

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 627 630**

51 Int. Cl.:

B60R 25/20 (2013.01)

B60R 25/24 (2013.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **02.12.2014** **E 14195885 (0)**

97 Fecha y número de publicación de la concesión europea: **10.05.2017** **EP 2881289**

54 Título: **Procedimiento para el desbloqueo de una instalación de bloqueo de vehículo**

30 Prioridad:

06.12.2013 DE 102013113667

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

28.07.2017

73 Titular/es:

**BUNDESDRUCKEREI GMBH (100.0%)
Oranienstraße 91
10958 Berlin, DE**

72 Inventor/es:

**SCHRÖDER, MARTIN;
MORGNER, FRANK y
DIETRICH, FRANK**

74 Agente/Representante:

ELZABURU, S.L.P

ES 2 627 630 T3

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

Procedimiento para el desbloqueo de una instalación de bloqueo de vehículo

La invención se refiere al campo del desbloqueo de instalaciones de bloqueo de vehículo.

5 La publicación para información de solicitud de patente DE 10 2012 009 019 A1 muestra un procedimiento para el funcionamiento de un vehículo, así como un dispositivo de funcionamiento correspondiente y un vehículo.

Las instalaciones de bloqueo de vehículo se usan para permitir un acceso a un vehículo a un círculo de personas limitado y predefinido.

10 Las instalaciones de bloqueo de vehículo se desbloquean la mayoría de las veces mediante una llave de vehículo que se introduce en una cerradura del vehículo. Debido a sus dimensiones geométricas, las llaves de vehículo se consideran con frecuencia como incómodas y difíciles de manejar.

Para el desbloqueo de las instalaciones de bloqueo de vehículo se usan además tarjetas inteligentes o las etiquetas de comunicación de campo cercano (Near-Field-Communication, NFC). A este respecto, éstas están diseñadas para instalaciones de bloqueo de vehículo especiales y se producen y configuran por separado para ello.

15 Por ello el objetivo de la presente invención es crear un concepto cómodo y flexible para el desbloqueo de una instalación de bloqueo de vehículo.

Este objetivo se consigue mediante las características de la reivindicación independiente. Formas de perfeccionamiento ventajosas son objeto de las reivindicaciones dependientes, de la descripción así como de los dibujos.

20 La invención se basa en el conocimiento de que el objetivo arriba mencionado se puede conseguir mediante un uso de un documento de identificación legible electrónicamente.

25 Según un primer aspecto, la invención se refiere a un procedimiento para el desbloqueo de una instalación de bloqueo de vehículo de un vehículo usando un documento de identificación legible electrónicamente, presentando el documento de identificación legible electrónicamente una característica de identificación ópticamente detectable, con detección óptica de la característica de identificación ópticamente detectable del documento de identificación legible electrónicamente, establecimiento de una primera conexión de comunicación entre el documento de identificación legible electrónicamente y la instalación de bloqueo de vehículo en base a la característica de identificación ópticamente detectada, establecimiento de una segunda conexión de comunicación entre la instalación de bloqueo de vehículo y un servidor de identificación, lectura de una identificación electrónica del documento de identificación por el servidor de identificación a través de la primera conexión de comunicación y la segunda conexión de comunicación y desbloqueo de la instalación de bloqueo de vehículo en el caso de concordancia entre la identificación electrónica leída y una identificación electrónica prealmacenada. De este modo se consigue la ventaja de que se puede implementar un concepto cómodo y flexible para el desbloqueo de una instalación de boqueo de vehículo.

35 La instalación de bloqueo de vehículo puede permitir o negar un acceso al vehículo. La instalación de bloqueo de vehículo puede ser, por ejemplo, una instalación de bloqueo de una puerta de vehículo. El vehículo puede ser, por ejemplo, un automóvil o un camión.

40 El documento de identificación legible electrónicamente puede ser uno de los documentos de identificación siguientes: documento de identidad, como carné de identidad, pasaporte, carné de control de accesos, credencial, carné de empresa, marca de control o tique, certificado de nacimiento, carné de conducir o documentación del vehículo, medio de pago, por ejemplo una tarjeta bancaria o tarjeta de crédito. El documento de identificación puede comprender además un circuito legible electrónicamente, por ejemplo un chip RFID. El documento de identificación puede ser monocapa o multicapa o a base de papel y/o plástico. El documento de identificación puede estar construido de láminas a base de plástico, que se ensamblan formando un cuerpo de tarjeta mediante pegado y/o laminado, presentando las láminas preferiblemente propiedades materiales similares.

45 La característica de identificación ópticamente detectable puede estar formada por una serie de letras, cifras y/o símbolos. La característica de identificación ópticamente detectable puede estar representada además en forma de un código de barras, un código bidimensional, por ejemplo, un código de respuesta rápida (Quick-Response, QR) o un holograma.

50 La identificación electrónica puede estar formada por una serie de letras, cifras, bytes y/o símbolos. La identificación electrónica puede comprender un dato personal sobre una persona, por ejemplo un nombre, y/o una característica electrónica del documento de identificación, por ejemplo un número de serie. La identificación electrónica se puede generar y/o almacenar además por el documento de identificación.

La identificación electrónica prealmacenada puede estar depositada, por ejemplo, en una memoria o una base de datos.

El servidor de identificación puede estar configurado para leer la identificación electrónica del documento de identificación. El servidor de identificación puede estar configurado para verificar la autenticidad u originalidad del documento de identificación.

5 La primera conexión de comunicación puede ser por cable o inalámbrica. La primera conexión de comunicación se puede autenticar y/o establecer de forma encriptada.

La segunda conexión de comunicación puede ser por cable o inalámbrica. La segunda conexión de comunicación se puede autenticar y/o establecer de forma encriptada. La segunda conexión de comunicación se puede establecer además a través de una red de comunicación, por ejemplo internet.

10 La detección óptica de la característica de identificación ópticamente detectable se puede llevar a cabo en base a un reconocimiento de patrones.

El establecimiento de la primera conexión de comunicación entre el documento de identificación legible electrónicamente y de la instalación de bloqueo de vehículo puede comprender una transmisión de claves criptográficas y/o certificados criptográficos. Las claves criptográficas y/o certificados criptográficos se pueden generar en base a la característica de identificación ópticamente detectada.

15 El establecimiento de la segunda conexión de comunicación entre la instalación de bloqueo de vehículo y el servidor de identificación puede comprender una transmisión de claves criptográficas y/o certificados criptográficos.

20 La lectura de la identificación electrónica del documento de identificación por el servidor de identificación a través de la primera conexión de comunicación y la segunda conexión de comunicación puede comprender una transmisión de claves criptográficas y/o certificados criptográficos entre el documento de identificación y el servidor de identificación. Además, la lectura de la identificación electrónica puede comprender una verificación de la autenticidad u originalidad del documento de identificación y/o de la identificación electrónica.

25 El desbloqueo de la instalación de bloqueo de vehículo se puede llevar a cabo en caso de concordancia entre la identificación electrónica leída y la identificación electrónica prealmacenada. Una concordancia entre la identificación electrónica leída y la identificación electrónica prealmacenada puede existir cuando son idénticas la identificación electrónica leída y la identificación electrónica prealmacenada. El desbloqueo de la instalación de bloqueo de vehículo se puede llevar a cabo además en respuesta a una recepción de una señal de autenticación a través de la instalación de bloqueo de vehículo.

30 Según una forma de realización, la instalación de bloqueo de vehículo no se desbloquea en el caso de falta de concordancia entre la identificación electrónica leída y la identificación electrónica prealmacenada. De este modo se consigue la ventaja de que la instalación de bloqueo de vehículo no se desbloquea en el caso de falta de concordancia entre la identificación electrónica leída y la identificación electrónica prealmacenada.

35 Según una forma de realización, para la detección óptica de la característica de identificación ópticamente detectable se toma una imagen óptica de la característica de identificación ópticamente detectable mediante una cámara de imágenes. De este modo se consigue la ventaja de que las propiedades ópticas de la característica de identificación ópticamente detectable se pueden detectar y procesar de forma eficiente.

La imagen óptica se puede tomar en el rango de longitud de onda visible. La imagen óptica puede ser una imagen en blanco y negro, una imagen en escala de grises o una imagen a color.

La cámara de imágenes puede estar configurada para tomar la imagen óptica en el rango de longitud de onda visible. La cámara de imágenes puede comprender un sensor de imagen y/o un objetivo de cámara.

40 Según una forma de realización, la detección de la característica de identificación ópticamente detectable comprende una extracción de la característica de identificación de una imagen óptica del documento de identificación. De este modo se consigue la ventaja de que la característica de identificación ópticamente detectable puede estar dispuesta en diferentes zonas de la imagen óptica.

45 La extracción de la característica de identificación puede comprender una exención, rectificación, giro y/o escalado de la característica de identificación. La extracción de la característica de identificación puede comprender un reconocimiento de texto o un reconocimiento óptico de caracteres (Optical Character Recognition, OCR). La extracción de la característica de identificación puede comprender además una decodificación de un código de barras, un código bidimensional, por ejemplo, un código de respuesta rápida (Quick-Response, QR) o un holograma.

50 Según una forma de realización, el establecimiento de la primera conexión de comunicación entre el documento de identificación legible electrónicamente y la instalación de bloqueo de vehículo se lleva a cabo mediante un protocolo de establecimiento de conexión autenticado por contraseña. De este modo se consigue la ventaja de que se puede establecer una conexión de comunicación autenticada y/o encriptada.

El protocolo de establecimiento de conexión autenticado por contraseña puede comprender una transmisión de claves criptográficas y/o certificados criptográficos. Las claves criptográficas y/o certificados criptográficos se pueden

generar en base a la característica de identificación ópticamente detectada. El protocolo de establecimiento de conexión autenticada por contraseña se puede basar además en un intercambio de claves Diffie-Hellmann. La característica de identificación ópticamente detectada se puede usar como contraseña para el protocolo de establecimiento de conexión autenticada por contraseña.

- 5 Según una forma de realización, el protocolo de establecimiento de conexión autenticada por contraseña es un protocolo de establecimiento de conexión autenticada por contraseña (Password Authenticated Connection Establishment Protokol). De este modo se consigue la ventaja de que se puede usar un protocolo de establecimiento de conexión autenticada por contraseña estandarizado.

- 10 El protocolo de establecimiento de conexión autenticada por contraseña (Password Authenticated Connection Establishment, PACE) se puede implementar, por ejemplo, según la directiva técnica BSI TR-03110.

Según una forma de realización, el establecimiento de la segunda conexión de comunicación entre la instalación de bloqueo de vehículo y el servidor de identificación se lleva a cabo mediante un protocolo de seguridad de la capa de transporte. De este modo se consigue la ventaja de que se puede establecer una conexión de comunicación autenticada y/o encriptada.

- 15 El protocolo de seguridad de la capa de transporte puede comprender una transmisión de claves criptográficas y/o certificados criptográficos. El protocolo de seguridad de la capa de transporte se puede basar además en un intercambio de claves Diffie-Hellmann. El protocolo de seguridad de la capa de transporte puede ser, por ejemplo, un protocolo de Transport Layer Security (TLS)

- 20 Según una forma de realización, el documento de identificación legible electrónicamente comprende un circuito integrado y la lectura de la identificación electrónica del documento de identificación comprende una realización de un procedimiento de autenticación de chip para la autenticación del circuito integrado del documento de identificación. De este modo se obtiene la ventaja de que se puede verificar la autenticidad u originalidad del circuito integrado del documento de identificación.

- 25 El circuito integrado puede ser legible electrónicamente. El circuito integrado puede ser, por ejemplo, un chip de identificación por radiofrecuencia (Radio Frequency Identification, RFID).

El procedimiento de autenticación de chip puede comprender una transmisión de claves criptográficas y/o certificados criptográficos. El procedimiento de autenticación de chip puede estar configurado para verificar la autenticidad y originalidad del circuito integrado. El procedimiento de autenticación de chip puede ser, por ejemplo, un procedimiento de Chip Authentication (CA) e implementarse según la directiva técnica BSI TR-03110.

- 30 Según una forma de realización, la primera conexión de comunicación con el documento de identificación legible electrónicamente se establece a través de un terminal para una comunicación con el documento de identificación legible electrónicamente, y la lectura de la identificación electrónica del documento comprende una realización de un procedimiento de autenticación de terminal para la autenticación del terminal o del servidor de identificación. De este modo se obtiene la ventaja de que se puede verificar la autenticidad u originalidad del terminal o del servidor de identificación.
- 35

El terminal puede ser un lector para una comunicación con el documento de identificación legible electrónicamente.

- 40 El procedimiento de autenticación de terminal puede comprender una transmisión de claves criptográficas y/o certificados criptográficos. El procedimiento de autenticación de terminal puede estar configurado para verificar la autenticidad u originalidad del terminal o del servidor de autenticación. El procedimiento de autenticación de terminal puede ser, por ejemplo, un procedimiento de Terminal Authentication (TA) e implementarse según la directiva técnica BSI TR-03110.

Según una forma de realización, el desbloqueo de la instalación de bloqueo de vehículo comprende un envío de una señal de autenticación a la instalación de bloqueo de vehículo. De este modo se consigue la ventaja de que el desbloqueo de la instalación de bloqueo de vehículo se puede iniciar por una señal externa.

- 45 La señal de autenticación puede estar formada por un mensaje electrónico, una orden, un comando y/o un proceso. La señal de autenticación se puede generar y enviar por el servidor de identificación.

- 50 Según una forma de realización, el procedimiento comprende además una transmisión de una clave criptográfica pública por el servidor de identificación al documento de identificación, una generación de una identificación electrónica mediante una vinculación de una clave criptográfica privada del documento de identificación y de la clave criptográfica pública transmitida por el documento de identificación, y un almacenamiento de la identificación electrónica generada, a fin de obtener la identificación electrónica prealmacenada. De este modo se consigue la ventaja de que se puede proporcionar una identificación electrónica prealmacenada, que está asociada al documento de identificación.

La clave criptográfica pública puede ser parte de un par de claves criptográficas y haberse generado según la

infraestructura de clave pública (Public-Key).

La clave criptográfica privada del documento de identificación puede ser parte de un par de claves criptográficas y haberse generado según la infraestructura de clave pública (Public-Key).

5 La vinculación de la clave criptográfica privada del documento de identificación y de la clave criptográfica pública transmitida se puede implementar mediante vinculación binaria, como por ejemplo OR exclusiva, mediante algoritmos criptográficos, como por ejemplo el estándar avanzado de encriptación (Advanced Encryption Standard, AES) y/o mediante algoritmos de formación de valor Hash, como por ejemplo el algoritmo de Hash seguro (Secure Hash Algorithm, SHA). La vinculación puede comprender además un cálculo de sumas de comprobación de la clave criptográfica privada del documento de identificación y/o clave criptográfica pública transmitida.

10 La transmisión de la clave criptográfica pública se puede llevar a cabo, por ejemplo, a través de la primera conexión de comunicación y la segunda conexión de comunicación.

La generación de la identificación electrónica puede comprender una generación o facilitación de la identificación electrónica.

15 El almacenamiento de la identificación electrónica generada puede comprender una transmisión de la identificación electrónica generada del documento de identificación al servidor de identificación. El almacenamiento de la identificación electrónica generada puede comprender además depositar la identificación electrónica transmitida en una memoria o una base de datos del servidor de identificación.

20 Según una forma de realización, la identificación electrónica del documento de identificación es una identificación restringida (Restricted Identification) del documento de identificación. De este modo se consigue la ventaja de que se puede usar una identificación electrónica seudónima del documento de identificación.

La identificación restringida (Restricted Identification) del documento de identificación se puede generar en base a un intercambio de claves Diffie-Hellmann por el documento de identificación. La identificación restringida (Restricted Identification) se puede implementar, por ejemplo, según la directiva técnica BSI TR-03110.

25 Según una forma de realización, la característica de identificación ópticamente detectable del documento de identificación es un número de acceso de tarjeta (Card Access Number) del documento de identificación. De este modo se consigue la ventaja de que se puede usar una característica de identificación numérica del documento de identificación.

30 El número de acceso de tarjeta (Card Access Number CAN) del documento de identificación puede ser un número decimal de seis dígitos. El número de acceso de tarjeta (Card Access Number) puede estar impreso sobre el documento de identificación legible electrónicamente y se puede detectar ópticamente. El número de acceso de tarjeta (Card Access Number) se puede usar además como contraseña para un protocolo de establecimiento de conexión autenticada por contraseña (Password Authenticated Connection Establishment, PACE) y presentar, por ejemplo, las propiedades según la directiva técnica BSI TR-03127.

35 Según una forma de realización, el servidor de identificación es un servidor eID. De este modo se consigue la ventaja de que se puede usar un servidor de identificación estandarizado.

El servidor eID puede estar implementado, por ejemplo, según la directiva técnica BSI TR-03130 e interactuar con el documento de identificación.

40 Según un segundo aspecto, la invención se refiere a una instalación de bloqueo de vehículo, que se puede desbloquear usando un documento de identificación legible electrónicamente, con un terminal, que está configurado para leer una identificación electrónica de un documento de identificación legible electrónicamente, una cámara de imágenes, que está configurada para detectar ópticamente una característica de identificación ópticamente detectable del documento de identificación legible electrónicamente, y una interfaz de comunicación, que está configurada para enviar la identificación electrónica leída a través de la conexión de comunicación y recibir una señal de autenticación para el desbloqueo de la instalación de bloqueo de vehículo. De este modo se consigue la ventaja de que se puede implementar un concepto cómodo y flexible para el desbloqueo de una instalación de boqueo de vehículo.

45 La instalación de bloqueo de vehículo puede permitir o negar un acceso al vehículo. La instalación de bloqueo de vehículo puede ser, por ejemplo, una instalación de bloqueo de una puerta de vehículo. El vehículo puede ser, por ejemplo, un automóvil o un camión.

50 El documento de identificación legible electrónicamente puede ser uno de los documentos de identificación siguientes: documento de identidad, como carné de identidad, pasaporte, carné de control de accesos, credencial, carné de empresa, marca de control o tique, certificado de nacimiento, carné de conducir o documentación del vehículo, medio de pago, por ejemplo una tarjeta bancaria o tarjeta de crédito. El documento de identificación puede comprender además un circuito legible electrónicamente, por ejemplo un chip RFID. El documento de identificación

puede ser monocapa o multicapa o a base de papel y/o plástico. El documento de identificación puede estar construido de láminas a base de plástico, que se ensamblan formando un cuerpo de tarjeta mediante pegado y/o laminado, presentando las láminas preferiblemente propiedades materiales similares.

5 El terminal puede ser un equipo lector para una comunicación con el documento de identificación legible electrónicamente. El terminal puede estar dispuesto, por ejemplo, en o detrás de la luna del vehículo, por ejemplo, entre un pilar B y un pilar C del vehículo. El terminal puede estar dispuesto además, por ejemplo, en un pilar del vehículo.

10 La identificación electrónica puede estar formada por una serie de letras, cifras, bytes y/o símbolos. La identificación electrónica puede comprender un dato personal sobre una persona, por ejemplo un nombre, y/o una característica electrónica del documento de identificación, por ejemplo un número de serie. La identificación electrónica se puede generar y/o almacenar además por el documento de identificación.

15 La cámara de imágenes puede estar configurada para tomar una imagen óptica en el rango de longitud de onda visible. La cámara de imágenes puede comprender un sensor de imagen y/o un objetivo de cámara. La cámara de imágenes puede estar dispuesta, por ejemplo, en o detrás de la luna del vehículo, por ejemplo, entre un pilar B y un pilar C del vehículo. La cámara de imágenes puede estar dispuesta además, por ejemplo, en un pilar del vehículo.

La característica de identificación ópticamente detectable puede estar formada por una serie de letras, cifras y/o símbolos. La característica de identificación ópticamente detectable puede estar representada además en forma de un código de barras, un código bidimensional, por ejemplo, un código de respuesta rápida (Quick-Response, QR) o un holograma.

20 La interfaz de comunicación puede estar configurada para comunicarse con el servidor de identificación. La comunicación entre la interfaz de comunicación y el servidor de identificación se puede llevar a cabo a través de una red de comunicación por ejemplo internet.

La conexión de comunicación puede ser por cable o inalámbrica. La conexión de comunicación se puede autenticar y/o establecer de forma encriptada.

25 La señal de autenticación puede estar formada por un mensaje electrónico, una orden, un comando y/o un proceso. La señal de autenticación se puede generar y enviar por el servidor de identificación.

Otras características de la instalación de bloqueo de vehículo se deducen directamente de la funcionalidad del procedimiento para el desbloqueo de una instalación de bloqueo de vehículo.

30 El procedimiento para el desbloqueo de una instalación de bloqueo de vehículo se puede realizar mediante la instalación de bloqueo de vehículo.

35 Según una forma de realización, la cámara de imágenes es una cámara de imágenes de un equipo de comunicación móvil, estando configurada la interfaz de comunicación además para recibir la característica de identificación ópticamente detectable por el equipo de comunicación móvil y llevándose a cabo el establecimiento de la primera conexión de comunicación entre el documento de identificación legible electrónicamente y la instalación de bloqueo de vehículo en base a la característica de identificación recibida, ópticamente detectada. De este modo se consigue la ventaja de que se puede usar la cámara de imágenes de forma sencilla.

El equipo de comunicación móvil puede ser, por ejemplo, un ordenador portátil, un teléfono móvil o un smartphone.

40 Según un tercer aspecto, la invención se refiere a un programa informático con un código de programa para la realización del procedimiento para el desbloqueo de una instalación de bloqueo de vehículo cuando se ejecuta el código de programa en un ordenador. De este modo se consigue la ventaja de que se puede automatizar el procedimiento y realizar de forma reproducible.

El programa informático puede comprender una serie de órdenes para un procesador de un ordenador. El programa informático puede existir en forma de un código de programa legible a máquina.

45 El ordenador puede comprender un procesador, una memoria, una interfaz de entrada y/o una interfaz de salida. El procesador del ordenador puede estar configurado para ejecutar el programa informático.

La invención se puede implementar en el hardware y/o software.

Otros ejemplos de realización se explican más en detalle en referencia a los dibujos adjuntos. Estos muestran:

Fig. 1 un diagrama esquemático de un procedimiento para el desbloqueo de una instalación de bloqueo de vehículo de un vehículo usando un documento de identificación legible electrónicamente;

50 Fig. 2 un diagrama esquemático de una instalación de bloqueo de vehículo, que se puede desbloquear usando un documento de identificación legible electrónicamente; y

Fig. 3 una disposición esquemática para el desbloqueo de una instalación de bloqueo de vehículo de un vehículo usando un documento de identificación legible electrónicamente.

5 La fig. 1 muestra un diagrama esquemático de un procedimiento 100 para el desbloqueo de una instalación de bloqueo de vehículo de un vehículo usando un documento de identificación legible electrónicamente. El documento de identificación legible electrónicamente presenta una característica de identificación ópticamente detectable.

10 El procedimiento 100 comprende una detección óptica 101 de la característica de identificación ópticamente detectable del documento de identificación legible electrónicamente, un establecimiento 103 de una primera conexión de comunicación entre el documento de identificación legible electrónicamente y la instalación de bloqueo de vehículo en base a la característica de identificación ópticamente detectable, un establecimiento 105 de una segunda conexión de comunicación entre la instalación de bloqueo de vehículo y un servidor de identificación, una lectura 107 de una identificación electrónica del documento de identificación mediante el servidor de identificación a través de la primera conexión de comunicación y la segunda conexión de comunicación, y un desbloqueo 109 de la instalación de bloqueo de vehículo en el caso de concordancia entre la identificación electrónica leída y una identificación electrónica prealmacenada.

15 La detección óptica 101 de la característica de identificación ópticamente detectable se puede llevar a cabo en base a un reconocimiento de patrones.

20 El establecimiento 103 de la primera conexión de comunicación entre el documento de identificación legible electrónicamente y la instalación de bloqueo de vehículo puede comprender una transmisión de claves criptográficas y/o certificados criptográficos. Las claves criptográficas y/o certificados criptográficos se pueden generar en base a la característica de identificación ópticamente detectada.

El establecimiento 105 de la segunda conexión de comunicación entre la instalación de bloqueo de vehículo y el servidor de identificación puede comprender una transmisión de claves criptográficas y/o certificados criptográficos.

25 La lectura 107 de la identificación electrónica del documento de identificación por el servidor de identificación a través de la primera conexión de comunicación y la segunda conexión de comunicación puede comprender una transmisión de claves criptográficas y/o certificados criptográficos entre el documento de identificación y el servidor de identificación. Además, la lectura 107 de la identificación electrónica puede comprender una verificación de la autenticidad u originalidad del documento de identificación y/o de la identificación electrónica.

30 El desbloqueo 109 de la instalación de bloqueo de vehículo se puede llevar a cabo en caso de concordancia entre la identificación electrónica leída y la identificación electrónica prealmacenada. Una concordancia entre la identificación electrónica leída y la identificación electrónica prealmacenada puede existir cuando son idénticas la identificación electrónica leída y la identificación electrónica prealmacenada. El desbloqueo 109 de la instalación de bloqueo de vehículo se puede llevar a cabo además en respuesta a una recepción de una señal de autenticación por la instalación de bloqueo de vehículo.

35 La fig. 2 muestra un diagrama esquemático de una instalación de bloqueo de vehículo 200, que se puede desbloquear usando un documento de identificación legible electrónicamente.

40 La instalación de bloqueo de vehículo 200 comprende un terminal 201, que está configurado para leer una identificación electrónica de un documento de identificación legible electrónicamente, una cámara de imágenes 203, que está configurada para detectar ópticamente una característica de identificación ópticamente detectable del documento de identificación legible electrónicamente, y una interfaz de comunicación 205, que está configurada para enviar la identificación electrónica leída a través de una conexión de comunicación y recibir una señal de autenticación para el desbloqueo de la instalación de bloqueo de vehículo.

La instalación de bloqueo de vehículo 200 puede permitir o negar un acceso al vehículo. La instalación de bloqueo de vehículo 200 puede ser, por ejemplo, una instalación de bloqueo de una puerta de vehículo. El vehículo puede ser, por ejemplo, un automóvil o un camión.

45 El terminal 201 puede ser un equipo lector para una comunicación con el documento de identificación legible electrónicamente. El terminal 201 puede estar dispuesto, por ejemplo, en o detrás de la luna del vehículo, por ejemplo, entre un pilar B y un pilar C del vehículo. El terminal 201 puede estar dispuesto además, por ejemplo, en un pilar del vehículo.

50 La cámara de imágenes 203 puede estar configurada para tomar una imagen óptica en el rango de longitud de onda visible. La cámara de imágenes 203 puede comprender un sensor de imagen y/o un objetivo de cámara. La cámara de imágenes 203 puede estar dispuesta, por ejemplo, en o detrás de la luna del vehículo, por ejemplo, entre un pilar B y un pilar C del vehículo. La cámara de imágenes 203 puede estar dispuesta además, por ejemplo, en un pilar del vehículo.

La interfaz de comunicación 205 puede estar configurada para comunicarse con el servidor de identificación. La comunicación entre la interfaz de comunicación 205 y el servidor de identificación se puede llevar a cabo a través de una red de comunicación, por ejemplo internet.

5 El terminal 201, la cámara de imágenes 203 y la interfaz de comunicación 205 pueden estar conectadas entre sí de forma recíproca.

10 La fig. 3 muestra una disposición 300 esquemática para el desbloqueo de una instalación de bloqueo de vehículo 200 de un vehículo usando un documento de identificación legible electrónicamente 301. La instalación de bloqueo de vehículo 200 comprende un terminal 201, una cámara de imágenes 203 y una interfaz de comunicación 205. El documento de identificación legible electrónicamente 301 comprende una característica de identificación ópticamente detectable 303. La disposición 300 comprende además un servidor de identificación 305 y una red de comunicación 307.

La disposición 300 puede permitir un desbloqueo de la instalación de bloqueo de vehículo 200 de un vehículo usando el documento de identificación legible electrónicamente 301.

15 El documento de identificación legible electrónicamente 301 puede ser uno de los documentos de identificación siguientes: documento de identidad, como carné de identidad, pasaporte, carné de control de accesos, credencial, carné de empresa, marca de control o tique, certificado de nacimiento, carné de conducir o documentación del vehículo, medio de pago, por ejemplo una tarjeta bancaria o tarjeta de crédito. El documento de identificación 301 puede comprender además un circuito legible electrónicamente, por ejemplo un chip RFID. El documento de identificación 301 puede ser monocapa o multicapa o a base de papel y/o plástico. El documento de identificación 20 301 puede estar construido de láminas a base de plástico, que se ensamblan formando un cuerpo de tarjeta mediante pegado y/o laminado, presentando las láminas preferiblemente propiedades materiales similares.

25 La característica de identificación ópticamente detectable 303 puede estar constituida por una serie de letras, cifras y/o símbolos. La característica de identificación ópticamente detectable 303 puede estar representada además en forma de un código de barra, un código bidimensional, por ejemplo, un código de respuesta rápida (Quick-Response, QR) o un holograma.

El servidor de identificación 305 puede estar configurado para leer la identificación electrónica del documento de identificación 301. El servidor de identificación 305 puede estar configurado para verificar la autenticidad u originalidad del documento de identificación 301.

30 La red de comunicación 307 puede estar configurada por una disposición de una multiplicidad de servidores, clientes y/o ordenadores. La red de comunicación 307 puede ser por ejemplo internet.

El procedimiento para el desbloqueo de la instalación de desbloqueo de vehículo 200 de un vehículo usando el documento de identificación legible electrónicamente 301 se puede llevar a cabo, por ejemplo, de la siguiente manera:

35 La característica de identificación legible ópticamente 303 del documento de identificación legible electrónicamente 301 se puede detectar ópticamente mediante la cámara de imágenes 203 de la instalación de bloqueo de vehículo 200. Acto seguido se puede establecer una primera conexión entre el documento de identificación legible electrónicamente 301 y el terminal 201 de la instalación de bloqueo de vehículo 200 en base a la característica de identificación ópticamente detectada 303. Acto seguido se puede establecer una segunda conexión de comunicación entre la interfaz de comunicación 205 de la instalación de bloqueo de vehículo 200 y el servidor de identificación 305 a través de la red de comunicación 307. La identificación electrónica se puede leer a continuación por el servidor de identificación 305 del documento de identificación 301 a través de la primera conexión de comunicación y la segunda 40 conexión de comunicación. En caso de concordancia entre la identificación electrónica leída y una identificación electrónica almacenada previamente se puede desbloquear la instalación de bloqueo de vehículo 200. Para ello el servidor de identificación 305 puede generar una señal de autenticación y enviarla a la instalación de bloqueo de 45 vehículo 200.

Según una forma de realización, la invención se refiere a un bloqueo central de un automóvil con un documento de identificación, por ejemplo un nuevo carné de identidad (nPA).

50 Según una forma de realización el protocolo de establecimiento de conexión autenticada por contraseña (Password Authenticated Connection Establishment, PACE) se lleva a cabo con el número de acceso de tarjeta (Card Access Number, CAN).

Según una forma de realización se leen una identificación electrónica o los datos del documento de identificación a través de un canal, los cuales se usan para autenticar una persona o un usuario.

Según una forma de realización se puede usar una función eID de un documento de identificación, por ejemplo, de un nuevo carné de identidad (nPA), para la apertura de un automóvil. Para ello se puede llevar a cabo un protocolo

de establecimiento de conexión autenticada por contraseña (Password Authenticated Connection Establishment, PACE) con el documento de identificación, por ejemplo el nuevo carné de identidad (nPA).

5 Según una forma de realización se puede llevar a cabo un protocolo de establecimiento de conexión autenticada por contraseña (Password Authenticated Connection Establishment, PACE) con un número de acceso de tarjeta (Card Access Number, CAN), que está impreso sobre el documento de identificación, por ejemplo el nuevo carné de identidad (nPA) u otro carné.

10 Según una forma de realización, una instalación de bloqueo de vehículo o vehículo o una máquina automática comprende una luna, detrás del que se sitúan una cámara de imágenes o cámara, así como un terminal o lector de tarjetas. Además, comprende una conexión inalámbrica, por ejemplo, una segunda conexión de comunicación o
 15 conexión 1 con un servidor de identificación, por ejemplo, un servidor eID. Una persona o un usuario mantiene un documento de identificación o un nuevo carné de identidad (nPA) delante de la cámara de imágenes o cámara de la instalación de bloqueo de vehículo o del vehículo. Ésta lee el CAN impreso. La instalación de bloqueo de vehículo o el vehículo usa el CAN leído para establecer un canal PACE a través del terminal o el lector de tarjetas, por ejemplo una primera conexión de comunicación o conexión 2, para el documento de identificación o nuevo carné de
 identidad (nPA). A continuación el servidor de identificación, a través de la primera conexión de comunicación y la segunda conexión de comunicación o las conexiones 1 y 2 lleva a cabo los protocolos de autenticación (TA, CA) con el documento de identificación, por ejemplo el nuevo carné de identidad (nPA), lee la identificación electrónica o los datos requeridos o el identificador del documento de identificación o carné, autentifica la persona o el usuario y envía una señal de autenticación o señal de apertura a la instalación de bloqueo de vehículo o al vehículo.

20 Según una forma de realización se permite una autenticación de dos factores de una persona o de un usuario.

Según una forma de realización se puede usar un token de identificación o token ID disponible.

LISTA DE REFERENCIAS

- 100 Procedimiento para el desbloqueo de una instalación de bloqueo de vehículo
- 101 Detección óptica de la característica de identificación ópticamente detectable
- 25 103 Establecimiento de una primera conexión de comunicación
- 105 Establecimiento de una segunda conexión de comunicación
- 107 Lectura de una identificación electrónica
- 109 Desbloqueo de la instalación de bloqueo de vehículo
- 200 Instalación de bloqueo de vehículo
- 30 201 Terminal
- 203 Cámara de imágenes
- 205 Interfaz de comunicación
- 300 Disposición para el desbloqueo de una instalación de bloqueo de vehículo
- 301 Documento de identificación legible electrónicamente
- 35 303 Característica de identificación ópticamente detectable
- 305 Servidor de identificación
- 307 Red de comunicación

REIVINDICACIONES

1. Procedimiento (100) para el desbloqueo de una instalación de bloqueo de vehículo (200) de un vehículo usando un documento de identificación legible electrónicamente (301), en donde el documento de identificación legible electrónicamente (301) presenta una característica de identificación ópticamente detectable (303), con:
- 5 detección óptica (101) de la característica de identificación ópticamente detectable (303) del documento de identificación legible electrónicamente (301);
- establecimiento (103) de una primera conexión de comunicación entre el documento de identificación legible electrónicamente (301) y la instalación de bloqueo de vehículo (200) en base a la característica de identificación ópticamente detectada (303);
- 10 establecimiento (105) de una segunda conexión de comunicación entre la instalación de bloqueo de vehículo (200) y un servidor de identificación (305);
- lectura (107) de una identificación electrónica del documento de identificación (301) por el servidor de identificación (305) a través de la primera conexión de comunicación y la segunda conexión de comunicación; y
- 15 desbloqueo (109) de la instalación de bloqueo de vehículo (200) en caso de concordancia entre la identificación electrónica leída y una identificación electrónica prealmacenada.
2. Procedimiento (100) según la reivindicación 1, en donde la instalación de bloqueo de vehículo (200) no se desbloquea en el caso de falta de concordancia entre la identificación electrónica leída y la identificación electrónica prealmacenada.
- 20 3. Procedimiento (100) según una de las reivindicaciones anteriores, en donde para la detección óptica (101) de la característica de identificación ópticamente detectable (303) se toma una imagen óptica de la característica de identificación ópticamente detectable (303) mediante una cámara de imágenes (203).
4. Procedimiento (100) según una de las reivindicaciones anteriores, en donde la detección (101) de la característica de identificación ópticamente legible (303) comprende una extracción de la característica de identificación (303) de una imagen óptica del documento de identificación (301).
- 25 5. Procedimiento (100) según una de las reivindicaciones anteriores, en donde el establecimiento (103) de la primera conexión de comunicación entre el documento de identificación legible electrónicamente (301) y la instalación de bloqueo de vehículo (200) se lleva a cabo mediante un protocolo de establecimiento de conexión autenticado por contraseña.
- 30 6. Procedimiento (100) según la reivindicación 5, en donde el protocolo de establecimiento de conexión autenticado por contraseña es un protocolo de Password Authenticated Connection Establishment.
7. Procedimiento (100) según una de las reivindicaciones anteriores, en donde el establecimiento (105) de la segunda conexión de comunicación entre la instalación de bloqueo de vehículo (200) y el servidor de identificación (305) se lleva a cabo mediante un protocolo de seguridad de capa de transporte.
- 35 8. Procedimiento (100) según una de las reivindicaciones anteriores, en donde el documento de identificación legible electrónicamente (301) comprende un circuito integrado, y en donde la lectura (107) de la identificación electrónica del documento de identificación (301) comprende una realización de un procedimiento de autenticación de chip para la autenticación del circuito integrado del documento de identificación (301).
- 40 9. Procedimiento (100) según una de las reivindicaciones anteriores, en donde la primera conexión de comunicación con el documento de identificación legible electrónicamente (301) se establece a través de un terminal (201) para una comunicación con el documento de identificación legible electrónicamente (301), y en donde la lectura (107) de la identificación electrónica del documento de identificación (301) comprende una realización de un procedimiento de autenticación de terminal para la autenticación del terminal (201) o del servidor de identificación (305).
- 45 10. Procedimiento (100) según una de las reivindicaciones anteriores, en donde el desbloqueo (109) de la instalación de bloqueo de vehículo (200) comprende un envío de una señal de autenticación a la instalación de bloqueo de vehículo (200).
11. Procedimiento (100) según una de las reivindicaciones anteriores, con:
- transmisión de una clave criptográfica pública a través del servidor de identificación (305) al documento de identificación (301);
- 50 generación de una identificación electrónica mediante una vinculación de una clave criptográfica privada del documento de identificación (301) y de la clave criptográfica pública transmitida por el documento de identificación (301); y

almacenamiento de la identificación electrónica generada para obtener la identificación electrónica prealmacenada.

12. Procedimiento (100) según una de las reivindicaciones anteriores, en donde la identificación electrónica del documento de identificación (301) es una identificación restringida (Restricted Identification) del documento de identificación (301).

5 13. Procedimiento (100) según una de las reivindicaciones anteriores, en donde la característica de identificación ópticamente detectable (303) del documento de identificación (301) es un número de acceso de tarjeta (Card Access Number) del documento de identificación (301).

14. Instalación de bloqueo de vehículo (200), que se puede desbloquear usando un documento de identificación legible electrónicamente (301), con:

10 una cámara de imágenes (203), que está configurada para detectar ópticamente una característica de identificación ópticamente detectable (303) del documento de identificación legible electrónicamente (301); y

un terminal (201) con una primera interfaz de comunicación, que está configurado para leer una identificación electrónica del documento de identificación legible electrónicamente (301) en base a la característica de identificación detectada ópticamente (303); y

15 una segunda

interfaz de comunicación (205), que está configurada para enviar la identificación electrónica leída a través de una conexión de comunicación a un servidor de identificación (305) y recibir una señal de autenticación para el desbloqueo (109) de la instalación de bloqueo de vehículo (200).

20 15. Programa informático con un código de programa para la realización del procedimiento (100) según una de las reivindicaciones 1 a 13 cuando el código de programa es ejecutado en un ordenador.

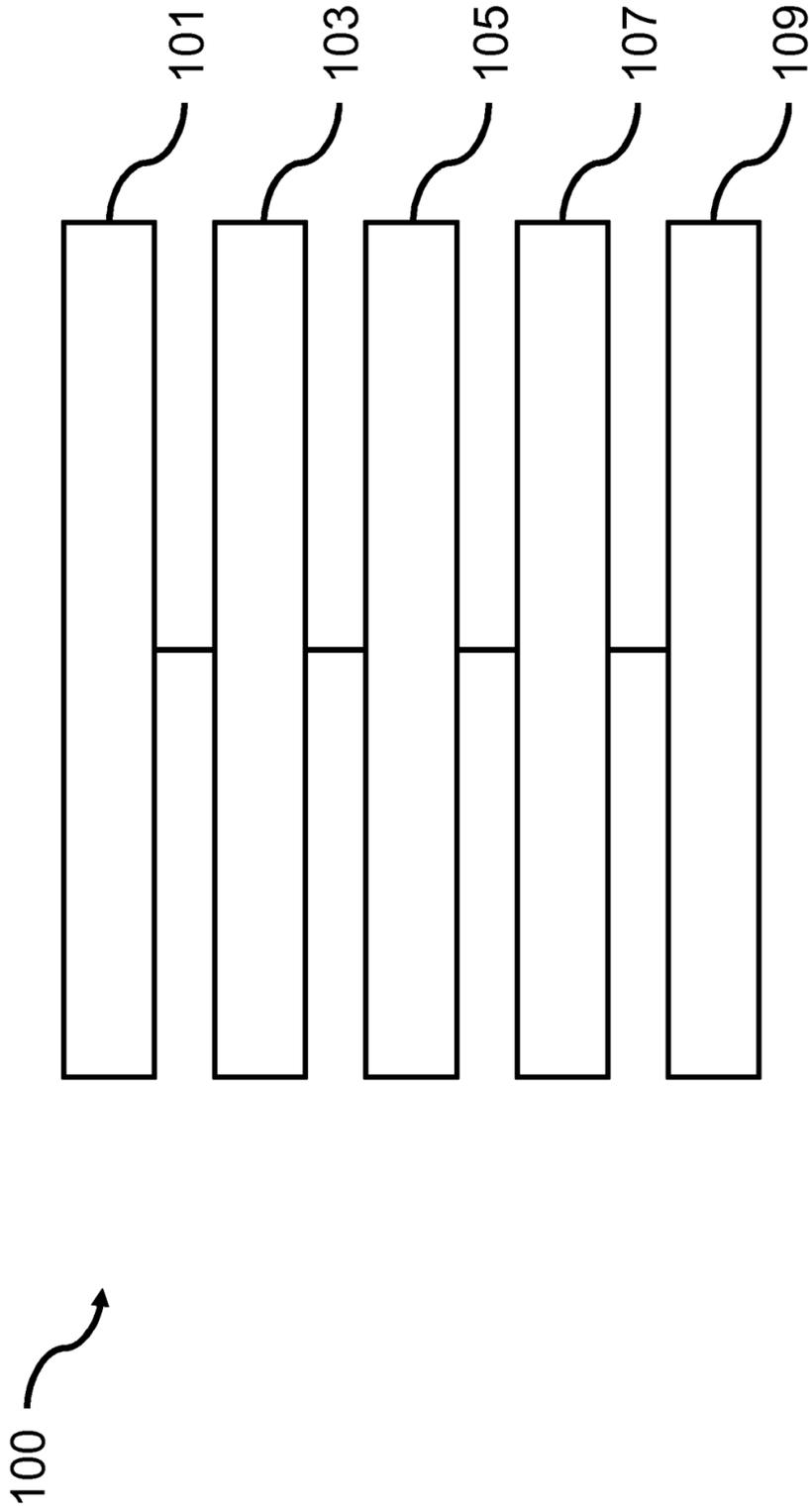


Fig. 1

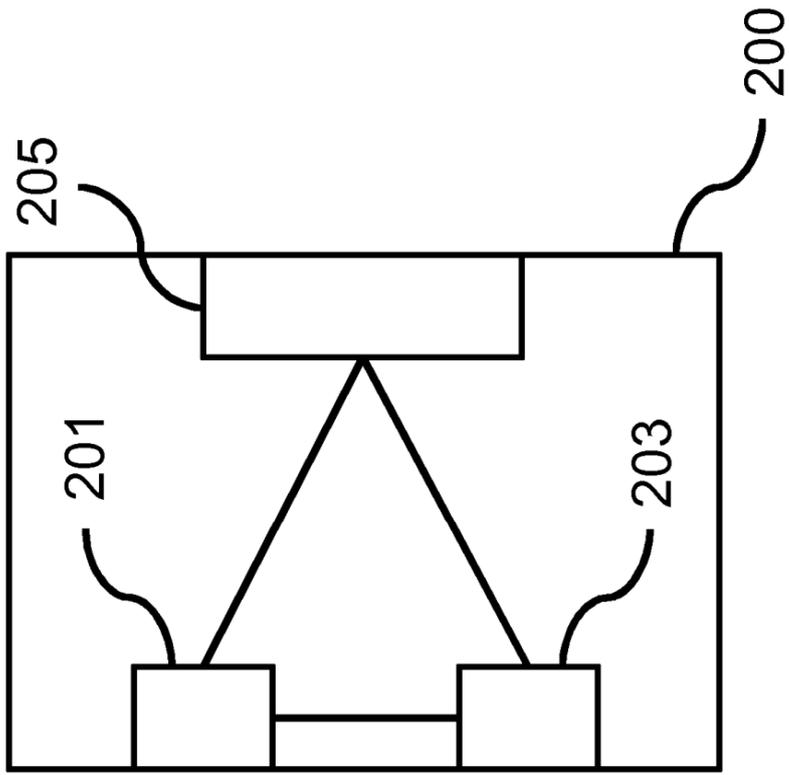


Fig. 2

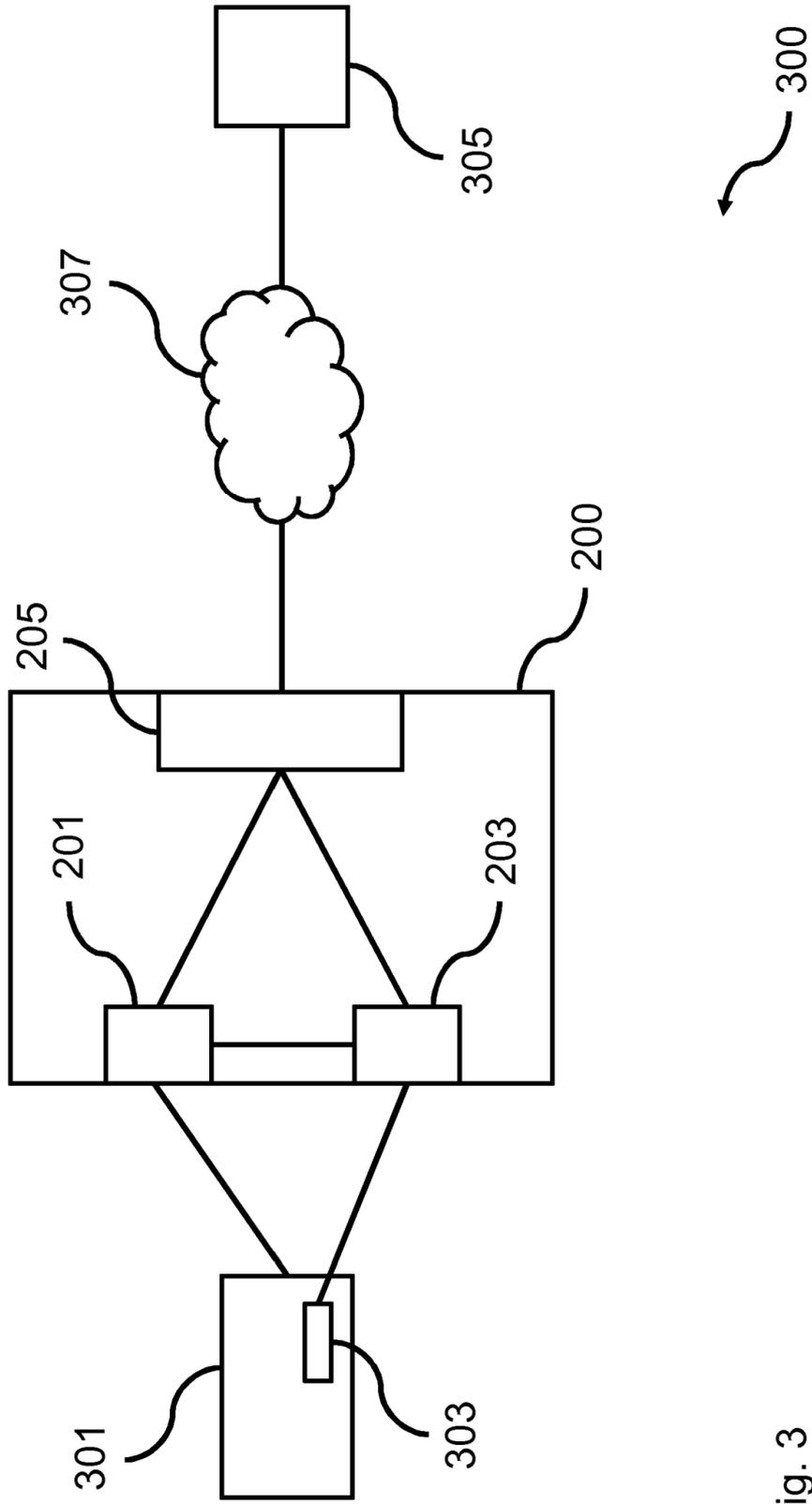


Fig. 3