(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 941 982**

(51) Int. CI.:

G09C 5/00 (2006.01)
G06F 21/32 (2013.01)
G07C 9/25 (2010.01)
H04L 9/32 (2006.01)
G06Q 50/26 (2012.01)
G06K 9/00 (2012.01)
H04L 9/40 (2012.01)
G06V 40/16 (2012.01)
G06V 40/70 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **10.10.2018 PCT/NL2018/050669**

(87) Fecha y número de publicación internacional: **18.04.2019 WO19074366**

(96) Fecha de presentación y número de la solicitud europea: **10.10.2018 E 18812342 (6)**

(97) Fecha y número de publicación de la concesión europea: **11.01.2023 EP 3695397**

(54) Título: **Autenticación de una persona usando una tarjeta de identidad virtual**

(30) Prioridad:

10.10.2017 NL 2019698

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
29.05.2023

(73) Titular/es:

IDEMIA THE NETHERLANDS B.V. (100.0%)
Oudeweg 32
2031 CC Haarlem, NL

(72) Inventor/es:

DE VOS, JOURI;
VAN PROOIJEN, JOOST;
BOUATOU, VINCENT y
WATTEBLED, CYRIL

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Autenticación de una persona usando una tarjeta de identidad virtual

Campo de la invención

La presente invención se refiere a un método y sistema para autenticar a un usuario, usando un terminal de inspección que está provisto de una cámara digital, en el que la información que incluye una representación visual reconocible por humanos de los datos biométricos del usuario se captura usando la cámara digital, se genera un descriptor de características biométricas a partir de los datos biométricos capturados del usuario, y el descriptor de características se transmite a un servidor de inspección adaptado para validar si el descriptor de características biométricas transmitido corresponde a un descriptor de características biométricas almacenado centralmente de datos biométricos del usuario. La invención proporciona además un método para registrar, en un servidor de inspección de este tipo, información que permite autenticar a un usuario.

Antecedentes de la técnica

A partir del documento DE 10 2014 100 463 A1 se conoce un método para identificar a un usuario por medio de un dispositivo de comunicación, tal como un teléfono inteligente, en donde se asocia un documento de identificación con el usuario. El método conocido comprende: capturar una característica biométrica del usuario por medio del dispositivo de comunicación para obtener una característica biométrica capturada; transmitir, por el dispositivo de comunicación, la característica biométrica capturada a un servicio de identificación electrónica a través de una red de comunicaciones; y comparar la característica biométrica capturada con una característica de referencia biométrica por el servicio de identificación electrónica, para identificar al usuario. En una realización, la característica biométrica se captura como una secuencia de imágenes del usuario usando una cámara digital del dispositivo de comunicación. Además de requerir una potencia de procesamiento significativa en el servicio de identificación electrónica, este método es propenso a errores ya que la apariencia del usuario cambia con el tiempo. En una realización alternativa del método conocido, los datos biométricos se leen directamente del documento de identificación, por ejemplo, usando tecnología RFID o NFC, que, sin embargo, requeriría que el usuario tenga a mano el documento de identificación para ser identificado.

El documento US 2016/0239653 A1 describe un método para autenticar una credencial digital de un portador mediante un dispositivo de validación. El método incluye capturar la credencial del portador, que puede tener la forma de un código QR, por el dispositivo de validación y transmitir a un servicio de validación la credencial del portador con una credencial del validador vinculada al dispositivo de validación. El método también incluye, en el servicio de validación, validar la credencial del portador y la credencial de validación y, si la credencial del validador es válida, usar la credencial del portador para acceder a un elemento de datos de un perfil digital y crear un mensaje electrónico para su transmisión al dispositivo de validación, indicando el mensaje electrónico el elemento de datos y que comprende una credencial de validador reciente generada por el servicio de validación. El mensaje electrónico puede contener además una foto del usuario. Es un objeto de la presente invención proporcionar un método y sistema para autenticar a un usuario de un terminal de usuario móvil, sin requerir que el terminal de usuario móvil pueda recibir datos de un terminal de inspección que se usa durante la autenticación.

El documento US 2011/089233 divulga un documento de identificación que está vinculado a una persona, particularmente para la autenticación de autorizaciones o calificaciones de la persona. El documento de identificación incluye un dispositivo de comunicación móvil que puede mostrar imágenes y asignarse a la persona, en donde un conjunto de datos de identificación que se almacena en la memoria se asigna a los datos que se almacenan y administran en una base de datos central, y en donde un atributo de reconocimiento óptico que se asigna al conjunto de datos de identificación se puede visualizar en la unidad de visualización del dispositivo de comunicación.

El documento US 2015/086088 divulga un método para verificar que un usuario firme un documento. En particular, ciertas realizaciones divulgadas se refieren a verificar que un usuario que firma un documento corresponde a un usuario autenticado previamente, habiendo sido autenticado previamente el usuario usando una fuente de datos de identidad legibles por máquina. La verificación se puede realizar recibiendo, desde la fuente de datos de identidad legibles por máquina, primeros datos de imagen digital indicativos de una primera imagen del usuario previamente autenticado y primeros datos de identidad, y recibiendo de una cámara, una segunda imagen capturada que comprende segundos datos de imagen digital que corresponden al usuario. En respuesta a que se determina que la primera imagen y la segunda imagen representan al mismo usuario, se generan datos de verificación y se asocian con el documento.

Es otro objeto de la invención proporcionar un método de este tipo que permita al usuario seleccionar qué información se comparte para completar la autenticación del usuario. También en vista del Reglamento General de Protección de Datos (UE) 2016/67, es deseable que los terminales de inspección solo puedan obtener acceso a los datos de personalización para los que el usuario haya dado permiso.

Adicionalmente, la invención pretende proporcionar un método de este tipo que esté protegido contra ataques de reproducción.

Sumario de la invención

Para este fin, de acuerdo con un primer aspecto, la invención proporciona un método de autenticación de un usuario de un terminal de usuario móvil que está provisto de una pantalla, en donde el método comprende, usar un terminal de inspección provisto de una cámara digital, las etapas de: i) capturar, con la cámara digital, información presentada en la pantalla del terminal de usuario, comprendiendo la información: una representación visual reconocible por humanos de los datos biométricos del usuario, un identificador de documento para identificar un documento de identidad que ha sido expedido para el usuario, un perfil de usuario que especifica un subconjunto de datos de personalización derivados del documento de identidad, que van a proporcionarse al terminal de inspección, y un sello de un solo uso; ii) calcular un descriptor de características biométricas a partir de la representación visual reconocible por humanos capturada de los datos biométricos del usuario, en donde la representación visual reconocible por humanos de los datos biométricos del usuario corresponde a una imagen del usuario almacenada en el documento de identidad del usuario; iii) transmitir el identificador de documento capturado, el descriptor de características biométricas, el perfil de usuario y el sello de un solo uso a un servidor de inspección, en donde el servidor de inspección comprende o está conectado a un servidor de documentos de identidad (IDS) que almacena, para cada documento de identidad de una pluralidad de documentos de identidad expedidos a diferentes personas, datos de personalización acerca de la persona a la que se ha expedido el documento de identidad y un identificador de documento asociado que identifica de forma única el respectivo documento de identidad, en donde el servidor de inspección está adaptado para devolver una señal de "autenticación aprobada" junto con un subconjunto de los datos de personalización definidos por el perfil de usuario, si

a) el descriptor de características biométricas transmitido corresponde a un descriptor de características biométricas de datos biométricos almacenados en el IDS para un documento de identidad para el cual el identificador de documento asociado corresponde al identificador de documento transmitido, y

b) el sello de un solo uso no se ha recibido antes para el identificador de documento transmitido;

iv) en el terminal de inspección, esperar la señal de "autenticación aprobada", y tras la recepción de dicha señal, generar una señal audible y/o visual que indica que se ha aprobado la autenticación del usuario para el objetivo de autenticación especificado.

Ejemplos de un documento de identidad cuyos datos de personalización, por ejemplo, nombre completo, altura, género, firma, fecha y lugar de nacimiento y/o número de seguridad social, pueden almacenarse en el IDS, incluyen un pasaporte, un permiso de conducción y una cédula de identidad nacional. Típicamente, tales documentos de identidad se expiden por una autoridad central, tal como un gobierno o municipio, que conserva una copia almacenada centralmente de los datos de personalización correspondientes a cada documento de identidad expedido. Un ejemplo típico de un terminal de usuario es un teléfono inteligente que está provisto de una pantalla en la que se puede mostrar la representación visual reconocible por humanos de los datos biométricos del usuario y la información adicional. La información adicional, es decir, el identificador de documento, el perfil de usuario y el sello de un solo uso, se presentan preferentemente en la pantalla en un formato legible por máquina, y puede ser difícil de descifrar por una persona sin usar un ordenador. Los datos biométricos del usuario generalmente comprenden o consisten en una imagen del usuario, normalmente una imagen de la cara del usuario, por ejemplo, una ID con foto, o de una o más de sus huellas digitales, que una persona puede comprobar visualmente sin requerir equipo adicional, tal como una cinta métrica, equipo de escaneo 3D. Por tanto, una persona que opera el terminal de inspección de usuario puede comparar fácilmente las características biométricas en vivo de una persona que se encuentra directamente frente a él o ella con los datos biométricos mostrados en el terminal de usuario. Los datos biométricos mostrados en el terminal de usuario, junto con el identificador de documento, el perfil de usuario y el sello de un solo uso forman de esta manera una tarjeta de identidad virtual que puede ser mostrada por un usuario que lo solicite. Esta tarjeta de identidad virtual está disponible para el usuario en cualquier lugar donde el usuario lleve el terminal de usuario, y no requiere que el usuario lleve el documento de identidad real. Además, la autenticación de un usuario de acuerdo con el método de la invención no requiere el almacenamiento central de la representación visual reconocible por humanos de los datos del usuario. Aunque para cada usuario se almacena un descriptor de características biométricas en el IDS, el descriptor de características se calcula de tal manera que no es posible calcular a partir del mismo una representación visual reconocible por humanos de los datos biométricos del usuario que permitiría que el usuario sea identificado. Por tanto, la imagen del usuario, por ejemplo, de su cara, que se almacena en el documento de identidad del usuario, no necesita copiarse o almacenarse en el IDS o el servidor de inspección y, preferentemente, no se hace.

Sin embargo, los datos que permiten visualizar en la pantalla del terminal de usuario móvil una representación visual reconocible por humanos de los datos biométricos del usuario, se almacenan preferentemente en una memoria del terminal de usuario móvil. Existen documentos de identidad que almacenan una representación digital de la cara de un usuario, además de su representación visual reconocible por humanos, lo que permite leer una copia exacta de la representación digital y almacenarla en una memoria del terminal de usuario que se usará para mostrar la imagen en una pantalla más adelante. Si el terminal de usuario está equipado con un lector inalámbrico, por ejemplo, un lector

NFC o RFID, el terminal de usuario puede leer directamente la representación digital exacta del documento. Alternativamente, la lectura puede llevarse a cabo usando un dispositivo de lectura separado, por ejemplo, que comprende un lector de NFC y/o RFID, y posteriormente transferirse al terminal de usuario, por ejemplo, a través de Internet, una conexión Bluetooth o similar. En cualquier caso, la descripción de la característica biométrica se calcula en la etapa ii) basándose en una representación visual reconocible por humanos capturada de los datos biométricos del usuario que corresponde a una imagen del usuario, tal como una fotografía de la cara del usuario, que se almacena en el documento de identidad del usuario.

La inclusión de un sello de un solo uso en la tarjeta de identidad virtual protege sustancialmente contra los ataques de reproducción.

Como la información que se presenta en la pantalla del terminal de usuario móvil al terminal de inspección se captura por una cámara del terminal de inspección, no hay necesidad de una conexión, tal como un conector de Internet o una conexión Bluetooth, para la transferencia de datos desde el terminal de inspección al terminal de usuario para llevar a cabo el método. En principio, las etapas i) - iv) del método pueden incluso llevarse a cabo sin que exista ninguna comunicación desde el servidor de inspección hacia el terminal móvil del usuario.

Dependiendo de un propósito de autorización pretendido, el usuario puede elegir entre diferentes perfiles de usuario que se presentarán en la pantalla, especificando cada uno de los cuales un subconjunto diferente de datos de personalización que van a proporcionarse al terminal de inspección. Por ejemplo, si el usuario desea usar la tarjeta de identidad virtual para identificarse ante un oficial de policía, los datos de personalización que se comparten pueden ser datos de personalización correspondientes a datos del documento de identidad correspondiente del usuario, tales como fecha y lugar de nacimiento, género, altura y/o número de seguro social. En otras circunstancias, es posible que el usuario no desee compartir tanta información. Por ejemplo, en muchos hoteles, se requiere algún tipo de identificación antes de entregar la llave de una habitación de hotel. En este caso, el usuario puede desear compartir solo su nombre y si tiene o no 18 años o más como datos de personalización para permitir que el hotel autentique al usuario, sin compartir su fecha exacta de nacimiento y número de seguridad social. Cuando se selecciona un perfil de usuario para permitir que las tiendas autentiquen si una persona tiene autorización legal para comprar alcohol, la información que se proporciona al terminal de inspección puede consistir únicamente en si la persona tiene la edad legal para comprar alcohol. De esta manera, la cantidad de información de personalización que un usuario tiene que compartir con terceros se minimiza a solo la información que se requiere para el propósito de autenticación pretendido y se reduce el riesgo de robo de identidad. Además de la indicación del subconjunto de datos de personalización que el usuario está dispuesto a permitir que se transmita desde el servidor de inspección al terminal de inspección, el perfil de usuario también puede comprender información sobre el propósito de la autorización pretendida.

El identificador de documento, que identifica de forma única un documento de identificación que se ha expedido para el usuario, se almacena preferentemente en una memoria del terminal de usuario. Este identificador preferentemente no puede derivarse solamente de los datos en el documento de identificación y, más preferentemente, el identificador de documento no contiene ninguna información de personalización que esté almacenada en el documento de identificación.

La etapa ii) se lleva a cabo en el terminal de inspección, de modo que la representación visual reconocible por humanos real de los datos biométricos del usuario no tiene que transmitirse desde el terminal de inspección al servidor de inspección. El cálculo de un descriptor de características biométricas a partir de una representación visual de datos biométricos es conocido en la técnica. El cálculo típicamente comprende la determinación de puntos destacados en los datos biométricos capturados y el cálculo de un vector de valores de características basándose en las propiedades de estos puntos. Alternativamente, el cálculo del descriptor de características biométricas puede comprender calcular uno o más histogramas de valores de píxeles de la representación visual reconocible por humanos capturada de los datos biométricos del usuario.

El descriptor de características biométricas se puede usar para determinar un nivel de similitud de la imagen con otra imagen, pero no contiene información suficiente para reconstruir la imagen y, por lo tanto, se puede ver para formar una clase de función de troceo (hash) de los datos biométricos. Por ejemplo, el terminal de inspección puede calcular un primer descriptor de características biométricas basándose en la representación visual reconocible por humanos capturada de los datos biométricos del usuario. En el servidor de documentos de identificación, se almacena un segundo descriptor de características biométricas que se ha calculado anteriormente basándose en una copia digital de la foto en el pasaporte que se ha leído usando tecnología RFID y/o NFC. Como la representación visual reconocible por humanos capturada y la copia digital de la foto diferirán, el primer y el segundo vector de características no serán idénticos. Sin embargo, se puede determinar una medida de similitud entre la representación visual reconocible por humanos y la copia digital de la foto basándose en una similitud entre el primer y el segundo descriptores de características biométricas, por ejemplo, calculando una medida de distancia entre el primer y el segundo descriptores de características. Una medida de distancia adecuada que puede usarse es la distancia de Hamming. En una realización, la etapa iv) comprende, tras la recepción de la señal de "autenticación aprobada", mostrar en una pantalla del terminal de inspección, todo o parte del subconjunto de los datos de personalización del usuario que corresponden al perfil de usuario. Los datos se muestran preferentemente en un formato legible por humanos. La transmisión de los datos de personalización del usuario desde el servidor de inspección al terminal de inspección está preferentemente

encriptada, por ejemplo, usando encriptación AES, para evitar que otras partes accedan a los datos de personalización del usuario, así como para evitar que envíen una señal falsificada de "autenticación aprobada" al terminal de inspección.

En una realización, la información sobre el perfil de usuario que se muestra en el terminal de usuario se selecciona de un conjunto predeterminado de perfiles de usuario que se soporta por el IDS. Por tanto, la información de personalización que el usuario puede compartir con el terminal de inspección se limita a la información de personalización correspondiente a un perfil de usuario en el conjunto predeterminado. De esta manera, se evita sustancialmente que un usuario comparta inadvertidamente más información de la requerida para permitir que el terminal de inspección autentique al usuario. Además, la entidad que opera el IDS, que típicamente será una agencia gubernamental o una entidad en la que confía un gobierno nacional, puede decidir qué perfiles de usuario formarán parte del conjunto predeterminado de perfiles de usuario, basándose en qué datos de personalización del usuario pueden compartirse con terceros.

En una realización, la señal de "autenticación aprobada" preferentemente también comprende una suma de comprobación que se basa en la información que se transmitió al servidor de inspección. Esto permite que el terminal de inspección solo genere la señal audible y/o visual que indica que la autenticación del usuario ha sido aprobada cuando el terminal de inspección ha verificado que la suma de verificación de la señal de "autenticación aprobada" corresponde a la información que el terminal de inspección envió al servidor de inspección. Tal verificación puede realizarse, por ejemplo, calculando, tanto en el terminal de inspección como en el servidor de inspección, una suma de comprobación de la información que se envía al servidor de inspección.

En una realización, el identificador de documento, el perfil de usuario y/o el sello de un solo uso se presentan en la pantalla del terminal de usuario en formato de código de barras y/o código QR, por ejemplo, el formato PDF417, en donde esta información se combina preferentemente en un único código de barras y/o código QR. Ya existe una diversidad de software y herramientas para decodificar de manera confiable la información almacenada en tales formatos.

En una realización, el sello de un solo uso incluye un código de tiempo que indica la hora y la fecha en que se generó el sello de un solo uso en el terminal de usuario, en donde el servidor de inspección solo devuelve la señal de "autenticación aprobada" si el código de tiempo indica que el sello de un solo uso se generó dentro de un período de tiempo predeterminado desde la recepción del mismo en el servidor de inspección. De esta manera, el código de un solo uso se proporciona con un tiempo de caducidad después del cual ya no puede usarse para autenticar a un usuario. El tiempo de caducidad puede ser, por ejemplo, menor que 1 minuto o 30 segundos.

En una realización, la etapa iii) comprende además enviar un identificador único del terminal de inspección al servidor de inspección, en donde el servidor de inspección comprende una lista de identificadores únicos de los terminales de inspección y tipos asociados de datos de personalización que cada terminal de inspección está permitido a recibir, en donde el servidor de inspección está adaptado para devolver únicamente la señal de "autenticación aprobada" junto con el subconjunto de datos de personalización definidos por el perfil de usuario, si el terminal de inspección con dicho identificador único está permitido a recibir los datos de personalización indicados en el perfil de usuario. De esta manera, un terminal de inspección puede obtener acceso a los datos de personalización del usuario solo si se ha registrado en el servidor de inspección, e incluso entonces no puede acceder a la personalización a la que no está permitido a acceder.

En una realización, los datos de personalización comprenden o consisten en la información sobre la persona que se incluye en el documento de identidad expedido a la persona, en donde el identificador de documento no está incluido en el documento de identidad. Por lo tanto, el identificador de documento no puede derivarse basándose solamente en la información del documento de identidad. De esta manera, se asegura que ninguna de la información que se transmite a la inspección sirva como copia directa de la información que se incluye en el documento de identidad del usuario. Incluso si esta información transmitida se obtiene por un tercero no confiable, esto no permite que el tercero reconstruya o robe la identidad del usuario.

En una realización, el método comprende además enviar al terminal de usuario una señal indicativa de que el servidor de inspección ha recibido un identificador de documento que corresponde al identificador de documento presentado en la pantalla del terminal de usuario. Esto permite que el terminal de usuario proporcione realimentación al usuario sobre si el terminal de inspección ha transmitido de hecho información a un servidor de identidad. Preferentemente, esta señal se envía al terminal de usuario independientemente del terminal de inspección, por ejemplo, la señal puede enviarse desde el servidor de inspección sin pasar a través del terminal de inspección. Más preferentemente, la señal se envía desde el servidor de inspección al terminal de usuario a través de un medio de comunicación diferente al usado para la comunicación entre el terminal de inspección y el servidor de inspección. Por ejemplo, si el terminal de inspección se comunica con el servidor de inspección a través de Internet, a continuación, la señal se envía preferentemente desde el servidor de inspección al terminal de usuario a través de otro canal de comunicación, tal como SMS o Bluetooth. La señal enviada al usuario puede incluir información sobre el perfil de usuario que se capturó por el terminal de inspección. Esto permite al usuario comprobar si el terminal de inspección ha recibido los datos especificados en el perfil de usuario pretendido o si ha recibido información especificada en algún otro perfil de usuario.

En una realización, la representación visual reconocible por humanos de los datos biométricos del usuario corresponde a la imagen del usuario que está impresa visualmente en el documento de identidad del usuario. Por ejemplo, la representación puede estar formada por una foto del usuario en su pasaporte.

En una realización, el método comprende, antes de la etapa i), expedir un documento de identidad para el usuario y asignar un identificador de documento único al documento de identidad, en donde el identificador de documento no está incluido en el documento de identidad, y almacenar, en el servidor de documentos de identidad, datos de personalización correspondientes a los datos de personalización incluidos en el documento de identidad y el identificador de documento asociado. La autoridad que expide el documento de identidad, por tanto, puede garantizar que los datos de personalización y el identificador de documento en el IDS se corresponden a los datos de personalización que se incluyen en el documento de identidad y el identificador de documento que se almacena en la memoria del terminal del usuario. El identificador de documento único se genera preferentemente independientemente del contenido de datos del documento de identidad del usuario, de modo que el identificador por sí mismo no puede usarse para derivar información que también se almacena en el documento de identidad.

La invención también proporciona un producto de programa informático que comprende instrucciones que, cuando son ejecutadas por un procesador de un terminal de inspección, hacen que el procesador lleve a cabo el método descrito anteriormente.

En una realización, el método comprende, además, la devolución, por un servidor de inspección que comprende o está conectado a un servidor de documentos de identidad (IDS) que almacena, para cada documento de identidad de una pluralidad de documentos de identidad expedidos a diferentes personas, datos de personalización acerca de la persona a la que se ha expedido el documento de identidad y un identificador de documento asociado que identifica de forma única el respectivo documento de identidad, una señal de "autenticación aprobada" junto con un subconjunto de los datos de personalización definidos por el perfil de usuario, si

- el descriptor de características biométricas transmitido corresponde a un descriptor de características biométricas de datos biométricos almacenados en el IDS para un documento de identidad para el cual el identificador de documento asociado corresponde al identificador de documento transmitido, y
- el sello de un solo uso no se ha recibido antes para el identificador de documento transmitido.

Estas etapas se llevan a cabo tras la recepción en la etapa iii) del identificador de documento capturado, el descriptor de características biométricas, el perfil de usuario y el sello de un solo uso en el servidor de inspección.

En una realización, el método comprende además para presentar datos de autenticación de usuario en el terminal de usuario que está provisto de una pantalla, un dispositivo de entrada y una memoria, almacenando la memoria: datos biométricos del usuario, un identificador de documento para identificar un documento de identidad que se ha expedido al usuario, uno o más perfiles de usuario, especificando cada perfil de usuario un subconjunto de datos de personalización derivados del documento de identidad expedido al usuario, para ser proporcionados al terminal de inspección, en donde el método comprende las etapas de: presentar, en la pantalla, múltiples del uno o más perfiles de usuario; recibir, a través del dispositivo de entrada, la entrada del usuario en qué perfil de usuario del uno o más perfiles de usuario se va a usar; y presentar, en la pantalla: una representación visual reconocible por humanos de los datos biométricos del usuario almacenados en la memoria, una representación legible por máquina del identificador de documento, una representación legible por máquina del perfil de usuario que se usará, y un sello de un solo uso. Este método puede llevarse a cabo en el terminal de usuario y usarse en combinación con el método de acuerdo con el primer aspecto de la invención. Preferentemente, el sello de un solo uso se genera por el terminal de usuario o se almacena en la memoria del terminal de usuario.

En una realización, el subconjunto o subconjuntos de datos de personalización especificados por los perfiles de usuario no están presentes en la memoria del terminal de usuario a la que se accede para llevar a cabo el método. Por lo tanto, incluso si el terminal del usuario es incautado por una parte no autorizada, ningún dato de personalización del usuario que se derive de los datos de personalización que se incluyen en el documento de identidad del usuario se puede encontrar en la memoria del terminal del usuario que se usa para llevar a cabo el método. En particular, no está presente en la memoria ni un número de seguridad social, "número de servicio al ciudadano", ni cualquier otro código alfanumérico que se copia del documento de identidad y que identifica de manera única a un usuario.

La invención también proporciona un producto de programa informático que comprende instrucciones que, cuando son ejecutadas por un procesador de un terminal de usuario móvil, hacen que el procesador lleve a cabo un método de acuerdo con el segundo aspecto de la invención.

De acuerdo con un segundo aspecto, la invención proporciona un sistema que comprende: un servidor de inspección que comprende o está conectado a un servidor de documentos de identidad (IDS) que almacena, para cada documento de identidad de una pluralidad de documentos de identidad expedidos a diferentes personas, datos de personalización acerca de la persona a la que se ha expedido el documento de identidad y un identificador de documento asociado que identifica de forma única el respectivo documento de identidad; un terminal de inspección provisto de una cámara

digital y una pantalla, en donde el terminal de inspección está adaptado para: i) capturar, con la cámara digital, una imagen que contiene: - una representación visual reconocible por humanos de los datos biométricos del usuario, - un identificador de documento para identificar un documento de identidad que se ha expedido al usuario, - un perfil de usuario que especifica un subconjunto de datos de personalización derivados del documento de identidad expedido al usuario, que se proporcionará al terminal de inspección, y - un sello de un solo uso; en donde el terminal de inspección está adaptado además para ii) calcular un descriptor de características biométricas a partir de la representación visual reconocible por humanos capturada de los datos biométricos del usuario; y iii) transmitir el identificador de documento capturado, el descriptor de características biométricas, el perfil de usuario y el sello de un solo uso a un servidor de inspección; en donde el servidor de inspección está adaptado para devolver una señal de "autenticación aprobada" junto con un subconjunto de los datos de personalización definidos por el perfil de usuario, si

- el descriptor de características biométricas transmitido corresponde a un descriptor de características biométricas de datos biométricos almacenados en el IDS para un documento de identidad para el cual el identificador de documento asociado corresponde al identificador de documento transmitido, y
- el sello de un solo uso no se ha recibido antes para el identificador de documento transmitido;

y, en donde el terminal de inspección está adaptado para esperar la señal de "autenticación aprobada", y tras la recepción de dicha señal, generar una señal audible y/o visual que indica que se ha aprobado la autenticación del usuario para el objetivo de autenticación especificado.

En una realización, el servidor de inspección no almacena una copia de la representación visual reconocible por humanos de los datos biométricos del usuario. Por lo tanto, el sistema puede usarse para autenticar a un usuario de un terminal de usuario móvil como se ha descrito anteriormente, sin que se almacene o transmita una imagen del usuario al servidor de inspección o IDS. Preferentemente, el servidor de inspección no almacena ninguna información a partir de la cual se pueda reconstruir una representación visual reconocible por humanos de los datos biométricos del usuario.

En una realización, el descriptor de características biométricas se calcula a partir de la representación visual reconocible por humanos capturada de tal manera que una representación visual reconocible por humanos del usuario no pueda reconstruirse a partir del descriptor de características biométricas, por ejemplo, usando una función unidireccional. El tamaño en bits del descriptor de características biométricas es más pequeño que el tamaño en bits de la representación visual reconocible por humanos capturada del usuario. Por ejemplo, el descriptor de características biométricas tendrá típicamente un tamaño de 1000 bits o menor, mientras que la representación visual del usuario reconocible por humanos capturada tendrá típicamente un tamaño de al menos 200 kilobytes.

De acuerdo con un tercer aspecto, la invención proporciona un método para registrar, en el servidor de inspección del sistema de acuerdo con el tercer aspecto de la invención, un descriptor de características biométricas de una representación visual reconocible por humanos de datos biométricos de un usuario a quien se le ha expedido un documento de identidad tangible, así como un identificador de documento para identificar de manera única el documento de identidad tangible y la información de personalización que se almacena en el documento de identidad tangible, comprendiendo el método las etapas de:

leer una cadena de identificación de documento del documento de identidad tangible;

leer electrónicamente información de personalización y una representación visual reconocible por humanos de datos biométricos del usuario que se almacenan en el documento de identidad tangible;

enviar la cadena de identificación del documento a un servidor de verificación y recibir una respuesta que indica si el documento de identidad asociado con la cadena de identificación del documento es válido o no;

capturar una imagen en vivo del usuario;

calcular una medida de diferencia indicativa de una diferencia entre la representación visual reconocible por humanos de los datos biométricos del usuario y la imagen en vivo capturada del usuario; y

si la medida de diferencia está por debajo de un umbral predeterminado y el documento de identidad asociado con la cadena de identificación del documento es válido, llevar a cabo las etapas adicionales de:

- generar un identificador de documento para identificar de forma única el documento de identidad, en donde el identificador de documento no puede derivarse únicamente de los datos del documento de identificación;
- calcular un descriptor de características biométricas a partir de la representación visual reconocible por humanos leída electrónicamente de los datos biométricos del usuario;

- transmitir el descriptor de características biométricas y la información de personalización al servidor de inspección y almacenarlos junto con el identificador de documento en el servidor de inspección; y

- transmitir (524) el identificador de documento a un terminal de usuario móvil, tal como un teléfono móvil del usuario.

Con este método, los datos relevantes que permiten la autenticación del usuario se almacenan en el servidor de inspección. Basándose en estos datos, el sistema se puede usar para autenticar a un usuario que muestra en una pantalla de un terminal de usuario la información que comprende una representación visual reconocible por humanos de los datos biométricos del usuario, un identificador de documento, un perfil de usuario y un sello de un solo uso. Cuando el usuario está presente cerca del terminal de inspección durante la autenticación, la persona que opera el terminal de inspección también puede comprobar visualmente si la persona mostrada en la pantalla del terminal de usuario es de hecho el usuario.

Aunque se almacena un descriptor de características biométricas en el servidor de inspección, no es necesario almacenar una ID de foto o huella digital del usuario en el servidor de inspección una vez que se ha completado el registro y, preferentemente, una vez que se ha completado el registro, el servidor de inspección no contiene ningún dato que permita reconstruir la ID de foto o la huella digital. Típicamente, el identificador de documento único se genera independientemente de la cadena de identificación del documento, por ejemplo, usando un generador de números pseudoaleatorios. Típicamente, la medida de diferencia se calcula basándose en las diferencias entre las características de la imagen capturada en vivo del usuario y la representación visual reconocible por humanos de los datos biométricos del usuario. Las características en las que se basa el cálculo de la medida de la distancia pueden incluir una distancia entre los ojos, la anchura de la boca, la distancia de cada ojo a la nariz y similares. El servidor de verificación está preferentemente adaptado para indicar que el documento de identidad asociado con la cadena de identificación del documento no es válido cuando la fecha de vencimiento del documento de identidad ha vencido o cuando el documento de identidad ha sido revocado, por ejemplo, en caso de que sea denunciado como robado. Un servidor de verificación de este tipo generalmente será operado por una agencia gubernamental.

En una realización, las etapas de: leer una cadena de identificación de documento del documento de identidad; leer electrónicamente información de personalización y una representación visual reconocible por humanos de datos biométricos del usuario que se almacenan en el documento de identidad; y capturar una imagen en vivo del usuario; se llevan a cabo usando el terminal móvil del usuario, tal como un teléfono móvil. Esto permite que el usuario se registre a sí mismo usando el terminal de usuario móvil, sin necesidad de una persona, por ejemplo, un funcionario del gobierno similar, para confirmar que el usuario corresponde de hecho a la representación visual reconocible por humanos leída. En esta realización, se almacena una copia del identificador de documento y de la representación visual reconocible por humanos de los datos biométricos leídos electrónicamente del usuario en el terminal de usuario móvil.

En una realización alternativa, las etapas de: leer una cadena de identificación de documento del documento de identidad; leer electrónicamente información de personalización y una representación visual reconocible por humanos de datos biométricos del usuario que se almacenan en el documento de identidad; y capturar una imagen en vivo del usuario; se llevan a cabo en un sistema de registro que es diferente del terminal de usuario móvil. El sistema de registro es preferentemente un sistema certificado y/o de propiedad de una agencia gubernamental que tiene la tarea de expedir documentos de identificación tangibles para los usuarios. Para registrarse a sí mismo o misma, el usuario tendrá que ir físicamente al sistema de registro, normalmente en un ayuntamiento, para poder registrarse. Esta forma de registro proporciona un mayor nivel de autenticación de confianza que cuando se llevan a cabo las etapas anteriores por un usuario usando su terminal de usuario móvil. En esta realización, se transmite y se almacena una copia del identificador de documento y de la representación visual reconocible por humanos de los datos biométricos leídos electrónicamente del usuario en el terminal de usuario móvil.

En una realización, el método comprende además la etapa de transmitir, al terminal de usuario móvil, un acuse de recibo de que el registro está completo.

En una realización, el método comprende además la etapa de recibir y transmitir, desde el terminal de usuario móvil, un acuse de recibo de que el terminal de usuario móvil ha recibido el identificador de documento. El acuse de recibo se recibe preferentemente en el sistema de registro y/o en el servidor de inspección, y puede enviarse, por ejemplo, a través de Internet, SMS, un conector Bluetooth o similar,

En una realización, el método comprende, además, después de la etapa de capturar la imagen en vivo del usuario y antes de llevar a cabo las etapas adicionales: generar un código de registro de un solo uso en el sistema de registro o el servidor de inspección y transmitir el código de registro de un solo uso al terminal de usuario móvil; recibir, desde el terminal de usuario móvil, un mensaje que indica si el usuario ha recibido el código de un solo uso y desea registrar sus datos de personalización en el servidor de inspección; recibir, desde el terminal de usuario móvil, una imagen en vivo adicional del usuario capturada por la cámara del terminal de usuario móvil; calcular una medida de diferencia adicional indicativa de una diferencia entre la representación visual reconocible por humanos de los datos biométricos del usuario y la imagen en vivo adicional capturada del usuario; en donde las etapas adicionales del método se llevan

a cabo solo si la medida de diferencia adicional está por debajo de un umbral predeterminado adicional y el mensaje se recibe desde el terminal de usuario móvil dentro de un tiempo predeterminado después de generar el código de registro de un solo uso e indica que el usuario recibió el código de un solo uso y desea registrar sus datos de personalización en el servidor de inspección.

En una realización, el método comprende, después de completar el registro, llevar a cabo las etapas del método del primer aspecto de la invención.

Breve descripción de los dibujos

La presente invención se analizará con más detalle a continuación, con referencia a los dibujos adjuntos, en los que

Las Figuras 1A y 1B son esquemáticamente un terminal de usuario como el que puede usarse en el método de la invención, presentando respectivamente al usuario una selección de perfiles de usuario y presentando un terminal de inspección con una tarjeta de identidad virtual,

Las Figuras 1C-1E muestran esquemáticamente un terminal de inspección que puede usarse de acuerdo con la invención, indicando respectivamente que la autenticación de un usuario ha sido aprobada, ha sido desaprobada y que se ha producido un error de tiempo de espera,

La Figura 2 muestra esquemáticamente un diagrama de flujo de las etapas del método para autenticar a un usuario de acuerdo con la presente invención,

La Figura 3 muestra esquemáticamente un sistema de acuerdo con la invención, que comprende un terminal de inspección y un servidor de inspección,

La Figura 4 muestra un diagrama de flujo de un método para registrarse usando un teléfono móvil del usuario;

La Figura 5 muestra un diagrama de flujo de un método para registrarse en un sistema de registro que es diferente del teléfono móvil del usuario.

Descripción de realizaciones

Las Figuras 1A y 1B muestran respectivamente un terminal de usuario móvil 10 como el que puede usarse de acuerdo con la invención, la pantalla de la Figura 1A presenta al usuario una selección de perfiles de usuario 13, 14, 15, 16 para su selección por el usuario, y la pantalla en la Figura 1B, que muestra información que va a capturarse por un dispositivo de inspección que puede usarse de acuerdo con la invención. La Figura 1A muestra el terminal de usuario 10 que, en la realización mostrada, es un teléfono inteligente. El terminal de usuario es portátil, por ejemplo, pesa menos de 350 g, y puede ser llevado por el usuario en un bolsillo de su ropa o en un bolso. Los teléfonos inteligentes ya son de uso generalizado, de modo que se puede evitar el inconveniente de llevar consigo un terminal de usuario adicional además del teléfono inteligente. El terminal de usuario 10 comprende una pantalla táctil 11 para presentar información a un usuario y para recibir la entrada del usuario, así como una memoria 12, mostrada en este punto solo esquemáticamente, en la que se almacena un programa informático que permite al usuario, dependiendo de un propósito de autenticación pretendido por el usuario, seleccionar entre diferentes perfiles de usuario. La pantalla muestra un número de perfiles de usuario diferentes 13, 14, 15, 16, cada uno de los cuales especifica qué datos de personalización que se derivan del documento de identidad física del usuario está dispuesto a compartir el usuario para permitir que otra parte autentique al usuario. Los perfiles de usuario, por ejemplo, de acuerdo con la siguiente tabla:

Perfil de usuario mostrado en la Figura 1A	**Propósito de autenticación pretendido**	**Datos de personalización derivados del documento de identidad del usuario que se van a compartir con la otra parte:**
13	Comprar sustancias controladas, tales como alcohol o tabaco	ID de foto y si el usuario tiene o no edad para beber / edad para comprar tabaco (por ejemplo, al menos 18 o 21 años)
14	Despacho de fronteras	ID de foto, nombre completo, edad e identificador alfanumérico único del usuario copiado del documento de identidad del usuario
15	Registrarse en un hotel	ID de foto, nombre completo y edad
16	Identificación del usuario ante la policía	ID de foto, nombre completo, edad e identificador alfanumérico único del usuario copiado del documento de identidad del usuario

Otro perfil de usuario que se puede seleccionar tiene como propósito de autenticación pretendido obtener acceso, por ejemplo, a un concierto o festival, y los datos de personalización asociados al perfil de usuario son una ID de foto y un número de entrada.

Una vez que el usuario ha seleccionado qué perfil de usuario va a ser el usuario, la pantalla del terminal de usuario 11 cambia para presentar una tarjeta de identidad virtual como se muestra en la Figura 1B a un terminal de inspección. Independientemente del perfil de usuario que se haya seleccionado, la tarjeta de identidad virtual que se muestra en el terminal de usuario comprende una ID de foto 20, es decir, una imagen del usuario, así como información 21 sobre el perfil de usuario seleccionado, una ID de documento único que está asociado a un documento de identidad física que ha sido expedido al usuario, y un sello de un solo uso. La información 21 se muestra en un formato de código de barras que una máquina puede leer fácilmente y que es difícil de decodificar por un ser humano sin una máquina.

Aunque no es esencial, para proporcionar seguridad adicional, la información 21 se renueva preferentemente periódicamente, en donde cada vez se incluye un sello de un solo uso diferente en la información 21. Por ejemplo, la información 21 puede renovarse cada 5, 10 o 30 segundos. La seguridad se mejora aún más si la información 21 comprende un código de tiempo que indica la hora y la fecha en que se generó la información 21. Este código de tiempo se puede decodificar en el servidor de inspección, lo que le permite evitar que se envíe una señal de "autenticación aprobada" si el código de tiempo indica que el código de un solo uso se generó más de una cantidad de tiempo predeterminada antes de recibirse en el servidor de inspección, por ejemplo, más de 10 segundos.

La ID de foto 20 se recupera de la memoria 12, en este punto se muestra esquemáticamente, y es preferentemente una copia digital exacta de una ID de foto que se ha leído electrónicamente de un documento de identificación física en un momento anterior a su presentación en la pantalla 11. Las tarjetas de identidad modernas, como los pasaportes, tarjetas de ID nacionales y permisos de conducción, pueden contener información, que incluye un ID de foto, que se puede leer usando tecnología NFC o RFID. Tales tarjetas de identidad modernas generalmente están equipadas con un mecanismo de control de acceso básico (BAC), para garantizar que solo las partes autorizadas puedan leer de forma inalámbrica la información almacenada en los chips de las tarjetas. Para leer los datos almacenados electrónicamente de tales documentos, se supone que se requiere acceso al documento de identificación físico. Una vez que se ha almacenado una copia digital del ID de foto en la memoria del terminal del usuario, no se necesita más acceso físico al documento de identidad para autenticar al usuario.

El terminal de usuario 10, que no está necesariamente equipado con una cámara en funcionamiento, puede por tanto acceder a una representación del ID de foto que se almacena en su memoria 11, incluso cuando el documento de identificación física se almacena de forma remota. En la figura, la ID de foto y la información 21 en formato de código de barras forman juntos la tarjeta de identidad virtual. Además de la tarjeta de identidad virtual, el nombre del usuario 22, así como una indicación 23 de la edad del usuario, también se muestran en la pantalla en un formato legible por humanos, aunque mostrar y compartir esta información es opcional. Puede omitirse mostrar el nombre del usuario y la indicación de edad para minimizar la cantidad de información de personalización legible por humanos que puede leer la pantalla por una persona que la ve, sin afectar las etapas posteriores de la autenticación.

Una vez que la tarjeta de identidad virtual se presenta en la pantalla del terminal de usuario, puede capturarse por un terminal de inspección. Un terminal de inspección 50 de este tipo se muestra en la Figura 1C y comprende una cámara digital 52 para capturar la información presentada en la pantalla del terminal de usuario, información que incluye una ID de foto reconocible por humanos del usuario, así como el perfil de usuario seleccionado por el usuario y un sello de un solo uso. El terminal de inspección 50 está adaptado para calcular un descriptor de características biométricas a partir de la representación visual reconocible por humanos capturada de los datos biométricos del usuario. Después de calcular este descriptor de características, el terminal de inspección transmite el identificador de documento capturado, el descriptor de características biométricas, el perfil de usuario y el sello de un solo uso a un servidor de inspección, y espera a que el servidor de inspección devuelva una señal de "autenticación aprobada", junto con los datos de personalización especificados en el perfil de usuario seleccionado. Si el terminal de inspección recibe una señal de este tipo y datos de personalización dentro de un período de tiempo predeterminado, por ejemplo, dentro de los 30 segundos, de transmisión de los datos al servidor de inspección, muestra información 60 en su pantalla 51 que es indicativa de que la autenticación ha tenido éxito, así como los datos de personalización 61, como se muestra en la Figura 1C.

Si en lugar de la señal de "autenticación aprobada", el terminal de inspección recibe una "autenticación no aprobada", esto se muestra en la pantalla 51, como se ilustra en la Figura 1D. En la Figura 1D, la pantalla 51 muestra la información 63, en este punto en forma de un icono, que indica que la autenticación no ha sido aprobada. Como, cuando no se aprueba la autenticación, no se envían datos de personalización del usuario desde el servidor de inspección al terminal de inspección, la pantalla 51 no muestra tales datos de personalización del usuario.

Si la señal de "autenticación aprobada" no se recibe en el terminal de inspección dentro de un período de tiempo predeterminado desde el punto en el tiempo en que se generó el sello de un solo uso, a continuación, esto se muestra como la información 64, de nuevo en forma de icono, en la pantalla. 51 del terminal de inspección 50, como se muestra en la Figura 1E. El sello de un solo uso capturado por el terminal de inspección puede incluir un código de tiempo que indica la hora y la fecha en que se generó el sello de un solo uso en el terminal de usuario, lo que permite que el

terminal de inspección compruebe si ha pasado un período de tiempo predeterminado desde la hora y la fecha en que se generó el sello de un solo uso. A continuación, se muestra el icono 64 si no se ha recibido ninguna "autenticación aprobada" dentro del período de tiempo predeterminado después de la generación del sello de un solo uso. Como alternativa, este icono puede mostrarse simplemente si ha pasado más de una cantidad de tiempo predeterminada entre la transmisión de la información desde el terminal de inspección al servidor de inspección y la recepción de una señal de "autenticación aprobada" del servidor de inspección. La cantidad de tiempo predeterminada es preferentemente menor que 30 segundos, más preferentemente menor que 10 segundos.

La Figura 2 muestra esquemáticamente un diagrama de flujo de etapas para autenticar a un usuario. En el diagrama de flujo, las etapas del método que se llevan a cabo en el terminal de inspección se indican con los números de referencia 100-102, las etapas del método que se llevan a cabo en el terminal de usuario se indican con los números de referencia 200-205 y las etapas del método que se llevan a cabo en un servidor de inspección se indican usando los números de referencia 300-304.

La autenticación comienza en la etapa 100, en la que un usuario abre una aplicación de coche de identidad virtual en su teléfono inteligente. La aplicación puede estar protegida por un PIN o una exploración de huellas dactilares ("exploración táctil") o similar para evitar que personas no autorizadas abran la aplicación. Una vez que se ha introducido el PIN correcto o similar, se presenta un número de perfiles de usuario en la pantalla del teléfono inteligente en la etapa 101. En la etapa 102, se recibe una selección de usuario de uno de estos perfiles de usuario y, posteriormente, en la etapa 103, se muestra una tarjeta de identidad virtual correspondiente, que comprende la ID de foto de los usuarios, el identificador de documento, el perfil de usuario seleccionado y un sello de un solo uso en la pantalla. A continuación, en la etapa 200, la ID de foto mostrada, el identificador de documento, el perfil de usuario seleccionado y el sello de un solo uso se capturan por el terminal de inspección usando una cámara digital. Basándose en la ID de foto capturada, en la etapa 201, se calcula un descriptor de características biométricas. Un descriptor de este tipo puede comprender, por ejemplo, información sobre características destacadas de la cara de la persona, tales como la distancia entre los ojos, la anchura de la boca, la distancia a la nariz, histogramas de valores de píxeles de la imagen capturada y así sucesivamente. Además, en la etapa 201, se genera un sello de un solo uso. Este sello de un solo uso puede comprender información sobre la hora y la fecha en que se generó el sello de un solo uso, así como una suma de comprobación del perfil de usuario. En la etapa 202, el descriptor de características biométricas calculado, junto con el identificador de documento capturado, el perfil de usuario y el sello de un solo uso, se transmite a un servidor de inspección.

El servidor de inspección comprende o está conectado a un servidor de documentos de identidad (IDS) que almacena, para cada documento de identidad de una pluralidad de documentos de identidad expedidos a diferentes personas, datos de personalización acerca de la persona a la que se ha expedido el documento de identidad y un identificador de documento asociado que identifica de manera única el respectivo documento de identidad. El servidor de inspección y el IDS generalmente estarán ubicados en una ubicación altamente segura, y los canales de comunicación entre el terminal de inspección y el servidor de inspección también estarán protegidos, por ejemplo, usando encriptación AES, para evitar que terceros intercepten la comunicación entre ambos.

En la etapa 300, el servidor de inspección comprueba si el descriptor de características biométricas transmitido corresponde a un descriptor de características biométricas de datos biométricos almacenados en el IDS para un documento de identidad para el cual el identificador de documento asociado corresponde al identificador de documento transmitido, y también comprueba que el sello de un solo uso no se ha recibido antes para el identificador de documento transmitido. Si ambos son el caso, el servidor de inspección continúa a la etapa 301 y devuelve una señal de "autenticación aprobada" junto con un subconjunto de los datos de personalización definidos por el perfil de usuario, al terminal de inspección. De lo contrario, el servidor de inspección continúa en su lugar con la etapa 302 y devuelve una señal de "autenticación no aprobada" al terminal de inspección. En cualquier caso, el sello de un solo uso se almacena en el servidor de inspección y se asocia con el identificador de documento transmitido.

En las etapas 303 y 304, que son opcionales, el servidor de inspección envía al terminal de usuario una señal indicativa que el servidor de inspección ha recibido un identificador de documento que corresponde al identificador de documento presentado en la pantalla del terminal de usuario.

En la etapa 203, el terminal de inspección, tras la recepción de la señal de "autenticación aprobada", genera una indicación visual en su pantalla para notificar al operador del terminal de inspección que el usuario ha sido autenticado satisfactoriamente. Opcionalmente, la información especificada en el perfil de usuario seleccionado también se muestra en la etapa 204. En caso de que el terminal de inspección no reciba una señal de "autenticación aprobada" dentro de un tiempo predeterminado, o en caso de que, en su lugar, se reciba una señal de "autenticación no aprobada", el terminal de inspección notifica al operador del terminal de inspección en la etapa 205 que la autenticación del usuario no ha sido aprobada.

La Figura 3 muestra esquemáticamente un sistema 400 de acuerdo con la invención. El sistema comprende un terminal de inspección 450, por ejemplo, correspondiente al terminal de inspección 50 de la Figura 1B, un servidor de inspección 480 en una ubicación remota del terminal 450, así como un servidor de documentos de identidad, IDS. Además, se muestra un terminal de usuario 410, con una pantalla 411 en la que se muestra en una sola ID de foto del usuario,

junto con un identificador de documento, el perfil de usuario y sello de un solo uso como se describió anteriormente en el presente documento. La información de esta imagen se captura por la cámara digital 452 del terminal de inspección 450, y el terminal calcula un descriptor de características biométricas a partir del ID de foto capturada del usuario. El intercambio de información entre el terminal de usuario 410 y el terminal de inspección 450 es unidireccional únicamente, desde el terminal de usuario al terminal de inspección, como indica la flecha 490. Posteriormente, el terminal transmite el identificador de documento capturado, el descriptor de características biométricas, el perfil de usuario y el sello de un solo uso al servidor de inspección 460, como se indica mediante la flecha 491.

Tras la recepción de esta información, el servidor de inspección 460 contacta con un servidor de documentos de identidad, IDS, 470 que almacena, para cada documento de identidad de una pluralidad de documentos de identidad expedidos a diferentes personas, datos de personalización acerca de la persona a quien se ha expedido el documento de identidad y un identificador de documento que identifica de forma única el documento de identidad pero que no puede derivarse simplemente del documento de identidad por sí mismo. El IDS 470 almacena, además, para cada documento de identidad, una copia de la ID de foto que está presente en el documento de identidad. Aunque en la Figura 3 se muestra que el IDS es parte del sistema 400, se apreciará que, en su lugar, se puede usar un IDS separado del sistema, siempre que el servidor de inspección 460 pueda comunicarse con el IDS.

La línea 492 indica que el perfil de usuario y el identificador de documento se transmiten desde el servidor de inspección al IDS 470. Basándose en esto, el IDS devuelve un descriptor de características biométricas de la ID de foto del documento correspondiente al identificador de documento al servidor de inspección, como se indica por la línea 493.

Ya sea en el servidor de inspección 460 o en el IDS 470, se comprueba posteriormente si el descriptor de características biométricas de la ID de foto que se capturó por el terminal de inspección corresponde al descriptor de características biométricas de la ID de foto para el documento identificado por el identificador de documento. Si este es el caso, y si el sello de un solo uso no se recibió antes en el servidor de inspección, el servidor de inspección envía una señal de "autenticación aprobada" 494 al terminal de inspección, junto con los datos de personalización del usuario como se especifica en el perfil de usuario y se proporciona por el IDS 470. La línea de puntos 494' indica una señal de "autenticación no aprobada", que, como alternativa, se expediría al terminal de inspección si el sello de un solo uso hubiera sido utilizado antes, o si los descriptores de características biométricas no coincidieran.

En algunas aplicaciones, también puede ser útil incluir el terminal de usuario 410 en el sistema 400, aunque generalmente se prefiere que el terminal de usuario no forme parte del sistema, sino que simplemente se le proporcionen instrucciones de programa informático que permiten que el terminal de usuario presente la información apropiada al terminal de inspección. El servidor de inspección solo se comunica con terminales de inspección autorizados y, preferentemente, usa canales de comunicación encriptados para la comunicación. Como no hay transferencia de información desde el servidor de inspección al terminal de usuario 410, incluso en caso de pérdida o robo del terminal de usuario, no hay riesgo de que se extraigan datos de personalización sensibles del terminal de usuario.

La Figura 4 muestra un diagrama de flujo de un método para registrar un descriptor de características biométricas de una representación visual reconocible por humanos de datos biométricos de un usuario a quien se le ha expedido un documento de identidad tangible, así como un identificador de documento para identificar de manera única el documento de identidad tangible y la información de personalización que se almacena en el documento de identidad tangible. En la etapa 501, se lee una cadena de identificación de documento del documento de identidad tangible, por ejemplo, usando el reconocimiento óptico de caracteres. Esta cadena puede usarse para acceder a la información que se almacena en un chip del documento de identidad tangible en caso de que el documento esté protegido por medio de un control de acceso básico (BAC). A continuación, en la etapa 502, los datos almacenados en el chip se leen electrónicamente, que incluyen datos de personalización, así como una representación visual reconocible por humanos de los datos biométricos del usuario que se almacena en el chip del documento de identidad tangible. Los datos que se leen electrónicamente también pueden incluir una copia digital de la cadena de identificación del documento que puede compararse opcionalmente con la cadena de identificación del documento que se leyó en la etapa 501 para garantizar que el chip y el documento tangible coinciden. En caso de que estos no coincidan, el método de registro finaliza.

En la etapa 503, la cadena de identificación del documento se envía a un servidor de verificación, que comprueba si el documento asociado a dicha cadena sigue siendo válido, por ejemplo, no ha caducado y no ha sido informado como robado o revocado de otra manera. En la etapa 505, se recibe esta respuesta, típicamente en el servidor de inspección. A continuación, en la etapa 505, se captura una imagen en vivo del usuario. Esto se hace de modo que se pueda determinar con un mayor grado de certeza que la persona para la cual se registran los datos de personalización y descripción de características biométricas está de hecho implicada en el proceso de registro. En la etapa 506, se calcula una medida de diferencia entre la imagen en vivo capturada y la representación visual reconocible por humanos de los datos biométricos del usuario que se leyeron electrónicamente. Esto se puede hacer de una manera conocida en la técnica del reconocimiento facial. En la etapa 520, se comprueba si la medida de diferencia está por debajo de un umbral predeterminado y se comprueba además si el servidor de verificación indicó que el documento de identidad asociado con la cadena de identificación es válido. Si cualquiera de estos no es el caso, se aborta el registro. De lo

contrario, el método continúa con una etapa 521 de generación de un identificador de documento para identificar de manera única el documento de identidad. Este identificador de documento puede generarse usando un generador de números pseudoaleatorios y es independiente de la cadena de identificación del documento en el sentido de que la cadena de identificación del documento no puede reconstruirse a partir del identificador de documento. En la etapa 522, se calcula un descriptor de características biométricas a partir de la representación visual reconocible por humanos leída electrónicamente de los datos biométricos del usuario. El descriptor de características se calcula de tal manera que no es posible reconstruir una representación visual reconocible por humanos de los datos biométricos del usuario a partir del descriptor de características. En cualquier caso, el tamaño en bits del descriptor de característica es órdenes de magnitud menor que el tamaño en bits de la representación visual reconocible por humanos leída electrónicamente de los datos biométricos del usuario. Por ejemplo, una foto de ID del usuario puede tener un tamaño de al menos 200 kilobytes, mientras que el descriptor de características normalmente tiene un tamaño de 1000 bits o menor. En la etapa 523, el descriptor de características biométricas y la información de personalización al servidor de inspección y almacenarlos junto con el identificador de documento en el servidor de inspección. Para garantizar que el terminal móvil del usuario pueda mostrar información que comprende el identificador de documento en su pantalla, el identificador de documento se transmite a un terminal móvil del usuario en la etapa 524.

En el método mostrado en el diagrama de flujo de la Figura 4, las etapas 501, 502, 504, 505, 506 y típicamente también 520 y/o 521, se llevan a cabo en un sistema de registro que es diferente del terminal de usuario móvil. Generalmente, solo se podrá acceder al sistema de registro desde una ubicación certificada y confiable, tal como un mostrador de una municipalidad donde se expiden documentos de identidad tangibles a los usuarios. Esto proporciona un alto grado de seguridad para el proceso de registro y, en consecuencia, un alto grado de confianza de autenticación usando los datos registrados de esta manera.

Para fines en los que sea suficiente un menor grado de confianza de la autenticación, es posible llevar a cabo una parte considerable del proceso de registro en el terminal móvil del usuario. Esto se ilustra en la Figura 5, en la que las etapas 504 y 521-524 son las mismas que en la Figura 4. Sin embargo, la etapa 601 de leer la cadena de identificación del documento, por ejemplo, usando OCR, se lleva a cabo por el terminal de usuario móvil. Asimismo, el terminal de usuario móvil también lleva a cabo la etapa 602 de leer electrónicamente nuestra información de personalización y la representación visual reconocible por humanos, por ejemplo, usando un lector de NFC del terminal de usuario móvil. La etapa 603 comprende que el terminal móvil envíe la cadena de identificación del documento al servidor de inspección que, a su vez, reenvía la cadena de identificación al servidor de verificación y, posteriormente, recibe una respuesta del servidor de inspección que indica si el documento de identificación es válido o no. En caso de que la respuesta indique que el método de identificación no es válido, se aborta el registro y, de lo contrario, el método continúa con la etapa 504 de recibir la respuesta del servidor de verificación, que típicamente se lleva a cabo en el servidor de inspección. La etapa 605 de capturar una imagen en vivo del usuario se lleva a cabo usando una cámara del terminal de usuario móvil, y la etapa 606 de calcular una medida de diferencia también se lleva a cabo en el terminal de usuario móvil. En la etapa 620, se comprueba en el terminal de usuario móvil si la medida de diferencia está por debajo de un umbral predeterminado, y si no es así, se aborta el registro. De lo contrario, el proceso de registro continúa con las etapas 521-524.

En resumen, la invención proporciona un método y un sistema para autenticar a un usuario basándose en una representación visual reconocible por humanos de los datos biométricos del usuario capturados usando la cámara digital, en donde se genera un descriptor de características biométricas a partir de los datos biométricos capturados del usuario, y el descriptor de características, junto con un perfil de usuario seleccionado por el usuario, se transmite a un servidor de inspección adaptado para validar si el descriptor de características biométricas transmitido corresponde a un descriptor de características biométricas almacenado centralmente de datos biométricos del usuario. Si este es el caso, el servidor de inspección transmite una señal de "autenticación aprobada" junto con los datos de personalización del usuario especificados en el perfil de usuario seleccionado al terminal de inspección.

La presente invención se ha descrito anteriormente con referencia a un número de realizaciones ilustrativas como se muestra en los dibujos. Son posibles modificaciones e implementaciones alternativas de algunas partes o elementos, y están incluidas en el alcance de protección tal como se define en las reivindicaciones adjuntas.

REIVINDICACIONES

1. Método de autenticación de un usuario de un terminal de usuario móvil (10) que está provisto de una pantalla (11), en donde el método comprende, usando un terminal de inspección (50) provisto de una cámara digital (52), las etapas de:

i) capturar (200), con la cámara digital (52), información presentada en la pantalla (11) del terminal de usuario (10), comprendiendo la información:

- una representación visual reconocible por humanos (20) de los datos biométricos del usuario,
- un identificador de documento (21) para identificar un documento de identidad que ha sido expedido al usuario,
- un perfil de usuario (21) que especifica un subconjunto de datos de personalización derivados del documento de identidad expedido al usuario, que van a proporcionarse al terminal de inspección, y
- un sello de un solo uso (21);

ii) calcular un descriptor de características biométricas (201) a partir de la representación visual reconocible por humanos capturada de los datos biométricos del usuario; en donde la representación visual reconocible por humanos de los datos biométricos del usuario corresponde a una imagen del usuario almacenada en el documento de identidad del usuario,

iii) transmitir (202) el identificador de documento capturado, el descriptor de características biométricas, el perfil de usuario y el sello de un solo uso a un servidor de inspección (120), en donde el servidor de inspección comprende o está conectado a un servidor de documentos de identidad (IDS) que almacena, para cada documento de identidad de una pluralidad de documentos de identidad expedidos a diferentes personas, datos de personalización acerca de la persona a la que se ha expedido el documento de identidad y un identificador de documento asociado que identifica de forma única el respectivo documento de identidad, en donde el servidor de inspección está adaptado para devolver una señal de "autenticación aprobada" junto con un subconjunto de los datos de personalización definidos por el perfil de usuario, si

- el descriptor de características biométricas transmitido corresponde a un descriptor de características biométricas de datos biométricos almacenados en el IDS para un documento de identidad para el cual el identificador de documento asociado corresponde al identificador de documento transmitido, y
- el sello de un solo uso no se ha recibido antes para el identificador de documento transmitido;

iv) en el terminal de inspección, esperar la señal de "autenticación aprobada", y tras la recepción de dicha señal, generar una señal audible y/o visual que indica que se ha aprobado la autenticación del usuario.

2. Método de acuerdo con la reivindicación 1, en donde la etapa iv) comprende, tras la recepción de la señal de "autenticación aprobada", mostrar en una pantalla del terminal de inspección, todo o parte del subconjunto de los datos de personalización del usuario que corresponden al perfil de usuario,
en donde la información sobre el perfil de usuario que se muestra en el terminal de usuario se selecciona de un conjunto predeterminado de perfiles de usuario que se soporta por el IDS.

3. Método de acuerdo con una cualquiera de las reivindicaciones anteriores, en donde el sello de un solo uso incluye un código de tiempo que indica la hora y la fecha en que se generó el sello de un solo uso en el terminal de usuario, en donde el servidor de inspección solo devuelve la señal de "autenticación aprobada" si el código de tiempo indica que el sello de un solo uso se generó dentro de un período de tiempo predeterminado desde la recepción del mismo en el servidor de inspección.

4. Método de acuerdo con una cualquiera de las reivindicaciones anteriores, que comprende, además, en la etapa iii) enviar un identificador único del terminal de inspección al servidor de inspección, en donde el servidor de inspección comprende una lista de identificadores únicos de los terminales de inspección y tipos asociados de datos de personalización que cada terminal de inspección está permitido a recibir, en donde el servidor de inspección está adaptado para devolver únicamente la señal "autenticación aprobada" junto con el subconjunto de los datos de personalización definidos por el perfil de usuario, si el terminal de inspección con dicho identificador único está permitido a recibir los datos de personalización indicados en el perfil de usuario.

5. Método de acuerdo con una cualquiera de las reivindicaciones anteriores, en donde los datos de personalización comprenden o consisten en la información sobre la persona que se incluye en el documento de identidad expedido a la persona, en donde el identificador de documento no está incluido en el documento de identidad.

6. Método de acuerdo con una cualquiera de las reivindicaciones anteriores, que comprende además enviar al terminal de usuario una señal indicativa de que el servidor de inspección ha recibido un identificador de documento que corresponde al identificador de documento presentado en la pantalla del terminal de usuario.

7. Método de acuerdo con una cualquiera de las reivindicaciones anteriores, en donde la representación visual reconocible por humanos de los datos biométricos del usuario corresponde a la imagen del usuario que está impresa visualmente en el documento de identidad del usuario.

8. Método de acuerdo con una cualquiera de las reivindicaciones anteriores, que comprende, antes de la etapa i), expedir un documento de identidad para el usuario y asignar un identificador de documento único al documento de identidad, en donde el identificador de documento no está incluido en el documento de identidad, y almacenar, en el servidor de documentos de identidad, datos de personalización correspondientes a los datos de personalización incluidos en el documento de identidad y el identificador de documento asociado.

9. Método de acuerdo con una cualquiera de las reivindicaciones anteriores, que comprende, antes de la etapa i), para presentar datos de autenticación de usuario en el terminal de usuario que está provisto de una pantalla, un dispositivo de entrada y una memoria,almacenando la memoria:

datos biométricos del usuario,
un identificador de documento para identificar un documento de identidad que se ha expedido para el usuario, uno o más perfiles de usuario, especificando cada perfil de usuario un subconjunto de datos de personalización derivados del documento de identidad expedido para el usuario, que van a proporcionarse al terminal de inspección,
en donde el método comprende las etapas de:

presentar, en la pantalla, múltiples del uno o más perfiles de usuario;
recibir, a través del dispositivo de entrada, la entrada del usuario sobre qué perfil de usuario de uno o más perfiles de usuario va a usarse; y
presentar, en la pantalla:

- una representación visual reconocible por humanos de los datos biométricos del usuario almacenados en la memoria,
- una representación legible por máquina del identificador del documento,
- una representación legible por máquina del perfil de usuario que va a usarse, y
- un sello de un solo uso;

en donde el subconjunto o subconjuntos de datos de personalización especificados por los perfiles de usuario no están presentes en la memoria del terminal de usuario a la que se accede para llevar a cabo el método.

10. Sistema (400) que comprende:

un servidor de inspección (460) que comprende o está conectado a un servidor de documentos de identidad (470) que almacena, para cada documento de identidad de una pluralidad de documentos de identidad expedidos a diferentes personas, datos de personalización (471) acerca de la persona a la que se le ha expedido el documento de identidad y un identificador de documento asociado que identifica de manera única el documento de identidad respectivo;
un terminal de inspección (450) provisto de una cámara digital y una pantalla, en donde el terminal de inspección está adaptado para:

i) capturar, con la cámara digital, una imagen que contiene:

- una representación visual reconocible por humanos de los datos biométricos del usuario,
- un identificador de documento para identificar un documento de identidad que ha sido expedido al usuario,
- un perfil de usuario que especifica un subconjunto de datos de personalización derivados del documento de identidad expedido al usuario, que van a proporcionarse al terminal de inspección, y
- un sello de un solo uso;

en donde el terminal de inspección está adaptado además para

ii) calcular un descriptor de características biométricas a partir de la representación visual reconocible por humanos capturada de los datos biométricos del usuario; en donde la representación visual reconocible por humanos de los datos biométricos del usuario corresponde a una imagen del usuario almacenada en el documento de identidad del usuario; y
iii) transmitir el identificador de documento capturado, el descriptor de características biométricas, el perfil de usuario y el sello de un solo uso a un servidor de inspección;

en donde el servidor de inspección (460) está adaptado para devolver una señal de "autenticación aprobada" junto con un subconjunto de los datos de personalización definidos por el perfil de usuario, si

- el descriptor de características biométricas transmitido corresponde a un descriptor de características biométricas de datos biométricos almacenados en el IDS para un documento de identidad para el cual el identificador de documento asociado corresponde al identificador de documento transmitido, y
- el sello de un solo uso no se ha recibido antes para el identificador de documento transmitido;

y, en donde el terminal de inspección está adaptado para esperar la señal de "autenticación aprobada", y tras la recepción de dicha señal, generar una señal audible y/o visual que indica que se ha aprobado la autenticación del usuario para el objetivo de autenticación especificado,
en donde el descriptor de características biométricas se calcula a partir de la representación visual reconocible por humanos capturada de tal manera que una representación visual reconocible por humanos del usuario no pueda reconstruirse a partir del descriptor de características biométricas, por ejemplo, usando una función unidireccional.

11. Sistema de acuerdo con la reivindicación 10, en donde el servidor de inspección no almacena una copia de la representación visual reconocible por humanos de los datos biométricos del usuario.

12. Método para registrar, en un servidor de inspección, un descriptor de características biométricas de una representación visual reconocible por humanos de datos biométricos de un usuario a quien se le ha expedido un documento de identidad tangible, así como un identificador de documento para identificar de manera única el documento de identidad tangible y la información de personalización que se almacena en el documento de identidad tangible, comprendiendo el método las etapas de:

leer (501; 601) una cadena de identificación de documento del documento de identidad tangible;
leer electrónicamente (502; 602) información de personalización y una representación visual reconocible por humanos de datos biométricos del usuario que se almacenan en el documento de identidad;

enviar (503; 603) la cadena de identificación del documento a un servidor de verificación y recibir (504) una respuesta que indica si el documento de identidad asociado con la cadena de identificación del documento es válido o no;
capturar (505; 605) una imagen en vivo del usuario;
calcular (506) una medida de diferencia indicativa de una diferencia entre la representación visual reconocible por humanos de los datos biométricos del usuario y la imagen en vivo capturada del usuario; y
si la medida de diferencia está por debajo de un umbral predeterminado y el documento de identidad asociado con la cadena de identificación del documento es válido, llevar a cabo las etapas adicionales de:

- generar (521) un identificador de documento para identificar de forma única el documento de identidad, en donde el identificador de documento no puede derivarse únicamente de los datos del documento de identificación;
- calcular (522) un descriptor de características biométricas a partir de la representación visual reconocible por humanos leída electrónicamente de los datos biométricos del usuario;
- transmitir (523) el descriptor de características biométricas y la información de personalización al servidor de inspección y almacenarlos junto con el identificador de documento en el servidor de inspección; y
- transmitir (524) el identificador de documento a un terminal de usuario móvil;

en donde las etapas de:

leer una cadena de identificación de documento (601) del documento de identidad tangible; leer electrónicamente (602) información de personalización y una representación visual reconocible por humanos de los datos biométricos del usuario que se almacenan en el documento de identidad; y
capturar (605) una imagen en vivo del usuario;
se llevan a cabo usando el terminal de usuario móvil, o se llevan a cabo en un sistema de registro diferente al del terminal de usuario móvil.

13. Método de acuerdo con la reivindicación 12, que comprende, después de la etapa de capturar la imagen en vivo del usuario y antes de llevar a cabo las etapas adicionales:

generar un código de registro de un solo uso en el sistema de registro o el servidor de inspección y transmitir el código de registro de un solo uso al terminal de usuario móvil;
recibir, desde el terminal de usuario móvil, un mensaje que indica si el usuario ha recibido el código de un solo uso y desea registrar sus datos de personalización en el servidor de inspección;
recibir, desde el terminal de usuario móvil, una imagen en vivo adicional del usuario capturada por la cámara del terminal de usuario móvil;
calcular una medida de diferencia adicional indicativa de una diferencia entre la representación visual reconocible por humanos de los datos biométricos del usuario y la imagen en vivo adicional capturada del usuario;
en donde las etapas adicionales del método se llevan a cabo solo si la medida de diferencia adicional está por debajo de un umbral predeterminado adicional y el mensaje se recibe desde el terminal de usuario móvil dentro de un tiempo predeterminado después de generar el código de registro de un solo uso e indica que el usuario recibió el código de un solo uso y desea registrar sus datos de personalización en el servidor de inspección.

14. Método de acuerdo con la reivindicación 12 o 13, que comprende además llevar a cabo posteriormente las etapas de una cualquiera de las reivindicaciones 1 a 8.

15. Producto de programa informático que comprende instrucciones que, cuando son ejecutadas por un procesador de un terminal de usuario móvil, hacen que el procesador lleve a cabo el método de la reivindicación 9 o 10, o que,

cuando son ejecutadas por un procesador de un terminal de inspección, hacen que el procesador lleve a cabo el método de una cualquiera de las reivindicaciones 1 a 8.

Fig. 1A

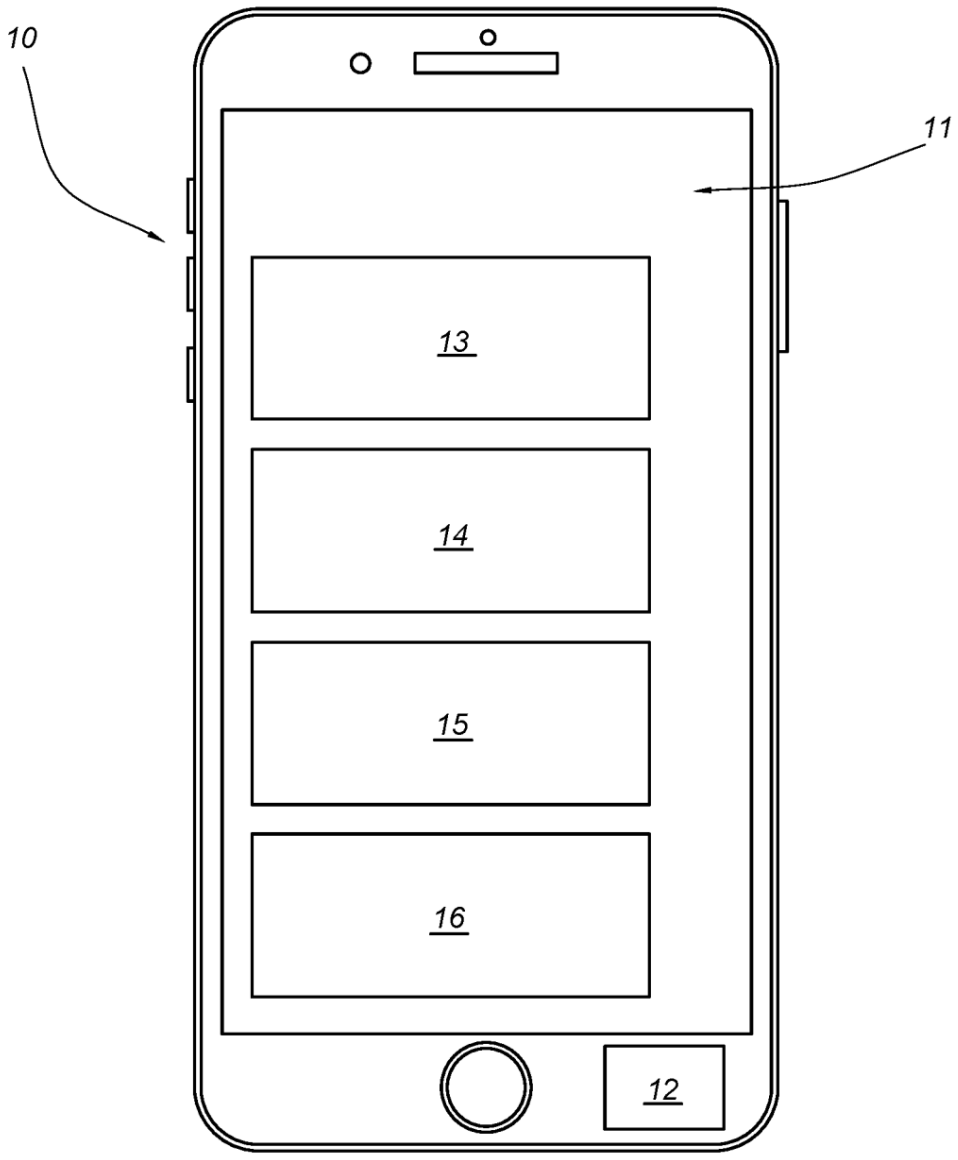


Fig. 1B

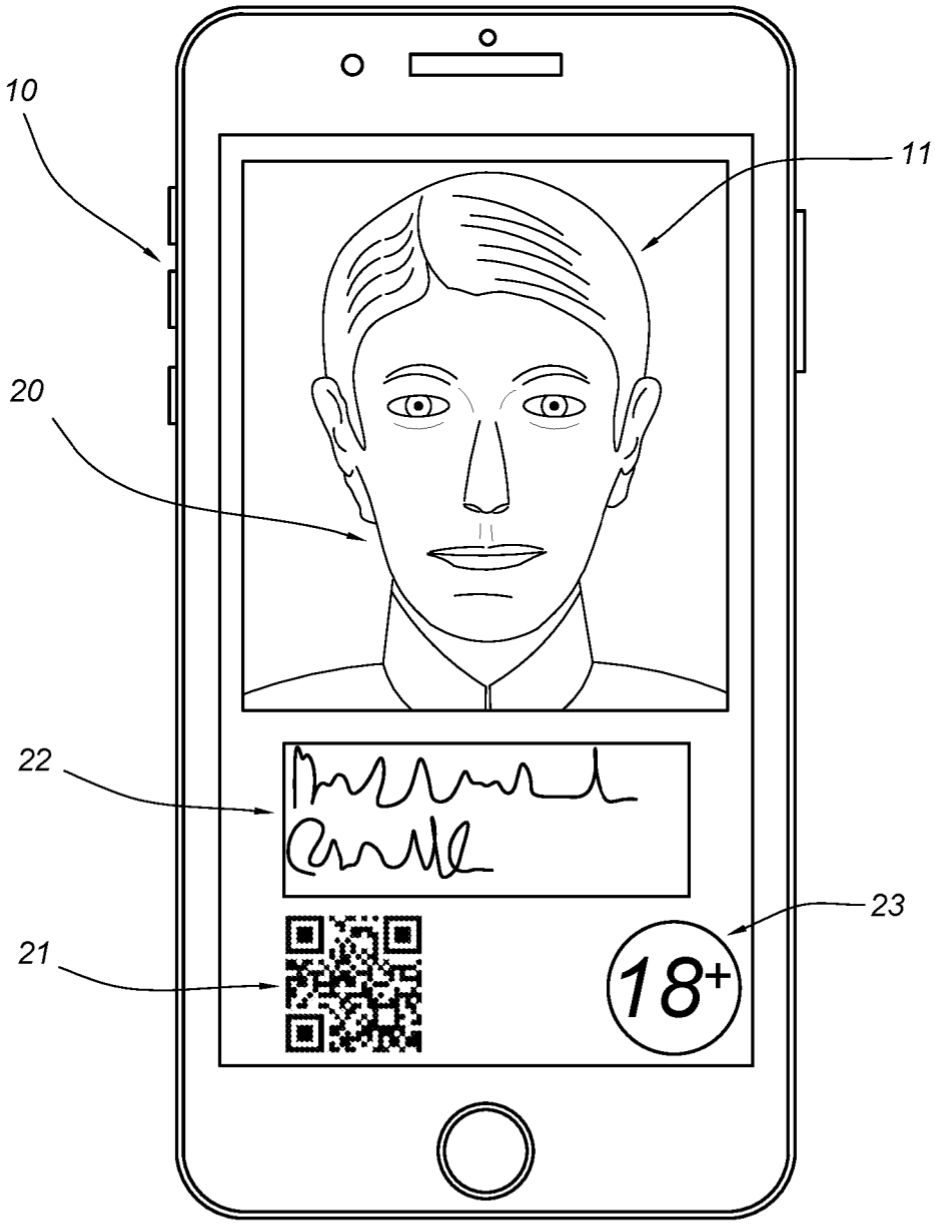


Fig. 1C

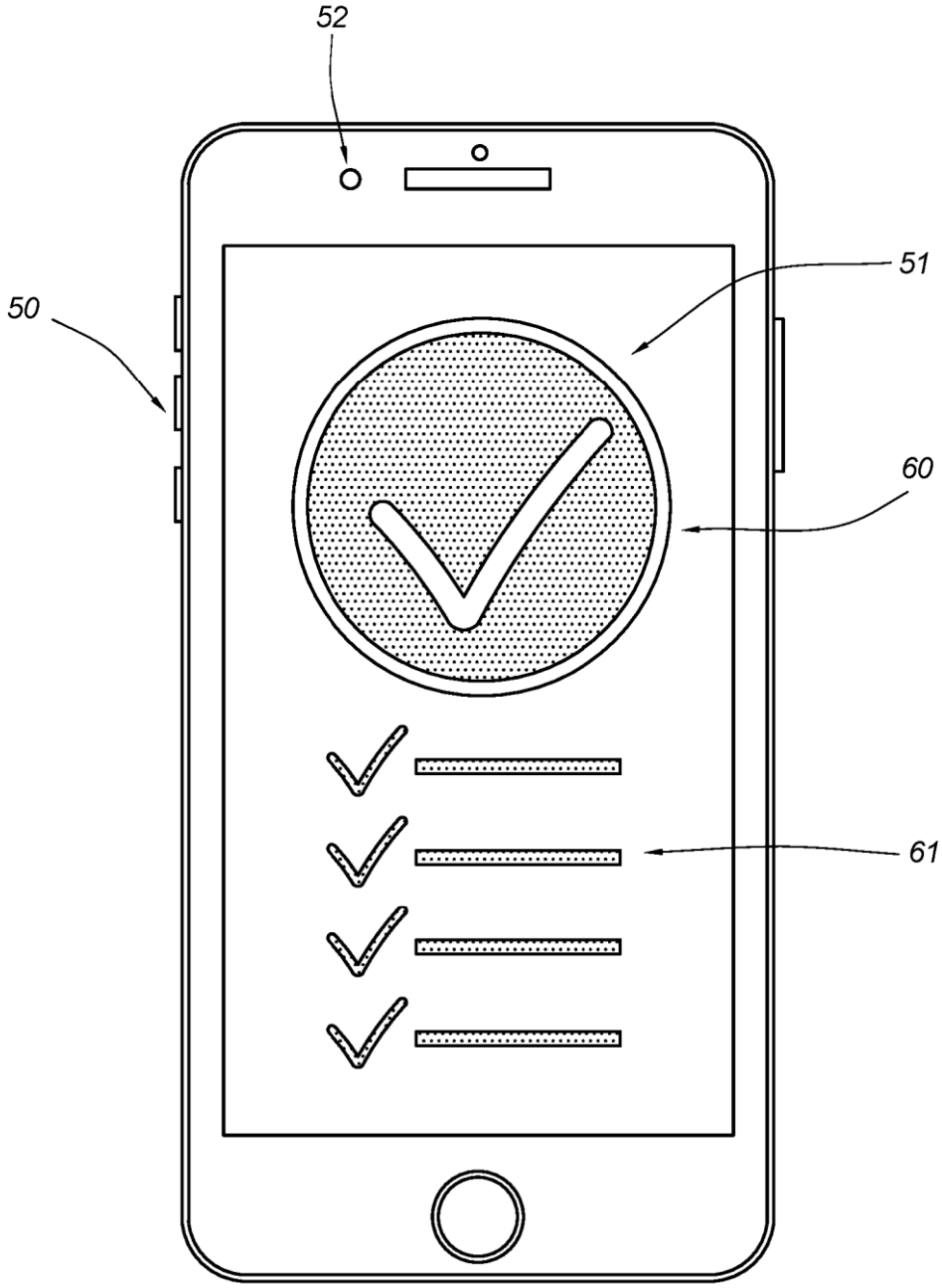


Fig. 1D

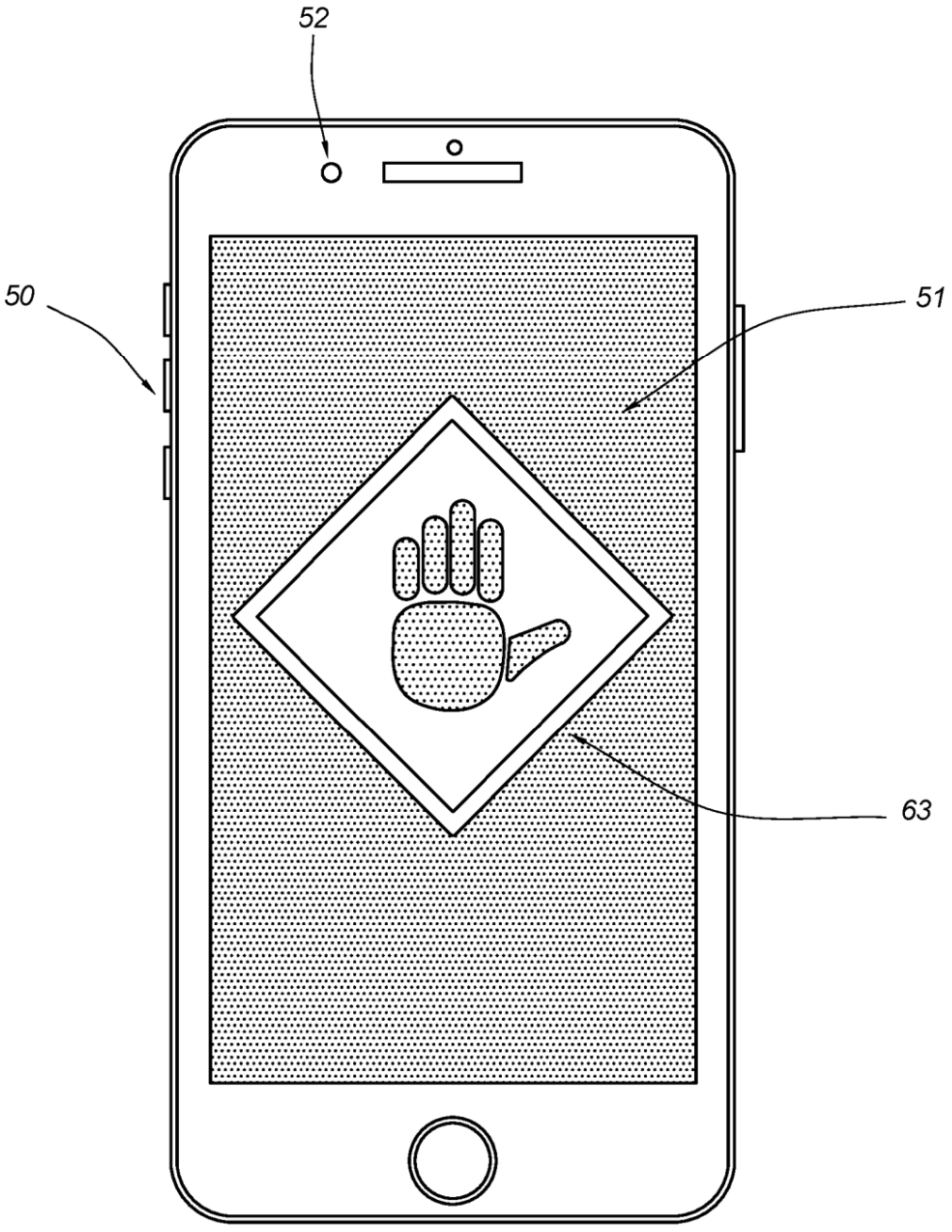


Fig. 1E

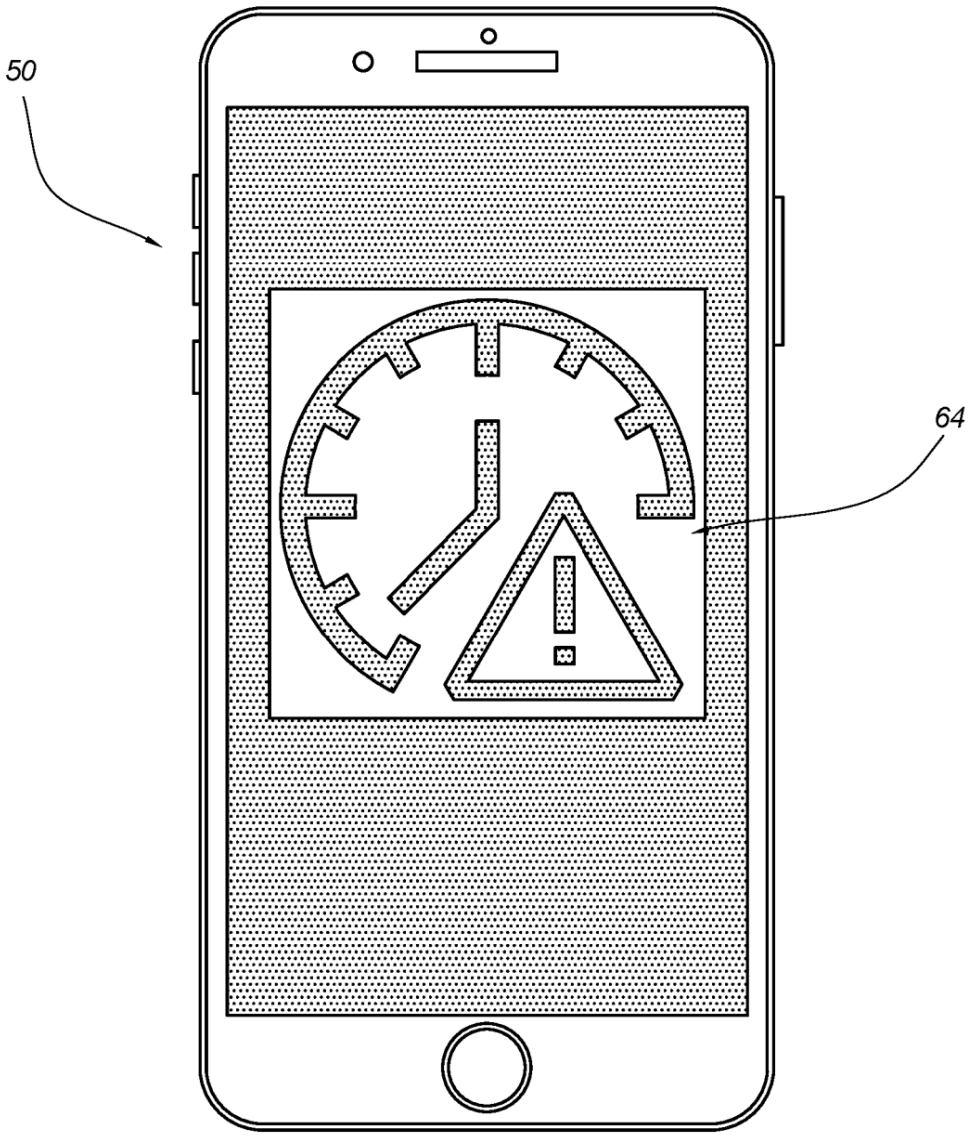
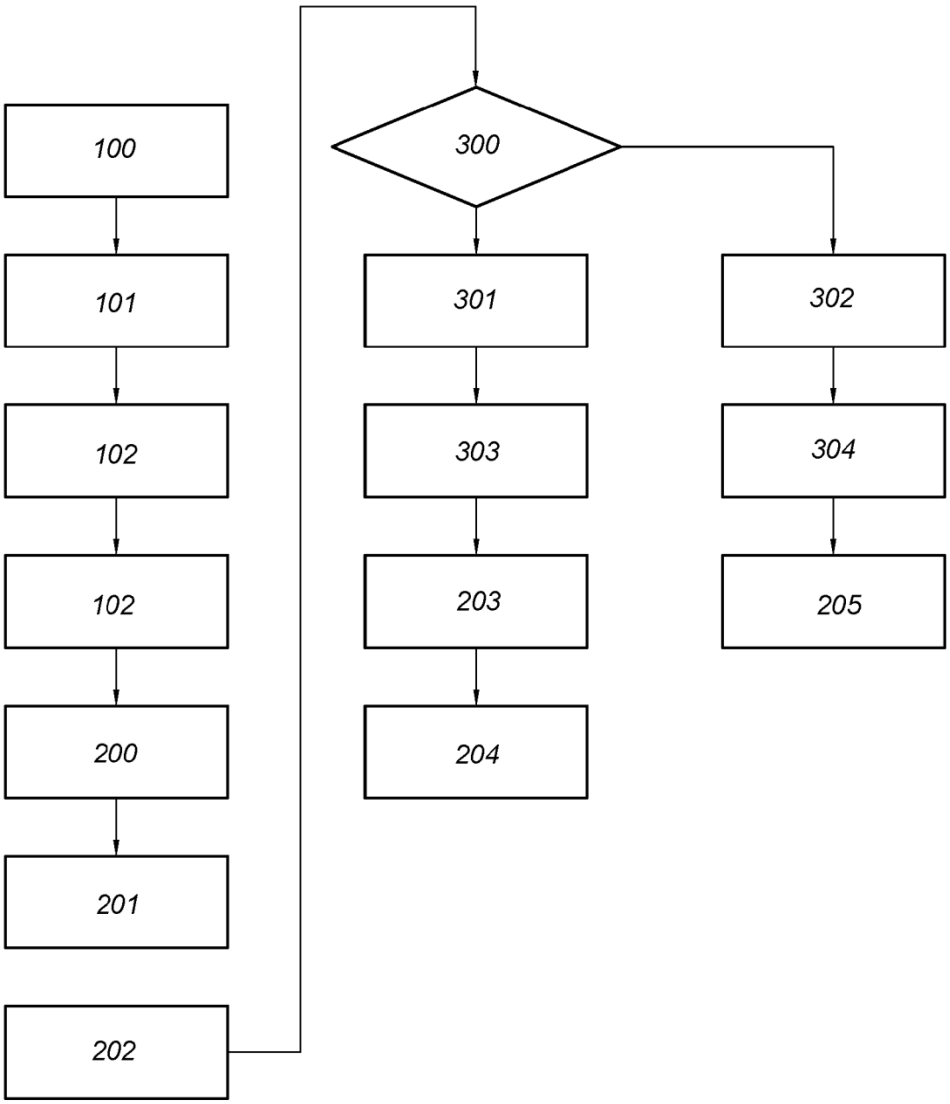


Fig. 2



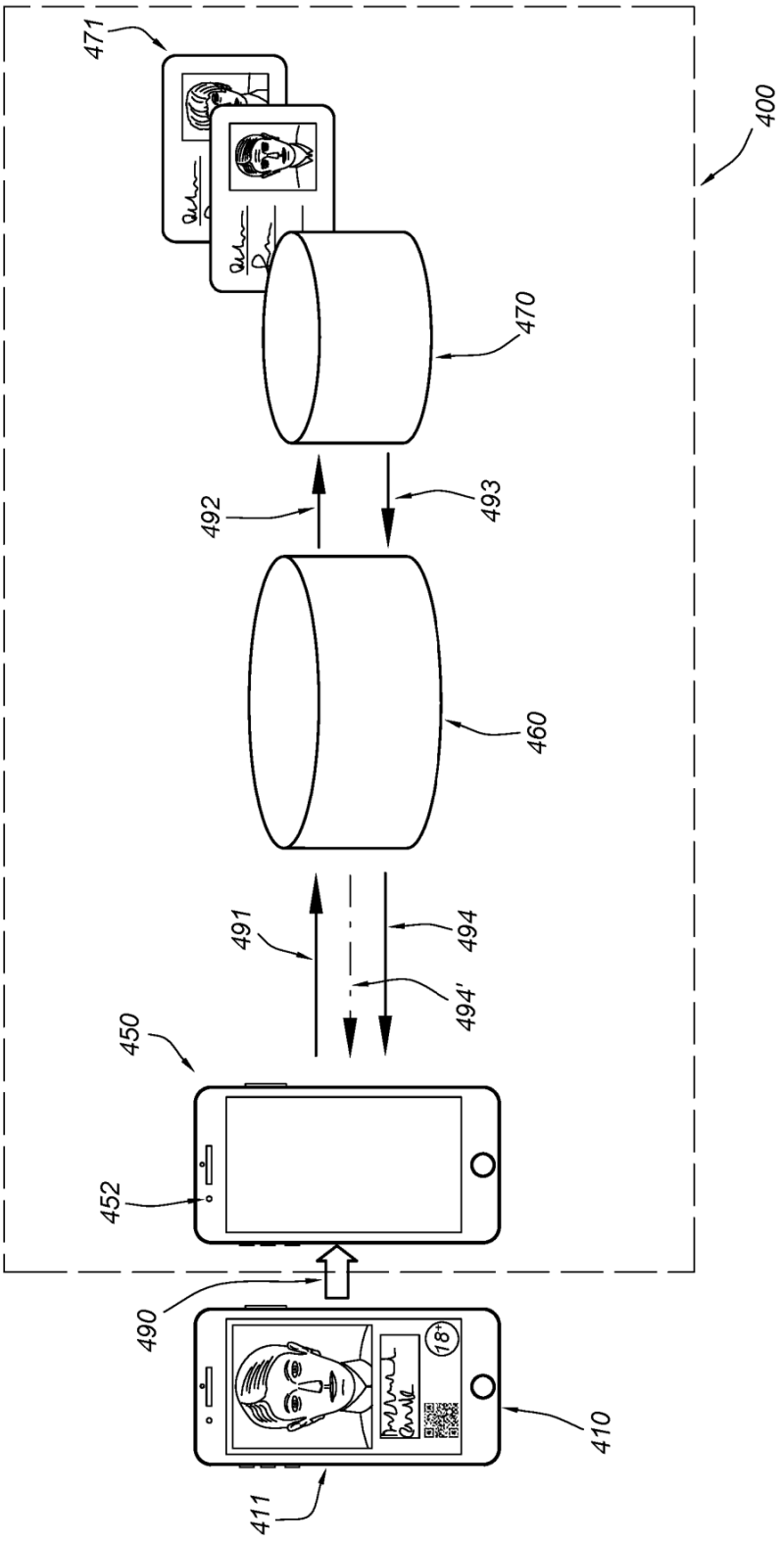


Fig. 3

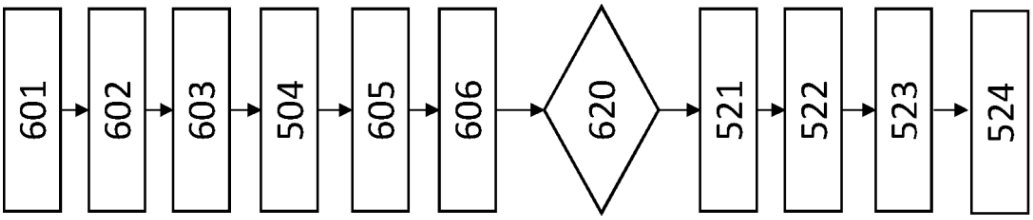

601
602
603
504
605
606
620
521
522
523
524

Fig. 5

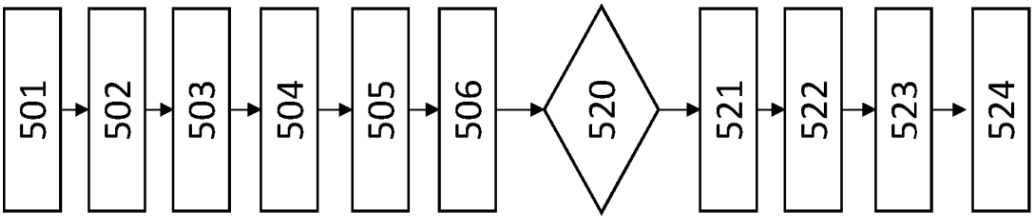

501
502
503
504
505
506
520
521
522
523
524

Fig. 4