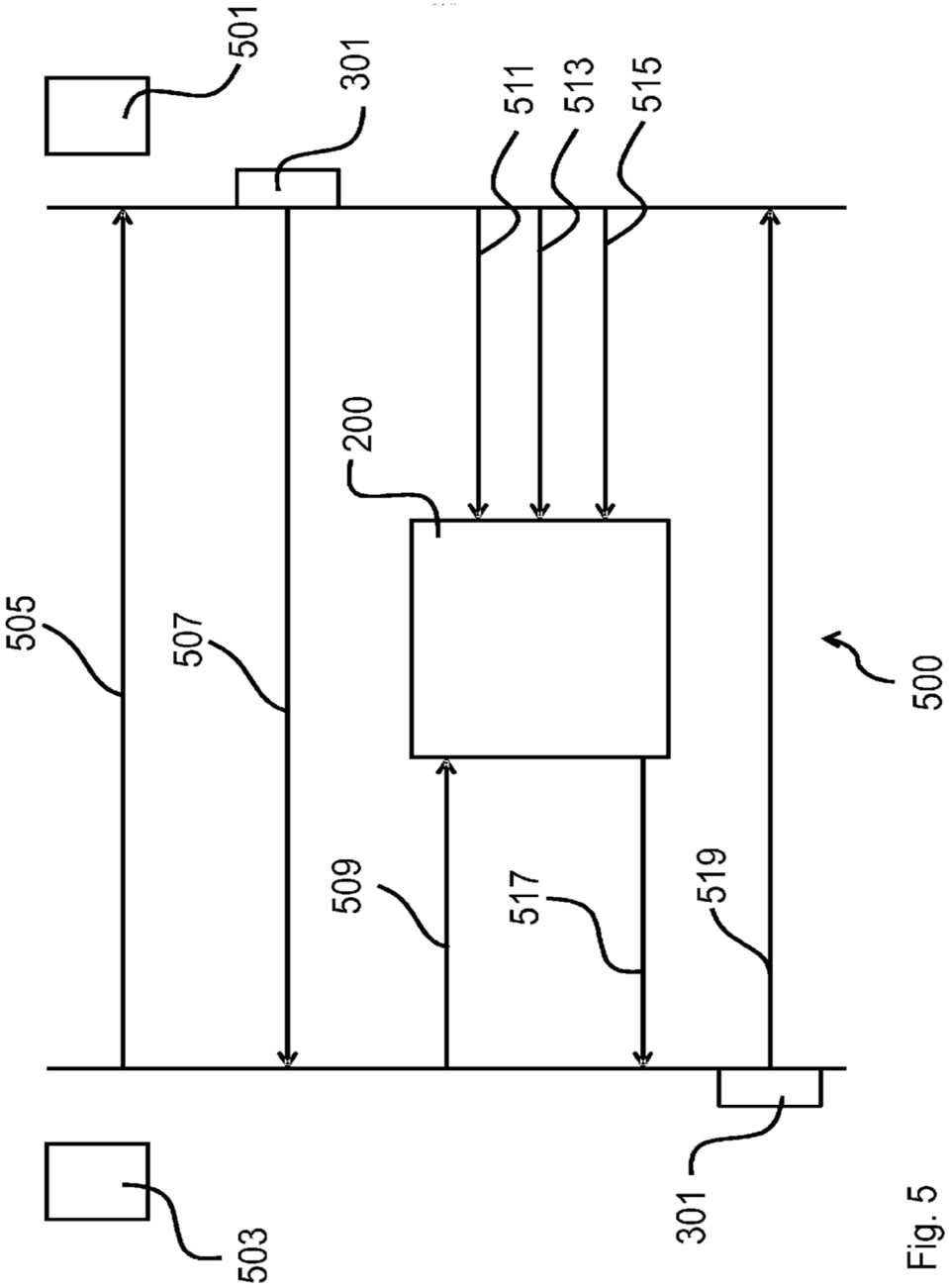

Fig. 5

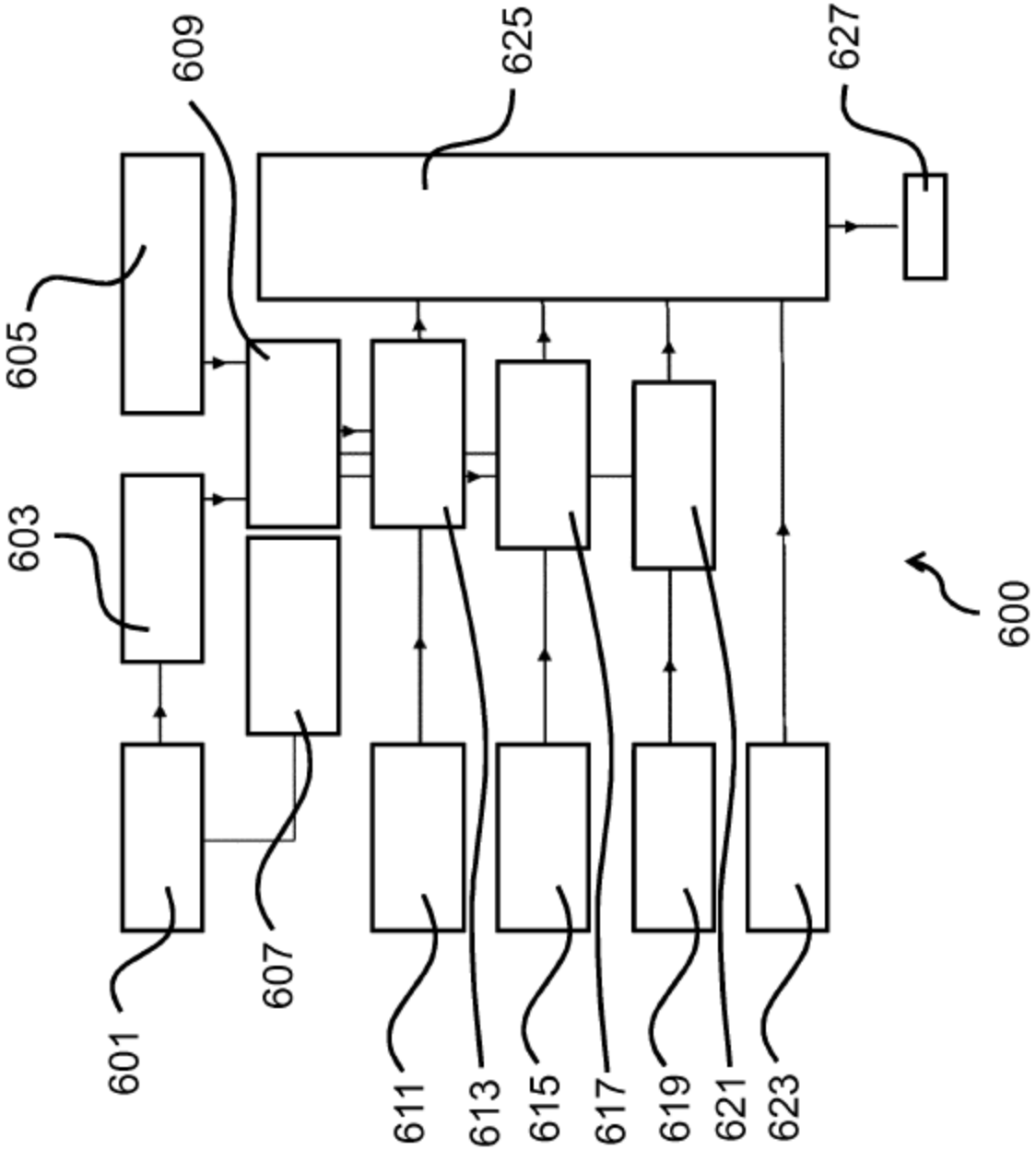

Fig. 6