(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 793 306**

(51) Int. CI.:

G06F 21/32 (2013.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **13.01.2014 E 16169902 (0)**

(97) Fecha y número de publicación de la concesión europea: **26.02.2020 EP 3086251**

(54) Título: **Identificación de usuario**

(30) Prioridad:

22.01.2013 DE 102013100635

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
13.11.2020

(73) Titular/es:

IDNOW GMBH (100.0%)
Auenstraße 100
80469 München, DE

(72) Inventor/es:

BAUER, ARMIN

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Identificación de usuario

Diversas formas de realización se refieren a un procedimiento para la identificación de un usuario y a un sistema para identificar a un usuario. En particular, diversas formas de realización se refieren a técnicas que posibilitan la identificación de un usuario por medio de primeros y segundos datos de imagen transmitidos desde un terminal del usuario a un servidor de identificación.

Son conocidos escenarios en los que se pretende la identificación de un usuario. La identificación del usuario puede significar en este caso: verificar o proporcionar la identidad del usuario o verificar o proporcionar uno o varios criterios de identidad del usuario. Tales criterios de identidad pueden ser en diferentes escenarios, por ejemplo: una edad del usuario, un lugar de residencia del usuario y/o un nombre del usuario.

Tales escenarios pueden ser, por ejemplo, en particular, transacciones en las que la identidad es crítica, tales como contratos de compra o transferencias bancarias o controles de acceso, en los que debido a las regulaciones legales o intereses personales debe asegurarse que se constata la identidad del copartícipe de la transacción y/o que los criterios de identidad satisfagan determinados prerrequisitos – por ejemplo, la mayoría de edad o un lugar de residencia en un país determinado, etc. Esto significa que dependiendo de la identificación puede realizarse una autenticación del usuario.

Sin embargo, puede pretenderse en otros escenarios que no sean críticos en cuanto a identidad, o no particularmente críticos, proporcionar técnicas sencillas y rápidas para la identificación del usuario.

Típicamente, tales escenarios pueden requerir en la identificación un grado relativamente alto de fiabilidad y/o de seguridad frente a falsificación y/o seguridad frente a fraude. Por ejemplo, puede pretenderse configurar de forma segura la identificación del usuario frente a la falsificación de documentos de identificación y/o fraudes deliberados.

Son conocidas a este respecto técnicas de identificación que se basan en que un usuario se presenta personalmente en un centro autorizado. Allí, puede ser empleado para la identificación un documento de identificación con una foto del usuario.

Son conocidos diferentes tipos de documentos de identificación, por ejemplo: pasaporte, carnet de identidad y/o carnet de conducir.

Otros procedimientos de identificación ya conocidos se basan en la identificación mediante sistemas de base de datos, que vinculan una cuenta bancaria del usuario con la identidad del usuario. Entonces, mediante la capacidad del usuario de acceder a la cuenta bancaria, por ejemplo, mediante una transacción bancaria, puede ser verificada la identidad y así realizada la identificación.

Sin embargo, tales procedimientos de identificación ya conocidos presentan la peculiaridad de que la identificación es relativamente complicada y/o requieren un período de tiempo relativamente largo. Por ejemplo, los procedimientos de identificación que se basan en que el usuario se presenta personalmente en un centro autorizado, requieren que el usuario consulte los horarios de oficina del centro autorizado para presentar su documento de identificación. Esto puede ser particularmente costoso y requerir mucho tiempo, especialmente cuando el centro autorizado está relativamente lejos del lugar de residencia o de trabajo del usuario. También puede no ser posible, o serlo solo de un modo limitado, realizar la identificación espontánea de un usuario por ejemplo fuera de las horas de oficina del centro autorizado, por la noche o en días festivos.

En los procedimientos de identificación que requieren la realización de una transacción bancaria utilizando la cuenta bancaria del usuario se puede producir un período de latencia relativamente largo. Esto puede ser debido a que típicamente la realización de transacciones bancarias requiere un período de tiempo relativamente largo, por ejemplo, en el intervalo de días. También en tales escenarios, la identificación espontánea el usuario puede no ser posible o serlo solo de forma limitada.

Precisamente en lo que respecta a las operaciones comerciales en línea basadas en Internet, que el usuario realiza por ejemplo desde su casa a través de un terminal, tal como un ordenador, un teléfono móvil, un televisor, una tableta, un ordenador portátil, etc., puede pretenderse a menudo la identificación del usuario. Este puede ser el caso, por ejemplo, si la operación comercial del usuario comprende transacciones relevantes a la edad o especialmente críticas en cuanto a identidad. En tal caso, puede ser particularmente deseable llevar a cabo la identificación del usuario en una escala de tiempo corta y/o de forma espontánea. En particular, puede pretenderse llevar a cabo la identificación del usuario de tal manera que esta sea independiente de una posición del usuario o de su terminal, de modo que el usuario pueda conseguir la identificación incluso desde casa o desde el lugar de trabajo.

El documento US 2012/0106805 A1 da a conocer un procedimiento para la comprobación de la identidad de un usuario alejado que incluye que durante una sesión de autenticación sean proporcionadas por parte de un ordenador central indicaciones de cómo posar para un aparato alejado. Además, el ordenador central recibe una imagen del aparato que puede analizar para determinar si fueron seguidas las indicaciones para posar. Basándose en esta

determinación y otros factores opcionales el ordenador central verifica un atributo de identidad del usuario.

La página web de la empresa IDscan (URL: https://web.archive.org/web/20121116001247/http://idscan.co.uk/id-check-idsmart) describe un procedimiento que comprende la captura de imagen de un documento de identidad y la rápida validación del mismo por comparación con una biblioteca de documentos. Además, la autenticación se puede conseguir si se le pide al usuario la captura de una foto. A continuación, mediante algoritmos de reconocimiento de rostro se valida si la imagen del documento de identidad y del usuario coinciden.

Por tanto, hay una necesidad de mejorar las técnicas para la identificación de un usuario. En particular, hay una necesidad para aquellas técnicas que posibilitan una identificación relativamente simple y relativamente rápida del usuario. Además, hay una necesidad para aquellas técnicas que posibilitan una identificación del usuario independientemente de la posición del usuario y que permiten una identificación segura frente a falsificación y fraude.

Este objeto se consigue mediante las reivindicaciones independientes. Las reivindicaciones dependientes definen otras formas de realización.

De acuerdo con un aspecto, la invención se refiere a un procedimiento para la identificación de un usuario. El procedimiento comprende la recepción en un servidor de identificación de primeros datos de imagen desde un terminal del usuario. Los primeros datos de imagen representan un documento de identificación con una fotografía del usuario. El procedimiento comprende además la recepción en el servidor de identificación de segundos datos de imagen desde el terminal del usuario, representando los segundos datos de imagen una parte de la cara del usuario. El procedimiento comprende además la identificación del usuario, comprendiendo la identificación la comparación de los primeros datos de imagen con los segundos datos de imagen para determinar una semejanza de la fotografía del usuario de los primeros datos de imagen con la parte de la cara del usuario de los segundos datos de imagen. El procedimiento puede comprender además la determinación de datos de identificación del usuario a partir del documento de identificación.

Por ejemplo, el servidor de identificación puede ser un servidor web que esté conectado a Internet. En consecuencia, la recepción de los primeros y/o los segundos datos de imagen desde el terminal del usuario se puede realizar a través de Internet.

La comparación de los primeros datos de imagen con los segundos datos de imagen se puede hacer de forma automática, parcialmente automática o manual. Por ejemplo, en técnicas automáticas y/o parcialmente automáticas la comparación de los datos de imagen puede comprender: la extracción de una representación de la fotografía del usuario a partir de los primeros datos de imagen; y la realización de un registro de imágenes entre la representación de la fotografía y los segundos datos de imagen para obtener un grado de similitud entre la representación de la fotografía y los segundos datos de imagen; y la realización de una comparación de valor de umbral entre el grado de similitud y un valor umbral de referencia predeterminado. También es posible que el valor umbral de referencia sea predeterminado en función de un nivel de seguridad, pudiendo ser el nivel de seguridad indicativo de una seguridad frente a falsificación y fraude pretendida. Los datos, que son indicativos del nivel de seguridad, pueden ser recibidos en el servidor de identidad de otro servidor.

De este modo puede ser posible comprobar de forma automática o parcialmente automática si la fotografía del usuario, tal como se recibió en los primeros datos de imagen, presenta una similitud grande o pequeña con la parte de la cara del usuario, tal como es obtenida de los segundos datos de imagen. En caso de un grado suficientemente grande de similitud, es decir, en caso de un resultado positivo de la comparación de valor umbral, se puede aceptar que el documento de identificación y el usuario se corresponden. Los datos de identificación describen entonces con gran probabilidad la identidad del usuario y pueden ser utilizados para la identificación. Puede ser obtenido un resultado de identificación positivo.

En consecuencia, también sería posible que la comparación de los primeros datos de imagen con los segundos datos de imagen se llevara a cabo manualmente, por ejemplo, por un personal operario. El personal operario puede obtener por ejemplo los primeros y los segundos datos de imagen del servidor de identificación y realizar la comparación de los primeros y los segundos datos por inspección. Por ejemplo, la comparación manual puede solo ser realizada de forma selectiva cuando con las técnicas automáticas no fue determinado un grado de similitud suficientemente grande de la fotografía del usuario con la parte de la cara.

En caso de una gran (pequeña) similitud de la fotografía del usuario con la parte de la cara del usuario, se puede aceptar con alta (baja) probabilidad que el usuario es la persona identificada por el documento de identificación. Si ,por ejemplo, esta similitud es mayor que un valor umbral predeterminado, entonces la identidad o determinados criterios de identidad, como por ejemplo la edad o el nombre del usuario, pueden ser determinados a partir de determinados datos de identificación del documento de identificación.

La determinación de los datos de identificación del usuario a partir de los primeros datos de imagen en base al documento de identificación puede comprender, por ejemplo: la realización de un reconocimiento de texto automático de los primeros datos de imagen para determinar los datos de identificación en forma legible electrónicamente. Opcionalmente, la determinación de los datos de identificación puede comprender: el

reconocimiento de un tipo de documento de identificación en base a los primeros datos de imagen. Como se describió anteriormente, son conocidos diferentes tipos de documentos de identificación, tales como pasaportes, carnets de identidad, carnets de conducir, etc., cada uno con una forma diferente para diferentes países o territorios soberanos o jurisdicciones. Por regla general, los diferentes tipos de documentos de identificación presentan diferentes datos de identificación del usuario. Por tanto, puede ser deseable reconocer en primer lugar el tipo de documento de identificación y, a continuación, determinar los datos de identificación.

Por ejemplo, los datos de identificación pueden comprender: la edad del usuario, el nombre de usuario, la dirección del usuario, la cuenta bancaria del usuario y/o la fecha de nacimiento del usuario, el número de identificación del documento de identificación, el lugar de expedición del documento de identificación, la fecha de expedición del documento de identificación, la validez del documento de identificación, etc.

Es posible que el procedimiento comprenda, además: la comparación de los datos de identificación determinados con datos de identificación de referencia. Es posible que el procedimiento comprenda la recepción de los datos de identificación de referencia de identificación en el servidor de identificación. Alternativa o adicionalmente sería posible que el procedimiento comprendiera: en función de la comparación, el envío de los datos de identificación del usuario a otro servidor. Entonces sería posible que la comparación de los datos de identificación determinados con datos de identificación de referencia se llevara a cabo en el otro servidor. El otro servidor puede ser, por ejemplo, un servidor de una parte que solicita la identificación, es decir, por ejemplo, un servidor de tienda en Internet, un servidor de banco, etc.

Por las técnicas descritas anteriormente puede ser posible realizar una identificación relativamente rápida del usuario. Por ejemplo, puede ser posible que el usuario capte los primeros y los segundos datos de imagen por medio del terminal y los envíe a través de Internet al servidor de identificación. Para ello, el usuario no tiene que encontrarse en una relación de localización determinada con respecto al servidor de identificación, el usuario puede encontrase por ejemplo en casa o en su lugar de trabajo. Cuando son recibidos los primeros y los segundos datos de imagen en el servidor de identificación, puede ser posible, sin tiempo de espera adicional significativo, llevar a cabo la identificación del usuario mediante la comparación de los primeros y los segundos datos de imagen, y la determinación de los datos de identificación en base al documento de identificación.

Además, mediante la comparación de los primeros y segundos datos de imagen para determinar la similitud puede ser posible una identificación relativamente segura. A continuación, se describirán escenarios que pueden favorecer adicionalmente la seguridad de la identificación.

El procedimiento puede comprender, además: la generación de datos de validación en el servidor de identificación y el envío de los datos de validación desde el servidor de identificación al terminal. Los datos de validación pueden permitir al terminal contener información de validación adicional en los primeros datos de imagen y/o en los segundos datos de imagen. La identificación puede comprender además la determinación de la información de validación a partir de los primeros datos de imagen y/o de los segundos datos de imagen y la validación de la información de validación en base a los datos de validación generados.

Es posible que la generación de los datos de validación en el servidor de identificación comprenda: la consideración de resultados aleatorios y/o la consideración de la hora de generación y/o la consideración de una identificación del terminal de usuario.

Tales técnicas pueden permitir que datos de validación generados de manera diferente presenten diferentes valores. De este modo puede ser posible que la forma concreta de los datos de validación dependa del proceso concreto de identificación del usuario. Por ejemplo, las informaciones de validación validadas pueden ser indicativas de una autenticidad de los primeros y/o segundos datos de imagen. Falsificaciones o fraudes pueden ser evitados.

Mediante la generación de los datos de validación en el servidor de identificación y la posterior validación de la información de validación determinada en base a los datos de validación generados se puede asegurar, por ejemplo, que existe una estrecha relación temporal entre la generación de los primeros y segundos datos de imagen y la generación de los datos de validación. Por ejemplo, concretamente la generación de los datos de validación puede realizarse usando una tecnología propietaria y/o mediante acciones generadas aleatoriamente (generador aleatorio), de manera que no sea posible o lo sea solo de forma limitada, que sean utilizados datos de imagen prefabricados, es decir datos de imagen que fueron generados antes de la generación de los datos de validación. En otras palabras, los datos de validación pueden presentar un instante de generación determinado y/o una determinada duración, y mediante la generación y el uso de los datos de validación se puede asegurar que los datos de imagen fueron creados después del instante de generación de los datos de validación o dentro de la duración de los datos de validación.

La información de validación puede comprender al menos uno de los siguientes elementos: una marca de agua, que está imprimida en los primeros y/o los segundos datos de imagen; y/o un código alfanumérico que está representado en los primeros datos de imagen y/o en los segundos datos de imagen; y/o una posición y/o una distancia de una cámara que capta los datos de imagen con respecto al documento de identificación y/o la parte de la cara; y/o un código alfanumérico que está representado en los primeros datos de imagen y/o en los segundos datos de imagen y

que contiene un instante o un período de tiempo.

Es posible incluir la información de validación automáticamente en los primeros datos de imagen y/o en los segundos datos de imagen, por ejemplo, mediante técnicas de procesamiento de imágenes simples.

La marca de agua puede ser, por ejemplo, un plano semitransparente superpuesto (en inglés “layer”) a los primeros y/o segundos datos de imagen. La marca de agua puede contener, por ejemplo, un código alfanumérico y/o un patrón legible por máquina. Estos pueden ser determinados, por ejemplo, como la información de validación de los primeros y/o segundos datos de imagen y ser comparados con los datos de validación. El código alfanumérico y/o el patrón legible por máquina pueden ser superpuestos en los primeros y/o los segundos datos de imagen.

En general, los primeros datos de imagen y/o los segundos datos de imagen pueden incluir también implícitamente información de validación. Es posible, por ejemplo, que los datos de validación contengan una indicación para el usuario, de qué manera, es decir, en qué la posición y/o a qué distancia, los primeros y/o segundos datos de imagen deben mostrar el documento de identificación y/o la parte de la cara, es decir, como deben ser captados los primeros y/o los segundos datos de imagen por medio del terminal. En este sentido, por ejemplo, sería posible una forma puramente de ejemplo y no limitativa de datos de validación: "distancia de 10 a 20 cm bajo una perspectiva de la parte superior izquierda". En tal escenario, los primeros y/o los segundos datos de imagen pueden contener implícitamente información de validación correspondiente, es decir, por ejemplo, en forma de las propiedades de perspectiva de los elementos mostrados en los primeros y/o en los segundos datos de imagen.

De acuerdo con ello, sería posible que se pidiera al usuario en base a los datos de validación, que escribiera la información de validación – por ejemplo, un código alfanumérico determinado o un patrón determinado – e incluirla en los primeros datos de imagen y/o los segundos datos de imagen. Esto se puede hacer, de manera que el usuario coloque la información de validación escrita, por ejemplo, en un trozo de papel o una hoja de papel, durante la captación de los primeros datos de imagen y/o los segundos datos de imagen en un campo de cara representado por los primeros y/o segundos datos de imagen.

El procedimiento puede comprender, además: la generación de datos de control en el servidor de identificación y el envío de los datos de control desde el servidor de identificación al terminal. Los datos de control pueden instruir al terminal para captar los primeros datos de imagen y/o los segundos datos de imagen con determinados parámetros de imagen. Los parámetros de imagen pueden ser seleccionados preferentemente del siguiente grupo: número de imágenes; parámetros de exposición; función de flash; resolución de la imagen. Los parámetros de exposición pueden ser seleccionados, por ejemplo, del siguiente grupo: número de diafragma, tiempo de exposición, sensibilidad de luz.

Los primeros datos de imagen y/o los segundos datos de imagen comprenden una secuencia de imágenes, por lo que los datos de control pueden ser respectivamente diferentes para las diferentes imágenes de la secuencia de imágenes.

Por ejemplo, la generación de los datos de control puede realizarse en función de un valor aleatorio, realizarse en función de un instante y/o realizarse en función de una identidad del terminal del usuario. De esta forma puede asegurarse que los diferentes datos de control generados presentan valores diferentes.

Sería posible que el procedimiento comprendiera: la validación de las propiedades ópticas de los primeros datos de imagen y/o los segundos datos de imagen basada en los datos de control. Por ejemplo, la validación de las propiedades ópticas puede comprender: determinar un histograma de luminosidad para los primeros y/o los segundos datos de imagen y correlacionar el histograma de luminosidad determinado con los parámetros de exposición de los datos de control. Sería posible que el procedimiento comprendiera: la determinación de un ruido de la imagen para los primeros y/o los segundos datos de imagen y la correlación del ruido de la imagen determinado con los parámetros de exposición de los datos de control. Por ejemplo, los primeros y/o los segundos datos de imagen pueden contener los parámetros de exposición y/o un indicador de la función de flash en forma legible electrónicamente. Luego, estos pueden ser comparados con los datos de control generados en el servidor.

Pueden conseguirse efectos, en particular con respecto de la seguridad frente a falsificación y engaño, que son comparables a los efectos que fueron tratados antes con respecto a los datos de validación y el formato de validación. Por tanto, por la predeterminación de los parámetros de imagen con los que el terminal capta los primeros y/o los segundos datos de imagen, se puede evitar que sean transmitidos al servidor de identificación primeros y segundos datos de imagen prefabricados en el marco del procedimiento actualmente discutido para la identificación del usuario.

Los primeros datos de imagen y/o los segundos datos de imagen pueden ser seleccionados del siguiente grupo: una imagen; una película; al menos dos imágenes o dos películas, que son captadas secuencialmente en diferentes instantes; al menos dos imágenes o dos películas que son captadas, respectivamente, con diferentes parámetros de exposición, al menos dos imágenes o películas que muestran el documento de identificación o una parte de la cara desde diferentes perspectivas y/o distancias.

Por ejemplo, los datos de control descritos anteriormente pueden determinar qué elementos contienen los primeros

datos de imagen y/o los segundos datos de imagen.

En diferentes escenarios puede ser posible por ejemplo que los primeros datos de imagen y/o los segundos datos de imagen contengan, respectivamente, tres imágenes del documento de identificación y de la parte de la cara del usuario, captadas desde perspectivas respectivamente diferentes y secuencialmente en diferentes instantes.

Por ejemplo, puede ser posible de este modo evitar fraudes que se basan en que es captada una representación de fotografías prefabricadas para los primeros datos de imagen y/o los segundos datos de imagen. Este puede ser el caso, ya que por ejemplo una representación de la parte de la cara en los segundos datos de imagen es diferente para un escenario en el que los segundos datos de imagen son captados en base a la parte real de la cara del usuario, por ejemplo, por medio de una cámara, y para un escenario en el que los segundos datos de imagen son obtenidos mediante la captación de una fotografía bidimensional prefabricada de la parte de la cara del usuario.

Mediante el uso de al menos dos imágenes, que son captadas con parámetros de exposición respectivamente diferentes, por ejemplo, diferentes tiempos de exposición, puede ser posible hacer bien visibles determinadas características de seguridad del documento de identificación en los primeros datos de imagen. Por ejemplo, diferentes tipos de documentos de identificación pueden incluir tales características de seguridad, como marcas de agua, hologramas, estructuras de seguridad, etc. Típicamente, tales características de seguridad pueden ser en particular visibles cuando se utilizan diferentes parámetros de exposición y/o funciones de flash.

También con respecto a los segundos datos de imagen puede ser comprobada la autenticidad de la parte de la cara del usuario mediante el uso de diferentes parámetros de exposición y/o funciones de flash. Así, por ejemplo, mediante el uso de funciones de flash puede ser posible estimular o evitar de forma selectiva el llamado “efecto de ojos rojos” en los segundos datos de imagen para la parte de la cara del usuario. Si, por ejemplo, son recibidas dos imágenes en el marco de los segundos datos de imagen que una vez fueron captadas con tales parámetros de flash que estimulan el "efecto de ojos rojos", y una vez fueron recibidos con tales parámetros de flash que suprimen el "efecto de ojos rojos", entonces la presencia del "efecto de ojos rojos" en los segundos datos de imagen pueden ser un indicio de la autenticidad de los segundos datos de imagen recibidos.

El procedimiento comprende, además: la recepción de una petición de identificación de otro servidor en el servidor de identificación. El procedimiento puede comprender: en respuesta a la identificación, el envío de un resultado de identificación desde el servidor de identificación al otro servidor con referencia a la solicitud de identificación recibida.

Por ejemplo, el otro servidor puede ser un servidor de tienda por internet o un servidor de banco. Sin embargo, la configuración especial del otro servidor no está particularmente limitada y pueden ser empleadas técnicas correspondientes para una amplia variedad de otros servidores.

El procedimiento puede comprender, por ejemplo, además: la comprobación de si es necesaria una identificación del usuario, en el que la comprobación tiene lugar basándose en una conexión entre otro servidor y el terminal del usuario.

El procedimiento comprende, además: en respuesta a la recepción de la petición de identificación, el envío de una frase clave desde el servidor de identificación al otro servidor. En respuesta a la frase clave recibida, el otro servidor envía la clave-frase a otro terminal del usuario o al terminal, preferiblemente para iniciar la identificación. Por ejemplo, la frase clave puede designar de forma unívoca un proceso de identificación en el servidor de identificación (en inglés “token”). El terminal establece una conexión con el servidor de identificación utilizando la frase clave; por ejemplo, para ello se le pedirá al usuario que introduzca en el terminal la frase clave que le ha sido trasmitida desde el otro terminal. Por ejemplo, si la frase clave es enviada directamente al terminal del usuario, entonces el terminal puede también establecer automáticamente la conexión con el servidor de identificación utilizando la frase clave. Mediante el uso de una frase clave que designa de forma unívoca el proceso de identificación puede evitarse, por ejemplo, que un tercero no autorizado interfiera con la identificación. Para ello, la frase clave puede ser, por ejemplo, un código alfanumérico de longitud suficientemente grande para evitar de este modo que la frase clave se pueda adivinar.

En cada caso, el contenido de información de la petición de identificación y del resultado de identificación puede ser diferente en diferentes escenarios. Por ejemplo, la petición de identificación puede indicar solamente la necesidad del otro servidor para la identificación. Por ejemplo, la petición de identificación puede contener los datos de identificación de referencia.

El resultado de la identificación y/o la petición de identificación pueden comprender al menos uno de los siguientes: un indicador que muestra un resultado de identificación positivo o negativo; un nombre del usuario; un nombre de pila y/o apellido del usuario; una fecha de nacimiento y/o una edad del usuario; un indicador que indica si la edad del usuario es mayor que un valor umbral de edad; un lugar de residencia del usuario; una dirección del usuario; un código postal del lugar de residencia del usuario; datos de identificación anonimizados del usuario; una clasificación de datos de identificación del usuario con respecto a una clasificación de referencia; una contraseña de usuario.

Por ejemplo, la clasificación de referencia puede especificar un intervalo determinado de datos de identificación, por ejemplo, un intervalo de códigos postales determinado, determinados números de teléfono, etc. A continuación, se

puede comprobar si los datos de identificación están dentro del intervalo o no. El valor umbral de la edad puede ser, por ejemplo 18 o 21, y, corresponder, por tanto, a la mayoría de edad.

La identificación de usuario puede comprender además la comparación de los datos de identificación determinados con la petición de identificación.

A través de esta comparación puede ser posible permitir una autenticación del usuario basada en la identificación. El usuario puede en primer lugar transmitir al otro servidor criterios de identificación necesarios, de modo que estos puedan ser transmitidos al servidor de identificación en el marco de la petición de identificación. En el marco de las técnicas de identificación descritas anteriormente, son determinados a continuación los datos de identificación y estos comparados con los criterios de identificación. En caso de coincidencia puede ser concedida una autorización y en caso contrario ser denegada. La comparación puede tener lugar en diferentes escenarios también en el otro servidor – para ello los datos de identificación pueden ser enviados al otro servidor, en su totalidad o parcialmente, como parte del resultado de identificación.

Por ejemplo, en un escenario sería posible que la petición de identificación, que el servidor de identificación recibe del otro servidor, contenga el nombre del usuario. El servidor de identificación, mediante las técnicas descritas en el presente documento, podría realizar el procedimiento para la identificación del usuario y comparar los datos de identificación determinados del usuario con el nombre del usuario que figura en la petición de identificación. Dependiendo de si este criterio de identificación proporciona o no una coincidencia, el resultado de identificación enviado puede incluir un indicador que indique un resultado de identificación positivo o negativo. Alternativa o adicionalmente, el resultado de identificación podría incluir un indicador que indique si la edad del usuario es mayor que un valor umbral de edad, por ejemplo, mayor de 18 años.

En un escenario correspondiente sería posible que la petición de información recibida por el otro servidor no contenga más detalles sobre la identidad del usuario. En tal caso, en el marco de la identificación del usuario no podría tener lugar ninguna comparación entre los datos de identificación determinados del usuario e informaciones que estuvieran contenidas en la petición de identificación. En consecuencia, sería posible que el resultado de identificación enviado presentara un contenido de información correspondientemente grande, por ejemplo, el nombre del usuario y/o la fecha de nacimiento o la edad del usuario.

Por ejemplo, sería posible que el servidor de identificación recibiera la contraseña de usuario desde el terminal. Por ejemplo, la contraseña del usuario puede ser elegida por el usuario. Entonces sería posible que el servidor de identificación enviara la contraseña de usuario al otro servidor, por ejemplo, en el marco del resultado de identificación y/o por separado. De esta forma puede ser posible que, para una identificación posterior en el otro servidor, el usuario solo tenga que introducir su contraseña de usuario, que junto con los datos de identificación es conocida para el otro servidor.

Como puede verse de lo anterior, en diferentes escenarios puede estar incluido un contenido de información mayor o menor, respectivamente, en la petición de identificación o en el resultado de identificación. En otras palabras, la lógica de la comprobación de un criterio de identificación puede estar presente en mayor o menor parte en el servidor de identificación (el otro servidor).

Además, dependiendo del escenario, un tipo de la información contenida en el resultado de identificación y/o en la petición de identificación puede ser diferente. Por ejemplo, en el caso de una verificación de edad o una autenticación de la edad del usuario puede ser suficiente que el resultado de identificación contenga la edad del usuario o únicamente un indicador que indique si la edad del usuario es mayor que un valor umbral de edad. Sin embargo, si se desea una identificación adicional a la del usuario, entonces las informaciones adicionales correspondientes, por ejemplo: el nombre, lugar de residencia y otros datos, puede incluirse en el resultado de la identificación. En el caso de una verificación de los datos de usuario, es posible que los datos de usuario a ser verificados estén incluidos en la petición de identificación y el resultado de identificación incluya solamente un indicador positivo o negativo que indique una verificación positiva o negativa de los datos de usuario. Son posibles diferentes combinaciones de los escenarios descritos anteriormente.

La identificación puede comprender además al menos una de las siguientes etapas: la verificación de características de integridad del documento de identificación de los primeros datos de imagen, de modo que las características de integridad contienen: números de comprobación y/o marcas de agua y/o imágenes de holograma y/o datos biométricos; y la verificación de metadatos que son recibidos con los primeros datos de imagen y/o con los segundos datos de imagen, de modo que los metadatos comprenden un instante de registro de los primeros datos de imagen y/o un instante de registro de los segundos datos de imagen y/o una identificación del terminal y/o una posición de registro de los primeros datos de imagen y/o una posición de registro de los segundos datos de imagen.

El procedimiento puede comprender: la realización de una comprobación de consistencia del documento de identificación en base a las características de integridad del documento de identificación. Por ejemplo, se pueden comprobar mediante sumas de comprobación si las cifras o letras individuales de los datos de identificación del documento de identificación han sido cambiados, por ejemplo, si de un "1" se hizo un "4" etc. Las falsificaciones pueden ser evitadas.

Para los diferentes tipos de documentos de identificación son conocidos diferentes tipos de características de integridad. Por ejemplo, por medio de la suma de comprobación puede ser posible reconocer falsificaciones y/o errores de los datos de identificación del usuario. La presencia de características de integridad, tales como marcas de agua y/o imágenes de holograma pueden también hacer que sea posible verificar la integridad del documento de identificación mostrado en los primeros datos de imagen. También es posible que a partir de los primeros datos de imagen puedan ser determinados datos biométricos del usuario, por ejemplo, un color de ojos, etc. La comparación de los primeros datos de imagen con los segundos datos de imagen puede incluir entonces también una comparación de los datos biométricos con los segundos datos de imagen. Por ejemplo, un color de ojos del usuario, como está especificado en los datos biométricos del documento de identificación, es comparado con el color de ojos de la parte de la cara del usuario mostrado en los segundos datos de imagen.

El procedimiento puede comprender además la captación de los primeros datos de imagen mediante una cámara, representando los primeros datos de imagen un documento de identificación con una fotografía del usuario. El procedimiento puede además comprender la captación de los segundos datos de imagen mediante la cámara, representando los segundos datos de imagen una parte de la cara del usuario. Además, el procedimiento puede comprender el envío de los primeros datos de imagen y de los segundos datos de imagen desde el terminal del usuario al servidor de identificación para la identificación del usuario. La identificación se basa en una comparación de los primeros datos de imagen con los segundos datos de imagen para determinar una semejanza de la fotografía del usuario de los primeros datos de imagen con la parte de la cara del usuario de los segundos datos de imagen. La identificación se basa además en una determinación de datos de identificación del usuario a partir de los primeros datos de imagen en virtud del documento de identificación.

Por ejemplo, la cámara puede ser parte del terminal. Sería posible también que el terminal controlara una cámara externa. Por ejemplo, la cámara puede ser una cámara óptica o una cámara web o similar.

El procedimiento puede comprender, además: la recepción de datos de validación en el terminal, de modo que los datos de validación permiten incluir información de validación adicional en los primeros datos de imagen y/o en los segundos datos de imagen. La captación de los primeros datos de imagen y/o la captación de los segundos datos de imagen puede comprender, además: incluir la información de validación en los primeros datos de imagen y/o en los segundos datos de imagen.

Es posible, por ejemplo, que la información de validación contenga para los primeros datos de imagen una perspectiva determinada y/o una distancia determinada de la cámara al documento de identificación. Alternativa o adicionalmente, es posible por ejemplo que la información de validación para los segundos datos de imagen incluya una perspectiva determinada y/o una distancia determinada de la cámara a la parte de la cara.

En particular, en tal caso sería posible que el procedimiento comprendiera, además: la emisión al usuario de indicaciones, dependientes de la información de validación, por medio de una interfaz de usuario del terminal. La interfaz de usuario puede, por ejemplo, contener una indicación gráfica, un texto y/o una indicación de voz. Por ejemplo, la indicación puede solicitar al usuario que posicione la cámara con respecto al documento de identificación y/o la parte de la cara bajo una determinada perspectiva y/o distancia.

El procedimiento puede comprender además: la recepción de datos de control desde el servidor de identificación en el terminal, de modo que la captación de los primeros datos de imagen y/o la captación de los segundos datos de imagen se realiza con una secuencia determinada de parámetros de imagen que están incluidos en los datos de control, de manera que los parámetros de imagen son seleccionados del siguiente grupo: número de imágenes; parámetros de exposición; función de flash; resolución de la imagen.

Por los diferentes parámetros de exposición pueden ser producidas y comprobadas reflexiones en los primeros y/o segundos datos de imagen, que pueden ser en particular características de una autenticidad del patrón. Características de integridad, como por ejemplo hologramas o marcas de agua del documento de identificación representado, pueden ser comprobadas de esta forma.

Mediante funciones técnicas adecuadas puede ser asegurado, además, que no es posible para el usuario, o lo es solo de un modo limitado, modificar estos parámetros de imagen automáticamente, es decir, son fijados de forma independiente de los datos de control. En otras palabras, puede no ser posible o serlo solo de un modo limitado, realizar la captación de los primeros datos de imagen y/o la captación de los segundos datos de imagen dependiendo del terminal e independientemente de los datos de validación recibidos y/o de los datos de control recibidos. Esto puede en particular elevar la seguridad frente a fraudes y/o falsificaciones al identificar al usuario.

El servidor de identificación puede comprender una interfaz de comunicación, estando dicha interfaz de comunicación configurada para recibir primeros datos de imagen desde un terminal de un usuario y recibir segundos datos de imagen desde el terminal. Los primeros datos de imagen representan un documento de identificación con una fotografía del usuario. Los segundos datos de imagen representan una parte de la cara del usuario. El servidor de identificación puede además comprender un procesador que está diseñado para identificar al usuario, comprendiendo la identificación: la comparación de los primeros datos de imagen con los segundos datos de imagen para determinar una semejanza de la fotografía del usuario de los primeros datos de imagen con la parte de la cara

del usuario de los segundos datos de imagen; y la determinación de datos de identificación del usuario a partir de los primeros datos de imagen en virtud del documento de identificación.

El servidor de identificación puede estar diseñado para ejecutar el procedimiento para la identificación de un usuario.

Según otro aspecto la invención se refiere a un sistema para la identificación de un usuario según la reivindicación 11. El sistema comprende un terminal de un usuario, un servidor de identificación y otro servidor. El servidor de identificación comprende una interfaz de comunicación, estando diseñada la interfaz de comunicación para recibir primeros datos de imagen desde el terminal de un usuario y recibir segundos datos de imagen desde el terminal. Los primeros datos de imagen representan un documento de identificación con una fotografía del usuario. Los segundos datos de imagen representan una parte de la cara del usuario. El servidor de identificación comprende además un procesador que está configurado para identificar al usuario, en el que la identificación comprende: la comparación de los primeros datos de imagen con los segundos datos de imagen para determinar una similitud de la fotografía del usuario procedente de los primeros datos de la imagen con la parte de la cara del usuario procedente de los segundos datos de imagen y la determinación de datos de identificación del usuario procedentes de los primeros datos de imagen en base al documento de identificación. El otro servidor comprende además un procesador que está configurado para comprobar si es necesaria una identificación del usuario, en el que la comprobación se lleva a cabo basándose en una conexión entre el otro servidor y un terminal del usuario. El otro servidor comprende además una interfaz de comunicación que está configurada para, en función de la comprobación, enviar una petición de identificación al servidor de identificación, y para recibir un resultado de identificación desde el servidor de identificación.

El sistema puede además estar configurado para realizar un procedimiento para la identificación de un usuario de acuerdo con otro aspecto de la invención.

Para tal sistema pueden conseguirse efectos que son comparables con los efectos que pueden conseguirse para el procedimiento de identificación de un usuario de acuerdo con otro aspecto de la presente invención.

Las características expuestas anteriormente y características que serán descritas a continuación, se pueden utilizar no solo en las combinaciones correspondientes expuestas explícitamente, sino también en otras combinaciones o aisladamente, sin apartarse del alcance de protección de la presente invención.

Las propiedades, características y ventajas de esta invención, así como la manera de conseguirlas, descritas anteriormente, se harán más claras y evidentes y se podrán entender mejor en relación con la siguiente descripción de ejemplos de realización, que se explican en detalle en relación con los dibujos, en los que

Fig. 1: ilustra esquemáticamente un sistema de servidor de identificación con un servidor de identificación y otro servidor, así como un terminal de usuario;

Fig. 2, ilustra un documento de identificación de un usuario;

Fig. 3, ilustra primeros datos de imagen que representan el documento de identificación;

Fig. 4, es un diagrama de flujo de señal para la identificación de un usuario;

Fig. 5, es un diagrama de flujo de un procedimiento para la identificación de un usuario;

Fig. 6, es un diagrama de flujo que ilustra en detalle la etapa de identificación del usuario de la Fig. 5; y

Fig. 7, ilustra esquemáticamente un sistema de servidor de identificación con un servidor de identificación y otro servidor, así como un terminal de usuario y otro terminal de usuario

A continuación, se explicará en detalle la presente invención en virtud de formas de realización preferidas con referencia a los dibujos. En las figuras, los mismos números de referencia designan elementos iguales o similares. Las figuras son representaciones esquemáticas de diferentes formas de realización de la invención. Los elementos representados en las figuras no están necesariamente dibujados a escala. Más bien, los diferentes elementos representados en las figuras están reproducidos de manera que su función y propósito general puedan ser entendidos por el experto.

En las conexiones y acoplamientos entre unidades funcionales y elementos representados en las figuras pueden también ser implementados como conexión o acoplamiento indirecto. Una conexión o acoplamiento puede ser implementado con cable o de forma inalámbrica. Las unidades funcionales pueden implementarse como hardware, software o una combinación de hardware y software.

En las figuras se explican técnicas que permiten la identificación de un usuario. Aquí la identificación se realiza con ayuda de un terminal de usuario y de un servidor de identificación. El terminal del usuario y el servidor de identificación puede encontrarse en diferentes lugares y comunicarse por ejemplo por Internet. La identificación tiene en cuenta una comparación de una representación de una fotografía del usuario, que es obtenida de un documento de identificación, con una representación del propio usuario. De esta forma puede garantizarse una alta seguridad

de la identificación frente a falsificaciones, fraudes, etc. Además, la identificación se puede llevar a cabo de forma rápida y mediante acceso remoto.

En la Fig. 1 está representado un servidor de identificación 101. El servidor de identificación 101 se comunica con un terminal 103 de un usuario a través de una interfaz de comunicación 101a. Por ejemplo, esta comunicación puede realizarse a través de Internet. El servidor de identificación permite llevar a cabo una identificación del usuario. Para ello, la interfaz de comunicación 101a está configurada para recibir primeros datos de imagen 301 y segundos datos de imagen 302 desde el terminal de 103. Un procesador 101b del servidor de identificación 101 está configurado para realizar la identificación del usuario basándose en los primeros datos de imagen 301 y los segundos datos de imagen 302.

Los primeros y los segundos datos de imagen 301, 302 pueden contener, por ejemplo, una o varias imágenes, una película o similar. Los primeros y los segundos datos de imagen 301, 302 pueden ser captados con una cámara 103b del terminal 103 y luego enviados al servidor de identificación 101 a través de una interfaz de comunicación 103a del terminal 103. El terminal puede ser, por ejemplo: un teléfono móvil, un ordenador portátil, un ordenador, una cámara web, un televisor, una tableta o similar.

Además, en la Fig.1 está representado otro servidor 102. El servidor de identificación 101 forma junto con el otro servidor 102 un sistema de servidor de identificación 100. El otro servidor 102 y el servidor de identificación 101 están acoplados entre sí a través de las interfaces 102a, 101a, por ejemplo, de nuevo a través de Internet. De forma correspondiente, el otro servidor 102 está acoplado al terminal 103; sin embargo, esto es opcional. Por ejemplo, el otro servidor 102 podría establecer alternativa o adicionalmente una conexión con otro terminal del usuario. El otro servidor 102 comprende un procesador 102b que está configurado para comprobar si es necesaria una identificación del usuario. Esta comprobación puede tener lugar, por ejemplo, basándose en la conexión entre el otro servidor 102 y el terminal 103 y/o el otro terminal del usuario. Por ejemplo, el otro servidor puede ser una tienda en línea, un servidor de banco o similar y el usuario puede pretender hacer una transacción posibilitada por el otro servidor 102. Sin embargo, esta transacción puede requerir la identificación del usuario, por ejemplo, porque es crítica en cuanto a la identificación o específica para personas.

Si se determina que es necesaria la identificación del usuario, entonces la interfaz de comunicación 102a del otro servidor 102 está configurada para enviar una petición de identificación al servidor de identificación 101 en función de la comprobación. Correspondientemente, la interfaz de comunicación 102a está configurada para recibir un resultado de identificación desde el servidor de identificación 101 de acuerdo con la identificación positiva o negativa del usuario. Basándose en el resultado de la identificación, puede ser concedida o denegada una autenticación del usuario, de manera que este resultado de identificación puede determinar el progreso de la transacción perseguida mencionada antes.

Para aumentar la seguridad de la identificación frente a falsificaciones y fraudes, es posible llevar a cabo la transferencia de datos a lo largo de las conexiones entre las unidades 101, 102, 103 de forma cifrada. Las técnicas correspondientes, como por ejemplo el cifrado de Secure Sockets Layer (SSL) (“capa de puertos seguros”) son conocidos para el experto, por lo que aquí no hay que mencionar otros detalles.

A continuación, se expondrán otros detalles relativos a la identificación del usuario con referencia a la Fig. 2 y siguientes. En esencia, la identificación de usuario según diferentes escenarios se basa en la determinación de datos de identificación del usuario, tales como el nombre, la edad, la dirección, etc. en base a un documento de identificación del usuario. Además, mediante la comparación de la fotografía del documento de identificación con una parte de la cara del usuario se verifica que el documento de identificación identifica realmente al usuario - y no a otra persona. Todo esto se hace basándose en los primeros y segundos datos de imagen 301, 302.

En la Fig. 2 está representado un documento de identificación 200. El documento de identificación 200 contiene los datos de identificación 201 del usuario, tales como el nombre y la fecha de nacimiento, así como un número de serie del documento de identificación 200. Además, el documento de identificación 200 presenta una fotografía 202 del usuario. En particular, la fotografía 202 representa una parte de la cara del usuario. El documento de identificación 200 presenta además características de integridad 203, tal como una suma de comprobación, que es formada a partir del resto de datos, en particular los datos de identificación 201.

En la Fig. 2, el documento de identificación 200 es del tipo de carnet de identidad. Sin embargo, debería entenderse que en general podría ser utilizado cualquier otro documento de identificación con fotografía 202, por ejemplo, en particular pasaportes o carnets de conducir. Además, los diferentes documentos de identificación 200 puede tener informaciones diferentes, en particular con respecto a los datos de identificación 201. Dependiendo del tipo y del alcance de los datos de identificación 201 existentes, puede realizarse la identificación basándose en un fundamento de información diferente. Sin embargo, las técnicas básicas, aquí descritas no se ven afectadas en general.

En la Fig. 3 están representados los primeros datos de imagen 201. Los primeros datos de imagen 301 representan el documento de identificación 200. En particular, los primeros datos de imagen 300 contienen tres imágenes 301-1, 301-2, 301-3, que representan el documento de identificación 200 desde perspectivas y distancias diferentes. Además, dos imágenes 301-2, 301-3 de los primeros datos de imagen 301 contienen información de validación 310;

en la forma de realización representada en la Fig. 3 en forma de un patrón legible por máquina semitransparente superpuesto como marca de agua. Las informaciones de validación 310 están impresas en las imágenes 301-2, 301-3. Además, los primeros datos de imagen 301 contienen metadatos 303 que comprenden, por ejemplo: un instante de la captación de las imágenes 301-1, 301-2, 301-3, un lugar de captación de las imágenes y una ID del terminal con el que fueron captadas las imágenes 301-1, 301-2, 301-3. Por ejemplo, el lugar, como está especificado en los metadatos 303, puede especificar un grado de longitud y/o latitud.

Para que la información de validación 310 pueda ser contenida en los primeros datos de imagen 301, pueden ser generados por ejemplo datos de validación correspondientes en el servidor de identificación 101 y ser enviados al terminal 103. Puesto que los datos de validación y las informaciones de validación 310, derivadas de ellos y contenidas en los primeros datos de imagen 301, son generadas por primera vez en el marco de la identificación, es decir son generadas en un contexto temporal estrecho, puede ser asegurada una actualidad de los primeros datos de imagen 301. En particular, se puede evitar que el usuario utilice primeros datos de imagen 301 prefabricados.

Además, es posible generar datos de control en el servidor de identificación 101 y enviar estos al terminal 103. Los datos de control pueden instruir al terminal 103 para captar los primeros datos de imagen 301 con una secuencia determinada de parámetros de imagen, como por ejemplo el número de imágenes, los parámetros de exposición, la función de flash, y la resolución de la imagen. En el caso de la Fig. 3 se determinó por medio de los datos de control que debe ser captado un número de tres imágenes 301-1, 301-2, 301-3. Por ejemplo, es posible que la primera imagen 301-1 presente una sobreexposición de por ejemplo dos niveles de diafragma, la segunda imagen 301-2 presente una subexposición de dos niveles de diafragma y la tercera imagen 301-3 presente una exposición normal con flash adicional disparado. Esto es puramente ilustrativo y no limitativo. Es posible otra elección y combinación de parámetros de imagen. Mediante la validación de los parámetros de imagen por medio de los datos de control es posible en particular evitar que el usuario utilice primeros datos de imagen prefabricados 301 para la identificación. Concretamente, puede ser posible dentro del marco de la identificación en el servidor de identificación 101 comprobar o validar si las imágenes 301-1, 301-2, 301-3 de los primeros datos de imagen presentan propiedades ópticas que están caracterizadas por los parámetros de imagen.

En el escenario que se describe en referencia a la Fig. 3, en el marco de los datos de validación fueron transmitidos al usuario comandos de con qué posición y distancia se han de captar las imágenes 301-1, 301-2, 301-3 del documento de identificación 200. Por tanto, las imágenes 301-1, 301-2, 301-3 presentan perspectivas diferentes del documento de identificación 200. Estas perspectivas diferentes pueden ser validadas como información de validación contenida implícitamente en los datos de imagen 301 basándose en los datos de validación.

Anteriormente, con referencia a la Fig. 3 fueron explicadas técnicas en relación con los primeros datos de imagen 301. Sin embargo, debería entenderse que, alternativa o adicionalmente, pueden ser empleadas de forma análoga técnicas correspondientes también en relación con los segundos datos de imagen 302. En particular, alternativa o adicionalmente, puede ser posible incluir información de validación 310 en los segundos datos de imagen 302. Los datos de control pueden también ser aplicados con respecto a los segundos datos de imagen 302.

Mediante técnicas apropiadas, en el marco de la identificación son determinados los datos de identificación 201 del documento de identificación 200 procedentes de los primeros datos de imagen 301, por ejemplo, mediante reconocimiento de texto. Además, la fotografía 202 del documento de identificación 200 es comparada con la parte de la cara del usuario, lo que es posible con base en los primeros y segundos datos de imagen 301, 302. En caso de una coincidencia suficientemente buena entre la fotografía 202 y la parte de la cara, se puede aceptar que el documento de identificación 200 pertenece realmente al usuario y este está identificado por los datos de identificación 201.

En la Fig. 4 está representado el flujo de señal para una identificación del usuario mediante técnicas según la invención. En primer lugar, el otro servidor 102 envía en la etapa S1 una petición de identificación al servidor de identificación 101. Esto puede hacerse como resultado de que se ha determinado la necesidad de una identificación del usuario. Por ejemplo, el usuario puede desear realizar una transacción, tal como una compra de un producto o una transacción bancaria o similar a través del otro servidor 102, por ejemplo, por medio del terminal 103 o por medio de otro terminal (no mostrado en la Fig. 4). Si para esta transacción se requiere la identificación del usuario, se puede disparar la petición de identificación en la etapa S1. La petición de identificación en la etapa S1 puede presentar en diferentes escenarios, diferentes contenidos de información. Por ejemplo, la petición de identificación puede hacerse de forma anónima, sin ningún tipo de información adicional sobre el usuario. Pero también sería posible que la petición de identificación contenga ya datos de identificación del usuario a verificar determinados, es decir, que especifiquen un criterio de identificación.

El servidor de identificación 101 envía una frase clave al otro servidor 102 (etapa S2). A continuación, el otro servidor 102 envía la frase clave, por ejemplo, al terminal 103 (etapa S4), de modo que este por ejemplo puede registrarse automáticamente en la etapa S4 en el servidor de identificación 101 utilizando la frase clave. Sería posible también alternativamente que el otro servidor 102 enviara la frase clave no al terminal 103, sino a otro terminal del usuario, por ejemplo, un televisor, un ordenador, un portátil, un teléfono móvil, una tableta, etc. Este terminal adicional podría reproducir la frase clave al usuario. A continuación, el usuario podría, por ejemplo, manualmente, introducir la frase clave en el terminal 103 - es decir, el registro del servidor de identificación 101

puede hacerse de forma parcialmente automática (véase también la Fig. 7). La frase clave puede caracterizar de forma única el proceso de identificación determinado como “token”, de manera que puedan evitarse cambios entre los diferentes usuarios.

A continuación, en las etapas S5 y S6, el servidor de identificación envía los datos de control y los datos de validación al terminal 103. Los datos de control determinan una secuencia y los parámetros de exposición de las imágenes que son captadas para los primeros y segundos datos de imagen (etapa S7). Los datos de validación especifican informaciones de validación que están contenidos en los primeros y segundos datos de imagen.

En las etapas S8 y S9 son enviados los primeros y segundos datos de imagen 301, 302 desde el terminal 103 al servidor de identificación 101. El servidor de identificación 101 realiza en la etapa S10 la identificación del usuario basándose en los primeros y segundos datos de imagen 301, 302 recibidos. En la etapa S11, el resultado de identificación es enviado al otro servidor 102. El resultado de identificación, en correspondencia con la petición de identificación de la etapa S1, puede presentar un contenido de información diferente. Por ejemplo, el resultado de la identificación puede contener los datos de identificación determinados 201 del usuario. También sería posible que el resultado de identificación contuviera solo determinados datos de identificación, por ejemplo, como fueron solicitados en la petición de identificación. También sería posible que el resultado de identificación indicara únicamente una identificación positiva o negativa del usuario, por ejemplo, basándose en el criterio de identificación. Por ejemplo, el criterio de identificación puede especificar una edad mínima del usuario o un lugar de residencia del usuario. Entonces, el resultado de identificación puede ser una simple respuesta sí/no. Dependiendo del resultado de identificación puede realizarse una autorización de la transacción pretendida por el usuario.

Además, sería posible opcionalmente que a continuación de la identificación (etapa S10) fuera enviada una contraseña de usuario al otro servidor 102. Por ejemplo, la contraseña de usuario puede ser generada en el terminal 103, por ejemplo, por introducción del usuario. A continuación, la contraseña del usuario es enviada desde el terminal 103 al servidor de identificación 101 y desde allí, por ejemplo, en el marco del resultado de identificación, al otro servidor 102. El otro servidor 102 puede almacenar la contraseña de usuario asociada con el usuario y/o los datos de identificación identificados. Opcionalmente, el terminal 103 puede almacenar también la contraseña.

Esto puede posibilitar una nueva identificación posterior del usuario basándose en la contraseña de usuario almacenada. En otras palabras, por tanto, en una nueva identificación posterior puede ser innecesario transmitir de nuevo los primeros y segundos datos de imagen 301, 302, etc. Más bien, puede ser suficiente realizar únicamente la identificación basándose en la contraseña del usuario. Para ello sería posible también opcionalmente que la contraseña de usuario se almacenase en el terminal 103, por ejemplo, para una identificación automática posterior. Una nueva identificación especialmente rápida y simple basándose en la contraseña de usuario sería entonces posible.

En la Fig. 5 está representado un diagrama de flujo de un procedimiento para la identificación del usuario. El procedimiento comienza en la etapa T1. En la etapa T2 se comprueba si es necesaria la identificación del usuario. Si no se requiere la identificación del usuario, el procedimiento termina en la etapa T3. En caso contrario, el servidor de identificación 101 recibe la petición de identificación del otro servidor 102 (etapa T4). En la etapa T5 se realiza el registro del terminal 103 en el servidor de identificación 101. Esto se puede hacer por ejemplo por medio de la frase clave.

En las etapas T6 y T7 son captados en el terminal 103 los primeros y segundos datos de imagen 301, 302. Alternativamente, el terminal 103 podría controlar una unidad externa, por ejemplo, un televisor o una cámara web o similar, para la captación de los primeros y segundos datos de imagen 301, 302.

A continuación, son recibidos los primeros y segundos datos de imagen 301, 302 en el servidor de identificación (etapa T8) y se realiza la identificación del usuario (etapa T9). En función de si la identificación tiene éxito (etapa T10), en la etapa T11 es enviado un resultado de identificación positivo desde el servidor de identificación 101 al otro servidor 102, o en la etapa T12 es enviado un resultado de identificación negativo desde el servidor de identificación 101 al otro servidor de 102. El procedimiento termina en la etapa T13.

En la Fig. 6 están representados a continuación otros detalles relativos a la etapa T9 de la Fig. 5 de la identificación del usuario en el servidor de identificación 101.

En primer lugar, en la etapa U1, los metadatos de los primeros y segundos datos de imagen 301, 302 son comprobados en cuanto a validez. Esto puede significar, por ejemplo, que se comprueba si los primeros y segundos datos de imagen 301, 302 incluyen imágenes que fueron captadas dentro de un determinado período de tiempo antes del tiempo real en el que es ejecutada la etapa U1, o no son más antiguos que un determinado valor de tiempo máximo. También sería posible comprobar si las distintas imágenes de los primeros y segundos datos de imagen 301, 302 no han sido captadas en distintos lugares y/o por uno y el mismo terminal 103. Si en la etapa U1 se determina la falta de validez de los metadatos 303 de los primeros y segundos datos de imagen 301, 302, en la etapa U9 se deniega la identificación.

De lo contrario, en la etapa U2 la información de validación 310 es determinada a partir de los primeros y/o segundos datos de imagen 301, 302. La etapa U2 puede incluir, por ejemplo, la aplicación de técnicas de

segmentación de imagen y/o de reconocimiento de texto o puede incluir la lectura automática de determinadas zonas de los primeros y/o segundos datos de imagen 301, 302 basándose en los datos de validación generados en el servidor de identificación 101.

En la etapa U3 es comprobada la integridad de la información de validación. Si no existen informaciones de validación o no completamente o modificadas (determinables, por ejemplo, basándose en sumas de comprobación y/o los datos de validación), entonces en la etapa U9 es denegada la identificación.

En caso contrario, en la etapa U4 se puede realizar un reconocimiento de texto para el documento de identificación 200 por ejemplo en particular para leer las características de integridad 203 del documento de identificación 200 y/o los datos de identificación 201. En la etapa U5 pueden ser validadas las características de integridad 203. Esto puede hacerse basándose en el reconocimiento de texto realizado en la etapa U4 y, opcional o alternativamente, puede incluir técnicas de segmentación de imagen – por ejemplo, para reconocer marcas de agua u hologramas. Las características de integridad 203 pueden caracterizar, por ejemplo, a través de sumas de comprobación, una corrección de los datos de identificación 201 igualmente determinados.

Si en la etapa U5 son validadas las características de integridad 203 y/o los datos de identificación 201, entonces en la etapa U6 puede ser realizada una comparación de la fotografía 202 del documento de identificación 200 con la parte de la cara del usuario mostrada en los segundos datos de imagen 302. La etapa U6 puede ser realizada, por ejemplo: de forma automática, semiautomática o manual. Si la etapa U6 es realizada de forma automática o semiautomática, entonces la etapa U6 puede contener técnicas de segmentación de imagen y/o registro de imágenes. Puede ser determinado un valor de similitud entre la fotografía 202 y la parte de la cara del usuario mostrada en los segundos datos de imagen 302 y se comprueba si el valor de similitud es suficientemente alto. Si en la etapa U6 se determina que no hay un grado de similitud suficientemente grande, entonces en la etapa U9 puede ser denegada la identificación.

Opcionalmente, en la etapa U6 pueden ser comprobadas también las características de integridad 203 realizando una inspección manual, por ejemplo, en cuanto la presencia y/o la integridad. Para ello, una persona podría comprobar los primeros datos de imagen 301.

En caso contrario, en la etapa U7 se puede determinar si se cumple un criterio de la petición de identificación. Por ejemplo, la petición de identificación puede contener el criterio de si el usuario ya ha llegado a la edad de 18 años, es decir si es mayor de edad. Basándose en los datos de identificación determinados 201 se puede comprobar la edad es el usuario y en la etapa U7 la edad determinada es comparada con el criterio de la petición de identificación. Si no se cumple el criterio de la petición de identificación, la identificación de nuevo puede ser denegada en la etapa U9. En caso contrario, la identificación puede ser concedida en la etapa U8.

Debería entenderse que las diferentes etapas descritas anteriormente con referencia a la Fig. 6 no todas son necesarias o pueden ser realizadas opcionalmente. Por ejemplo, puede ser innecesario determinar las características de integridad en la etapa U5. En consecuencia, puede ser innecesario, comprobar los metadatos 303 en la etapa U1 o determinar y comprobar la información de validación 310 en las diferentes etapas U2 y U3. Además, la secuencia de las diferentes etapas no está particularmente limitada. Sería posible, por ejemplo, realizarla justo al principio de la etapa U6 y las otras etapas de identificación a continuación - son posibles otras disposiciones de etapas.

En la Fig. 7 está representado otro escenario en el que en comparación con el escenario representado en la Fig. 1 el otro servidor 102 no establece una conexión directa con el terminal 103 de usuario. Más bien, el otro servidor 102 está en conexión de comunicación con el otro terminal 104 del usuario, por ejemplo, por medio de la interfaz de comunicación 104a a través de Internet.

Un escenario concebible sería que el usuario deseara o activara, por ejemplo, la transacción crítica en cuanto a identificación a través de la conexión entre el otro terminal 104 y el otro servidor 102. Un ejemplo sería que el otro terminal 104 fuera un televisor con la funcionalidad de difusión continua de video (en inglés “Video-On-Demand”) y el usuario quisiera poner en el televisor una película con contenido crítico en cuanto a edad. Para la identificación del usuario, en particular con la autenticación de la edad, puede ser reproducida la frase clave en el otro terminal 104, aquí la televisión. Entonces, el usuario puede registrarse en el servidor de identificación 101 con la frase clave a través del terminal 103, por ejemplo, un ordenador, ordenador portátil, teléfono móvil, etc. Para ello, por ejemplo, puede introducir la frase clave enviada al otro terminal 104, en el terminal 103, de modo que este pueda establecer la conexión con el servidor de identificación 101.

De lo anterior se desprende que las técnicas para la identificación del usuario posibilitan una identificación segura, rápida y ligada al lugar. Por tanto, tales técnicas pueden ser utilizadas en múltiples ámbitos, tales como las compras en línea, transacciones bancarias, los inicios de sesión de usuario en las páginas web, la autorización de las transacciones, etc.

Naturalmente, las características de las formas de realización y aspectos de la invención descritos anteriormente pueden ser combinadas entre sí. En particular, las características se pueden utilizar no solo en las combinaciones descritas, sino también en otras combinaciones o por sí mismas, sin salirse del campo de la invención.

REIVINDICACIONES

1. Procedimiento para la identificación de un usuario, comprendiendo el procedimiento:

- la recepción de primeros datos de imagen (301) desde un terminal (103) del usuario en un servidor de identificación (101),

en el que los primeros datos de imagen (301) representan un documento de identificación (200) con una fotografía (202) del usuario,

- la recepción de segundos datos de imagen (302) desde el terminal (103) del usuario en el servidor de identificación (101),

en el que los segundos datos de imagen (302) representan una parte de la cara del usuario,

- la identificación del usuario, comprendiendo la identificación:

  - la comparación de los primeros datos de imagen (301) con los segundos datos de imagen (302) para determinar una similitud de la fotografía (202) del usuario procedente de los primeros datos de imagen (301) con la parte de la cara del usuario procedente de los segundos datos de imagen (302),

  - la determinación de datos de identificación (201) del usuario procedentes de los primeros datos de imagen (301) en virtud del documento de identificación (200),

en el que el procedimiento comprende, además:

la recepción de una petición de identificación de otro servidor (102) en el servidor de identificación (101),

en respuesta a la recepción de la petición de identificación, el envío de una frase clave desde el servidor de identificación (101) al otro servidor (102),

como respuesta a la frase clave recibida el otro servidor (102) envía la frase clave a otro terminal (104) del usuario o al terminal (103), y

el terminal (103) establece una conexión con el servidor de identificación (101) utilizando la frase clave.

2. Procedimiento según la reivindicación 1, en el que el procedimiento comprende, además:

- la generación de datos de validación en el servidor de identificación (101),

- el envío de los datos de validación desde el servidor de identificación (101) al terminal (103),

en el que los datos de validación permiten al terminal (103) incluir información de validación (310) adicional en los primeros datos de imagen (301) y/o en los segundos datos de imagen (302), comprendiendo la identificación, además:

- la determinación de la información de validación (310) procedente de los primeros datos de imagen (301) y/o de los segundos datos de imagen (302),

- la validación de la información de validación (310) determinada en virtud de los datos de validación generados.

3. Procedimiento según la reivindicación 2, en el que la información de validación (310) comprende al menos uno de los siguientes elementos:

- una marca de agua que está imprimida en los primeros datos de imagen (301) y/o en los segundos datos de imagen (302),

- un código alfanumérico que está representado en los primeros datos de imagen (301) y/o en los segundos datos de imagen (302),

- un patrón legible por máquina que está representado en los primeros datos de imagen (301) y/o en los segundos datos de imagen (302),

- una posición y/o una distancia de una cámara que registra los datos de imagen con respecto al documento de identificación (200) y/o con respecto a la parte de la cara,

- un código alfanumérico, que está representado en los primeros datos de imagen (301) y/o en los segundos datos de imagen (302) y que incluye un instante o un período de tiempo.

4. Procedimiento según una de las reivindicaciones anteriores, en el que el procedimiento comprende, además:

- la generación de datos de control en el servidor de identificación (101),
- el envío de los datos de control desde el servidor de identificación (101) al terminal (103),

en el que los datos de control instruyen al terminal (103) para registrar los primeros datos de imagen (301) y/o los segundos datos de imagen (302) con determinados parámetros de imagen,

en el que los parámetros de imagen son seleccionados preferentemente del siguiente grupo:

- número de imágenes;
- parámetros de exposición;
- función de flash;
- resolución de la imagen.

5. Procedimiento según una de las reivindicaciones anteriores, en el que los primeros datos de imagen (301) y/o los segundos datos de imagen (302) son seleccionados del siguiente grupo:

- una imagen (301-1, 301-2, 301-3);
- una película;
- al menos dos imágenes (301-1, 301-2, 301-3) o dos películas que son captadas secuencialmente en diferentes instantes;
- al menos dos imágenes (301-1, 301-2, 301-3) o dos películas que son captadas con parámetros de exposición y/o funciones de flash respectivamente diferentes,
- al menos dos imágenes (301-1, 301-2, 301-3) o películas que muestran el documento de identificación (200) o la parte de la cara desde diferentes perspectivas y/o distancias.

6. Procedimiento según una de las reivindicaciones anteriores, que comprende, además:

- como respuesta a la identificación, el envío de un resultado de identificación desde el servidor de identificación (101) al otro servidor (102) con referencia a la petición de identificación recibida.

7. Procedimiento según la reivindicación 6, en el que el resultado de la identificación y/o la petición de identificación comprende al menos uno de los siguientes elementos:

- un indicador que indica un resultado de identificación positivo o negativo,
- un nombre del usuario,
- un nombre de pila y/o un apellido del usuario,
- una fecha de nacimiento y/o una edad del usuario,
- un indicador que indica si la edad del usuario es mayor que un valor umbral de edad,
- un lugar de residencia del usuario,
- una dirección del usuario,
- un código postal del lugar de residencia del usuario,
- datos de identificación anonimizados del usuario,
- una clasificación de datos de identificación del usuario con respecto a

  una clasificación de referencia,
- una contraseña de usuario.

8. Procedimiento según una de las reivindicaciones 6 o 7, en el que la identificación del usuario comprende, además:

- la comparación de los datos de identificación (201) determinados con la petición de identificación.

9. Procedimiento según una de las reivindicaciones anteriores, en el que la identificación comprende además al menos una de las siguientes etapas:

- verificación de características de integridad del documento de identificación (200) procedentes de los primeros datos de imagen (301),

en el que las características de integridad comprenden sumas de comprobación y/o marcas de agua y/ o imágenes de hologramas y/o datos biométricos,

- la verificación de metadatos que son recibidos con los primeros datos de imagen (301) y/o con los segundos datos de imagen (302),

en el que los metadatos comprenden un instante de registro de los primeros datos de imagen (301) y/o un instante de registro de los segundos datos de imagen (302) y/o una identificación del terminal (103) y/o una posición de registro de los primeros datos de imagen (301) y/o una posición de registro de los segundos datos de imagen (302).

10. Procedimiento según una de las reivindicaciones anteriores, en el que el procedimiento comprende:

- la captación de los primeros datos de imagen (301) por medio de una cámara,

- la captación de los segundos datos de imagen (302) por medio de la cámara,

- el envío de los primeros datos de imagen (301) y de los segundos datos de imagen (302) desde el terminal (103) del usuario al servidor de identificación (101) para la identificación del usuario.

11. Sistema para la identificación de un usuario, comprendiendo el sistema:

- un terminal (103) de un usuario,

- un servidor de identificación (101), comprendiendo el servidor de identificación (101):

- una interfaz de comunicación (101a), de modo que la interfaz de comunicación (101a) está diseñada para recibir primeros datos de imagen (301) desde el terminal (103) y segundos datos de imagen (302) del terminal (103),

en el que los primeros datos de imagen (301) representan un documento de identificación (200) con una fotografía (202) del usuario,

en el que los segundos datos de imagen (302) representan una parte de la cara del usuario,

- un procesador (101b) que está configurado para identificar al usuario, en el que la identificación comprende:

- la comparación de los primeros datos de imagen (301) con los segundos datos de imagen (302) para determinar una similitud de la fotografía (202) del usuario procedente de los primeros datos de imagen (301) con la parte de la cara del usuario procedente de los segundos datos de imagen (302),

- determinación de datos de identificación (201) del usuario procedentes de los primeros datos de imagen (301) en virtud del documento de identificación (200),

en el que el sistema comprende, además:

- otro servidor (102) que comprende:

- un procesador (102b) que está diseñado para comprobar si es necesaria una identificación del usuario, teniendo lugar la comprobación basándose en una conexión entre el otro servidor (102) y el terminal (103) del usuario,

- una interfaz de comunicación (102a) que está diseñada para en función de la comprobación enviar una petición de identificación al servidor de identificación (101) y recibir un resultado de identificación del servidor de identificación (101),

en el que el servidor de identificación (101) está diseñado para en respuesta a la recepción de la petición de identificación enviar una frase clave al otro servidor (102),

en el que el otro servidor (102) está diseñado para como respuesta a la frase clave recibida enviar la frase clave a otro terminal (104) del usuario o al terminal (103),

en el que el terminal (103) está diseñado para establecer una conexión con el servidor de identificación (101) utilizando la frase clave.

12. Sistema según la reivindicación 11, en el que el sistema está diseñado para ejecutar un procedimiento según una de las reivindicaciones 1 – 10.

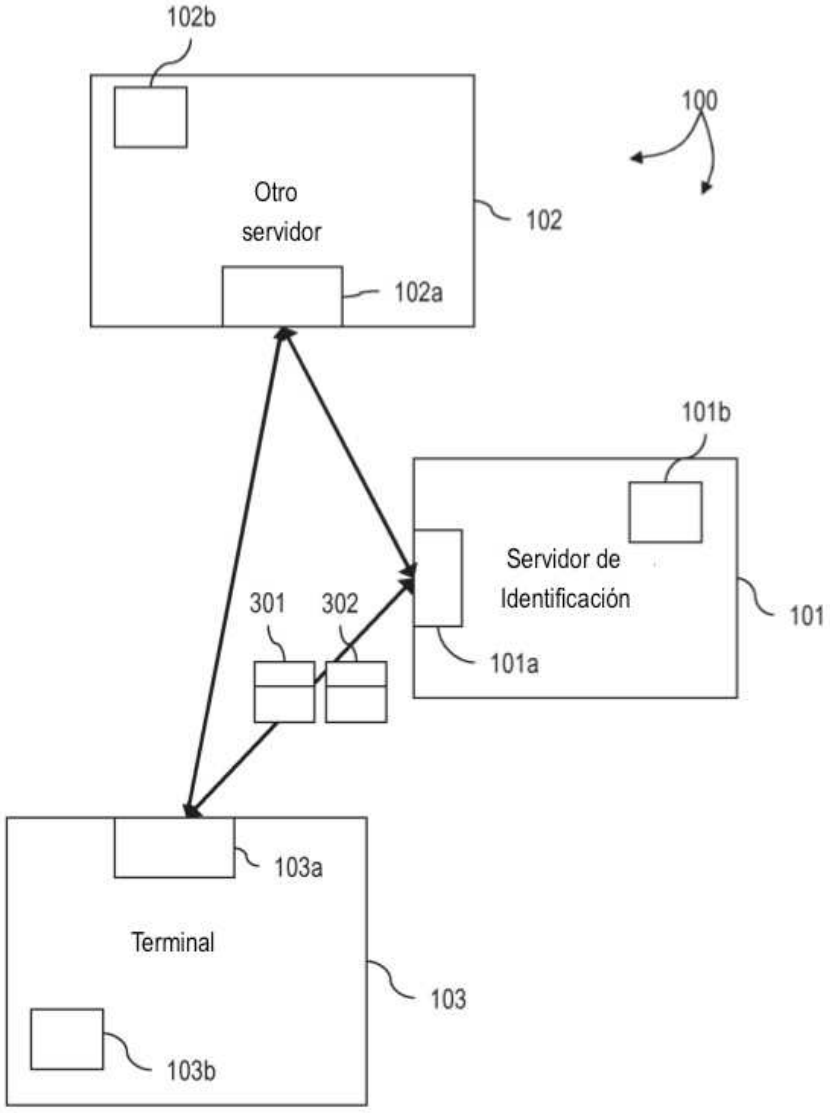
102b
100
Otro
servidor
102
102a
101b
Servidor de
Identificación
101
301
302
101a
103a
Terminal
103
103b

FIG. 1


Carnet de Identidad
Max Mustermann
ID: 5521142126
Fecha nacimiento: 12.12.2012
53778sd2S478234 • 23sdfa23a • 231yx411
201
202
200
203

FIG. 2

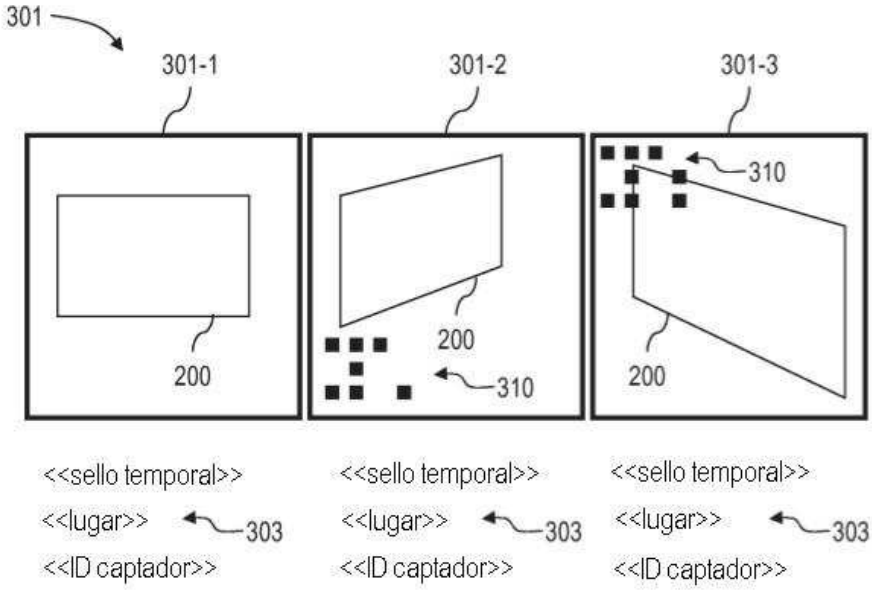
301
301-1
301-2
301-3
200
200
310
200
310
<<sello temporal>>
<<lugar>>
<<ID captador>>
303
<<sello temporal>>
<<lugar>>
<<ID captador>>
303
<<sello temporal>>
<<lugar>>
<<ID captador>>
303

FIG. 3

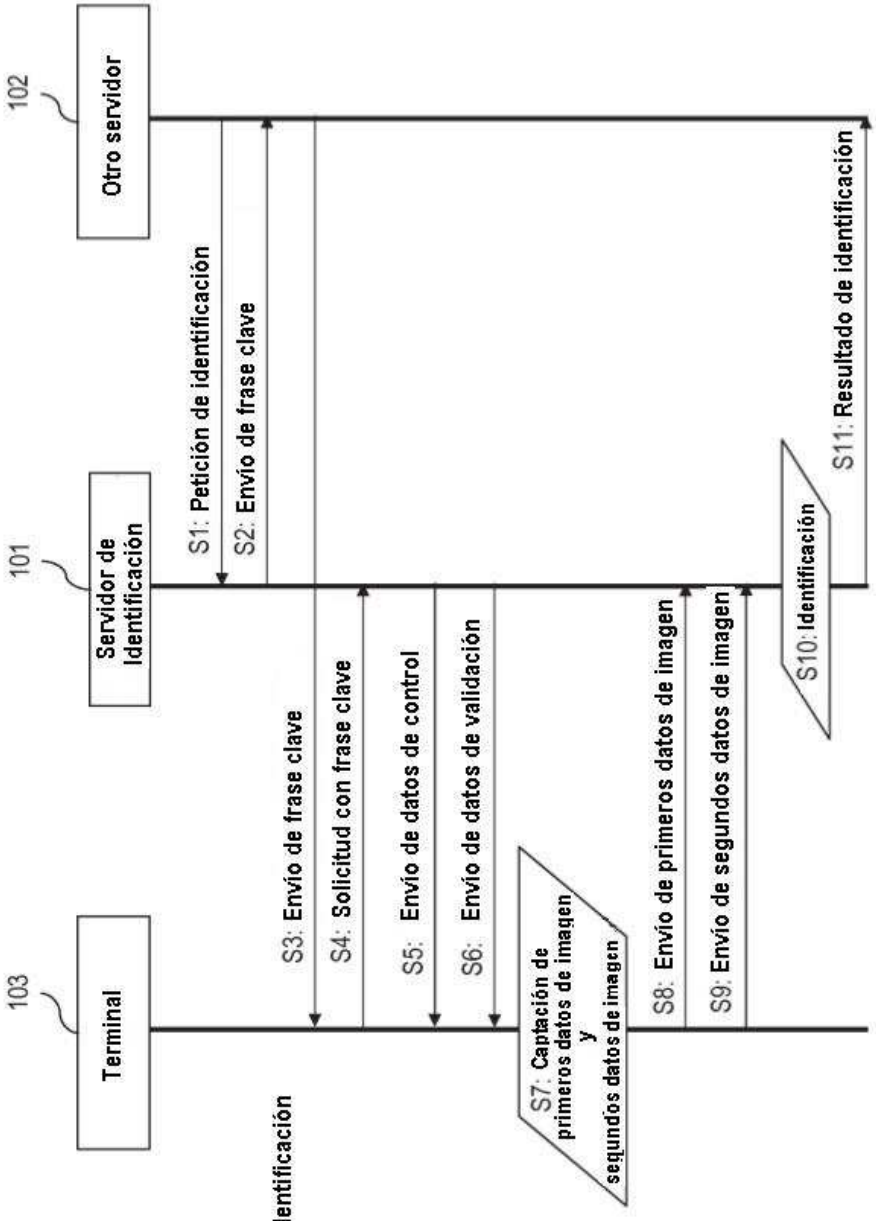
102
Otro servidor
101
Servidor de Identificación
103
Terminal
S1: Petición de identificación
S2: Envío de frase clave
S3: Envío de frase clave
S4: Solicitud con frase clave
S5: Envío de datos de control
S6: Envío de datos de validación
S7: Captación de primeros datos de imagen y segundos datos de imagen
S8: Envío de primeros datos de imagen
S9: Envío de segundos datos de imagen
S10: Identificación
S11: Resultado de identificación
Identificación

FIG. 4

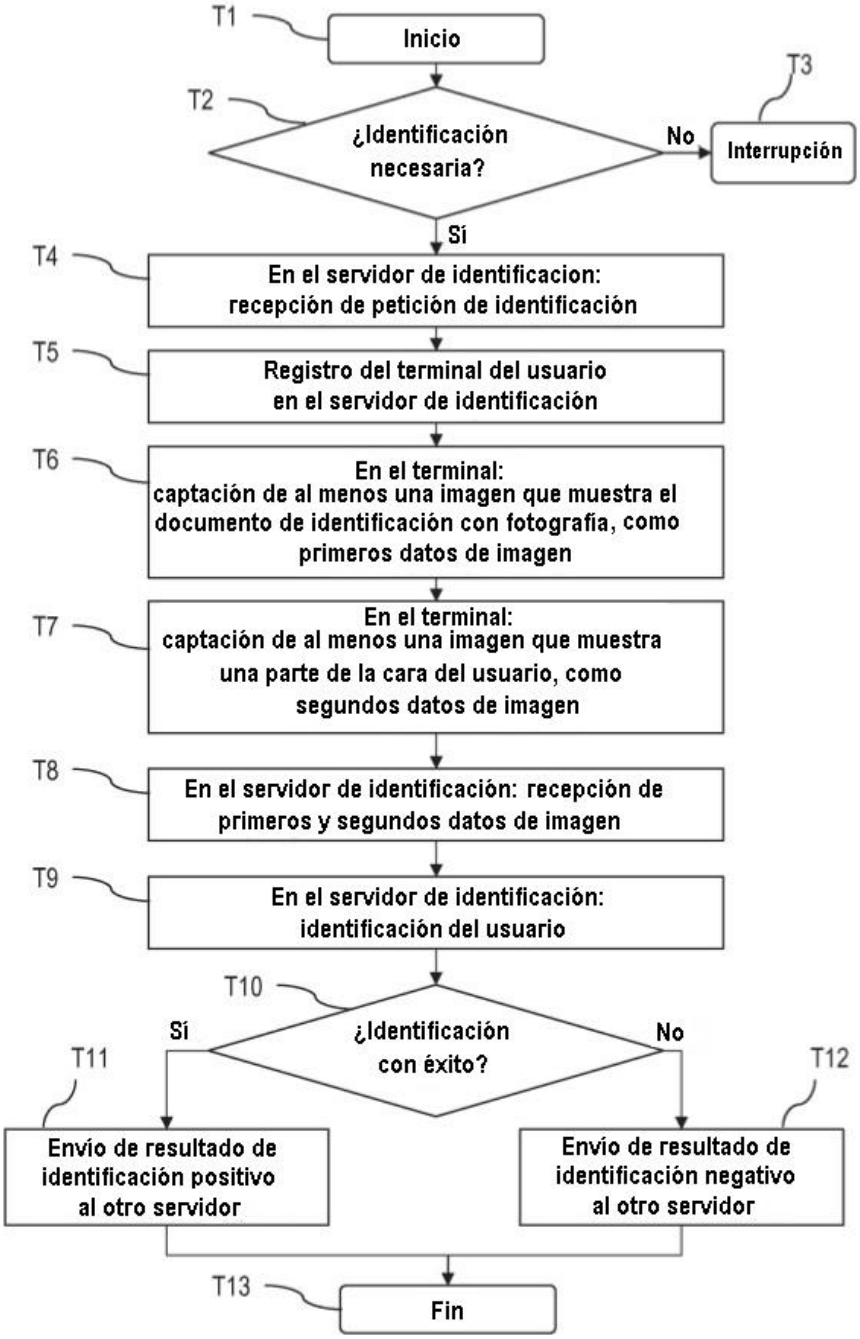
T1
Inicio
T2
¿Identificación necesaria?
No
T3
Interrupción
Sí
T4
En el servidor de identificacion: recepción de petición de identificación
T5
Registro del terminal del usuario en el servidor de identificación
T6
En el terminal: captación de al menos una imagen que muestra el documento de identificación con fotografía, como primeros datos de imagen
T7
En el terminal: captación de al menos una imagen que muestra una parte de la cara del usuario, como segundos datos de imagen
T8
En el servidor de identificación: recepción de primeros y segundos datos de imagen
T9
En el servidor de identificación: identificación del usuario
T10
¿Identificación con éxito?
Sí
No
T11
Envío de resultado de identificación positivo al otro servidor
T12
Envío de resultado de identificación negativo al otro servidor
T13
Fin

FIG. 5

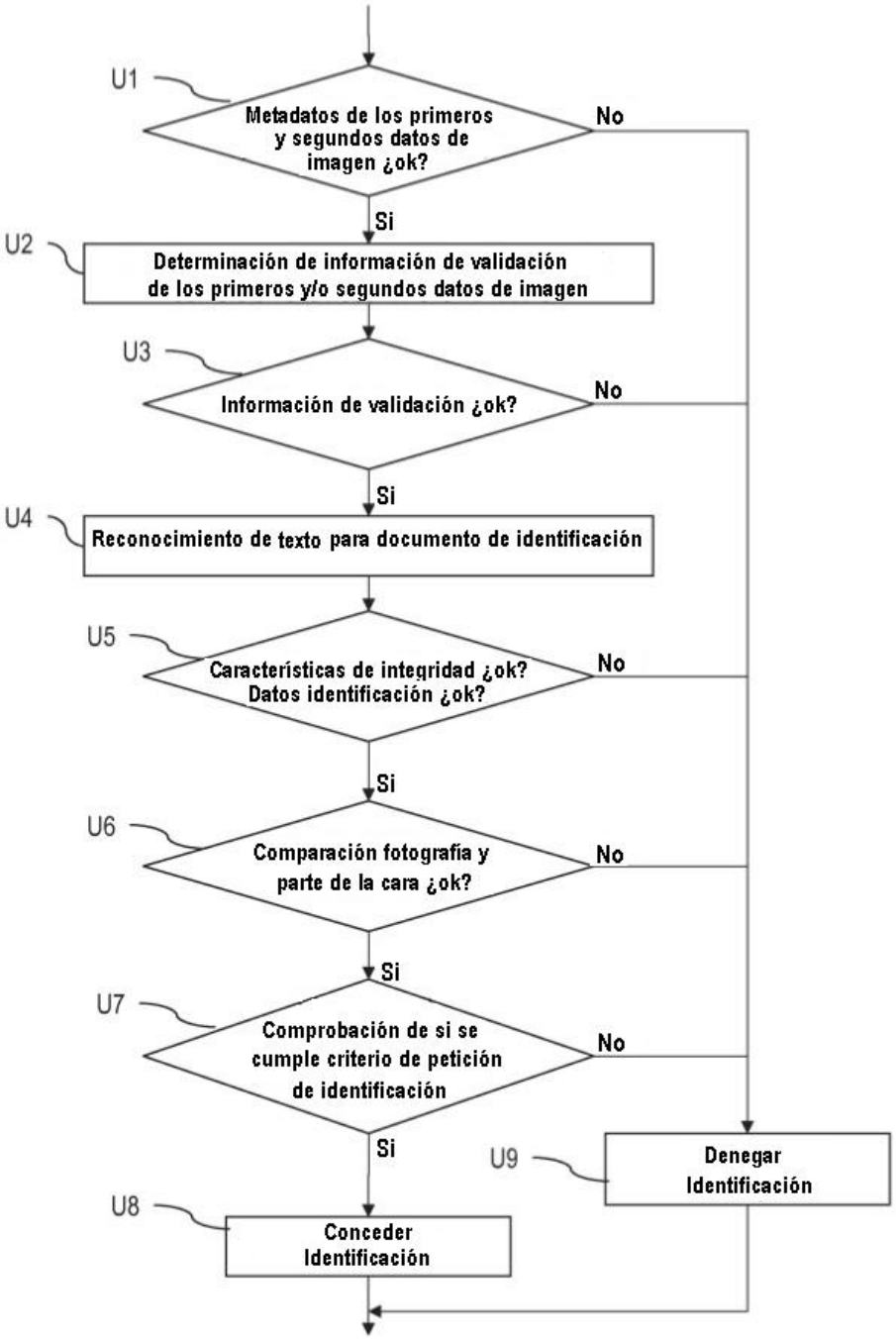
U1
Metadatos de los primeros y segundos datos de imagen ¿ok?
No
Si
U2
Determinación de información de validación de los primeros y/o segundos datos de imagen
U3
Información de validación ¿ok?
No
Si
U4
Reconocimiento de texto para documento de identificación
U5
Características de integridad ¿ok? Datos identificación ¿ok?
No
Si
U6
Comparación fotografía y parte de la cara ¿ok?
No
Si
U7
Comprobación de si se cumple criterio de petición de identificación
No
Si
U9
Denegar Identificación
U8
Conceder Identificación

FIG. 6

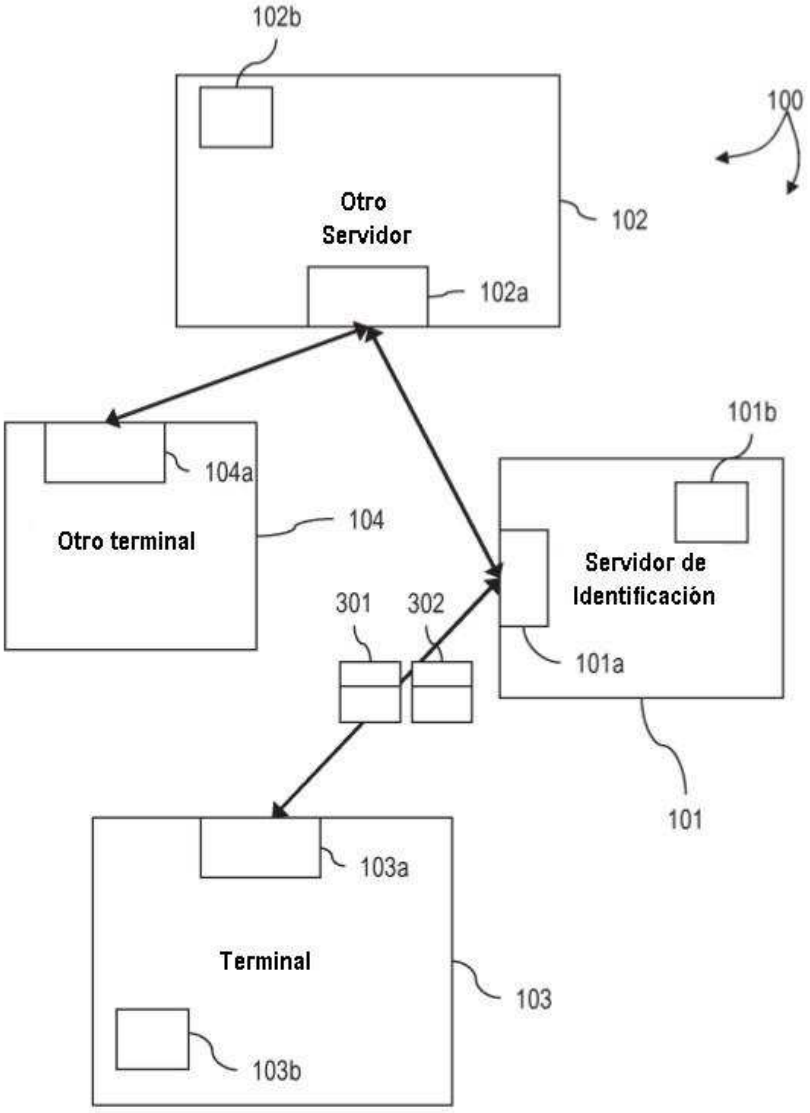
102b
100
Otro
Servidor
102
102a
101b
104a
104
Otro terminal
Servidor de
Identificación
301
302
101a
101
103a
Terminal
103
103b

FIG. 7