(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **3 014 378**

(51) Int. Cl.:

G06Q 10/02 (2012.01)
G06Q 20/32 (2012.01)
G06Q 20/04 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **29.05.2020 PCT/EP2020/064974**

(87) Fecha y número de publicación internacional: **10.12.2020 WO20245043**

(96) Fecha de presentación y número de la solicitud europea: **29.05.2020 E 20729729 (2)**

(97) Fecha y número de publicación de la concesión europea: **12.02.2025 EP 3977371**

(54) Título: **Método y dispositivo de control para la verificación segura de un billete electrónico**

(30) Prioridad:

03.06.2019 DE 102019114844

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
22.04.2025

(73) Titular/es:

VDV ETICKET SERVICE GMBH & CO. KG (100.00%)
Im Mediapark 8a
50670 Köln, DE

(72) Inventor/es:

LUTGEN, JOSEPH

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Método y dispositivo de control para la verificación segura de un billete electrónico

La presente invención se refiere a un método para la verificación segura de un billete electrónico y a un dispositivo de control correspondiente para la verificación segura.

Cada vez son más los consumidores que optan por comprar billetes de autobús y tren, pero también entradas para conciertos y otros eventos, por Internet. Al comprar online, el consumidor normalmente tiene la opción de recibir el billete adquirido por correo postal o por correo electrónico. Alternativamente, a menudo se le brinda la posibilidad de transferir el billete directamente a su teléfono inteligente.

Las dos variantes por las que el billete se entrega por correo electrónico o se transfiere directamente al teléfono inteligente del consumidor se denominan generalmente billetes electrónicos.

Si el consumidor solicita que el billete se envíe por correo electrónico, normalmente se enviará en formato PDF. Los datos del billete suelen almacenarse en forma de código de barras para que un dispositivo de control pueda leerlos de forma rápida y sencilla. Si corresponde, los datos del billete también se muestran como texto sin formato.

Si el consumidor decide transferir el billete directamente a su teléfono inteligente, los datos del billete se cargarán directamente en su teléfono inteligente a través de una aplicación correspondiente. Esta variante es especialmente popular para los billetes de tren. Por ejemplo, Deutsche Bahn AG ofrece una aplicación correspondiente (también conocida como DB Navigator) en donde se pueden almacenar los billetes electrónicos de un pasajero.

Cada vez que se debe controlar un billete electrónico, el estado actual de la técnica permite que los datos, que a menudo están almacenados en forma de código de barras 2D (a menudo como código Aztec), puedan ser leídos por el dispositivo de control de un revisor. El revisor recibe en el menor tiempo posible toda la información relevante sobre el billete electrónico, como el nombre del pasajero, la ruta reservada, el medio de transporte reservado (por ejemplo, expreso regional o ICE), la clase reservada (1.ª o 2.ª clase), el asiento reservado (si corresponde), las opciones de BahnCard, etc.

De esta manera, el revisor puede comprobar en el menor tiempo posible si un pasajero ha reservado el billete "correcto" y, por tanto, tiene el supuesto derecho a utilizar el medio de transporte seleccionado.

Sin embargo, el método descrito anteriormente solo permite al revisor comprobar de forma limitada si el billete es original, falso o una copia y si el pasajero está realmente autorizado a utilizar el medio de transporte seleccionado.

Por lo tanto, ya existen varios enfoques para hacer que los billetes sean a prueba de falsificaciones. Para aumentar la seguridad, los billetes electrónicos actuales suelen contener bits de control adicionales que se crean a partir de los datos del billete mediante un algoritmo. Si un estafador intenta manipular los datos del billete electrónico, por ejemplo, modificando la información sobre la ruta reservada, el revisor o su dispositivo de inspección puede detectar la manipulación de los datos del billete.

Si bien el mecanismo descrito anteriormente protege contra la manipulación no autorizada de los datos del billete, no impide que un estafador copie el billete electrónico completo. Por ejemplo, este podría copiar el código de barras perteneciente a un billete electrónico mediante una captura de pantalla y transferir esta captura de pantalla a uno o más teléfonos inteligentes. Para evitar este problema, la mayoría de los billetes electrónicos se emiten ahora personalizados. Por tanto, además de comprobar el billete electrónico, el revisor también podrá comprobar los datos personales del pasajero y pedirle que se identifique. Si el nombre del pasajero es idéntico al nombre almacenado en el billete electrónico, el pasajero se considera elegible. Si bien el método descrito anteriormente para verificar billetes electrónicos en combinación con la verificación de datos personales puede considerarse relativamente seguro, el método de verificación en dos etapas descrito (verificación de datos de billetes y datos personales) requiere bastante tiempo en la práctica y, por lo tanto, es muy impopular tanto entre los usuarios como entre los controladores. Además, el proceso de verificación en dos etapas es en algunos casos prácticamente imposible de implementar, por ejemplo, si un usuario afirma no tener consigo un documento de identidad.

Aunque el billete electrónico se puede leer automáticamente en pocos segundos, la verificación manual adicional del documento de identidad o del pasaporte del pasajero es relativamente engorrosa. A menudo el pasajero solo tiene a mano su billete electrónico, pero no sus documentos de identidad. Esto significa que comprobar los datos personales de un pasajero individual a veces puede llevar un minuto o incluso más. Si hay varios cientos de pasajeros cuyos billetes deben controlarse, esto supondrá una cantidad considerable de trabajo.

En consecuencia, el operador ferroviario tendría que emplear personal de inspección adicional para garantizar un control completo y exhaustivo de todas las autorizaciones de viaje. Alternativamente, el operador puede prescindir de personal de control adicional y aceptar solo una verificación superficial de la autorización de los pasajeros, por ejemplo, prescindiendo parcial o totalmente de la verificación de los datos personales.

En la práctica, esto significa que a menudo solo se comprueban los billetes electrónicos, y no adicionalmente los datos personales del pasajero. Sin embargo, este enfoque es insatisfactorio porque no ofrece al operador suficiente seguridad contra los estafadores.

En el documento EP 1 750 220 A1 se describe un método para crear y verificar automáticamente billetes electrónicos. En este método, los datos del usuario se almacenan en una base de datos de usuarios de un servidor de billetes y los datos de prestación del servicio se almacenan en una base de datos de servicios del servidor de billetes. Mediante el servidor de billetes se crea un billete electrónico y se almacena en el dispositivo móvil del usuario, basándose el billete electrónico en datos de usuario de la base de datos de usuarios y/o en datos de prestación de servicios de la base de datos de servicios. Además, una clave de control electrónica para verificar el billete electrónico se almacena en el dispositivo móvil de un revisor y el billete electrónico almacenado en el dispositivo móvil del usuario es verificado por el dispositivo móvil del revisor. La verificación se realiza mediante transferencia de datos a través de una interfaz NFC entre el dispositivo móvil del usuario y el dispositivo móvil del revisor.

Además, en el documento DE 10 2010 017861 A1 se describe un método para el manejo de billetes electrónicos. El billete electrónico se almacena en un dispositivo de almacenamiento de datos portátil del dispositivo móvil del usuario. En este proceso, el billete electrónico se genera fuera de línea utilizando el soporte de datos portátil del dispositivo móvil del usuario.

Partiendo del problema anteriormente descrito, la presente invención tiene por objeto proporcionar un método y un dispositivo de control para la verificación segura de un billete electrónico, en particular de un billete electrónico de autobús y/o de tren. Otro objetivo de la presente invención es que el método para verificación segura esté diseñado de manera eficiente.

Este objetivo se resuelve mediante un método para verificar de forma segura un billete electrónico según la reivindicación independiente 1. Otras formas de realización preferidas de la presente invención se definen en las reivindicaciones dependientes. En el método según la invención, el billete electrónico se almacena en un primer terminal móvil asignado a un usuario final, y el billete es comprobado por un segundo terminal asignado a un revisor o a un sistema de control. Método según la invención comprende las siguientes etapas:

- envío de un mensaje de solicitud desde el segundo terminal al primer terminal a través de un primer canal de comunicación;

- envío de un mensaje de respuesta desde el primer terminal al segundo terminal a través de un segundo canal de comunicación, estando el mensaje de respuesta firmado por el primer terminal y siendo el segundo canal de comunicación idéntico al primer canal de comunicación o diferente del primer canal de comunicación;

- verificación del mensaje de respuesta firmado por el segundo terminal; y

- confirmación de la autenticidad del mensaje de respuesta por el segundo terminal, siempre que la autenticidad de la firma haya podido ser verificada previamente por el segundo terminal.

El método según la invención y en particular la firma del mensaje de respuesta por parte del primer terminal, ofrecen un mecanismo de protección adicional para una protección eficaz contra los estafadores. El primer terminal en el que se encuentra el billete electrónico recibe una solicitud del segundo terminal para enviar un mensaje de respuesta. Este mensaje de respuesta está firmado por el primer terminal. La firma digital adjunta al mensaje de respuesta puede luego ser verificada por el segundo terminal. Al generar la firma digital, se utiliza una clave privada del primer terminal. La verificación posterior por parte del segundo terminal se realiza utilizando una clave pública del primer terminal. La clave pública y la clave privada del primer terminal forman juntas un par de claves y están vinculadas matemáticamente. Los pares de claves son generalmente conocidos en criptografía y se utilizan en métodos de cifrado asimétrico. La generación de dicho par de claves se puede realizar, por ejemplo, utilizando un método estándar de criptografía de curva elíptica o utilizando el método RSA.

Por ejemplo, la clave pública también se puede incluir en el mensaje de respuesta. Alternativamente, también se puede prever que la clave pública del primer terminal se almacene en el segundo terminal o en un medio de almacenamiento al que el segundo terminal pueda acceder a través de una conexión de red. Dado que el segundo terminal tiene la clave pública del primer terminal o tiene acceso a la clave pública, el segundo terminal puede verificar si la firma del primer terminal es válida o no. Si la firma no es válida, el segundo terminal puede concluir que es falsa o una copia del billete electrónico.

Según una forma de realización del método según la invención, el segundo terminal puede estar diseñado como un terminal móvil. Esto es especialmente ventajoso si el método según la invención se va a utilizar, por ejemplo, en el tren. Alternativamente, también se puede prever que el segundo terminal esté diseñado como terminal estacionario. Esto puede ser particularmente deseable si el método según la invención se va a utilizar en conexión con un sistema de control de acceso o un sistema de acceso. Un sistema de control de acceso de este tipo puede, por ejemplo, disponer de barreras de acceso controladas electrónicamente o puertas de acceso de apertura automática y realizar una comprobación automática de los billetes electrónicos o de la autorización de viaje de un consumidor.

El primer terminal según el método según la invención puede estar diseñado preferiblemente como un teléfono inteligente. El segundo terminal también puede ser un teléfono inteligente.

Además del mecanismo de control proporcionado mediante el envío del mensaje A de solicitud al primer terminal y el envío del mensaje de respuesta firmado al segundo terminal, los datos del billete también se pueden transmitir preferiblemente al segundo terminal. Existen varias alternativas para transferir datos de billetes. Por ejemplo, se puede prever que los datos del billete almacenados en un código de barras 2D se muestren inicialmente en una pantalla del primer terminal. El segundo terminal puede entonces leer el código de barras 2D y comprobar los datos del billete (en particular, la ruta, la clase reservada, etc.). En este contexto podemos hablar de una transmisión de datos de billetes a través de un canal de comunicación óptico. El segundo terminal puede entonces enviar un mensaje A de solicitud al primer terminal para verificar la identidad del pasajero y solicitar confirmación mediante un mensaje de respuesta firmado.

Según otra forma de realización del método según la invención, se puede prever que los datos del billete se transmitan dentro del mensaje de respuesta. De esta forma, todo el control o comunicación entre el dispositivo de control (segundo terminal) y el terminal del consumidor (primer terminal) se realiza en un total de dos etapas (envío del mensaje A de solicitud al primer terminal y envío del mensaje de respuesta con los datos del billete al segundo terminal). En este caso, los datos del billete se pueden almacenar como código de barras 2D o en otro formato (por ejemplo, en formato de texto).

Además, según una forma de realización del método según la invención, puede preverse que el mensaje de solicitud comprenda un mensaje de verificación. El mensaje de verificación puede ser, por ejemplo, una cadena de caracteres (en particular un texto generado aleatoriamente o un número generado aleatoriamente) generado según un algoritmo aleatorio o un algoritmo pseudoaleatorio, que fue generado previamente por el segundo terminal. En particular, se puede prever que el primer terminal, después de recibir el mensaje de solicitud que contiene el mensaje de verificación, encripte este mensaje de verificación con la clave privada y luego transmita una representación encriptada del mensaje de verificación al segundo terminal. Esta transmisión se realiza entonces mediante el mensaje de respuesta. El segundo terminal puede entonces descifrar el mensaje de verificación cifrado utilizando la clave pública del primer terminal y comprobar así si el primer terminal tiene realmente la clave asignada. De esta manera se puede aumentar aún más la seguridad del método de prueba de verificación según la invención, ya que se excluye que el mensaje de respuesta ya se genere antes de la generación del mensaje de verificación. En particular, el mensaje de verificación generado por el segundo terminal puede ser diferente para cada proceso de control. Esto hace que sea prácticamente imposible para un falsificador copiar un mensaje de respuesta en su posesión o reconstruir un mensaje de respuesta a partir de un mensaje de respuesta que conoce y que es reconocido por el segundo terminal como un mensaje de respuesta válido.

Según la presente invención, el mensaje de solicitud comprende un mensaje de verificación que contiene un número aleatorio de longitud L generado por el segundo terminal, donde L >= 1, y el mensaje de respuesta contiene una representación del número aleatorio generado por el segundo terminal cifrado con una clave privada del primer terminal. Por ejemplo, el número aleatorio puede tener 64 bits de longitud. Según una forma de realización del método según la invención, se puede prever además que el número aleatorio tenga una longitud de 128 bits. Al utilizar un número aleatorio especialmente largo, resulta particularmente difícil falsificar o copiar el billete electrónico. Según esta realización, el primer terminal no puede en particular utilizar una copia de un mensaje de respuesta generado previamente por otro terminal, sino que debe generar el mensaje de respuesta que contiene la representación cifrada del propio número aleatorio. De lo contrario, el segundo terminal determinaría que el primer terminal móvil está en posesión de una clave privada supuestamente correcta, pero ha cifrado un número diferente al número aleatorio generado previamente por el segundo terminal.

Según el método según la invención se prevé además que el mensaje de respuesta contenga un certificado digital que procede del proveedor de servicios que ha creado el billete electrónico o de una entidad clasificada como fiable por el proveedor de servicios (ancla de confianza). El certificado digital puede concebirse en particular como un certificado de clave pública. El certificado digital puede tener una clave pública, que junto con una clave privada del proveedor de servicios forma un par de claves. En principio, es posible que la clave pública esté contenida en el mensaje de respuesta y se transmita al segundo terminal, que la clave pública se almacene en un servidor o que la clave pública se almacene en el dispositivo de control. El ancla de confianza (en adelante también denominada entidad clasificada como fiable por el proveedor de servicios) determina si el primer terminal móvil es adecuado como host para la aplicación cliente fiable. Si es así, dota al dispositivo móvil de un ID único, una clave y un certificado o código de verificación. El código de verificación puede ser verificado fácilmente sin conexión por todos los participantes autorizados en el sistema y confirma la fiabilidad de la aplicación cliente.

El certificado digital puede contener en particular información sobre el emisor del certificado y el destinatario del certificado. El certificado digital también puede contener información sobre la función hash utilizada. Por ejemplo, el certificado digital puede especificar que el primer terminal utiliza SHA-1 o SHA-256 como función hash.

El segundo terminal puede utilizar los datos contenidos en el certificado digital para verificar si el propietario del primer terminal está realmente autorizado a utilizar el billete electrónico. El certificado digital también puede firmarse utilizando una clave privada del proveedor de servicios. La clave pública del proveedor de servicios asociada a la clave privada

se puede almacenar en el segundo terminal o en un dispositivo de almacenamiento accesible a través de una conexión de red. Esto permite que el segundo terminal verifique si el certificado fue realmente creado por el proveedor de servicios. Además, el certificado digital puede contener información sobre el período de validez del certificado. Por ejemplo, el certificado digital puede contener la fecha en que se creó el certificado y un período de validez (por ejemplo, 3 meses). De este modo, el segundo terminal puede comprobar si el certificado sigue siendo válido en el momento de comprobar el billete electrónico. Si el certificado ya no es válido, el segundo terminal puede concluir que el propietario del primer terminal no está autorizado a utilizar el billete almacenado en el primer terminal.

El método según la invención prevé también que

- el mensaje de respuesta contiene el billete electrónico, que además de la información del billete también contiene un primer identificador digital del primer terminal, y que el billete electrónico contiene una firma digital del proveedor de servicios;

- el mensaje de respuesta contiene, además del billete electrónico, un segundo identificador digital del primer terminal generado por el primer terminal; y

- el segundo terminal solo confirma la autenticidad del mensaje de respuesta si el primer identificador contenido en el billete electrónico y el segundo identificador generado por el primer terminal son idénticos.

En particular, una huella digital del primer terminal se puede utilizar como identificador (ID). En particular, se puede utilizar una huella digital de *hardware* o una huella digital de *software* del primer terminal. Una huella digital permite identificar de forma inequívoca un terminal. Por ejemplo, una huella digital de *hardware* puede incluir un ID de procesador, un ID de memoria y/o un ID de chip gráfico. La huella digital también puede estar compuesta por los identificadores mencionados anteriormente o calcularse a partir de ellos. En esta forma de realización del método según la invención se puede prever en particular que el ID del primer terminal se consulte o lea durante el registro del usuario final en el proveedor de servicios o durante la compra del billete electrónico. Para este propósito, se puede proporcionar una aplicación en el primer terminal (aplicación cliente fiable) que lea o genere esta ID. Para ello, por ejemplo, se puede leer un identificador de *hardware* (por ejemplo, el número de serie de la CPU o el número de serie de la RAM) y transmitirlo al proveedor de servicios, de modo que el proveedor de servicios personaliza el billete electrónico y el billete contiene los datos del comprador y/o el identificador del terminal (primer identificador). De esta manera, el billete queda vinculado al terminal del comprador. La aplicación cliente fiable protege la clave privada y los datos de la aplicación en los dispositivos móviles de los usuarios y está verificada y autorizada por el ancla de confianza para este propósito. Dado que el billete electrónico también está firmado por el proveedor de servicios, una persona no autorizada que no disponga de la clave privada del proveedor de servicios no puede manipular los datos del billete electrónico. Durante la inspección, el segundo terminal puede verificar si el billete que se está verificando fue realmente creado para el primer terminal móvil del pasajero o si el billete se creó para otro terminal y luego copiado al primer terminal que ahora se está verificando. Al comprobar el billete electrónico, además de los datos contenidos en el propio billete electrónico, se solicita también el identificador del primer terminal. Por ejemplo, el segundo terminal puede leer un ID de *hardware* del primer terminal (segundo identificador). El segundo terminal puede entonces comparar el primer identificador y el segundo identificador. Solo si los dos identificadores son idénticos se confirma la autenticidad del mensaje de respuesta. De esta manera se puede proporcionar un método de verificación especialmente seguro. Con la función de clave y firma establecida en la aplicación cliente fiable, un sistema de emisión de billetes o un dispositivo de control puede determinar su fiabilidad y la autenticidad del propio ID inequívoco. El sistema de emisión de billetes inserta este ID en los datos de un billete a emitir antes de firmar estos datos y enviarlos de vuelta a la aplicación cliente. Esto significa que el billete está vinculado a este ID.

Según otra forma de realización del método según la invención, se puede prever que el identificador del primer terminal se utilice independientemente del principio del mensaje de solicitud y del mensaje de respuesta descritos anteriormente. En otras palabras, para resolver el problema mencionado anteriormente, se propone un método para la verificación segura de un billete electrónico, por el cual el billete electrónico se almacena en un primer terminal móvil asociado a un usuario final y el billete es verificado por un segundo terminal asociado a un revisor o a un sistema de control. Método según la invención comprende las siguientes etapas:

- envío de un mensaje de verificación desde el primer terminal al segundo terminal a través de un canal de comunicación, el mensaje de verificación comprende el billete electrónico, que además de la información del billete también comprende un primer identificador digital del primer terminal y el billete electrónico contiene una firma digital del proveedor de servicios;

- el mensaje de verificación contiene, además del billete electrónico, un segundo identificador digital del primer terminal generado por el primer terminal; y

- el segundo terminal solo confirma la autenticidad del mensaje de verificación si el primer identificador contenido en el billete electrónico y el segundo identificador generado por el primer terminal son idénticos.

Una ventaja de esta realización es que se aumenta aún más la seguridad del método según la invención, ya que es casi imposible manipular el billete electrónico, que preferiblemente contiene una firma del proveedor de servicios. También es prácticamente imposible manipular el identificador del primer terminal, que puede ser en particular un ID de *hardware*. El identificador del primer terminal se genera preferiblemente mediante una aplicación proporcionada por el proveedor de servicios. Esto hace que sea especialmente difícil manipular esta aplicación para transmitir un identificador falso.

Alternativamente, se podrá prever que el segundo terminal solo confirme la autenticidad del mensaje de verificación si el identificador contenido en el billete electrónico y el identificador almacenado en el certificado digital son idénticos. Esto proporciona un método especialmente seguro, ya que tanto la manipulación del billete electrónico como la manipulación del certificado digital son casi imposibles.

Según una forma de realización de la presente invención, el método según la invención comprende las siguientes etapas:

- envío de un mensaje de verificación desde el primer terminal al segundo terminal a través de un canal de comunicación, el mensaje de verificación comprende el billete electrónico, que además de la información del billete también comprende un identificador digital del primer terminal y el billete electrónico contiene una firma digital del proveedor de servicios;

- el mensaje de verificación contiene, además del billete electrónico, un certificado digital firmado por el proveedor del servicio y que contiene el identificador digital del primer terminal; y

- el segundo terminal solo confirma la autenticidad del mensaje de verificación si el identificador contenido en el billete electrónico y el identificador contenido en el certificado digital son idénticos.

Además, en una forma de realización alternativa de la presente invención, se puede prever que el segundo terminal confirme la autenticidad del mensaje de verificación solo si el identificador almacenado en el certificado digital y el identificador generado por el primer terminal son idénticos. Esto garantiza un nivel de seguridad especialmente alto, ya que la manipulación del identificador almacenado en el certificado digital y del identificador del primer terminal es casi imposible.

En general, existen básicamente tres formas diferentes de verificar el identificador (comparación del ID almacenado en el billete con el ID almacenado en el certificado digital, comparación del ID almacenado en el billete con el ID leído por el primer terminal, comparación del ID almacenado en el certificado digital con el ID leído por el primer terminal), y cada variante tiene las ventajas mencionadas.

Además, el método según la invención puede prever que el mensaje de respuesta tenga una marca de tiempo y que la autenticidad del mensaje de respuesta solo sea confirmada por el dispositivo de control (segundo terminal) si la antigüedad de la marca de tiempo es inferior a un valor umbral predeterminado. Por ejemplo, se puede especificar que la autenticidad del mensaje de respuesta no se confirme si la marca de tiempo es anterior a 60 segundos. Esto también evita que un mensaje de respuesta generado por un terminal se transmita a un primer terminal no autorizado y se copie. En este caso, un mensaje de respuesta generado solo es válido durante 60 segundos y no se puede utilizar más allá de este período. Esto puede aumentar aún más la seguridad del método según la invención.

Según una forma de realización del método según la invención, puede preverse que la marca de tiempo esté integrada en un código de barras, en particular en un código de barras 2D. Por ejemplo, el segundo terminal puede enviar un mensaje A de solicitud al primer terminal y el primer terminal puede generar un mensaje de respuesta en respuesta al mensaje de solicitud que transmite la información relevante codificada en un código de barras. El segundo terminal puede leer el código de barras y comprobar si se trata realmente de un código de barras generado recientemente o si se generó, por ejemplo, hace 1 o 2 horas y posiblemente se transfirió más tarde al terminal verificado. En este caso, el revisor podrá solicitar al pasajero que muestre una identificación.

También se puede prever que el mensaje de respuesta contenga un certificado digital en donde se almacena un indicador de seguridad que caracteriza el cumplimiento de los requisitos de seguridad especificados por parte del primer terminal. El indicador de seguridad puede contener información relativa al resultado de una comprobación de seguridad previa del primer terminal. En particular, se puede prever que cuando el primer terminal esté registrado en el proveedor de servicios (servidor de billetes) o por una entidad clasificada como fiable por el proveedor de servicios (ancla de confianza), se realice una comprobación de seguridad del primer terminal para verificar si el terminal cumple los requisitos de seguridad especificados por el proveedor de servicios. Durante el control de seguridad, por ejemplo, se puede comprobar si el primer terminal tiene una versión actual del sistema operativo y/o si hay *software* antivirus instalado en el primer terminal. Si el primer terminal tiene un sistema operativo desactualizado o no tiene *software* antivirus, el atributo de seguridad puede contener información correspondiente que caracteriza al primer terminal como inseguro. El control de seguridad también puede verificar si el primer terminal es un teléfono inteligente enrutado o una tableta enrutada. Si la verificación determina que el terminal está enrutado, el atributo de seguridad puede contener información correspondiente que clasifica el primer terminal como inseguro. El control de seguridad puede estandarizarse y realizarse de forma idéntica para todos los terminales o bien de forma individual y en función del

terminal detectado. Por ejemplo, se puede estipular que los requisitos de seguridad para terminales con un sistema operativo Android difieran de los requisitos de seguridad para terminales con un sistema operativo iOS. De esta manera se puede realizar una verificación individualizada de los terminales sin necesidad de realizar etapas de verificación innecesarias. Al proporcionar el indicador de seguridad, se pueden controlar servicios individuales dependiendo de los terminales individuales. Por ejemplo, se puede establecer que los terminales que cumplan los requisitos de seguridad del proveedor de servicios tengan derecho a comprar billetes, mientras que los terminales que no cumplan los requisitos de seguridad no puedan comprar billetes. Por ejemplo, se podría pretender que los terminales que no cumplan los requisitos de seguridad solo puedan recuperar información sobre las conexiones. También se puede prever que el segundo terminal se niegue a verificar el billete comprobado si el primer terminal no cumple los requisitos de seguridad especificados. El certificado digital que contiene el indicador de seguridad puede, por ejemplo, estar incluido en el billete electrónico o, alternativamente, ser un elemento implementado independientemente del billete electrónico.

Según una forma de realización de la invención, se puede prever que el indicador de seguridad esté diseñado como una bandera de seguridad binaria, que

- contiene un valor igual a 1 si una comprobación de seguridad previa del primer terminal ha demostrado que el primer terminal cumple los requisitos de seguridad especificados, y

- contiene un valor igual a 0 si la comprobación de seguridad previa del primer terminal ha demostrado que el primer terminal no cumple los requisitos de seguridad especificados.

De esta manera, los resultados de una comprobación de seguridad previa del primer terminal se pueden codificar en un solo bit. Esto limita la cantidad de datos transmitidos en el marco del método según la invención.

Además, el método según la invención puede prever que el primer terminal y el segundo terminal dispongan cada uno de un módulo de comunicación de campo cercano (módulo NFC) y que el primer canal de comunicación esté basado en la comunicación de campo cercano (NFC). La transmisión del mensaje A de solicitud través de un canal de comunicación NFC tiene la ventaja de que el mensaje de solicitud no puede ser leído por un tercero, ya que los datos solo se transmiten a una distancia muy corta (normalmente unos pocos centímetros). Por lo tanto, es casi imposible para un tercero leer el mensaje de solicitud, que puede, por ejemplo, contener un número aleatorio generado como mensaje de verificación, y generar un mensaje de respuesta sobre la base de este mensaje de verificación, que luego podría transmitirse al primer terminal verificado por un controlador.

Además, el primer canal de comunicación puede basarse en un estándar de transmisión Bluetooth. Esto tiene la ventaja de que el proceso de verificación puede realizarse a distancias mayores (varios metros). Por ejemplo, se puede prever que un dispositivo de control envíe simultáneamente varios mensajes de solicitud a varios teléfonos inteligentes cercanos, permitiendo así controlar varios terminales o pasajeros simultáneamente. De esta forma se puede reducir significativamente el tiempo necesario para la inspección de billetes. Otra ventaja de utilizar el estándar de transmisión Bluetooth es que no todos los teléfonos inteligentes disponibles en el mercado tienen un módulo NFC. Los modelos más antiguos, en particular, no disponen de un módulo NFC o, al menos, no tienen ningún módulo NFC de libre uso, mientras que normalmente disponen de un módulo Bluetooth.

Además, se puede prever que el primer canal de comunicación esté diseñado como un canal de comunicación óptico. En particular, se puede prever que la comunicación entre el primer terminal y el segundo terminal se realice a través de códigos de barras, en particular a través de códigos de barras 2D, que pueden mostrarse en la pantalla de un terminal y leerse mediante una cámara o un escáner óptico del otro terminal.

Según otra forma de realización del método según la invención, se puede prever que tanto el primer terminal como el segundo terminal dispongan de una cámara frontal. En otras palabras, ambos terminales tienen una cámara, que está ubicada en el mismo lado de cada terminal que las pantallas del mismo. De esta manera, se puede prever que, para verificar los datos del billete, ambos terminales estén alineados frontalmente uno hacia el otro de manera que el mensaje de solicitud se pueda transmitir desde el segundo terminal al primer terminal y el mensaje de respuesta desde el primer terminal al segundo terminal. Los datos correspondientes se muestran en la pantalla de cada terminal (en forma codificada o no codificada) y se leen a través de la cámara del otro terminal.

Según otra forma de realización del método según la invención, también puede preverse que el módulo NFC del segundo terminal emule una etiqueta NFC. En otras palabras, el dispositivo de control se hace pasar por una etiqueta NFC. Esto tiene la ventaja de que incluso los teléfonos inteligentes que no pueden comunicarse a través de la interfaz NFC estándar, sino que solo leen etiquetas NFC, se pueden utilizar en el método según la invención. Este es especialmente el caso de algunos modelos del fabricante de teléfonos inteligentes Apple. Dado que la interfaz NFC solo está parcialmente abierta en varios modelos de iPhone, estos modelos no son adecuados para comunicarse con un dispositivo de control a través de una interfaz NFC. Sin embargo, si el segundo terminal emula una etiqueta NFC, esto también permite la comunicación con los modelos mencionados. Esto proporciona ventajosamente un método que puede utilizarse en todas las plataformas.

Según otra forma de realización del método según la invención, puede preverse que el mensaje de respuesta contenga datos biométricos del consumidor, en particular datos relativos a una huella dactilar, a una voz, a rasgos de una cara o a un patrón de iris. Esto tiene la ventaja de que la identidad del usuario se puede verificar adicionalmente comparando datos biométricos. La verificación la realiza el segundo terminal comparando los datos biométricos recibidos del primer terminal con los datos de una base de datos o directamente con las características del usuario, que están almacenadas bien en el segundo terminal o bien en un elemento de almacenamiento accesible a través de una conexión de red. Por ejemplo, la base de datos puede contener la huella digital de un usuario previamente registrado, así como su nombre completo y/o número de carné de identidad. De manera similar, por ejemplo, la voz de un usuario previamente registrado y su nombre o dirección podrán almacenarse en la base de datos. Esto permite que el segundo terminal verifique la identidad de la persona que se está verificando mediante la comprobación de los datos biométricos.

Además, se puede prever que el mensaje de respuesta contenga una imagen fotográfica del consumidor o una imagen fotográfica de la cara del consumidor. Esto tiene la ventaja de que el segundo terminal puede verificar posteriormente la imagen fotográfica del consumidor recibida del primer terminal. Según una forma de realización del método según la invención, se puede prever que la imagen fotográfica se convierta en primer lugar en una "imagen emoji de la vida real" y después solo dicha imagen emoji del usuario se transmita al dispositivo de control. En otras palabras, se genera una imagen del usuario con una cantidad reducida de datos y se transmite al dispositivo de control. La cantidad de datos en la imagen emoji se reduce considerablemente en comparación con la imagen fotográfica original. De este modo, la transmisión del mensaje de respuesta puede tener lugar ventajosamente en un tiempo muy breve. Sin embargo, la "imagen del emoji de la vida real" todavía ofrece al controlador un nivel de identificabilidad suficientemente alto para su uso en el transporte público. Al comprobar el billete electrónico, el revisor también puede comprobar directamente si el primer terminal pertenece realmente a la persona que lo posee. De este modo, los datos del billete y la imagen fotográfica del consumidor se pueden mostrar simultáneamente en el segundo terminal, de modo que el revisor puede realizar la comprobación en muy poco tiempo.

Según otra forma de realización del método según la invención, puede preverse también que el segundo terminal presente un elemento de memoria y/o esté conectado a un elemento de memoria externo en donde se almacena una lista de datos de identificación cuya probabilidad de falta de autenticidad supera un umbral de probabilidad predeterminado. Los datos de identificación pueden comprender en particular un número de billete o un identificador de un primer terminal. Esto puede reducir aún más el riesgo de que estafadores individuales copien los billetes. Por ejemplo, se puede prever que durante cada inspección se registren datos de identificación, como una huella digital de *hardware* de los terminales inspeccionados. Luego se puede utilizar una base de datos para almacenar con qué frecuencia se registraron estos datos de identificación durante controles anteriores. Si los datos de identificación de un terminal específico se registran con especial frecuencia, esto puede ser un indicio de que en circulación hay grandes cantidades de billetes copiados. Por ejemplo, se puede prever que en los casos en que los mismos datos de identificación se registren mediante dispositivos de control más de diez veces en un solo día, el dispositivo de control emita una señal de advertencia óptica. En este caso, el revisor también podrá solicitar la identidad de la persona controlada. De esta manera, los pasajeros son controlados de forma segura y eficaz, ya que la verificación adicional de los documentos de identificación, en particular el documento de identidad o el pasaporte, solo se realiza en los casos en que se observan irregularidades. El elemento de almacenamiento descrito anteriormente puede diseñarse como una memoria integrada o como un disco duro. Si el elemento de almacenamiento está diseñado como un elemento de almacenamiento externo, el elemento de almacenamiento puede diseñarse en particular como un almacenamiento en la nube al que pueden acceder todos los controladores o dispositivos de control. Los datos de identificación pueden incluir en particular un número de identificación del primer terminal y/o datos biométricos. La forma de realización descrita anteriormente puede proporcionar un método de verificación eficaz que sea capaz de detectar eficientemente cualquier fraude.

Además, según una forma de realización ventajosa del método según la invención, se puede prever que la selección del primer canal de comunicación y del segundo canal de comunicación se realice de forma automática. Por ejemplo, se puede seleccionar automáticamente un canal de comunicación basado en el estándar NFC cuando se detecta un dispositivo compatible con NFC en las inmediaciones. Además, se puede seleccionar automáticamente un canal de comunicación basado en el estándar Bluetooth si no se detecta ningún dispositivo con NFC cerca del dispositivo de control, pero hay dispositivos con Bluetooth disponibles. De manera análoga, se pueden utilizar, por ejemplo, señales ópticas y señales acústicas para la comunicación entre el primer terminal y el dispositivo de control, con el fin de seleccionar automáticamente un canal de comunicación óptico o acústico en consecuencia. Por ejemplo, también se puede utilizar un canal de comunicación acústico u óptico para seleccionar o comunicar direcciones dinámicas para otros canales de comunicación inalámbrica que se utilizarán (por ejemplo, Bluetooth o WLAN). Además, por ejemplo, uno de los terminales puede generar una señal de activación acústica que indica al otro terminal que se está realizando una comunicación a través de una señal acústica. La señal de activación acústica puede, por ejemplo, tener un espectro específico que puede ser registrado y evaluado por el otro terminal. De esta forma se proporciona un sistema inteligente que se adapta a la situación ambiental individual.

Según otra forma de realización del método según la invención, puede preverse también que para la selección automática de los canales de comunicación se utilice un clasificador entrenable. El clasificador entrenable puede ser en particular una red neuronal artificial. El clasificador se puede entrenar con datos del pasado que, por ejemplo, contienen información sobre qué canales de comunicación se prefirieron en qué situación.

Aunque el método según la invención descrito anteriormente se ha descrito a modo de ilustración práctica principalmente en relación con un método para comprobar un billete de tren electrónico, para el experto en la materia debe considerarse evidente que el método según la invención no se limita a métodos para comprobar billetes de tren, sino que el método según la invención también es adecuado para la verificación segura de todo tipo de billetes electrónicos. En particular, el método descrito también es adecuado para comprobar entradas electrónicas para conciertos, festivales y eventos deportivos.

Además, para resolver el problema mencionado anteriormente, se propone un dispositivo de control para comprobar un billete electrónico, en particular un billete electrónico de autobús y/o de tren, según la reivindicación independiente del dispositivo. El billete electrónico se almacena en un primer terminal móvil que se asigna a un consumidor final. El dispositivo de control según la invención tiene al menos un procesador, una memoria y un módulo de comunicación y está diseñado para

- enviar un mensaje A de solicitud al primer terminal a través de un primer canal de comunicación;

- recibir un mensaje de respuesta desde el primer terminal a través de un segundo canal de comunicación, estando el mensaje de respuesta firmado por el primer terminal y siendo el segundo canal de comunicación idéntico al primer canal de comunicación o diferente del primer canal de comunicación;

- verificar el mensaje de respuesta firmado; y

- confirmar la autenticidad del mensaje de respuesta, siempre que la autenticidad de la firma haya podido ser confirmada previamente por el dispositivo de control.

Según una forma de realización del dispositivo de control según la invención, puede preverse que el módulo de comunicación presente un módulo NFC, un módulo Bluetooth, una cámara y/o una pantalla.

Para el experto en la materia resulta evidente que todas las características descritas en relación con el método según la invención también se pueden combinar con el dispositivo de control según la invención.

En general, la presente invención proporciona un método de múltiples etapas, así como un ancla de confianza, una aplicación cliente fiable, un sistema de emisión de billetes, un dispositivo de control y un servicio de bloqueo. Cada uno de los componentes individuales de la presente invención contribuye a aumentar la seguridad global, con lo que un posible uso indebido del sistema de billetes proporcionado se hace significativamente más difícil en comparación con los sistemas conocidos hasta ahora.

La invención se explica a continuación con más detalle mediante ejemplos de realización y con referencia a los dibujos. En concreto se muestra en la:

Fig. 1 una representación esquemática de un método de verificación de billetes unidireccional según el estado de la técnica,

Fig. 2 una representación esquemática de un ejemplo de realización del método de verificación de billetes bidireccional según la invención,

Fig. 3 otra representación esquemática de un ejemplo de realización del método según la invención, en el que se intercambian un mensaje A de solicitud y un mensaje B de respuesta entre un dispositivo de control y un terminal móvil,

Fig. 4 otra representación esquemática de un ejemplo de realización del método según la invención, en el que un dispositivo de control y un terminal móvil se comunican adicionalmente con un servidor,

Fig. 5 otra representación esquemática de un ejemplo de realización del método según la invención, en el que el mensaje de respuesta contiene un certificado digital,

Fig. 6 una representación esquemática de un ejemplo de realización del método según la invención, en el que el mensaje de respuesta tiene una marca de tiempo,

Fig. 7 otra representación esquemática de un ejemplo de realización del método según la invención, en el que el servidor determina un identificador asignado al terminal móvil y crea un certificado digital que contiene el identificador,

Fig. 8 un diagrama de flujo para describir un ejemplo de realización del método según la invención y

Fig. 9 otro diagrama de flujo para describir otro ejemplo de realización del método según la invención, en el que el mensaje de solicitud comprende un mensaje de verificación.

La Fig. 1 muestra una representación esquemática de un método de verificación de billetes según el estado de la técnica. En el método presentado, se produce una comunicación unidireccional entre un primer terminal 10 móvil, que está asignado a un consumidor, y un segundo terminal 12, que está asignado a un controlador. En el ejemplo de

realización mostrado, el primer terminal móvil está diseñado como un teléfono inteligente. El segundo terminal 12, que en relación con la presente invención también se denomina dispositivo de control, está diseñado como un terminal móvil en el ejemplo mostrado. El primer terminal 10 móvil y el dispositivo 12 de control disponen en cada caso de un elemento 14, 16 de visualización. Los datos 18 del billete se muestran en forma de texto en el elemento 14 de visualización del primer terminal 10. Los datos 18 del billete pueden contener en particular información sobre el trayecto, la clase reservada (1ª clase o 2ª clase) o una reserva de asiento. Además, los datos del billete se muestran de forma cifrada mediante un código 20 de barras 2D en el elemento 14 de visualización del primer terminal 10. El primer terminal 10 envía los datos del billete al dispositivo 12 de control a través de un canal 24 de comunicación. El canal 24 de comunicación puede estar diseñado como un canal de comunicación óptico. El dispositivo 12 de control puede leer los datos del billete almacenados en el primer terminal 10 a través de una cámara o un escáner de código de barras (ambos no mostrados en la Fig. 1). A continuación, se evalúan y comprueban los datos del billete. Por ejemplo, se puede comparar la ruta reservada con la ruta real para comprobar si el pasajero está en el tren correcto. Si los datos del billete son correctos y el pasajero dispone de una autorización válida para utilizar el medio de transporte seleccionado, se puede mostrar un mensaje de confirmación en el elemento 16 de visualización del segundo terminal 12. De esta manera, el revisor sabe que el pasajero tiene un billete válido.

La Fig. 2 muestra una representación esquemática de un ejemplo de realización del método según la invención, en el que la comunicación entre el dispositivo 12 de control y el terminal 10 es bidireccional. El dispositivo 12 de control puede enviar datos al primer terminal 10 a través de un primer canal 22 de comunicación. El primer terminal 10 puede enviar datos al dispositivo 12 de control a través de un segundo canal 24 de comunicación. Los dos canales 22, 24 de comunicación pueden ser idénticos. Por ejemplo, ambos canales de comunicación pueden basarse en el estándar de transmisión NFC. También se puede prever que el primer canal 22 de comunicación esté basado en el estándar de transmisión NFC y el segundo canal 24 de comunicación esté diseñado como un canal de comunicación óptico. De esta manera, el mensaje A de solicitud puede enviarse a través de un canal de comunicación NFC, mientras que el mensaje B de respuesta se muestra como un código de barras y es leído ópticamente por el dispositivo 12 de control. La comunicación bidireccional durante la verificación de billetes puede aumentar la seguridad, como se muestra en las siguientes figuras.

La Fig. 3 muestra un ejemplo de realización concreto del método según la invención, en el que tanto el dispositivo 12 de control como el primer terminal 10 móvil están diseñados como teléfonos inteligentes. Según el método mostrado, el dispositivo 12 de control envía primero un mensaje A de solicitud al primer terminal 10 a través del primer canal 22 de comunicación. A continuación, el primer terminal 10 envía un mensaje B de respuesta al dispositivo 12 de control a través del segundo canal 24 de comunicación. El mensaje B de respuesta es firmado por el primer terminal 10. Mediante la firma del mensaje B de respuesta, el dispositivo 12 de control puede comprobar si el mensaje B de respuesta fue realmente creado por el primer terminal 10 o si el contenido del mensaje B de respuesta puede haber sido manipulado. La firma del mensaje B de respuesta por el primer terminal 10 se realiza utilizando una clave privada del primer terminal 10. Al comprobar el mensaje B de respuesta, se utiliza una clave pública del primer terminal 10 para comprobar la autenticidad del mensaje B de respuesta. Esta clave pública puede, por ejemplo, almacenarse previamente en el dispositivo 12 de control. Alternativamente, se puede prever que el mensaje B de respuesta contenga la clave pública. Si la firma del mensaje B de respuesta ha podido ser verificada por el dispositivo 12 de control y los datos del billete también son correctos, se puede mostrar un mensaje de confirmación en el elemento 16 de visualización del dispositivo 12 de control.

Además, la Fig. 4 muestra otro ejemplo de realización del método según la invención, en el que el primer terminal 10 y el dispositivo 12 de control se comunican con un servidor 26. En esta realización se puede prever en particular que la clave 28 pública del primer terminal 10 se almacene en un servidor 26 a través de un tercer canal 30 de comunicación. Esto puede ocurrir, por ejemplo, cuando un consumidor se registra en una empresa de transporte. En este caso, todas las claves públicas de cada consumidor se almacenan en el servidor 26. Durante la inspección del billete, el dispositivo 12 de control puede entonces acceder al servidor 26 y a la clave 28 pública del primer terminal 10 móvil almacenada en el mismo a través de un cuarto canal 31 de comunicación. El dispositivo 12 de control puede entonces verificar la firma del mensaje B de respuesta utilizando la clave 28 pública. Si esto se puede verificar y los datos del billete también son correctos, se puede mostrar un mensaje de confirmación en el elemento 16 de visualización del segundo terminal 12.

La Fig. 5 muestra otra representación esquemática de un ejemplo de realización del método según la invención. En este ejemplo de realización, el dispositivo 12 de control envía el mensaje A de solicitud al primer terminal 10 a través del primer canal 22 de comunicación. El primer terminal 10 envía entonces un mensaje B de respuesta al dispositivo 12 de control. El mensaje B de respuesta contiene un certificado 32 digital. El certificado 32 digital puede ser en particular un certificado de clave pública. El certificado 32 digital puede contener información sobre el emisor del certificado (por ejemplo, su nombre), el consumidor (por ejemplo, su nombre, fecha de nacimiento y dirección), el terminal del consumidor (por ejemplo, el ID del terminal) o el período de validez del certificado (por ejemplo, 3 meses). El certificado digital también puede contener la clave 28 pública del primer terminal 10 o la clave pública del emisor del certificado. Además, el certificado 32 digital puede contener una firma digital del emisor.

La Fig. 6 muestra otro ejemplo de realización del método según la invención, presentando el mensaje B de respuesta en este ejemplo de realización una marca de tiempo. La marca de tiempo documenta cuándo se generó el mensaje B de respuesta. El dispositivo 12 de control puede así comprobar, por ejemplo, si el mensaje B de respuesta se generó

después de que el dispositivo 12 de control enviara un mensaje A de solicitud al primer terminal 10, o si el mensaje B de respuesta ya se generó antes de que el dispositivo 12 de control enviara el mensaje A de solicitud al terminal 10. Si el mensaje B de respuesta ya se ha generado antes de que se haya transmitido el mensaje A de solicitud al primer terminal, se puede suponer que la autenticidad del billete es al menos dudosa. En este caso, puede aparecer una notificación correspondiente en el elemento 16 de visualización del segundo terminal 12, recomendando que el controlador compruebe también manualmente los datos de identificación del pasajero además del método de verificación según la invención. Una ventaja esencial del método según la invención es que esta verificación de los datos de identificación, que requiere más tiempo, solo debe realizarse si se observan anomalías durante el método de verificación de billetes según la invención. En el ejemplo de realización mostrado en la Fig. 6, alternativamente se puede prever que la marca 34 de tiempo se compare con la hora actual y el billete electrónico se clasifique como inválido si la marca de tiempo es más antigua que un período de tiempo predeterminado (por ejemplo, 1 minuto o 5 minutos). Por lo tanto, si el mensaje B de respuesta se generó hace 2 horas, esto puede considerarse una indicación de que el mensaje B de respuesta o el billete electrónico no es válido. En este caso, los datos de identificación del pasajero también se pueden comprobar manualmente.

Otro ejemplo de realización preferido del método según la invención se muestra en la Fig. 7. En este ejemplo de realización, el mensaje B de respuesta contiene un certificado 32 digital. El certificado 32 digital fue generado previamente por el servidor 26. El certificado 32 digital se puede generar, por ejemplo, cuando el usuario se registra en la empresa de transporte. Durante el registro, el servidor 26 determina un identificador 36 inequívoco del primer terminal 10. Este identificador 36 puede ser, por ejemplo, una huella digital de *hardware*. Como ya se ha explicado anteriormente, esto se puede determinar, por ejemplo, a través del número de serie de un componente de *hardware*, en particular un procesador o una RAM, del primer terminal 10. En otras palabras, el primer terminal 10 puede transmitir un identificador 36 al servidor 26 al registrarse en la empresa de transporte. Alternativamente, el servidor puede leer el identificador del primer terminal 10. El servidor 26 genera entonces un certificado 32 digital que contiene el identificador 36 del primer terminal 10. El identificador 36 permite identificar de forma inequívoca el primer terminal 10 durante el proceso de verificación del billete posterior. El certificado 32 digital está provisto preferiblemente de una firma digital. La comunicación entre el primer terminal 10 y el servidor 26 se realiza a través de un tercer canal 30 de comunicación. Cuando el billete electrónico es comprobado por el dispositivo 12 de control, se puede comprobar el mensaje B de respuesta y el certificado 32 digital contenido en el mismo. Durante la comprobación del billete electrónico también se lee el identificador del primer terminal 10, tal y como lo hacía hasta ahora el servidor 20. Si el dispositivo 12 de control llega a la conclusión de que el identificador del primer terminal 10 difiere del identificador almacenado en el certificado 32 digital, esto puede interpretarse como una indicación de que el billete electrónico no es válido o que el pasajero no dispone de una autorización válida para utilizar el medio de transporte. En este caso, se podrá mostrar una notificación en el elemento 16 de visualización del dispositivo 12 de control, recomendando al revisor comprobar manualmente los datos de identificación del pasajero. Alternativamente, se puede prever que el ID almacenado en el certificado digital se compare con el ID almacenado en el billete electrónico. En este caso, una discrepancia entre el ID del certificado digital y el ID almacenado en el billete puede interpretarse como un indicio de que el billete electrónico no es válido o que el pasajero no dispone de una autorización válida para utilizar el medio de transporte seleccionado. En principio, existen tres formas diferentes de verificar el ID (comparación del ID almacenado en el billete con el ID almacenado en el certificado digital, comparación del ID almacenado en el billete con el ID leído por el primer terminal, comparación del ID almacenado en el certificado digital con el ID leído por el primer terminal). En el ejemplo de realización ilustrado del método según la invención, opcionalmente se puede prever que el dispositivo 12 de control se comunique con el servidor 26 a través de un cuarto canal 31 de comunicación. Esto se puede utilizar, por ejemplo, para consultar la clave pública del servidor 26 o del primer terminal 10. Como alternativa, también se puede prever que las claves mencionadas anteriormente se almacenen de serie en el dispositivo 12 de control.

La Fig. 8 muestra las etapas individuales de un ejemplo de realización del método según la invención. En respuesta a un mensaje A de solicitud procedente del dispositivo 12 de control (segundo terminal), el primer terminal 10 genera un mensaje B de respuesta firmado. Al comprobar la firma contenida en el mensaje B de respuesta, el dispositivo 12 de control puede comprobar si el mensaje B de respuesta fue realmente generado por el primer terminal 10 y está intacto, o si la firma fue generada por otro dispositivo o el contenido del mensaje B de respuesta fue manipulado (principio de verificación de identidad e integridad). Para verificar la firma, el dispositivo de control requiere la clave 28 pública del primer terminal 10. Esta clave 28 pública puede incluirse opcionalmente en el mensaje B de respuesta. Alternativamente, también se puede prever que esta clave 28 pública se almacene en un servidor al que pueda acceder el dispositivo 12 de control.

Finalmente, la Fig. 9 muestra las etapas individuales de otro ejemplo de realización del método según la invención. En este ejemplo de realización, el mensaje B de solicitud, que se envía desde el dispositivo 12 de control al primer terminal 10, contiene un mensaje de verificación. El mensaje de verificación puede ser en particular un mensaje de texto o una secuencia de números generados por el dispositivo 12 de control. En particular, puede ser un número aleatorio particularmente largo generado por el dispositivo 12 de control. El primer terminal 10 recibe este mensaje de verificación y lo integra en el mensaje B de respuesta, que luego es firmado por el primer terminal 10. El primer terminal 10 envía entonces el mensaje B de respuesta firmado, que contiene el mensaje de verificación, al dispositivo 12 de control. El dispositivo 12 de control puede así comprobar si el primer terminal 10 ha recibido realmente el mensaje de verificación y también si dispone de una clave privada correspondiente para generar una firma digital. Esto hace que sea prácticamente imposible para el primer terminal 10 enviar un mensaje B de respuesta que fue generado

previamente por un tercero, ya que un tercero no puede saber qué mensaje de verificación es generado por el dispositivo 12 de control y enviado al primer terminal 10. Por lo tanto, el ejemplo de realización del método según la invención mostrado en la Fig. 9 puede garantizar un nivel de seguridad particularmente alto durante la comprobación de billetes electrónicos.

Lista de signos de referencia

10	primer terminal
12	segundo terminal
14	elemento de visualización del primer terminal
16	elemento de visualización del segundo terminal
18	datos del billete en formato de texto
20	código de barras con datos del billete
22	primer canal de comunicación
24	segundo canal de comunicación
26	servidor
28	clave pública
30	tercer canal de comunicación
31	cuarto canal de comunicación
32	certificado digital
34	marca de tiempo
36	identificador
S100	método según la invención en un primer ejemplo de realización
S110	primera etapa del método según el primer ejemplo de realización
S120	segunda etapa del método según el primer ejemplo de realización
S130	tercera etapa del método según el primer ejemplo de realización
S140	cuarta etapa del método según el primer ejemplo de realización
S200	método según la invención en un segundo ejemplo de realización
S210	primera etapa del método según el segundo ejemplo de realización
S220	segunda etapa del método según el segundo ejemplo de realización
S230	tercera etapa del método según el segundo ejemplo de realización
S240	cuarta etapa del método según el segundo ejemplo de realización
A	mensaje de solicitud
B	mensaje de respuesta

REIVINDICACIONES

1. Método para comprobar de forma segura un billete electrónico, en particular un billete electrónico de autobús y/o de tren, en el que el billete electrónico se almacena en un primer terminal (10) móvil asignado a un consumidor final, y el billete se comprueba utilizando un segundo terminal (12) asignado a un revisor o a un sistema de control, el método comprende las siguientes etapas:

- enviar un mensaje (A) de solicitud desde el segundo terminal (12) al primer terminal (10) a través de un primer canal (22) de comunicación;

- enviar un mensaje (B) de respuesta desde el primer terminal (10) al segundo terminal (12) a través de un segundo canal (24) de comunicación, estando firmado el mensaje (B) de respuesta por el primer terminal (10), y siendo el segundo canal (24) de comunicación idéntico al primer canal (22) de comunicación o diferente del primer canal (22) de comunicación;

- verificar el mensaje (B) de respuesta firmado por el segundo terminal (12); y

- confirmar la autenticidad del mensaje (B) de respuesta por el segundo terminal (12), si el segundo terminal (12) pudo verificar previamente la autenticidad de la firma;

- el mensaje (A) de solicitud comprende un número aleatorio de longitud L generado por el segundo terminal (12), donde L >=1, y el mensaje (B) de respuesta incluye una representación del número aleatorio generado por el segundo terminal (12) cifrado utilizando una clave privada del primer terminal (10);

- el mensaje (B) de respuesta incluye un certificado (32) digital que procede del proveedor de servicios que ha emitido el billete electrónico o de una entidad clasificada como fiable por el proveedor de servicios;

- el mensaje (B) de respuesta comprende un billete electrónico que, además de la información del billete, también comprende un primer identificador digital del primer terminal (10), y el billete electrónico comprende una firma digital del proveedor de servicios;

- el mensaje (B) de respuesta comprende, además del billete electrónico, un segundo identificador digital del primer terminal (10) generado por el primer terminal (10); y

- el segundo terminal (12) confirma la autenticidad del mensaje (B) de respuesta solo si el primer identificador contenido en el billete electrónico y el segundo identificador generado por el primer terminal (10) son idénticos.

2. Método según la reivindicación 1, caracterizado por que el mensaje (B) de respuesta comprende una marca (34) de tiempo, y por que la autenticidad del mensaje (B) de respuesta es confirmada por el dispositivo de control solo si la antigüedad de la marca (34) de tiempo está por debajo de un valor umbral predeterminado.

3. Método según la reivindicación 1, caracterizado por que el mensaje (B) de respuesta contiene un certificado (32) digital en donde se almacena un indicador de seguridad que caracteriza el cumplimiento de los requisitos de seguridad predeterminados por parte del primer terminal.

4. Método según la reivindicación 3, caracterizado por que el indicador de seguridad se implementa como una bandera de seguridad binaria, que

- tiene un valor de 1, si una comprobación de seguridad previa del primer terminal (10) ha demostrado que el primer terminal (10) cumple los requisitos de seguridad predeterminados, y

- tiene un valor de 0, si la comprobación de seguridad previa del primer terminal (10) ha demostrado que el primer terminal (10) no cumple los requisitos de seguridad predeterminados.

5. Método según cualquiera de las reivindicaciones 1 a 4, caracterizado por que el primer terminal (10) y el segundo terminal (12) comprenden cada uno un módulo de comunicación de campo cercano (módulo NFC), y el primer canal (22) de comunicación se basa en la comunicación de campo cercano (NFC).

6. Método según cualquiera de las reivindicaciones 1 a 5, caracterizado por que el módulo NFC del segundo terminal (12) emula una etiqueta NFC.

7. Método según cualquiera de las reivindicaciones 1 a 6, caracterizado por que el segundo canal (24) de comunicación se basa en comunicación de campo cercano, NFC.

8. Método según cualquiera de las reivindicaciones 1 a 7, caracterizado por que el mensaje (B) de respuesta contiene datos biométricos del consumidor, en particular datos relacionados con una huella dactilar, una voz, rasgos de una cara o un patrón de iris.

9. Método según cualquiera de las reivindicaciones 1 a 8, caracterizado por que el mensaje (B) de respuesta comprende una imagen fotográfica del consumidor o una imagen fotográfica de la cara del consumidor.

10. Método según cualquiera de las reivindicaciones 1 a 9, caracterizado por que el segundo terminal (12) comprende un elemento de memoria y/o está conectado con un elemento de memoria externo que almacena una lista de datos de identificación para los cuales la probabilidad de falta de autenticidad excede un umbral de probabilidad predeterminado.

11. Método según cualquiera de las reivindicaciones 1 a 10, caracterizado por que la selección del primer canal (22) de comunicación y del segundo canal (24) de comunicación está automatizada.

12. Método según cualquiera de las reivindicaciones 1 a 11, caracterizado por que el mensaje (B) de respuesta incluye información sobre una huella digital del primer terminal (10).

13. Dispositivo de control para comprobar un billete electrónico, en particular un billete electrónico de autobús y/o de tren, estando el billete electrónico almacenado en un primer terminal (10) móvil asociado a un consumidor final, que comprende al menos un procesador, una memoria y un módulo de comunicación, estando configurado el dispositivo de control para

- enviar un mensaje (A) de solicitud al primer terminal (10) a través de un primer canal (22) de comunicación;

- recibir un mensaje (B) de respuesta desde el primer terminal (10) a través de un segundo canal (24) de comunicación, estando firmado el mensaje (B) de respuesta por el primer terminal (10), y siendo el segundo canal de comunicación idéntico al primer canal de comunicación o diferente del primer canal (22) de comunicación;

- verificar el mensaje (B) de respuesta firmado; y

- confirmar la autenticidad del mensaje (B) de respuesta si la autenticidad de la firma pudo ser confirmada previamente por el dispositivo de control;

- el mensaje (A) de solicitud comprende un número aleatorio de longitud L generado por el segundo terminal (12), donde L >=1, y el mensaje (B) de respuesta incluye una representación del número aleatorio generado por el segundo terminal (12) cifrado utilizando una clave privada del primer terminal (10);

- el mensaje (B) de respuesta incluye un certificado (32) digital que procede del proveedor de servicios que ha emitido el billete electrónico o de una entidad clasificada como fiable por el proveedor de servicios;

- el mensaje (B) de respuesta comprende un billete electrónico que, además de la información del billete, también comprende un primer identificador digital del primer terminal (10), y el billete electrónico comprende una firma digital del proveedor de servicios;

- además del billete electrónico, el mensaje (B) de respuesta comprende un segundo identificador digital del primer terminal (10) generado por el primer terminal (10); y

- el segundo terminal (12) confirma la autenticidad del mensaje (B) de respuesta solo si el primer identificador contenido en el billete electrónico y el segundo identificador generado por el primer terminal (10) son idénticos.

14. Dispositivo de control según la reivindicación 13, caracterizado por que el módulo de comunicación comprende un módulo NFC, un módulo Bluetooth, una cámara y/o una pantalla.

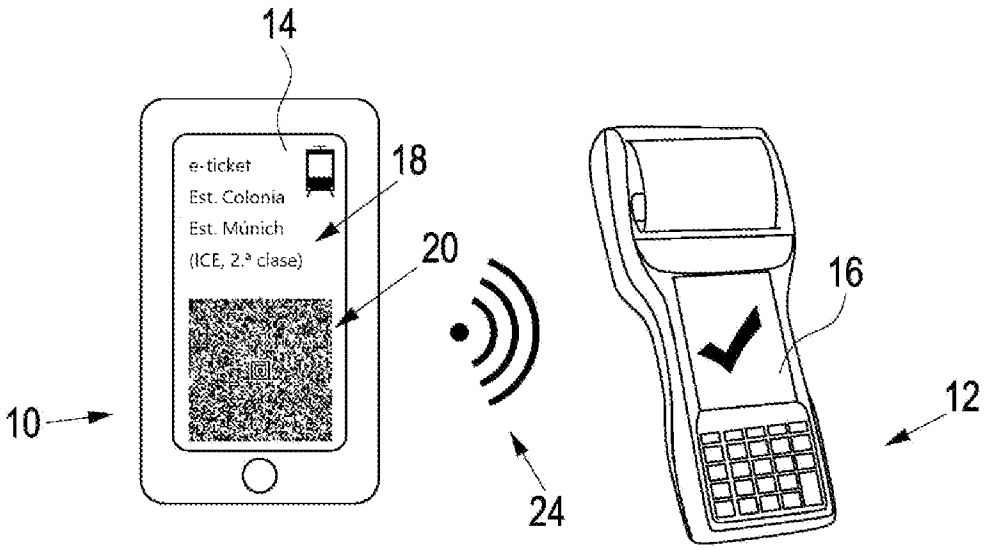
14
e-ticket
Est. Colonia
Est. Múnich
(ICE, 2.ª clase)
18
20
16
10
12
24

Fig. 1

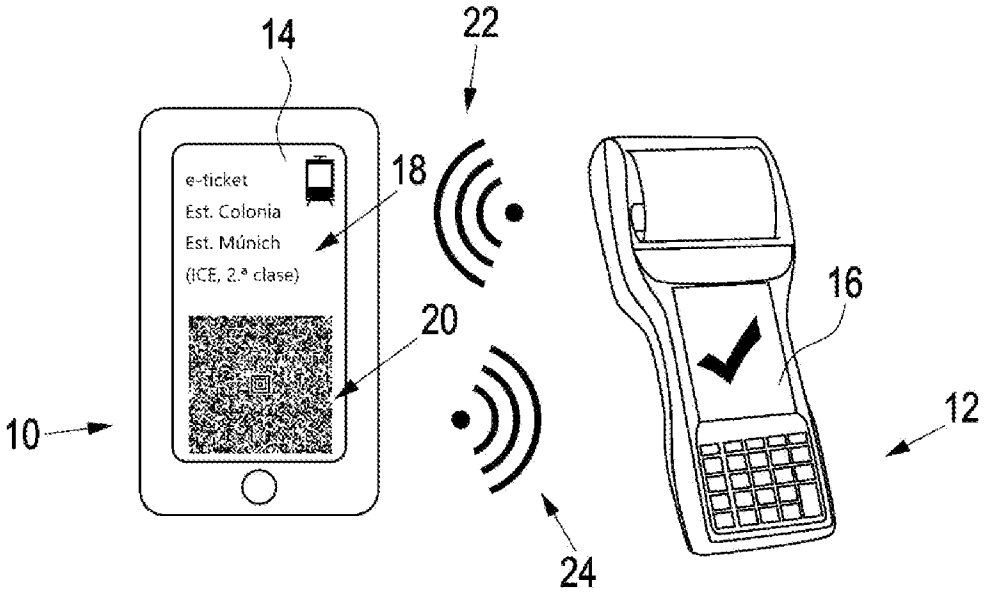
14
22
e-ticket
Est. Colonia
Est. Múnich
(ICE, 2.ª clase)
18
20
16
10
12
24

Fig. 2

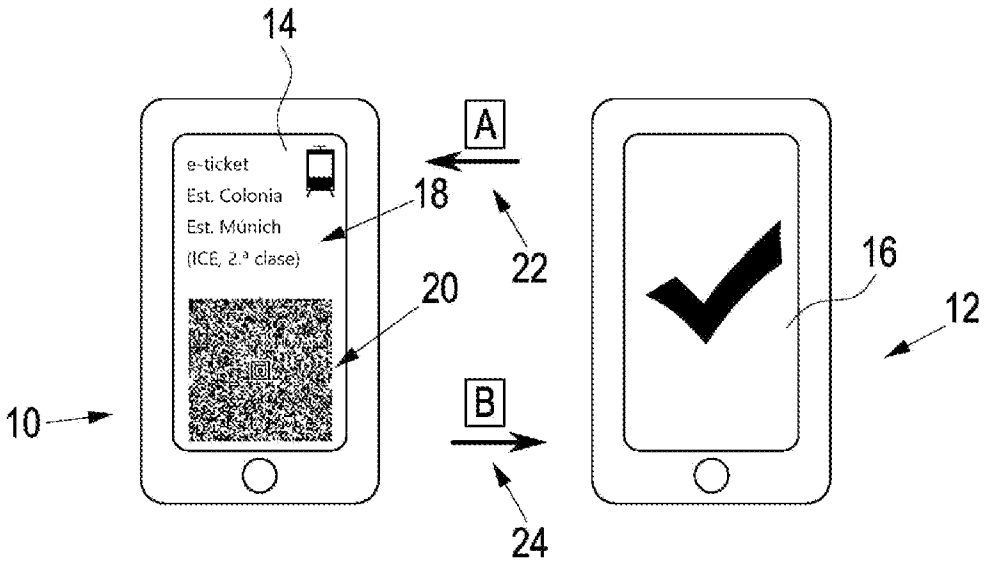
14
e-ticket
Est. Colonia
Est. Múnich
(ICE, 2.ª clase)
A
18
22
20
16
12
10
B
24

Fig. 3

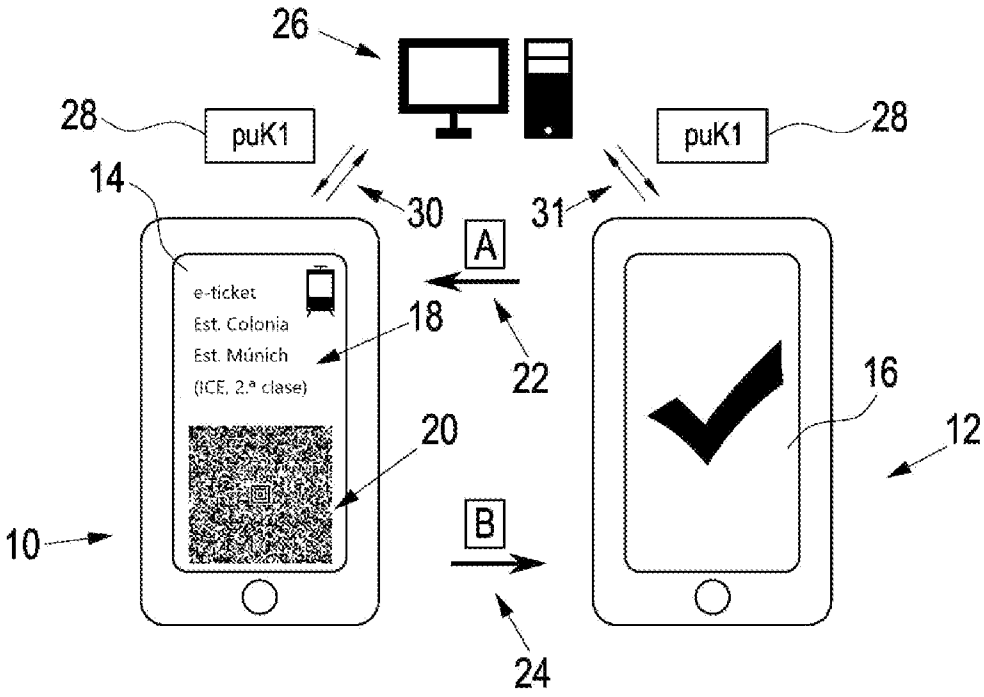
26
28
puK1
puK1
28
14
30
31
A
e-ticket
Est. Colonia
Est. Múnich
(ICE, 2.ª clase)
18
22
16
20
12
10
B
24

Fig. 4

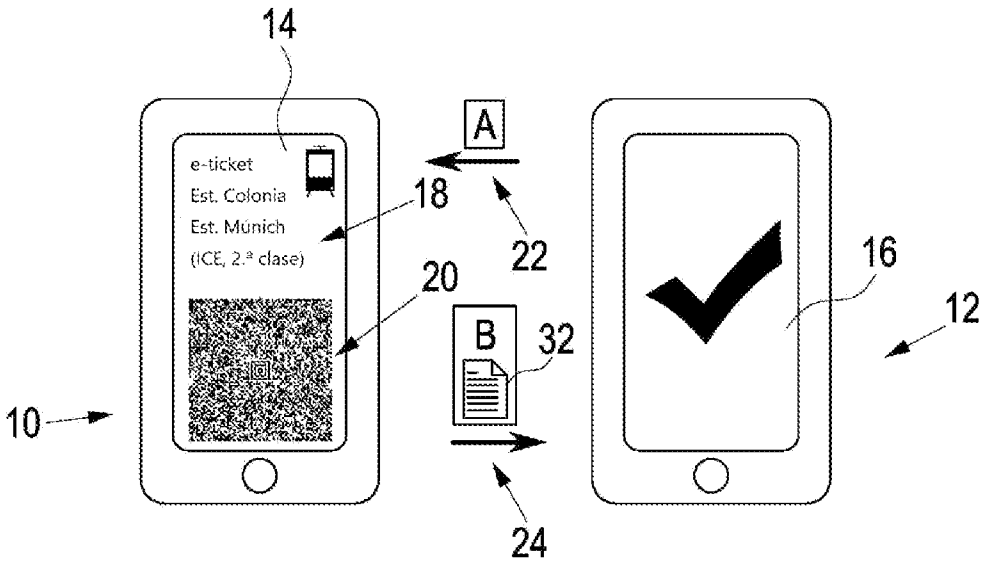
14
e-ticket
Est. Colonia
Est. Múnich
(ICE, 2.ª clase)
18
20
A
22
B
32
24
10
16
12

Fig. 5

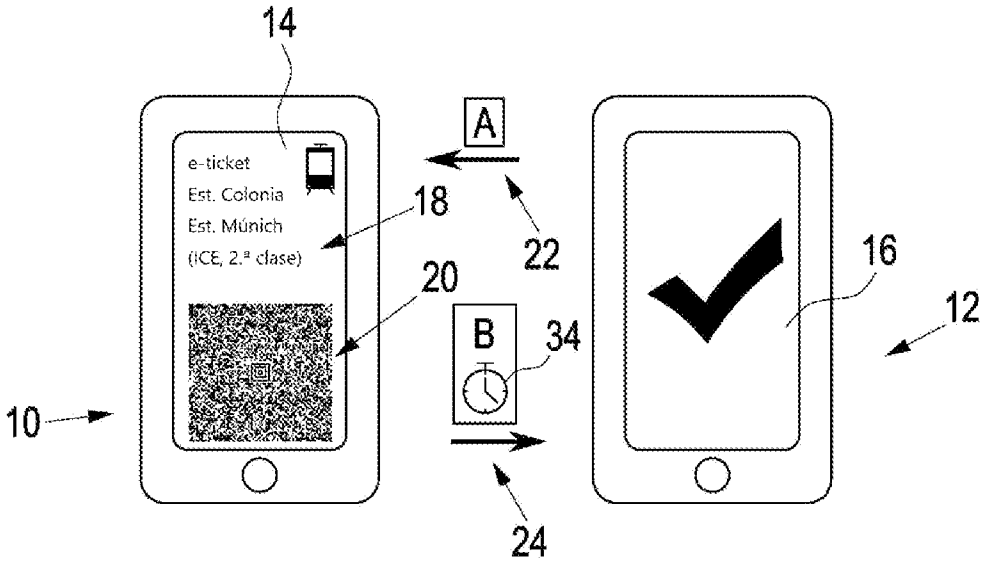
14
e-ticket
Est. Colonia
Est. Múnich
(ICE, 2.ª clase)
18
20
A
22
B
34
24
10
16
12

Fig. 6

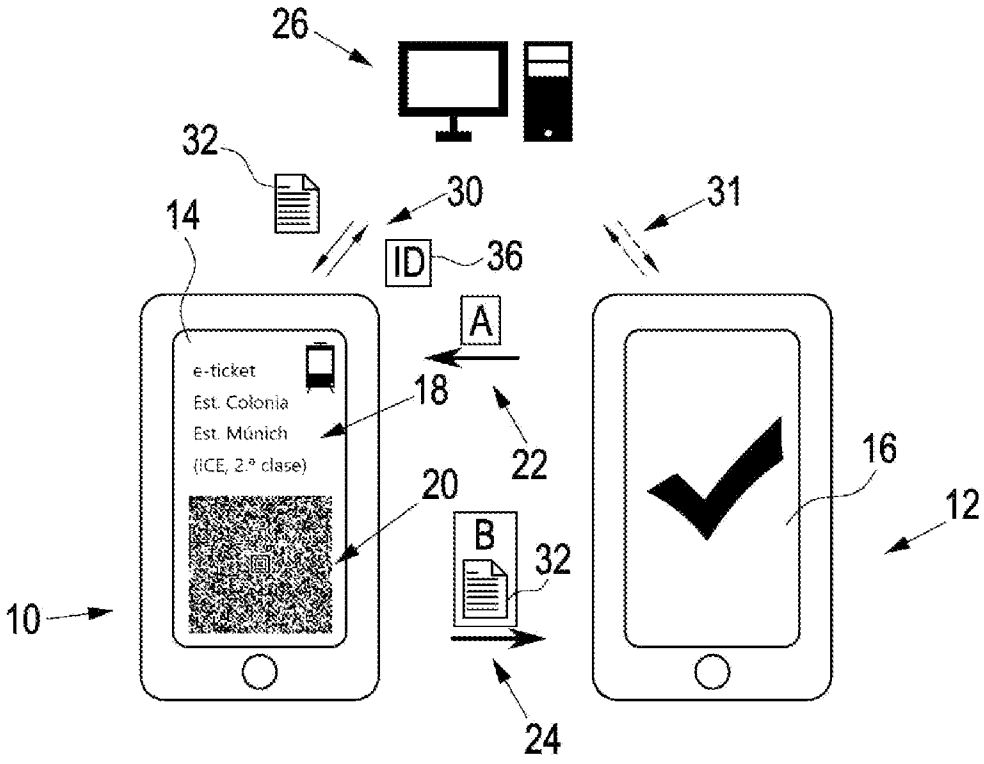
26
32
30
31
14
ID
36
A
e-ticket
Est. Colonia
Est. Múnich
(ICE, 2.ª clase)
18
22
16
12
20
B
32
10
24

Fig. 7

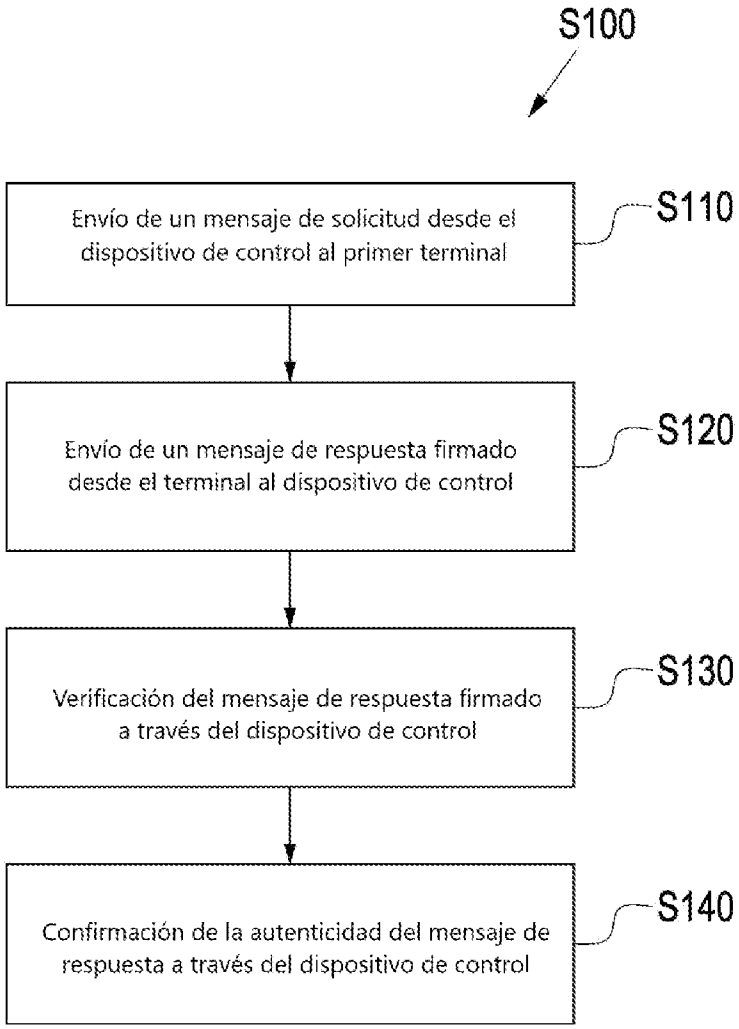
S100
Envío de un mensaje de solicitud desde el dispositivo de control al primer terminal
S110
Envío de un mensaje de respuesta firmado desde el terminal al dispositivo de control
S120
Verificación del mensaje de respuesta firmado a través del dispositivo de control
S130
Confirmación de la autenticidad del mensaje de respuesta a través del dispositivo de control
S140

Fig. 8

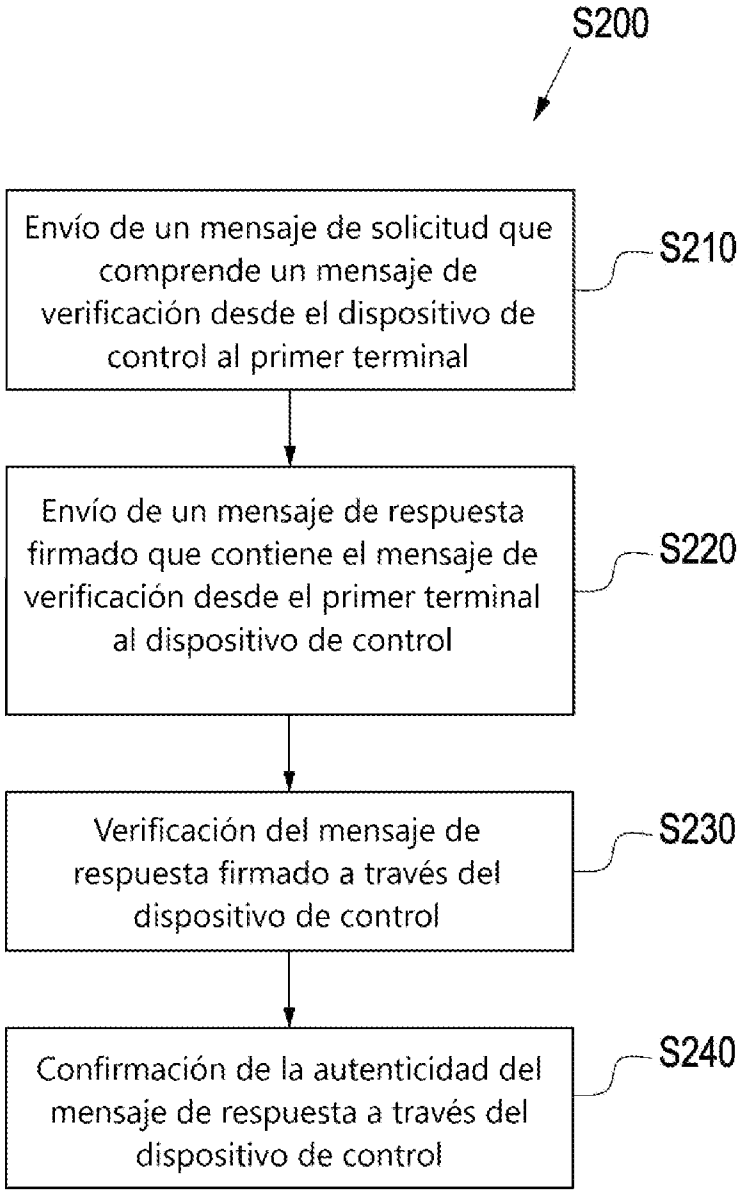
S200
Envío de un mensaje de solicitud que comprende un mensaje de verificación desde el dispositivo de control al primer terminal
S210
Envío de un mensaje de respuesta firmado que contiene el mensaje de verificación desde el primer terminal al dispositivo de control
S220
Verificación del mensaje de respuesta firmado a través del dispositivo de control
S230
Confirmación de la autenticidad del mensaje de respuesta a través del dispositivo de control
S240

Fig. 9