(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 981 613**

(51) Int. Cl.:

H04L 9/40 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **15.12.2021 E 21214682 (3)**

(97) Fecha y número de publicación de la concesión europea: **17.04.2024 EP 4199418**

(54) Título: **Verificación local de atributos mediante un dispositivo informático**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
09.10.2024

(73) Titular/es:

FUJITSU SERVICES LIMITED (100.0%)
Lovelace Road
Bracknell RG12 8SN, GB

(72) Inventor/es:

NICHOLLS, DAVID y
FEGAN, GARY

(74) Agente/Representante:

GONZÁLEZ PECES, Gustavo Adolfo

DESCRIPCIÓN

Verificación local de atributos mediante un dispositivo informático

Campo técnico

La presente invención se refiere a sistemas y métodos para verificar un atributo de usuario, tal como la edad o la identidad del usuario, mediante un dispositivo informático.

Antecedentes

En la vida moderna es frecuente la necesidad de que las personas verifiquen, es decir, certifiquen o prueben, un atributo personal. Por ejemplo, para comprar determinados bienes o acceder a determinados locales, un usuario puede necesitar verificar que tiene una determinada edad mínima. Del mismo modo, puede ser necesario verificar la identidad (por ejemplo, el nombre) de la persona para entrar en determinados edificios, pasar ciertos controles de autorización o de seguridad, o acceder a bienes y servicios.

Tradicionalmente, esta verificación de atributos se ha realizado utilizando identificadores IDs, en papel o impresos, tales como pasaportes, permisos de conducir o carnés de identidad. Lo que antecede es inadecuado porque los documentos de identidad impresos pueden perderse, dañarse, robarse o falsificarse con facilidad. Además, el uso de documentos de identidad impresos ha limitado la posibilidad de que los sistemas automatizados realicen transacciones con un usuario de forma automatizada. Por ejemplo, en la actualidad, los artículos restringidos por edad no pueden venderse por lo general a través de sistemas automatizados, tales como máquinas expendedoras o cajas de autoservicio, debido a la necesidad de inspeccionar los documentos de identidad antes de que pueda realizarse dicha transacción. Del mismo modo, la entrada automatizada a un edificio o recinto restringido puede ser problemática por razones similares.

Más recientemente, gracias a los avances tecnológicos, se ha hecho posible una forma limitada de verificación digital de atributos, en donde se utiliza un dispositivo informático, tal como un teléfono móvil, en lugar de un documento de identidad tradicional en papel. Sin embargo, estos sistemas existentes de verificación digital de atributos presentan diversos inconvenientes técnicos que han limitado su implantación generalizada.

La forma más común de sistema de verificación digital existente implica que un usuario se registre en una autoridad centralizada que mantiene registros o perfiles de varios usuarios en un servidor o base de datos centralizados. En un sistema de este tipo, para verificarse, el usuario se registra ante la autoridad centralizada y, por lo general, le proporciona algún tipo de Información de Identificación Personal (PII), tal como su nombre, fecha de nacimiento, dirección, etcétera. Basándose en la información PII, la autoridad central crea un perfil para el usuario en cuestión. Cuando, posteriormente, el usuario desea verificar un atributo, tal como su edad, el usuario transmite más información PII al servidor, que el servidor utiliza para emparejar al usuario con uno de los perfiles que posee. En respuesta, y suponiendo que se encuentre una coincidencia, la autoridad central puede certificar o avalar las credenciales de dicho usuario, por ejemplo, proporcionando una confirmación al usuario o a la parte que consulta el atributo del usuario.

Tal como será evidente, este sistema existente de verificación de atributos depende de que el usuario pueda mantener correspondencia con la autoridad centralizada tanto en el momento del registro como posteriormente en el momento de la verificación. Lo que antecede es inadecuado porque hace que el sistema dependa de que el usuario tenga una buena conexión de red (por lo general una conexión a Internet) para funcionar, tanto en el momento del registro como en el de la verificación. Si el usuario se encuentra en una ubicación remota o en algún lugar en donde su conexión a la red sea deficiente, es posible que no pueda completar el proceso de verificación. En el caso de una transacción, esto puede dar lugar a que la transacción no tenga lugar o no se complete. Cuando la verificación es necesaria para entrar en un local, el usuario puede quedar bloqueado y no poder entrar.

El enfoque conocido también requiere que una autoridad centralizada conserve datos de identificación personal potencialmente sensibles de todos sus usuarios, y que dichos datos de identificación personal sensibles se transmitan tanto en la fase de registro como en la de verificación entre el usuario y la autoridad central. Lo que antecede presenta una debilidad de seguridad y privacidad en el sistema, y las violaciones de datos en las que las autoridades centralizadas son pirateadas y se hace pública la información PII de potencialmente muchos usuarios que son ahora habituales como resultado de sistemas de esta naturaleza.

Tal como puede constatarse, los sistemas existentes de verificación de atributos digitales adolecen de importantes inconvenientes técnicos. Sería ventajoso proporcionar sistemas y métodos que aborden uno o varios de estos problemas, de forma aislada o combinada.

El documento GB2587075A da a conocer un dispositivo de prueba de identidad que incluye un almacenamiento electrónico configurado para almacenar una pluralidad de cargas útiles de identidad, pudiendo el dispositivo de prueba de identidad ser una tarjeta inteligente o una etiqueta. Cada carga útil tiene una firma de carga útil verificable de forma independiente, determinada mediante la firma criptográfica individual de dicha carga útil de identidad. Cada carga útil de identidad está asociada con un tipo de atributo identificado e incluye un atributo de identidad de dicho tipo de atributo. Los atributos pueden incluir nombre, datos biométricos tales como imagen facial, edad, nacionalidad. Realizar una función de compartición de identidad procesando una señal de interrogación recibida desde un dispositivo solicitante de identidad,

para determinar al menos un tipo de atributo solicitado, accediendo al almacenamiento electrónico para hacer coincidir el tipo de atributo solicitado con el tipo de atributo asociado con una de las cargas útiles de identidad almacenadas, y proporcionando directamente esa carga útil de identidad y su firma de carga útil al dispositivo solicitante de identidad. El dispositivo puede proporcionar tantas funciones de compartición de identidad como de pago electrónico.

El documento US2018189583A1 da a conocer un método puesto en práctica por ordenador que incluye la recepción, por parte de un dispositivo informático, de datos identificativos sobre un usuario, incluyendo los datos identificativos una autoimagen digital del usuario, y la extracción, por parte del dispositivo informático, de uno o más identificadores biométricos sobre el usuario. El método incluye, además, verificar, mediante el dispositivo informático, al menos un identificador biométrico comparándolo con una base de datos que contiene información sobre una pluralidad de individuos, y recibir, mediante el dispositivo informático, un indicador confirmatorio asociado con el usuario. En respuesta a la recepción del indicador confirmatorio, el método incluye, además, procesar una solicitud de preinscripción asociada con el usuario, estando la solicitud de preinscripción asociada con un programa de verificación de identidad.

El documento US11182774B1 da a conocer una transacción realizada entre una primera parte que utiliza un dispositivo de credencial de identificación móvil de usuario (UMD) y una segunda parte que utiliza un sistema de parte fiable (RPS), el sistema RPS recibe una solicitud del UMD para la transferencia de un artículo, solicita información de identificación de la primera parte al UMD, recibe, basándose en el consentimiento de la primera parte, parte o la totalidad de la información de identificación de usuario asociada con una credencial de identificación móvil (MIC) que el UMD recibió desde un sistema de parte autorizante (APS), recibe la verificación de la información de identificación de usuario recibida, utiliza la información de identificación de usuario verificada para verificar, o no, una identidad de la primera parte, concede la solicitud de transferir el artículo a cambio de un pago u otro artículo a transferir de la primera parte a la segunda parte cuando se verifica la identidad de la primera parte, y deniega la solicitud cuando no se verifica la identidad de la primera parte.

El documento US2017346851A1 da a conocer una solución informática de seguridad y autenticación. El flujo de un solo aspecto, la autenticación mutua reforzada visualmente es: el cliente visita la página de inicio de sesión de un sitio web protegido, se identifica mediante cookies, el sitio muestra una fotografía aleatoria en dicha página, hace que el teléfono inteligente del cliente muestre de manera automática una cuadrícula de fotos aleatorias, una de las cuales coincide con la foto de la página de inicio de sesión, y el cliente la toca para iniciar sesión. Las técnicas divulgadas enseñan a bloquear los sitios y la actividad fraudulenta impidiendo que éstos produzcan cualquier foto coincidente que el cliente pueda tocar.

El documento US2013138570A1 da a conocer una credencial emitida a un usuario y una aplicación de transacciones cargada en un dispositivo de usuario que se utiliza para asegurar las transacciones entre el usuario y una interfaz de proveedor de servicios, tal como un servidor web o un punto de venta. La aplicación de transacciones puede capturar datos de usuario en tiempo real y, comparando los datos de usuario en tiempo real con datos de usuario que anteceden almacenados en la credencial, autenticar la interfaz del proveedor de servicios para el usuario y el usuario para la interfaz del proveedor de servicios; y establecer una sesión cifrada entre la interfaz del proveedor de servicios y la aplicación de transacciones adaptada para autenticar las transacciones entre el usuario y la interfaz del proveedor de servicios.

Sumario

En un primer aspecto, se proporciona un método puesto en práctica por ordenador para verificar localmente un atributo asociado con un usuario según la reivindicación 1. En un segundo aspecto, se proporciona un dispositivo informático, un medio legible por ordenador o un programa informático correspondiente según la reivindicación 13.

Este sumario introduce conceptos que se dan a conocer con más detalle en la descripción detallada. No debe utilizarse para identificar características esenciales de la materia reivindicada, ni para limitar el alcance de la materia reivindicada.

Según un aspecto de la presente invención, se proporciona un método puesto en práctica por ordenador para verificar localmente un atributo asociado con un usuario, comprendiendo el método realizar, mediante un dispositivo informático, varias etapas. Dicho método puede considerarse relacionado con una fase de verificación, en el sentido de que permite a un usuario verificar un atributo personal utilizando un dispositivo informático.

El término "local", en este contexto, significa que la verificación se realiza localmente por el propio dispositivo informático, y no remotamente por algún servidor o base de datos de una autoridad centralizada. La verificación de un atributo puede considerarse una certificación o prueba del mismo. Por ejemplo, una persona que verifica su edad puede demostrar que tiene una determinada edad mínima para realizar un acto concreto.

El método dado a conocer comprende realizar, mediante el dispositivo informático, etapas que incluyen: capturar datos biométricos de verificación mediante el dispositivo informático; determinar si los datos biométricos de verificación corresponden al usuario comparando los datos biométricos de verificación con datos biométricos autenticados del usuario obtenidos previamente desde un identificador ID, y almacenados localmente en el dispositivo informático; y en respuesta a la determinación de que los datos biométricos de verificación corresponden al usuario, verificar el atributo asociado con el usuario basándose en información de atributos asociada con el usuario obtenida previamente desde el identificador ID y almacenada localmente en el dispositivo informático.

Mediante estas etapas, el método dado a conocer proporciona un mecanismo de verificación de atributos que puede realizarse localmente utilizando el dispositivo informático, con total independencia de cualquier autoridad o servidor centralizado. Este enfoque elimina la necesidad de que exista dicha autoridad centralizada, simplificando de este modo el sistema y evitando la necesidad de una base de datos central de PII de usuario. Lo que antecede, a su vez, proporciona ventajas de seguridad y privacidad, porque no es necesario transmitir ninguna información PII a o desde la autoridad central, y por tanto existen menos posibilidades de pérdida de datos sensibles, tal como, por ejemplo, mediante un pirateo malintencionado que libere la información PII del usuario.

Además, al no ser necesaria la comunicación con una autoridad central, el método dado a conocer es bastante más estable y fiable en lugares en donde la conectividad de red es deficiente. Por ejemplo, un usuario de una tienda situada en un entorno remoto en donde la cobertura de red es deficiente puede seguir haciendo uso del mecanismo de verificación dado a conocer, porque se produce localmente en el dispositivo informático y no depende de ninguna comunicación con un servidor o red central. Del mismo modo, en entornos muy concurridos, tal como en un estadio deportivo, la red local (por ejemplo, en el caso de una red móvil, la célula de red local) puede estar sobrecargada de tal forma que los usuarios individuales no puedan acceder a la red. El presente mecanismo de verificación funcionaría también en un entorno de este tipo, porque no se requiere conexión a una red, con lo que se subsana una limitación técnica de los sistemas que anteceden.

El mecanismo de verificación dado a conocer puede considerarse un mecanismo de verificación "offline", en el sentido de que no se requiere conexión a ninguna red o servidor centralizado en el momento de la verificación. Lo que antecede contrasta fuertemente con los mecanismos de verificación existentes, que dependen de la comunicación hacia y desde un servidor centralizado para verificar los atributos del usuario. Dichos sistemas existentes pueden considerarse mecanismos de verificación "online", porque una conexión de red es un requisito previo para que sea posible la verificación de atributos.

En una puesta en práctica, el dispositivo informático comprende un dispositivo móvil, por ejemplo, un dispositivo móvil del usuario. Por "dispositivo móvil" se entiende cualquier dispositivo informático móvil adecuado, por lo general portátil, que pueda ser transportado por un usuario y utilizado en un punto de interrogación para verificar un atributo. Ejemplos de dichos dispositivos móviles son, entre otros, los teléfonos móviles, los teléfonos inteligentes, los asistentes digitales personales (PDAs), los ordenadores portátiles, las tabletas electrónicas y otros dispositivos móviles "inteligentes", tal como los relojes inteligentes.

Cuando se utiliza un dispositivo móvil para llevar a cabo los métodos descritos, el mecanismo descrito ofrece la ventaja de no requerir la instalación de ningún hardware de verificación específico en el punto de verificación. En su lugar, el usuario simplemente utiliza su propio dispositivo móvil. Lo que antecede simplifica aún más el sistema, al utilizar el hardware existente en lugar de requerir la instalación de nuevo hardware. Tampoco se exige al usuario que un dispositivo de terceros, sobre el que no tiene ningún control, escanee o almacene información de identificación personal. En cambio, los métodos y el sistema dado a conocer implican que la información PII solamente se almacena en el propio dispositivo móvil del usuario. Al distribuir la información PII entre los dispositivos de los propios usuarios, se reduce la posibilidad de que un único pirateo libere datos de varios usuarios.

En una puesta en práctica, los datos biométricos de verificación comprenden una imagen de verificación capturada con una cámara del dispositivo informático y los datos biométricos autenticados comprenden una imagen autenticada del usuario obtenida previamente del identificador ID. En este caso, se pueden utilizar mecanismos tales como el reconocimiento facial para determinar si los datos biométricos de verificación (es decir, la imagen de verificación) corresponden (es decir, representan) al usuario, mediante una comparación con la imagen autenticada del usuario obtenida a partir del identificador ID.

En otra puesta en práctica, los datos biométricos de verificación comprenden una huella dactilar de verificación capturada mediante un escáner de huellas dactilares del dispositivo informático y los datos biométricos autenticados comprenden una huella dactilar autenticada del usuario obtenida previamente del identificador ID. En este caso, se pueden utilizar mecanismos tales como la comparación de huellas dactilares para determinar si los datos biométricos de verificación (es decir, la huella dactilar de verificación) corresponden (es decir, coinciden con la huella dactilar) al usuario, mediante una comparación con la huella dactilar autenticada del usuario obtenida del identificador ID.

Tal como ya se ha indicado, el atributo asociado con el usuario puede ser su edad. Otros atributos que pueden verificarse resultarán evidentes para el lector experto, e incluyen el nombre, la fecha de nacimiento, el sexo, la nacionalidad, la dirección, el derecho a entrar en un local, conducir un vehículo concreto o manejar maquinaria, etc., del usuario.

Tal como se mencionó con anterioridad, el mecanismo de verificación descrito se produce a nivel local. Es decir, no se requiere conexión a un servidor o a una red. En consecuencia, el atributo asociado con el usuario puede verificarse sin necesidad de transmitir Información de Identificación Personal (PII) desde el dispositivo informático. Lo que antecede contrasta con los sistemas existentes, en los que la información PII se transmite desde y hacia un servidor central para permitir la verificación de los atributos del usuario.

La verificación del atributo asociado con el usuario puede comprender el acceso a un certificado almacenado localmente en el dispositivo informático, conteniendo dicho certificado la información del atributo asociado con el usuario. Dicho

certificado suele tener un formato estándar, por ejemplo, determinado por un proveedor de software de verificación de atributos, y por tanto, presenta una representación fiable y reproducible de la información de atributos del usuario que permite una mayor interoperabilidad entre las aplicaciones de software, que pueden programarse para utilizar (es decir, efectuar la lectura y la escritura) con el mismo formato de certificado. De manera preferible, los datos biométricos autenticados del usuario también se almacenan o se integran en el mismo certificado, de forma que las aplicaciones de software que se ejecutan en el dispositivo informático puedan acceder tanto a la información de atributos como a los datos biométricos autenticados en la misma ubicación de memoria. De manera preferible, el certificado está encriptado, para mejorar la seguridad y la privacidad de los datos. Por ejemplo, solamente determinadas aplicaciones de software autorizadas que se ejecuten en el dispositivo informático pueden tener los permisos adecuados para descifrar el certificado y acceder a los datos almacenados o integrados en el mismo. Lo que antecede reduce la probabilidad de que la información de atributos o los datos biométricos autenticados sean pirateados u objeto de acceso por partes no autorizadas.

Las etapas realizadas por el dispositivo informático incluyen, además, proporcionar una confirmación del atributo verificado asociado con el usuario. La confirmación se presenta en una pantalla del dispositivo informático. La confirmación es legible por máquina, de modo que pueda ser objeto de lectura y el atributo pueda verificarse mediante una interfaz de máquina. En un ejemplo, la confirmación incluye un código QR que puede ser objeto de lectura por un escáner de códigos QR. Al escanear el código QR, un dispositivo de lectura o de consulta puede confirmar que el atributo del usuario ha sido verificado por el dispositivo informático. De manera preferible, el código QR es un código QR dinámico, que puede redirigir a un dispositivo de consulta a una ubicación concreta, tal como una URL, y/o codificar datos asociados a la verificación de atributos de forma legible por máquina, preferiblemente de forma codificada. El código QR dinámico puede actualizarse de manera periódica. El uso de un código QR dinámico puede mejorar la protección contra la suplantación de identidad, tal como se da a conocer con más detalle a continuación.

Proporcionar la confirmación de la verificación del atributo puede comprender, adicional o de manera alternativa, la transmisión de un mensaje que confirme el atributo verificado asociado con el usuario. Por ejemplo, el dispositivo informático puede transmitir un mensaje a otro dispositivo confirmando la verificación del atributo.

De manera alternativa, el mensaje puede transmitirse desde una aplicación de software que se ejecuta en el dispositivo informático a otra aplicación de software que se ejecuta en el dispositivo informático. Este último enfoque, en particular, puede permitir la compra sin pasar por caja, en donde la verificación y confirmación del atributo del usuario tiene lugar exclusivamente en el dispositivo informático (por ejemplo, un teléfono inteligente del usuario) y no existe la necesidad de un dispositivo de consulta o de pasar por caja.

Las etapas realizadas por el dispositivo informático pueden incluir, además: obtener información espaciotemporal asociada con la verificación del atributo asociado con el usuario. Las etapas pueden incluir, además, integrar la información espaciotemporal obtenida en la confirmación del atributo verificado. En este contexto, "espaciotemporal" significa relativo a un momento y/o lugar en donde tiene lugar la verificación del atributo asociado con el usuario.

Por ejemplo, la información espaciotemporal puede comprender información relativa a uno o más de los siguientes elementos: una fecha actual; una hora actual; una ubicación actual; y una identidad de un establecimiento en donde se está llevando a cabo la verificación del atributo asociado con el usuario. "Actual" en este contexto significa actual en el momento de la verificación, o dentro de un umbral de tiempo o distancia a partir del mismo. En un ejemplo, la confirmación del atributo verificado (por ejemplo, un código QR) incluye un sello de fecha y hora que confirma la fecha y hora en que tuvo lugar la verificación del atributo del usuario. La confirmación también puede incluir una ubicación, por ejemplo, el nombre de un establecimiento, una ubicación GPS o similar, asociada al lugar en donde tuvo lugar la verificación del atributo. La inclusión de dicha información en la confirmación de verificación puede reducir la posibilidad de suplantación de identidad, tal como se da a conocer con más detalle a continuación. Por tanto, el proceso de verificación es más seguro.

Las etapas realizadas por el dispositivo informático pueden incluir, además, antes de capturar los datos biométricos de verificación: obtener, a partir del identificador ID, los datos biométricos autenticados del usuario y la información de atributos asociada con el usuario; capturar los datos biométricos de registro utilizando el dispositivo informático; determinar si los datos biométricos de registro corresponden al usuario comparando los datos biométricos de registro con los datos biométricos autenticados; y en respuesta a la determinación de que los datos biométricos de registro corresponden al usuario, almacenar localmente en el dispositivo informático:

a) los datos biométricos autenticados del usuario; y

b) la información de atributos asociada con el usuario.

Las etapas que anteceden pueden considerarse una fase de registro o de configuración, mediante la cual el dispositivo informático se configura o registra para la verificación de un atributo asociado con un usuario. Esta fase de registro/configuración puede preceder a una fase de verificación posterior, durante la cual se verifica realmente el atributo del usuario.

La obtención de los datos biométricos autenticados del usuario y/o la información de atributos asociados con el usuario a partir del identificador ID, puede comprender la captura de una imagen del identificador ID, mediante una cámara del dispositivo informático. Por ejemplo, el dispositivo informático puede escanear o fotografiar un identificador ID, para

obtener los datos biométricos autenticados y la información de atributos. En algunos ejemplos, dicha información puede obtenerse mediante reconocimiento óptico de caracteres, OCR.

De manera adicional o alternativa, la obtención de los datos biométricos autenticados del usuario y/o la información de atributos asociada con el usuario puede comprender la interrogación de una memoria del identificador ID. Dicho de otro modo, el dispositivo informático puede comunicarse con una memoria incluida en el identificador ID, en donde dicha memoria almacena los datos biométricos autenticados del usuario y/o la información de atributos asociada con el usuario. El dispositivo informático puede obtener estos datos de la memoria.

De manera preferible, el identificador ID, es un documento emitido por una autoridad de provisión de identificador ID. Por ejemplo, la autoridad emisora de identificaciones puede ser una institución de confianza, tal como un gobierno, un departamento gubernamental, una oficina de pasaportes, una agencia de tráfico, un emisor de permisos de conducción o cualquier otra autoridad autorizada para proporcionar identificaciones IDs. Limitar los métodos dados a conocer a la utilización de formas específicas de documentos de identidad de confianza garantiza que los datos obtenidos del identificador ID, puedan relacionarse con exactitud con el propietario del identificador ID.

El identificador ID, puede ser un pasaporte. La memoria puede ser un circuito integrado de transferencia inalámbrica de datos, tal como un circuito integrado NFC. En un ejemplo, el identificador ID, es un pasaporte y la memoria es un circuito integrado ePassport NFC. Los circuito integrados ePassport NFC representan un mecanismo existente por el que los datos biométricos autenticados de un usuario y la información de atributos asociada con el usuario (por ejemplo, relativa al nombre del usuario, edad, fecha de nacimiento, etc.) se almacenan digitalmente en el circuito integrado ePassport NFC de un pasaporte. Este circuito integrado puede ser objeto de lectura y se puede acceder a la información almacenada en el mismo, por ejemplo, mediante el dispositivo informático de la presente invención. Los datos biométricos obtenidos de la identificación, en este ejemplo del circuito integrado NFC del pasaporte electrónico, pueden comprender una imagen del usuario, una huella dactilar del usuario y/o un primer plano de un iris del usuario. Estos datos biométricos pueden utilizarse como datos biométricos autenticados para cotejar los datos biométricos capturados posteriormente del usuario, tal como se da a conocer con más detalle en el presente documento.

Determinar si los datos biométricos de verificación y/o los datos biométricos de registro corresponden al usuario, tal y como se ha descrito con anterioridad, puede comprender la forma de realización de uno o más procedimientos antifalsificación. Por ejemplo, cuando los datos biométricos de verificación comprenden una imagen de verificación capturada por el dispositivo informático, este último puede ordenar al usuario que realice un determinado gesto, tal como "mirar a la izquierda", "mirar hacia arriba", "inclinar la cabeza", etc., mientras se captura la imagen de verificación. Basándose en la acción del usuario, se pueden realizar pruebas de actividad vital para garantizar que la imagen que se está capturando es una imagen de un humano real y no una imagen falsa (por ejemplo, una imagen de una foto fija). Pueden aplicarse mecanismos similares cuando el dispositivo informático captura una imagen de registro durante una fase de registro. Otros procedimientos antifalsificación que pueden utilizarse cuando los datos biométricos no son una imagen del usuario, resultarán evidentes para el experto en esta técnica. Por ejemplo, cuando los datos biométricos son una huella dactilar, las comprobaciones antifalsificación de actividad vital pueden consistir en determinar si el dedo cambia de color cuando se aplica presión al escáner de huellas dactilares, o en buscar puntos de referencia concretos que no suelen encontrarse en las huellas dactilares falsas.

Según otro aspecto de la presente invención, se proporciona un método puesto en práctica por ordenador para configurar un dispositivo informático para verificar un atributo asociado con un usuario. Se puede considerar que dicho método está relacionado con una fase de registro o de configuración, en el sentido de que configura (o registra) el dispositivo informático al usuario para ser utilizado posteriormente para la verificación de un atributo asociado con dicho usuario.

El método dado a conocer comprende realizar, mediante el dispositivo informático, las etapas que incluyen: a) obtener, a partir de un identificador ID, datos biométricos autenticados del usuario e información de atributos asociada con el usuario; b) capturar datos biométricos de registro mediante el dispositivo informático; c) determinar si los datos biométricos de registro corresponden al usuario comparando los datos biométricos de registro con los datos biométricos autenticados; y d) en respuesta a la determinación de que los datos biométricos de registro corresponden al usuario, almacenar localmente en el dispositivo informático:

i) los datos biométricos autenticados del usuario; y

ii) la información de atributos asociada con el usuario.

Al ejecutar este método, el dispositivo informático puede configurarse para realizar la verificación de atributos del usuario, tal como se ha expuesto con anterioridad y a lo largo de esta invención. En particular, el dispositivo informático puede configurarse para realizar la verificación de atributo local sin necesidad de un servidor centralizado. Tal como en el caso anterior, en una puesta en práctica, el dispositivo informático puede comprender un dispositivo móvil, por ejemplo, un dispositivo móvil del usuario. En ese caso, el método también puede realizarse sin necesidad de instalar hardware dedicado en el lugar de verificación. Tal como en el caso anterior, los datos biométricos registrados y autenticados pueden comprender, por ejemplo, imágenes del usuario o de la huella dactilar del usuario, capturadas por una cámara o un escáner de huellas dactilares del dispositivo informático, respectivamente.

Dicho almacenamiento local en el dispositivo informático puede consistir en integrar los datos biométricos autenticados del usuario y/o la información de atributos asociada con el usuario en un certificado y almacenar el certificado localmente en el dispositivo informático. Tal como se ha indicado con anterioridad, dicho certificado presenta una representación fiable y reproducible de los datos en cuestión, de modo que el dispositivo informático pueda acceder tanto a la información de atributos como a los datos biométricos autenticados en una ubicación conocida. De manera preferible, el certificado se encuentra encriptado, para mejorar la seguridad y la privacidad de los datos. Por ejemplo, solamente determinadas aplicaciones de software autorizadas que se ejecuten en el dispositivo informático pueden tener los permisos adecuados para descifrar el certificado y acceder a los datos almacenados o integrados en el mismo. Lo que antecede reduce la probabilidad de que la información de atributos o los datos biométricos autenticados sean pirateados o ser objeto de acceso por partes no autorizadas.

Los datos biométricos autenticados del usuario y la información de atributos asociada con el usuario pueden almacenarse de modo que sean accesibles a más de una aplicación de software que se ejecute en el dispositivo informático. Por ejemplo, los datos biométricos autenticados y la información de atributos pueden integrarse en un certificado y este último puede almacenarse en una ubicación predeterminada de la memoria del dispositivo informático. La ubicación puede anunciarse o hacerse accesible a más de una aplicación de software que se ejecute en el dispositivo informático, de modo que más de una aplicación pueda utilizar los mismos datos (por ejemplo, el certificado). Lo que antecede puede permitir que las aplicaciones posteriores que hagan uso de los datos almacenados se configuren y establezcan para la verificación de atributos sin la necesidad de obtener más datos desde un identificador ID, tal como se da a conocer con más detalle a continuación.

En un ejemplo, las etapas a) - d) que anteceden se realizan mediante una primera aplicación de software que se ejecuta en el dispositivo informático, y comprendiendo el método, además: e) acceder, mediante una segunda aplicación de software que se ejecuta en el dispositivo informático, a los datos biométricos autenticados del usuario y a la información de atributos asociada con el usuario almacenada localmente en el dispositivo informático. El método puede comprender, además: f) configurar la segunda aplicación de software para permitir la verificación del atributo asociado con el usuario, mediante la segunda aplicación de software. El método puede comprender, además: g) verificar, mediante la segunda aplicación de software, el atributo asociado con el usuario.

De este modo, la segunda aplicación de software puede configurarse para permitir la verificación de atributos del mismo modo que la primera aplicación de software, pero la configuración de la segunda aplicación de software no requiere acceso al identificador ID. Lo que antecede es beneficioso porque significa que se pueden configurar nuevas aplicaciones para la verificación de atributos de manera más rápida y en ausencia del identificador ID.

Según otro aspecto de la presente invención, se proporciona un dispositivo informático configurado para realizar cualquiera de los métodos o procesos aquí dado a conocer. Por ejemplo, el dispositivo informático puede incluir un procesador y una memoria. La memoria puede almacenar instrucciones que, al ser ejecutadas por el procesador, hacen que este último lleve a cabo una o varias de las etapas o procesos aquí descritos. El dispositivo informático puede ser un dispositivo móvil, por ejemplo, perteneciente a un usuario verificado.

Según otro aspecto de la presente invención, se proporciona un medio legible por ordenador que comprende instrucciones que, al ser ejecutadas por un procesador de un dispositivo informático, hacen que el dispositivo informático lleve a cabo cualquiera de los métodos o procesos aquí dados a conocer. El dispositivo informático puede ser un dispositivo móvil, por ejemplo, perteneciente a un usuario verificado.

Según otro aspecto de la presente invención, se proporciona un programa informático que comprende instrucciones que, cuando el programa es ejecutado por un dispositivo informático, hacen que el dispositivo informático realice cualquiera de los métodos o procesos aquí dados a conocer. El dispositivo informático puede ser un dispositivo móvil, por ejemplo, perteneciente a un usuario verificado.

Según otro aspecto de la presente invención, se proporciona un sistema que comprende: un dispositivo informático configurado para realizar cualquiera de los métodos o procesos aquí dados a conocer para la verificación de un atributo asociado con un usuario; y un dispositivo de consulta configurado para recibir, del dispositivo informático, la confirmación del atributo verificado asociado con el usuario. El dispositivo informático puede ser un dispositivo móvil, por ejemplo, perteneciente al usuario verificado.

Según otro aspecto de la presente invención, se proporciona un sistema que comprende: un programa informático que incluye instrucciones que, cuando el programa es ejecutado por un dispositivo informático, hacen que el dispositivo informático realice cualquiera de los métodos o procesos aquí dados a conocer; y un programa informático que incluye instrucciones que, cuando el programa es ejecutado por un dispositivo de consulta, configuran el dispositivo de consulta para recibir del dispositivo informático la confirmación del atributo verificado asociado con el usuario. El dispositivo informático puede ser un dispositivo móvil, por ejemplo, perteneciente al usuario verificado.

El dispositivo de consulta puede ser un dispositivo de punto de venta, POS, por ejemplo, en la caja de una tienda. En algunos ejemplos, el dispositivo de consulta puede ser un cajero automático.

La recepción de la confirmación del atributo verificado asociado con el usuario desde el dispositivo informático puede incluir el escaneado, por parte del dispositivo de consulta, de una pantalla del dispositivo informático.

Breve descripción de las figuras

A continuación se describirán, a modo de ejemplo solamente, puestas en práctica ilustrativas de la presente invención con referencia a los dibujos. En los dibujos:

la Figura 1 es una representación esquemática de un sistema existente de la técnica anterior para la verificación de atributos;

la Figura 2 es una representación esquemática de un sistema alternativo de verificación de atributos según la presente invención;

la Figura 3 es un diagrama de flujo de las etapas implicadas en una puesta en práctica de la fase de registro de la presente invención;

la Figura 4 es un diagrama de flujo de las etapas implicadas en una puesta en práctica de la fase de verificación de la presente invención;

la Figura 5 es un ejemplo de una confirmación de verificación que puede mostrarse tras la verificación correcta de atributos;

la Figura 6 es un diagrama de flujo de las etapas implicadas en una puesta en práctica de la presente invención que permite la interoperabilidad entre diferentes aplicaciones de software de verificación de atributos;

la Figura 7 es un diagrama de flujo de las etapas implicadas en un ejemplo de uso de los mecanismos de verificación de la presente invención; y

la Figura 8 es una representación esquemática de un dispositivo informático que puede utilizarse para llevar a cabo los métodos de la presente invención.

A lo largo de la descripción y de los dibujos, las referencias numéricas semejantes se refieren a características semejantes.

Descripción detallada

Esta descripción detallada da a conocer, con referencia a la Figura 1, un sistema existente de la técnica anterior para la verificación de atributos. A continuación, con referencia a las Figuras 2 a 7, se da a conocer un sistema alternativo y mejorado de verificación de atributos que supera varios inconvenientes técnicos del sistema anterior. Por último, con referencia a la Figura 8, se da a conocer un dispositivo informático que puede utilizarse para llevar a cabo los métodos de la presente invención.

Los métodos y sistemas aquí dados a conocer se refieren en general a la verificación de los atributos del usuario, tal como la edad o la identidad. Los procesos y mecanismos aquí descritos permiten que dicha verificación se realice localmente mediante un dispositivo informático. No es necesario intercambiar datos con una autoridad o base de datos central, a diferencia de los mecanismos existentes. En consecuencia, se abordan los inconvenientes técnicos asociados a los sistemas de la técnica anterior.

En una puesta en práctica, los métodos descritos pueden ser realizados por un dispositivo de consulta, por ejemplo, situado en una tienda o en una barrera o entrada a un local. El dispositivo de consulta puede ejecutar los métodos descritos para verificar a un usuario que desee, por ejemplo, comprar un artículo restringido en la tienda o acceder al local. En una puesta en práctica alternativa, los métodos dados a conocer son ejecutados por un dispositivo móvil, por lo general perteneciente o asociado a la persona que se está verificando. En este caso, los métodos dados a conocer proporcionan una ventaja adicional, ya que no es necesario instalar ningún hardware de verificación específico en el punto de verificación. En su lugar, el usuario simplemente utiliza su propio dispositivo.

Las ventajas de los sistemas y métodos descritos serán más evidentes si se consideran en el contexto de los sistemas existentes para la verificación digital de los atributos. En consecuencia, se describirá brevemente un ejemplo de dicho sistema en relación con la Figura 1.

Volviendo a la Figura 1, se muestra un servidor 102 asociado a una autoridad 101 de verificación de atributos. Esta autoridad centralizada 101 almacena perfiles de usuario, por ejemplo, en una base de datos 104, para poder proporcionar la funcionalidad de verificación de atributos. Por ejemplo, la base de datos 104 puede almacenar una lista de atributos asociados a cada usuario del sistema, tal como su edad, fecha de nacimiento, nombre, sexo, etc.

Cuando un nuevo usuario desea registrarse en el servicio, el usuario se comunica con el servidor o servidores de la autoridad central y la base o bases de datos a través de una red 106, por lo general Internet, mediante el dispositivo de usuario 100. Por ejemplo, el usuario puede transmitir una solicitud de registro junto con algún tipo de información de identificación personal, PII, que el servidor 102 puede asociar al usuario y almacenar en la base de datos 104.

Posteriormente, se puede pedir al usuario que verifique un atributo tal como su edad, por ejemplo, al comprar un determinado artículo en una tienda. En este punto, el usuario o una autoridad de consulta, tal como la tienda en donde se compra el producto, se comunica con la autoridad de verificación de atributos 101 a través de la red 106 para obtener los

datos de verificación necesarios para el usuario. Por ejemplo, el dispositivo del usuario 100 o la autoridad de consulta 108 pueden transmitir alguna información PII (por ejemplo, un nombre o una dirección) del usuario a la autoridad de verificación 101. Al recibirla, el servidor 102 puede cotejar esa información PII con uno de los perfiles de usuario que tiene en la base de datos 104 y responder al dispositivo del usuario 100 y/o a la autoridad de consulta 108 con una confirmación de la edad del usuario, verificando de este modo ese atributo del usuario.

Tal como se desprende con facilidad de lo que antecede y de la Figura 1, un sistema de este tipo la técnica anterior implica una comunicación constante entre los usuarios y/o las autoridades de consulta y la autoridad central de verificación de atributos 101. Esta comunicación bidireccional se muestra de manera esquemática en la Figura 1 mediante flechas de doble punta.

Un inconveniente técnico importante de este sistema existente de la técnica anterior es que depende totalmente de que el dispositivo de usuario 100 y/o la autoridad de consulta 108 tengan una conexión a la red 106 y, por tanto, a la autoridad centralizada de verificación de atributos 101. Lo que antecede plantea un problema, porque el sistema no puede funcionar de forma autónoma. Esto plantea un problema, porque el sistema puede ser inadecuado para su uso en zonas en donde la conexión a la red es poco fiable o incluso inexistente. Este puede ser el caso en lugares remotos, pero también puede ocurrir en zonas concurridas, tal como estadios deportivos o salas de conciertos, en donde las redes pueden sobrecargarse por el número de dispositivos que intentan conectarse a la misma célula de red. En un entorno así, el sistema de la técnica anterior de la Figura 1 fallaría y sería incapaz de proporcionar la verificación de atributos al usuario. Si la verificación de atributos es un etapa esencial, por ejemplo, en una transacción, el usuario no podría completarla. Del mismo modo, es posible que una persona no pueda entrar en un local o edificio si no puede verificar su identidad.

Otro inconveniente del sistema mostrado en la Figura 1 es el hecho de que la autoridad de verificación centralizada 101 debe conservar datos de atributos sensibles de muchos usuarios. Lo que antecede presenta una única superficie de intrusión a través de la cual un hacker o una entidad maliciosa podría acceder a volúmenes incalculables de datos personales de los usuarios. Asimismo, tal como se ha descrito con anterioridad, la información PII, tal como el nombre, la fecha de nacimiento o la dirección de un usuario, debe transmitirse a través de la red 106 como parte del proceso de registro o de verificación. Lo que antecede supone una oportunidad más de pirateo o de pérdida de datos.

Los sistemas y métodos dados a conocer, que ahora se describirán en detalle, proporcionan un mecanismo alternativo para la verificación de atributos que aborda las limitaciones técnicas descritas con anterioridad de los sistemas existentes. Conviene señalar que las limitaciones técnicas del sistema anterior se aplican independientemente del tipo de atributo de usuario que se verifique; es decir, son limitaciones técnicas sistemáticas resultantes de las deficiencias tecnológicas del sistema existente de la técnica anterior. Son estas limitaciones técnicas las que pretenden abordar los sistemas y métodos dados a conocer.

A un alto nivel, el sistema dado a conocer permite que la verificación de atributos se realice localmente en un dispositivo informático, tal como un dispositivo de consulta en una tienda o local o en el propio dispositivo móvil del usuario. Lo que antecede significa que no es necesario depender de ninguna autoridad central de verificación 101, a diferencia de los sistemas de la técnica anterior. El proceso por el que esto se hace posible se muestra de manera esquemática en la Figura 2 y se da a conocer con más detalle en las Figuras 3 y 4.

Volviendo primero a la Figura 2, tal como se muestra, el proceso de verificación de atributos descrito puede considerarse que comprende dos fases separadas. Una primera fase, que puede considerarse una fase de registro, configura el dispositivo informático 200 para su uso en el procedimiento de verificación de atributos. Conviene señalar que los términos "fase de registro" y "fase de configuración" se utilizan indistintamente a lo largo de esta invención. Tras el registro, durante una fase de verificación posterior, el dispositivo informático 200 se utiliza luego para verificar un atributo del usuario 201, tal como su edad.

Tal como se ha indicado con anterioridad, el dispositivo informático 200 puede ser fijo o móvil. En algunas puestas en práctica, el dispositivo informático es un terminal, una máquina, un escáner o un ordenador proporcionado en un lugar de verificación. Por ejemplo, el dispositivo informático 200 puede formar parte de una barrera de entrada en un edificio, o de una máquina de caja en una tienda. En otras puestas en práctica, el dispositivo informático puede ser un dispositivo móvil, por ejemplo, un dispositivo informático móvil que incluya, entre otros, un teléfono móvil, un teléfono inteligente, un asistente digital personal (PDA), un ordenador portátil, una tableta electrónica y otros dispositivos móviles "inteligentes", tal como un reloj inteligente. Los procesos realizados por el dispositivo informático 200 durante la fase de registro pueden ser controlados por el software que se ejecuta en el dispositivo. Por ejemplo, cuando el dispositivo informático 200 es un dispositivo móvil, el proceso puede controlarse mediante una aplicación de software o "app" que se ejecuta en el dispositivo móvil.

La fase de registro se describirá con más detalle en relación con la Figura 3 siguiente. En resumen, sin embargo, la fase de registro implica que el dispositivo informático 200 captura los datos biométricos del usuario que utiliza el dispositivo informático 200. Este proceso está representado por la flecha (a) de la Figura 2. Los datos biométricos capturados pueden considerarse datos biométricos de registro, ya que se utilizan para registrar al usuario 201 en el dispositivo informático 200 para la verificación de atributos.

El dispositivo informático 200 también obtiene información de atributos y datos biométricos autenticados del usuario a partir de un identificador ID 202. Este proceso está representado por la flecha (b) de la Figura 2. Los datos biométricos autenticados representan o comprenden los datos biométricos almacenados o incluidos en el identificador ID 202 del usuario.

Los datos biométricos autenticados pueden ser cualquier dato adecuado para identificar biométricamente al usuario 201. Por ejemplo, los datos biométricos autenticados pueden comprender uno o más de entre: una imagen del usuario (por ejemplo, una foto de pasaporte o de carné de conducir); una huella dactilar del usuario; y un detalle del iris (por ejemplo, un primer plano de un iris) del usuario. Estos datos biométricos pueden utilizarse posteriormente para identificar al usuario mediante, por ejemplo, el reconocimiento facial, la coincidencia de huellas dactilares y/o el reconocimiento del iris, respectivamente, cuando se reciban nuevos datos biométricos del usuario durante el registro o la verificación.

Por ejemplo, cuando el identificador ID 202 es un pasaporte, los datos biométricos autenticados comprenden la foto del pasaporte, la huella dactilar y el detalle del iris del usuario 201. Como resultado de su origen en un pasaporte, estos datos biométricos pueden considerarse autorizados o aprobados, de modo que representan con exactitud al usuario 201. Del mismo modo, puesto que la información de atributos también se obtiene del identificador ID 202, también puede considerarse exacta. La información de atributos puede referirse a cualquier atributo del usuario 201 que esté atestiguado por los datos que figuran en el identificador ID 202, tal como el nombre, la fecha de nacimiento, la edad, el sexo, la dirección, la nacionalidad, etc. del usuario.

De manera preferible, los métodos dados a conocer se limitan a la utilización de identificadores IDs emitidos por una autoridad proveedora de documentos de identidad de confianza o autorizada. Por ejemplo, la autoridad proveedora de identificadores IDs puede ser un gobierno, un departamento gubernamental, una oficina de pasaportes, una agencia de tráfico, un emisor de permisos de conducir o cualquier otra autoridad que haya sido verificada para proporcionar identificadores IDs. En ese caso, el dispositivo informático 200 puede tener acceso a una lista de autoridades autorizadas para el suministro de identificadores IDs y solamente puede aceptar el uso de un identificador ID expedido por una de dichas autoridades. La lista de autoridades de provisión de identificadores IDs autorizadas puede incluirse como parte de la aplicación o aplicaciones de software que realizan la verificación de atributos en el dispositivo informático 200, por ejemplo, tal como parte del SDK proporcionado por un proveedor de software de verificación de atributos.

Una vez obtenidos los datos biométricos autenticados del usuario 201 a partir del identificador ID 202 y capturados los datos biométricos de registro, estos datos pueden compararse. Si el dispositivo informático 200 determina, basándose en esta comparación, que los datos biométricos de registro y los datos biométricos autenticados no corresponden a la misma persona, entonces el proceso de registro falla. El usuario 201 puede tener la oportunidad de reintentar el proceso. Esta comprobación impide que un usuario se registre con el identificador ID 202 de otra persona.

Sin embargo, si el dispositivo informático 200 determina, basándose en esta comparación, que los datos biométricos de registro y los datos biométricos autenticados sí corresponden a la misma persona, es decir, que ambos corresponden al usuario 201, entonces el proceso de registro puede completarse y el dispositivo informático 200 puede configurarse para verificar uno o más atributos del usuario 201 en el futuro.

En particular, si se determina que los datos biométricos de registro corresponden al usuario 201, el dispositivo informático 200 puede almacenar localmente en el dispositivo informático: i) los datos biométricos autenticados del usuario obtenidos del identificador ID 202; y ii) la información de atributos asociada con el usuario obtenida del identificador ID 202. Los datos biométricos autenticados y la información de atributos almacenados pueden utilizarse posteriormente, durante una fase de verificación, para verificar uno o más atributos del usuario 201.

Dicha fase de verificación también se muestra de manera esquemática en la Figura 2. Tal como se muestra de manera esquemática, la fase de verificación implica de nuevo que el dispositivo informático 200 obtenga datos biométricos del usuario. En este caso, los datos biométricos obtenidos pueden considerarse datos biométricos de verificación, en el sentido de que se utilizan para permitir que el dispositivo informático verifique un atributo del usuario. Este proceso está representado por la flecha (c) de la Figura 2.

A continuación, el dispositivo informático 200 puede comparar los datos biométricos de verificación capturados con los datos biométricos autenticados del usuario obtenidos previamente del identificador ID 202 y almacenados en el dispositivo informático durante la fase de registro.

Si el dispositivo informático 200 determina, basándose en esta comparación, que los datos biométricos de verificación no corresponden a la misma persona que los datos biométricos autenticados, es decir, no corresponden al usuario 201, entonces el proceso de verificación falla. Se puede dar al usuario 201 la oportunidad de reintentar el proceso. Esta comprobación impide que un usuario utilice un dispositivo informático 200 registrado con el identificador ID 202 de otra persona durante la verificación de atributos.

Sin embargo, si el dispositivo informático 200 determina, basándose en esta comparación, que los datos biométricos de verificación sí corresponden a la misma persona que los datos biométricos autenticados, es decir, el usuario 201, se puede proceder a la verificación de atributos. En concreto, el dispositivo informático 200 puede acceder a la información de atributos obtenida previamente del identificador ID 202 y almacenada en el dispositivo informático 200 durante la fase de registro. Basándose en la información de atributos, se puede verificar un atributo asociado con el usuario. Por ejemplo, la

información de atributos puede incluir la fecha de nacimiento del usuario. Basándose en esta información, una vez superada con éxito la fase de verificación biométrica, el dispositivo informático 200 puede verificar o confirmar la edad del usuario, o que éste tiene una determinada edad mínima. En otro ejemplo, la información de atributos puede comprender el nombre del usuario. En ese caso, una vez superada con éxito la etapa de verificación biométrica, el dispositivo informático 200 puede verificar o confirmar el nombre del usuario, o que el usuario está en una lista de personas certificadas o aprobadas, o que tiene ciertas autorizaciones o privilegios.

En la invención, la confirmación de la verificación de atributos la realiza el dispositivo informático 200, por ejemplo, a una autoridad 108 que realiza consultas. Este proceso está representado por la flecha (d) de la Figura 2. En algunos ejemplos, la autoridad de consulta 108 puede ser un dispositivo de consulta, tal como una máquina de caja en una tienda, una barrera de entrada en un local u otro edificio, una máquina expendedora automática o un dispositivo de un repartidor, tal como cuando los métodos dados a conocer se utilizan en el contexto de la entrega a domicilio. Al recibir o escanear la confirmación, el dispositivo de consulta puede confirmar que el usuario está verificado para la transacción en cuestión, o para la entrada a un local. Lo que antecede facilita los flujos de transacciones totalmente automatizados y la entrada al local.

Mediante la funcionalidad descrita con anterioridad, se puede verificar un atributo del usuario 201 de forma totalmente local. No es necesaria ninguna conexión de red durante las fases de registro o verificación. Lo que antecede significa que la verificación de atributos puede realizarse en cualquier lugar y en cualquier momento, independientemente de la calidad o conectividad de la red. Además, no es necesario transmitir información de identificación personal PII ni datos confidenciales desde el dispositivo informático 200 a una red o servidor remotos en ningún momento, a diferencia del sistema existente de la técnica anterior de la Figura 1. Lo que antecede reduce la posibilidad de que un actor malintencionado obtenga datos de usuario o información PII, mejorando aún más la seguridad. Además, cuando el dispositivo informático 200 es un dispositivo móvil del usuario, no existe la necesidad de que una única autoridad centralizada conserve los datos sensibles de varias personas. Más bien, los datos se guardan de forma distribuida en los propios dispositivos informáticos personales de los usuarios. Lo que antecede distribuye las superficies de ataque disponibles para un actor malintencionado, y evita la posibilidad de que un único pirateo o pérdida de datos cause, por ejemplo, la publicación de datos sensibles de múltiples usuarios de manera simultánea.

Tal como puede constatarse, los métodos dados a conocer permiten un mecanismo más fiable y seguro para verificar los atributos del usuario, tal como la edad y la identidad. Para facilitar la comprensión de estos mecanismos, a continuación se explicarán con más detalle las dos fases descritas con anterioridad (registro y verificación) haciendo referencia a las Figuras 3 y 4, respectivamente.

Pasando en primer lugar a la Figura 3, se muestra con más detalle un ejemplo de la fase de registro o de configuración descrita con anterioridad y mostrada en la Figura 2. En particular, se muestran las distintas etapas realizadas por el dispositivo informático 200 durante la fase de registro. Tal como se ha indicado con anterioridad, este proceso se realiza por lo general bajo el control de un software que se ejecuta en el dispositivo informático 200 y que ordena al procesador del dispositivo informático 200 que realice las etapas mencionadas. Cuando el dispositivo informático 200 es un dispositivo móvil, tal como un teléfono inteligente, dicho software comprende por lo general una aplicación de software o "app" que se ejecuta en el dispositivo móvil 200.

En un ejemplo, el proceso comienza o se inicia cuando el software o la aplicación de software recibe una solicitud del usuario 201, por ejemplo, a través de una entrada en una pantalla del dispositivo informático 200, para iniciar el registro. En respuesta, se inicia el proceso de la Figura 3 y el dispositivo informático 200 obtiene, en el bloque 301, datos biométricos autenticados del usuario e información de atributos asociada con el usuario a partir del identificador ID 202.

En un ejemplo, los datos biométricos autenticados y la información de atributos se obtienen utilizando una cámara del dispositivo informático 200. Por ejemplo, se puede capturar una imagen del identificador ID 202. A continuación, se puede utilizar el reconocimiento óptico de caracteres (OCR) para extraer la información de atributos del identificador ID 202. Una imagen del usuario incluida en el identificador ID 202 puede escanearse o fotografiarse de forma similar y extraerse como los datos biométricos autenticados, es decir, tal como una imagen autenticada del usuario 201.

En otro ejemplo, algunos o la totalidad de los datos biométricos autenticados y/o la información de atributos se obtienen interrogando a una memoria del identificador ID 202. Por ejemplo, el identificador ID 202 puede incluir un circuito integrado de transferencia inalámbrica de datos, tal como un circuito integrado NFC. La memoria puede ser del tipo conocido de circuito integrado NFC de pasaporte electrónico. El dispositivo informático puede comunicarse con esta memoria o efectuar la lectura para obtener los datos biométricos autenticados del usuario y/o la información de atributos asociada con el usuario. La memoria puede estar protegida, por ejemplo, mediante una contraseña. En ese caso, el dispositivo informático 202 puede obtener la contraseña para permitir la comunicación con la memoria. En un ejemplo, la contraseña se obtiene capturando y realizando un OCR sobre caracteres o texto mostrados en el identificador ID 202 y determinando una contraseña basada en dichos caracteres o texto.

En algunos ejemplos, y como se ha mencionado con anterioridad, el tipo de identificación ID que puede utilizarse durante el registro puede limitarse a determinados formatos o tipos de documentos. En efecto, esto puede limitar los tipos de identificadores IDs que pueden utilizarse a determinados documentos acreditados emitidos por un subconjunto predeterminado de instituciones o gobiernos autorizados. Lo que antecede puede mejorar el grado de confianza que

puede asignarse a los datos biométricos autorizados y a la información de atributos obtenida del identificador ID 202. Ejemplos no limitativos de identificaciones IDs pueden ser pasaportes, permisos de conducir, documentos nacionales de identidad, tarjetas sanitarias, permisos biométricos tales como permisos de residencia y similares. En términos más generales, tal como se mencionó con anterioridad, los métodos descritos pueden limitarse a la utilización de identificadores IDs expedidos por una autoridad de provisión de ID autorizada, tal como un gobierno, una oficina de pasaportes, una agencia de tráfico o un emisor de permisos de conducir. Una autoridad de expedición de identificadores IDs acreditada puede ser la autorizada por el proveedor de software de verificación de atributos que ha proporcionado el software de verificación de atributos que se ejecuta en el dispositivo informático 200. En ese caso, dicho proveedor de software de verificación de atributos puede incluir una lista de tipos de identificación ID autorizados y/o autoridades de provisión de identificación autorizadas como parte del software de verificación de atributos, por ejemplo, integrado en el SDK.

A continuación, en el bloque 303, el dispositivo informático 200 captura datos biométricos de registro. En algunas puestas en práctica, los datos biométricos de registro comprenden una imagen del usuario, es decir, una imagen de registro. Si el dispositivo informático 200 es un terminal, se puede indicar al usuario que se coloque delante del terminal de forma que esté en el campo visual de la cámara del terminal. De manera alternativa, cuando el dispositivo informático 200 es un dispositivo móvil del usuario, tal como un teléfono inteligente, la imagen de registro puede ser un "selfie", es decir, una imagen del usuario tomada con la cámara frontal del dispositivo móvil. Otros métodos para obtener una imagen de registro utilizando una cámara del dispositivo informático 200 serán evidentes para un lector experto y dependerán de la naturaleza del dispositivo informático 200 y de la posición de su cámara. En otros ejemplos, los datos biométricos de registro comprenden una huella dactilar del usuario, o un primer plano de un iris del usuario. Estos datos pueden obtenerse de cualquier forma adecuada, por ejemplo, mediante un escáner de huellas dactilares o la cámara del dispositivo informático 200.

En algunas puestas en práctica, se pueden llevar a cabo procedimientos antifalsificación cuando se capturan los datos biométricos de registro en el bloque 303. Por lo general, los procedimientos antifalsificación incluirán algún tipo de comprobación de actividad vital para establecer que los datos biométricos de registro capturados proceden de un ser humano auténtico y no de una falsificación. En un ejemplo, los datos biométricos de registro comprenden una imagen capturada y el dispositivo informático 200 puede ordenar al usuario 201 que realice uno o más gestos, tal como "mirar a la izquierda", "mirar a la derecha", "girar la cabeza a la izquierda", etc. El dispositivo informático 200 puede entonces determinar si los gestos instruidos han sido realizados por la persona en el campo visual de la cámara. Si se siguen los gestos, el dispositivo informático 200 puede capturar la imagen de registro o utilizar un fotograma capturado durante el procedimiento antifalsificación como imagen de registro. Si no se siguen los gestos, se puede rechazar la imagen de registro. Si los datos biométricos de registro comprenden una huella dactilar o el iris, pueden realizarse otras pruebas antifalsificación o de actividad vital adecuadas. Los procedimientos antifalsificación de este tipo impiden que el usuario 201 falsifique sus datos biométricos de registro, por ejemplo, mostrando una fotografía o una falsificación similar a la cámara durante el registro, o utilizando un molde o un dedo falso durante la verificación de la huella dactilar. Otros ejemplos de comprobaciones de actividad vital y mecanismos antifalsificación que podrían emplearse como parte de los métodos descritos resultarán evidentes para el lector experto en esta técnica.

Una vez capturados los datos biométricos de registro, el método procede, en el bloque 305, a determinar si los datos biométricos de registro corresponden a la misma persona que el identificador ID 202. En concreto, los datos biométricos de registro se comparan con los datos biométricos autenticados obtenidos, en el bloque 301, del identificador ID 202 para determinar si coinciden, es decir, si corresponden a la misma persona. El mecanismo o mecanismos exactos de comparación mediante los cuales se realiza la determinación del bloque 305 están fuera del alcance de esta invención y serán evidentes para un lector experto en esta técnica. En el caso de una imagen de registro, por lo general se realizará algún tipo de procedimiento de reconocimiento facial tanto en la imagen de registro como en la autenticada para determinar si los rasgos faciales de cada imagen son lo suficientemente similares. Por ejemplo, el dispositivo informático 200 puede utilizar el análisis de puntos de referencia faciales para determinar si existe menos de un umbral predeterminado de diferencia en la posición relativa entre ciertos puntos de referencia faciales clave en cada una de las imágenes autenticadas y la imagen de registro. En otro ejemplo, puede utilizarse un método conocido como FaceNet, que extrae características de alta calidad del rostro y predice una representación vectorial de 128 elementos de estas características, denominada integración facial, para determinar una coincidencia. En algunos ejemplos, se puede utilizar el reconocimiento del iris y comparar un iris de la imagen de registro con un iris de la imagen autenticada. Cuando se utilizan huellas dactilares, la huella dactilar de registro obtenida en el bloque 303 se compara con la huella dactilar autenticada obtenida en el bloque 301 mediante un mecanismo apropiado de análisis de huellas dactilares. Otros mecanismos para comparar la similitud de los datos biométricos serán evidentes para un lector experto en esta técnica y pueden utilizarse como parte de los métodos dados a conocer.

Si se determina que los datos biométricos de registro no corresponden a la misma persona que los datos biométricos autenticados, el registro falla y se registra o se muestra un error de registro en el bloque 309. Se puede solicitar al usuario que vuelva a registrar los datos biométricos. Se puede solicitar al usuario que vuelva a intentar el proceso de registro. Esta comprobación evita que una persona se registre con el ID de otra persona.

Por otro lado, si la comparación realizada en el bloque 305 es correcta, es decir, si se determina que los datos biométricos autenticados y los datos biométricos de registro corresponden a la misma persona, el método pasa al bloque 307. En esta fase, los datos biométricos autenticados y los datos biométricos de registro corresponden a la misma persona. En esta fase, los datos biométricos autenticados y la información de atributos obtenida, en el bloque 301, del identificador ID 202

se almacenan a nivel local en el dispositivo informático 200. En una forma de realización preferida, los datos biométricos autenticados y la información de atributos se incorporan a un certificado que se almacena localmente en la memoria del dispositivo informático 200. El certificado se encripta de manera preferente para evitar que se produzcan errores. De manera preferible, el certificado está encriptado para mejorar la seguridad de los datos.

En algunas puestas en práctica, el dispositivo informático 200 simplemente obtiene la información de atributos del identificador ID 202 y la almacena tal cual, una vez superada la comprobación biométrica. Sin embargo, en otras puestas en práctica, el dispositivo informático 200 calcula alguna información de atributos adicional para el usuario 201 basándose en la información de atributos obtenida del identificador ID 202. Por ejemplo, puede obtenerse la fecha de nacimiento del usuario a partir del identificador ID 202. A partir de esto último, el dispositivo informático 200 puede determinar la edad del usuario o que el usuario cumple algún criterio predeterminado, por ejemplo, "el usuario tiene más de 18 años" o "el usuario tiene más de 21 años". En algunos ejemplos, si el proceso determina en esta fase que el usuario no cumple un criterio de edad mínima, el proceso de registro finaliza independientemente de si se supera la comprobación biométrica en el bloque 305. De manera preferible, se informa al usuario de que no cumple los requisitos mínimos de registro y, preferiblemente, se borran todos los datos obtenidos hasta el momento por el dispositivo informático 200.

Cuando el dispositivo informático 200 determina la edad del usuario basándose en la información obtenida del identificador ID 202, puede utilizarse una fecha actual para calcular la edad. De manera preferible, la fecha actual se obtiene de una fuente de confianza, tal como un proveedor de datos o una red de telefonía móvil a la que tenga acceso el dispositivo informático 200, en lugar de la fecha local en el dispositivo informático 200. Lo que antecede evita que el usuario modifique la fecha local en el dispositivo informático 200 y falsee su edad confundiendo el cálculo de la edad realizado por el dispositivo informático 200. Conviene señalar que, aunque este enfoque requiere un contacto muy limitado con una red o un operador, la única información que hay que obtener es una fecha actual (y, de manera opcional, la hora). Lo que antecede es extremadamente sencillo y no requiere transmisiones de gran cantidad de datos entre el dispositivo informático 200 y la red, a diferencia del sistema de la técnica anterior de la Figura 1. En concreto, basta con una conexión básica a la red telefónica y no se requiere conexión a Internet. Una vez establecida la fecha por el dispositivo informático, no es necesaria ninguna otra comunicación con la red.

De manera preferible, los datos biométricos autenticados y la información de atributos se almacenan en una ubicación y manera en el dispositivo informático 200 de modo que otras aplicaciones de software que realicen procesos similares de verificación de atributos puedan acceder a ellos en el futuro. Lo que antecede significa que el registro y la verificación pueden ser realizados por diferentes aplicaciones de software, mejorando la versatilidad del sistema en su conjunto. Lo que antecede es especialmente útil cuando el dispositivo informático 200 es un dispositivo móvil del usuario, en donde puede haber múltiples aplicaciones de verificación de la edad asociadas a diferentes vendedores y/o locales. En este caso, si una segunda aplicación de software posterior puede acceder a los datos biométricos autenticados almacenados y a la información de atributos almacenada por una primera aplicación de software, no es necesario que el usuario 201 utilice el identificador ID 202 durante la configuración de la segunda aplicación de software. Lo que antecede acelera de manera significativa el registro en las aplicaciones de software posteriores para la verificación de atributos, ya que, al utilizar el método con anterioridad expuesto, el usuario solamente necesita registrarse sustancialmente utilizando su identificador ID 202 una vez. Todas las aplicaciones que se utilicen posteriormente pueden acceder a los datos biométricos autenticados almacenados localmente y a la información de atributos sin que el usuario tenga que volver a registrarse por completo o presentar el identificador ID 202 al dispositivo informático 200. A continuación se da a conocer con más detalle un proceso para habilitar dicha funcionalidad con referencia a la Figura 6.

En algunos ejemplos, los datos biométricos autenticados y la información de atributos se almacenan en el bloque 307 utilizando un SDK proporcionado por un proveedor de software de verificación de atributos. En este caso, se pueden proporcionar ciertas medidas de seguridad, tal como el cifrado, para proteger los datos en cuestión. Posteriormente, en algunas puestas en práctica, solamente las aplicaciones que ejecutan el mismo SDK o que son proporcionadas por el mismo proveedor de software de verificación de atributos pueden acceder a los datos biométricos autenticados almacenados y a la información de atributos. Por ejemplo, los datos biométricos autenticados y la información de atributos pueden estar encriptados, de manera opcional como parte de un certificado, y en el SDK puede estar incorporada una clave de encriptación que permita desencriptar los datos almacenados. Otras aplicaciones solamente pueden acceder a los datos almacenados si tienen acceso a la clave, que puede limitarse a aquellas aplicaciones de software que ejecuten el mismo SDK o a las que el proveedor de software de verificación de atributos proporcione acceso a la clave. De este modo, la funcionalidad descrita con anterioridad, que permite la interoperabilidad entre aplicaciones de software, puede proporcionarse sin comprometer la seguridad de los datos almacenados, ya que solamente determinadas aplicaciones de software autorizadas pueden acceder a los datos almacenados.

En algunos ejemplos, los datos almacenados pueden asociarse adicional o de manera alternativa a un identificador de circuito integrado de dispositivo u otro identificador único del dispositivo informático 200 en donde se realiza el registro, o cifrarse mediante dicho identificador. Lo que antecede impide que los datos almacenados (es decir, los datos biométricos autenticados y la información de atributos) sean transferibles o utilizables para la verificación de atributos en un dispositivo de usuario diferente, mejorando aún más la seguridad y reduciendo la posibilidad de suplantación de identidad.

Mediante el procedimiento de registro de la Figura 3, un usuario 201 puede registrarse por sí mismo en un dispositivo informático 200 y configurar dicho dispositivo informático 200 para que realice la verificación de atributos en el futuro. El

mecanismo mediante el cual tiene lugar dicha verificación de atributos posterior se tratará ahora con más detalle en relación con la Figura 4.

Volviendo a la Figura 4, se muestra con más detalle un ejemplo de la fase de verificación descrita con anterioridad y mostrada en la Figura 2. En concreto, se muestran las distintas etapas realizadas por el dispositivo informático 200 durante la fase de verificación para llevar a cabo la verificación de atributos del usuario 201. Tal como en el caso de la fase de registro, el proceso asociado a la fase de verificación se realiza por lo general bajo el control de un software que se ejecuta en el dispositivo informático 200 y que ordena al procesador del dispositivo informático 200 que realice las etapas mencionadas. El software puede proporcionarse en forma de "app", tal como se ha descrito con anterioridad. El software responsable de realizar el proceso de verificación de la Figura 4 puede ser el mismo o diferente software que el que realiza el proceso de registro de la Figura 3. El único requisito es que el software que realiza el proceso de la Figura 4 tenga o pueda acceder a los datos biométricos autenticados y a la información de atributos almacenada localmente en el dispositivo informático 200 durante el proceso de la Figura 3.

En un ejemplo, el proceso de verificación comienza o se inicia cuando el software recibe una solicitud del usuario 201, por ejemplo, a través de una entrada en una pantalla del dispositivo informático 200, para comenzar la verificación de atributos. De manera alternativa, en particular cuando el dispositivo informático 200 es un dispositivo móvil, el dispositivo informático 200 puede recibir una solicitud de un dispositivo tal como un dispositivo de consulta local, por ejemplo, una máquina registradora de una tienda, una máquina expendedora o un dispositivo de consulta transportado, por ejemplo, por un repartidor. En respuesta, se inicia el proceso de la Figura 4 y el dispositivo informático 200 captura, en el bloque 401, datos biométricos de verificación mediante el dispositivo informático 200. Las mismas consideraciones expuestas con anterioridad en relación con la captura de los datos biométricos de registro de la Figura 3 se aplican en este caso a la captura de los datos biométricos de verificación. En particular, los datos biométricos de verificación pueden ser una imagen capturada por una cámara del dispositivo informático 200, una huella dactilar capturada por un escáner de huellas dactilares del dispositivo informático 200, o cualquier otro dato biométrico adecuado que permita la identificación biométrica. En el caso de una imagen, la imagen de verificación puede representar el campo de visión de un terminal o dispositivo fijo, o puede ser un "selfie" capturado por una cámara frontal de un dispositivo móvil del usuario. Pueden emplearse mecanismos antifalsificación para evitar la falsificación de los datos biométricos de verificación, tal como se ha descrito con anterioridad respecto a los datos biométricos de registro.

En el bloque 403, el dispositivo informático 200 determina si los datos biométricos de verificación corresponden a la misma persona que el identificador ID 202, es decir, si los datos biométricos coinciden. Concretamente, los datos biométricos de verificación se comparan con los datos biométricos autenticados obtenidos, en el bloque 301 de la fase de registro, del identificador ID 202. Tal como en el caso de la fase de registro, el mecanismo o mecanismos exactos de comparación mediante los cuales se realiza la determinación del bloque 403 están fuera del alcance de esta invención, y las mismas consideraciones comentadas con anterioridad en relación con el bloque 305 se aplican al bloque 403. Dicho de otro modo, puede realizarse cualquier forma adecuada de reconocimiento facial, análisis de huellas dactilares, análisis del iris o similar para determinar si los datos biométricos coinciden.

Si se determina que los datos biométricos de verificación no corresponden a la misma persona que los datos biométricos autenticados, entonces falla la verificación y se registra o se muestra un error de verificación 407. Se puede pedir al usuario que vuelva a intentar el proceso de verificación. Lo que antecede evita que alguien utilice un dispositivo informático para la verificación de atributos cuando el dispositivo informático se ha configurado utilizando el identificador ID 202 de otra persona.

Por otra parte, si se supera la comparación realizada en el bloque 403, es decir, si se determina que los datos biométricos autenticados y los datos biométricos de verificación corresponden a la misma persona, el método pasa al bloque 405. En esta fase, el dispositivo informático 200 verifica uno o más atributos asociados al usuario basándose en la información de atributos asociada con el usuario que se obtuvo del identificador ID 202 y se almacenó localmente en el dispositivo informático durante el bloque 307 de la fase de registro.

En un ejemplo, el bloque 405 implica acceder a la información de atributos relacionada con la edad obtenida durante el registro del identificador ID 202 y almacenada localmente en el dispositivo informático 200. Por ejemplo, la información de atributos puede incluir la fecha de nacimiento del usuario. A partir de ella, el dispositivo informático 200 puede determinar la edad del usuario o que éste sea mayor de una edad mínima, tal como 18 años. En otro ejemplo, el bloque 405 implica acceder a la información de atributos relacionados con la identidad obtenida durante el registro del identificador ID 202 y almacenada localmente en el dispositivo informático 200. Por ejemplo, el dispositivo informático 200 puede confirmar el nombre del usuario basándose en la información de atributos almacenada.

Tal como puede constatarse, el proceso de verificación de la Figura 4 puede realizarse de forma totalmente local, en el sentido de que no se requiere conexión entre el dispositivo informático 200 y ninguna red o servidor remoto para que tenga lugar la verificación de atributos. Lo que antecede contrasta con el sistema existente de la técnica anterior descrito con anterioridad con referencia a la Figura 1. También a diferencia de ese sistema, el método de la Figura 4 no requiere la transmisión de ninguna información PII desde el dispositivo informático 200.

En respuesta a la verificación de un atributo del usuario 201 en el bloque 405, el dispositivo informático 200 puede emprender otras acciones. Por ejemplo, cuando el dispositivo informático 200 forma parte de una barrera de entrada a un

local o edificio, al verificar el nombre del usuario y confirmar que está en una lista de personas autorizadas, el dispositivo informático 200 puede permitir que la persona acceda al local o edificio. En la invención, una vez verificados uno o varios atributos del usuario en el bloque 405, el dispositivo informático 200 procede a proporcionar una confirmación del atributo o atributos verificados asociados al usuario en una pantalla del dispositivo informático 200. El dispositivo informático puede transmitir, además, un mensaje de confirmación de los atributos verificados asociados al usuario, por ejemplo, a un dispositivo o red remotos y/o a otra aplicación de software que se ejecute en el dispositivo informático 200. La confirmación puede adoptar, además, otras formas, por ejemplo, la confirmación puede comprender una confirmación sonora, tal como un tono de confirmación o un mensaje de audio.

Cuando se proporciona una confirmación de verificación en la pantalla del dispositivo informático 200, la confirmación comprende elementos legibles por máquina. Por ejemplo, puede mostrarse la edad exacta del usuario, por ejemplo, "35 años". De manera alternativa, la pantalla puede indicar que el usuario tiene una determinada edad mínima, por ejemplo, "más de 18 años". En otra puesta en práctica, un gráfico puede acompañar o sustituir a dicha indicación textual de verificación de atributos. Por ejemplo, puede mostrarse una marca verde con la palabra "verificado". Cualquier mecanismo para confirmar la verificación de atributos en la pantalla del dispositivo informático de esta manera será evidente para el experto en esta técnica. Si la confirmación incluye un elemento legible por máquina, puede adoptar la forma de un código QR en donde esté integrada la verificación de atributos. Por ejemplo, el código QR puede, al ser objeto de lectura por un lector de códigos QR adecuado, confirmar la edad del usuario a dicho lector o confirmar que el usuario es mayor de una edad mínima requerida, tal como 18 años. Proporcionar esta confirmación visual de la verificación de atributos en una pantalla del dispositivo informático 200 puede ser especialmente útil cuando el dispositivo informático 200 es un dispositivo móvil del usuario 201, porque entonces el usuario 201 puede presentar su dispositivo móvil al dependiente de una tienda o local, a la interfaz de una máquina (tal como un escáner de códigos QR) de la tienda o local, o a cualquier otra autoridad o dispositivo de consulta, tal como un repartidor o una máquina expendedora. La presentación de la confirmación de la verificación de esta manera puede facilitar la forma de realización de una transacción o la entrada a un local, por ejemplo,.

En una puesta en práctica, el código QR que se muestra en el dispositivo informático 200 para confirmar la verificación es un código QR dinámico que puede redirigir un dispositivo de consulta (escáner QR) a una ubicación concreta, tal como una URL, o presentar determinados datos espaciotemporales obtenidos recientemente al dispositivo de consulta. El código QR dinámico puede actualizarse periódicamente. El uso de un código QR dinámico de este tipo puede mejorar la protección contra la suplantación de identidad, tal como se da a conocer con más detalle a continuación.

En un ejemplo, el procedimiento de verificación de la Figura 4 puede incluir la obtención de información espaciotemporal asociada con la verificación del atributo asociado con el usuario. Esta información espaciotemporal obtenida puede integrarse entonces en la confirmación del atributo verificado, tal como en un código QR dinámico mostrado por el dispositivo informático 200 tras la verificación. La información espaciotemporal proporciona alguna indicación de cuándo y/o dónde ha tenido lugar la verificación del atributo y puede ser especialmente útil cuando el dispositivo informático 200 es un dispositivo móvil del usuario y cuando se requiere que el usuario presente la confirmación de la verificación como parte de una transacción o procedimiento de entrada al recinto. Concretamente, la información espaciotemporal incluye una o más de entre una fecha actual, una hora actual, una ubicación actual y una identidad de un establecimiento en donde ha tenido lugar o está teniendo lugar la verificación.

En una puesta en práctica, el dispositivo informático 200 es un dispositivo móvil del usuario 201 y la información espaciotemporal referenciada con anterioridad se obtiene durante el proceso de verificación mediante el escaneo por parte del usuario, utilizando la cámara de su dispositivo móvil 200, de un código QR o de un indicador visual similar proporcionado en el lugar en donde se está realizando la verificación. Por ejemplo, si la verificación se refiere a la verificación de la edad en una tienda, el usuario puede escanear un código QR proporcionado en una máquina de caja de la tienda. En algunas puestas en práctica, el usuario puede escanear de manera alternativa una memoria, tal como un circuito integrado NFC o un elemento similar, para obtener la información espaciotemporal. La información espaciotemporal obtenida en este ejemplo también puede indicar la ubicación y el nombre de la tienda. Esta información de ubicación obtenida puede combinarse, por ejemplo, con la fecha y hora actuales proporcionadas por un reloj local del dispositivo móvil 200, una red móvil o, preferiblemente, por el código QR escaneado.

La información espaciotemporal combinada puede entonces incorporarse a la confirmación de verificación mostrada en el dispositivo móvil 200. Por lo tanto, cuando un dependiente o un escáner (si es legible por máquina) de la tienda o del local, esté presente y proceda a la lectura de la confirmación de la verificación, este último confirmará no solamente que se ha verificado el atributo del usuario, sino también la fecha, la hora y la identidad de la tienda o del local en donde se ha realizado la verificación. Lo que antecede proporciona una capa añadida de seguridad al proceso de verificación, porque significa que será inmediatamente evidente si el usuario está intentando presentar una captura de pantalla o imagen de una confirmación de verificación anterior en el dispositivo móvil 200. En tal caso, los datos de hora y/o ubicación incorporados en la confirmación no coincidirán con una hora y/o ubicación esperadas, de modo que la confirmación podrá ser rechazada. En una puesta en práctica preferida, la confirmación (por ejemplo, el código QR) proporcionada en la pantalla del dispositivo móvil 200 tras la verificación de atributos está limitada en el tiempo, en el sentido de que caduca de manera automática o se actualiza periódicamente. Lo que antecede evita, además, la suplantación del proceso de verificación, ya que las confirmaciones de verificación antiguas no se pueden reutilizar.

En la Figura 5 se muestra un ejemplo de una confirmación de verificación que puede mostrarse en el dispositivo informático 200 después de que la verificación de atributos haya tenido éxito en el bloque 405. En este ejemplo, el dispositivo

informático 200 es un dispositivo móvil 500 del usuario, en donde se muestra una confirmación visual de que la verificación de atributos se ha realizado correctamente. En este ejemplo, el atributo que se verifica es la edad del usuario, concretamente que el usuario es mayor de 18 años. Tal como puede constatarse, la confirmación incluye tanto elementos legibles por humanos 501 como un elemento legible por máquinas 503. Ambos tipos de elementos 501, 503 contienen, en este ejemplo, información espaciotemporal sobre dónde y cuándo ha tenido lugar la verificación de atributos. En concreto, los elementos legibles por el ser humano contienen información espaciotemporal relativa al nombre y a la ubicación de la tienda en donde ha tenido lugar la verificación ("Tienda X", en Oxford Street, Londres). Esta información, en un ejemplo, puede obtenerse realizando la lectura, mediante el dispositivo móvil 500, de un código QR proporcionado en la caja de la tienda de la manera descrita con anterioridad. Los elementos legibles por humanos también incluyen una marca de tiempo que indica la hora y la fecha en que tuvo lugar la verificación (miércoles 6 de enero de 2021 a las 13:29:43). Esta hora puede representar el momento en que se completó el proceso de la Figura 4, o el momento en que se realizó la lectura de un código QR o de un elemento similar en la tienda. Por último, los elementos legibles por humanos incluyen un indicador visual de que el usuario es mayor de 18 años, es decir, que se ha verificado este atributo. La confirmación mostrada también incluye un código QR 503 legible por máquina, que incluye toda la información antes mencionada incorporada de forma legible por máquina.

De este modo, la confirmación mostrada puede confirmar tanto a un humano (como a un dependiente) como a una máquina (tal como un escáner QR proporcionado en la caja o en una máquina expendedora automática) que se ha verificado la edad del usuario, y que la verificación tuvo lugar recientemente y en la tienda actual. Será evidente que el dispositivo o autoridad que realiza la consulta puede establecer un tiempo umbral, tras el cual no se aceptarán confirmaciones de verificación. Por ejemplo, si la marca de tiempo es de hace más de 30 segundos, puede que no se acepte la confirmación. Del mismo modo, si la tienda o ubicación identificada no es la tienda o ubicación en donde se encuentra el cliente, la confirmación también puede ser rechazada. El propio software que se ejecuta en el dispositivo informático 200 puede limitar el tiempo de la confirmación, por ejemplo, después de un determinado umbral de tiempo, la confirmación puede ser nula y/o ilegible. Limitar la confirmación de este modo impide que un cliente utilice una confirmación obtenida en el pasado o en una tienda diferente por otra persona.

Cuando se utiliza la verificación de atributos para permitir que el usuario 201 acceda a un local o edificio, la aplicación de software que realiza la verificación de atributos puede confirmar por sí misma que el usuario 201 tiene las autorizaciones requeridas. Por ejemplo, la aplicación de software puede contener o tener acceso a una lista de personas con autorizaciones. Si durante el registro se comprueba que el usuario 201 coincide con uno de los nombres de la lista de autorizaciones, se puede almacenar una indicación de este hecho como parte de la información de atributos. En el momento de la verificación, ésta puede confirmar simplemente que el usuario 201 tiene permisos de acceso. De manera alternativa, en algunos ejemplos la verificación simplemente confirma el nombre del usuario 201 y un dispositivo de consulta, tal como una barrera de entrada, que comprueba entonces el nombre verificado del usuario con una lista de personas autorizadas.

Volviendo ahora a la Figura 6, se expone un ejemplo de otro método según la presente invención. Tal como ya se ha descrito brevemente, al almacenar los datos biométricos autenticados y los datos de atributos obtenidos del identificador ID 202 de una determinada manera, el procedimiento de verificación dado a conocer puede hacerse más versátil y eficaz en el tiempo, al permitir que múltiples aplicaciones de software accedan a la información almacenada. Lo que antecede puede ser especialmente útil cuando el dispositivo informático 200 es un dispositivo móvil, tal como un teléfono inteligente, en donde puede haber instaladas múltiples aplicaciones de software para la verificación de atributos. El método de la Figura 6, que puede considerarse una ampliación del método mostrado en la Figura 3, permite una mayor interoperabilidad entre dichas aplicaciones de software plurales.

Tal como ya se ha indicado, el bloque 307 de la Figura 3 consiste en almacenar los datos biométricos autenticados y la información de atributos localmente en la memoria del dispositivo informático 200, utilizando una primera aplicación de software. A continuación, el método de la Figura 6 garantiza, en el bloque 601, que los datos biométricos autenticados y la información de atributos almacenados en el bloque 307 sean accesibles a más de una aplicación de software, en particular que las aplicaciones distintas de la que realizó el proceso de registro de la Figura 3 puedan, con los permisos adecuados, acceder a los datos biométricos autenticados y a la información de atributos almacenados. Tal como se apreciará, la funcionalidad del bloque 601 puede incorporarse o incluirse como parte del proceso del bloque 307, es decir, no sea necesario que sean etapas separados.

En algún momento posterior, el método de la Figura 6 implica, en el bloque 603, el acceso por parte de una segunda aplicación de software a los datos biométricos autenticados y a la información de atributos almacenada en el bloque 307 y accesible en el bloque 601. Cuando los datos biométricos autenticados y la información de atributos estén encriptados o protegidos de algún modo, el bloque 603 puede implicar que se proporcione a la segunda aplicación de software una clave o contraseña adecuada para desencriptar o acceder de otro modo a los datos biométricos autenticados y a la información de atributos. Tal como ya se ha indicado, los datos biométricos autenticados y la información de atributos pueden almacenarse como un certificado, que a su vez puede estar cifrado o protegido por contraseña. En ese caso, la segunda aplicación de software tiene acceso y, si es necesario, medios para descifrar o acceder al certificado.

A continuación, en el bloque 605, la segunda aplicación de software se configura para la verificación de atributos. En un ejemplo, esto implica llevar a cabo el método de registro de la Figura 3 utilizando la segunda aplicación de software. Sin embargo, tal como la segunda aplicación de software ya tiene acceso a los datos biométricos autenticados almacenados

y a la información de atributos, se puede omitir el uso del identificador ID 202 al configurar la segunda aplicación de software. Lo que antecede simplifica y acelera de manera significativa el proceso de configuración, porque no se requiere ningún identificador ID 202 ni es necesario obtener datos por el mismo. Por último, en el bloque 607, se realiza la verificación de atributos utilizando la segunda aplicación de software. Lo que antecede puede implicar realizar, utilizando la segunda aplicación de software, el método de la Figura 4.

Por tanto, tal como puede constatarse, la configuración de la segunda aplicación de software puede agilizarse haciendo uso de los datos almacenados previamente por una primera aplicación de software. La segunda aplicación de software puede utilizarse entonces para realizar la verificación de atributos del mismo modo que la primera aplicación de software. Lo que antecede es beneficioso porque distintos establecimientos pueden tener sus propias aplicaciones de software respectivas para realizar la verificación de atributos dentro de sus establecimientos o tiendas. El método de la Figura 6 garantiza que el registro mediante un identificador ID 202 solamente tenga que realizarse una vez en todas dichas aplicaciones. Siempre que las aplicaciones de software utilizadas posteriormente puedan acceder a los datos biométricos autenticados almacenados y a la información de atributos, estas aplicaciones pueden configurarse de forma racionalizada sin necesidad del identificador ID 202 y cada una de ellas puede utilizarse posteriormente para realizar la verificación de atributos. Tal como ya se ha mencionado con anterioridad, el acceso a la información necesaria puede garantizarse, por ejemplo, asegurando que todas las aplicaciones destinadas a la verificación de atributos incluyan el mismo SDK que les permita compartir y acceder a los datos biométricos autenticados almacenados pertinentes y a la información de atributos.

Con referencia ahora a la Figura 7, se describirá un caso de uso detallado de los sistemas y métodos de la presente invención para facilitar su comprensión. Este caso de uso debe entenderse simplemente como un ejemplo destinado a mostrar, en su totalidad, cómo pueden utilizarse los sistemas y métodos dados a conocer. Muchas etapas descritas en relación con la Figura 7 pueden omitirse en otros ejemplos, y podrían añadirse etapas adicionales. Por lo tanto, la secuencia de la Figura 7 no debe interpretarse como limitativa en modo alguno ni como identificativa de características esenciales.

El proceso de ejemplo de la Figura 7 implica que un usuario 201 utilice su propio dispositivo móvil 500 para realizar una verificación de atributos en locales posteriores, con el fin de verificar tanto su edad como su identidad. El método de la Figura 7 utiliza la verificación por imagen, aunque se apreciará que el método podría utilizar igualmente otra forma de datos biométricos, tal como datos de huellas dactilares o del iris, para permitir la verificación de atributos.

El proceso comienza en el bloque 701, cuando el dispositivo móvil 500 recibe una solicitud del usuario 201 para registrarse en una primera aplicación de software que se ejecuta en el dispositivo móvil 500. La primera aplicación de software es proporcionada por un proveedor de servicios de Internet. La primera aplicación de software la proporciona un proveedor de software de verificación de atributos. En respuesta a la recepción de esta solicitud de registro, la primera aplicación de software lleva a cabo el procedimiento de registro/configuración descrito con anterioridad en relación con la Figura 3.

En particular, la primera aplicación de software solicita al usuario que obtenga los datos biométricos autenticados necesarios desde un identificador ID. En el bloque 703, el dispositivo móvil obtiene los datos biométricos autenticados, en este ejemplo una imagen autenticada del usuario 201, del identificador ID 202. El dispositivo móvil también obtiene la información de atributos del identificador ID 202. En este ejemplo, el identificador ID 202 es un pasaporte que tiene un circuito integrado NFC denominado ePassport, por lo que la imagen autenticada y la información de atributos se obtienen cuando el usuario realiza la lectura del circuito integrado NFC ePassport con un lector NFC del dispositivo móvil 500. A continuación, la primera aplicación de software pide al usuario que obtenga datos biométricos de registro, en este ejemplo una imagen de registro. Por lo tanto, en el bloque 705, la primera aplicación de software captura una primera imagen de registro del usuario 201 utilizando la cámara del dispositivo móvil 500, por ejemplo, un "selfie" utilizando la cámara frontal del dispositivo móvil 500.

En el bloque 707, se comparan la primera imagen de registro y la imagen autenticada obtenida del pasaporte 202. La primera aplicación de software confirma, mediante un análisis de marcadores faciales, que ambas imágenes representan a la misma persona, es decir, al usuario 201. En respuesta a una coincidencia satisfactoria, la primera aplicación de software incorpora la imagen autenticada y la información de atributos obtenida del pasaporte 202 en un certificado con un formato predeterminado y un tipo de archivo establecido por el SDK que utiliza la primera aplicación de software. La primera aplicación de software cifra el certificado y lo almacena localmente en la memoria del dispositivo móvil 500 en el bloque 709. En este ejemplo, la información de atributos obtenida del pasaporte 202 incluye la fecha de nacimiento, el nombre, la nacionalidad y la dirección del usuario 201. La primera aplicación de software calcula, basándose en la fecha de nacimiento y en una hora actual obtenida de un proveedor de red móvil, que el usuario 201 es mayor de 18 años. En consecuencia, también se almacena una indicación adecuada de ello como parte de la información de atributos del certificado. A continuación, la primera aplicación de software confirma, en una pantalla del dispositivo móvil 500, que el registro se ha completado de manera satisfactoria.

Más tarde, el usuario 201 entra en una tienda y desea comprar un producto asociado a restricciones de edad. En concreto, el usuario 201 debe verificar que es mayor de 18 años para comprar el producto como parte del flujo de la transacción en una máquina de caja. En consecuencia, el usuario 201 abre la primera aplicación de software y solicita la verificación del atributo de edad. En respuesta, la primera aplicación de software inicia el procedimiento de verificación descrito con anterioridad en relación con la Figura 4. En particular, la primera aplicación de software solicita al usuario 201 que capture

datos biométricos de verificación, que en este ejemplo comprenden una imagen de verificación. Se captura una primera imagen de verificación, utilizando la cámara del dispositivo móvil 500, en el bloque 711.

En el bloque 713, la primera aplicación de software accede al certificado almacenado previamente durante el registro. La primera aplicación de software tiene acceso, a través del SDK proporcionado con la primera aplicación de software por el proveedor de software de verificación de atributos, a la contraseña o clave necesaria para descifrar el certificado. Una vez que ha accedido a la imagen autenticada incluida en el certificado, la primera aplicación de software confirma, mediante un análisis de marcadores faciales, que la primera imagen de verificación que acaba de capturar representa a la misma persona que la imagen autenticada, es decir, el usuario 201. En respuesta a una coincidencia satisfactoria, la primera aplicación de software accede a la información de atributos almacenada localmente en el certificado para verificar la edad del usuario. En concreto, la primera aplicación de software confirma que la información de atributos incluye una indicación de que el usuario es mayor de 18 años.

A continuación, la primera aplicación de software indica al usuario 201 que escanee un código QR presente en la máquina de caja de la tienda. El código QR proporciona información espaciotemporal sobre la hora y la ubicación actuales. Una vez realizada la lectura del código QR, la primera aplicación de software presenta, en el bloque 715, la confirmación de que el usuario es mayor de 18 años en una pantalla del dispositivo móvil 500. La confirmación se parece a la mostrada en la Figura 5 y descrita con anterioridad. La confirmación incluye un indicador visual de que el usuario es mayor de 18 años, que puede presentarse a un dependiente de la tienda. La confirmación también incluye la información espaciotemporal obtenida del código QR en la caja. En concreto, la confirmación incluye una indicación de la hora y de la fecha actuales proporcionadas por el código QR, así como la ubicación y la marca de la tienda. Esta información espaciotemporal y la confirmación de verificación de atributos también están incorporadas en un código QR dinámico presentado en la pantalla del dispositivo móvil 500 como parte de la confirmación. El empleado de la tienda o, en una forma de realización alternativa, un escáner de una máquina de autopago, escanea el código QR en la pantalla del dispositivo móvil para confirmar, de forma legible por máquina, que el usuario 201 es mayor de 18 años y que los datos espaciotemporales coinciden con la hora y la ubicación previstas. Si la confirmación es correcta, la transacción se completa y el usuario 201 puede comprar el producto restringido.

A continuación, el usuario desea entrar en otro local. El acceso a este local está restringido a un subconjunto específico de personas, que deben verificar su identidad utilizando una segunda aplicación de software proporcionada para la verificación de atributos.

En consecuencia, el usuario 201 descarga la segunda aplicación de software en el dispositivo móvil 500. A continuación, el usuario inicia la configuración de la segunda aplicación de software para la verificación de atributos, de forma que la segunda aplicación de software recibe una solicitud para registrar al usuario 201, en el bloque 717. Lo que antecede inicia el proceso de registro habitual descrito con anterioridad, esta vez en la segunda aplicación de software. Es importante destacar que la configuración de la segunda aplicación de software no requiere que la segunda aplicación de software acceda a ninguna información del pasaporte 202 del usuario ni a ningún otro identificador ID. Lo que antecede se debe a que la segunda aplicación de software también incluye el SDK proporcionado por el proveedor de software de verificación de atributos. En consecuencia, la segunda aplicación de software también puede acceder y descifrar el certificado almacenado previamente en la memoria local del dispositivo móvil 500 por la primera aplicación de software. Al hacerlo, la segunda aplicación de software obtiene los datos biométricos autenticados (en este ejemplo la imagen autenticada, es decir, la foto del pasaporte) y la información de atributos en el bloque 719. Como es habitual, la segunda aplicación de software solicita entonces al usuario que capture los datos biométricos de registro, que en este ejemplo comprenden una imagen de registro. Este segundo registro se captura, utilizando la cámara del dispositivo móvil 500, en el bloque 721. Como es habitual, la segunda aplicación de software procede a confirmar que la segunda imagen de registro y la imagen autenticada representan a la misma persona, en el bloque 723. En respuesta a una coincidencia satisfactoria, la segunda aplicación de software confirma, en una pantalla del dispositivo móvil 500, que el registro se ha completado de manera satisfactoria.

A continuación, el usuario 201 llega al local y un empleado o una barrera automatizada le solicita que verifique su nombre para cotejarlo con una lista de personas con permiso de acceso al local. En consecuencia, el usuario 201 abre la segunda aplicación de software y solicita la verificación del atributo del nombre. En respuesta, la segunda aplicación de software inicia el procedimiento de verificación descrito con anterioridad en relación con la Figura 4. En concreto, la segunda aplicación de software captura una segunda imagen de verificación, en el bloque 725, y confirma que esta imagen coincide con la imagen autenticada en el bloque 727. Si la coincidencia es correcta, la segunda aplicación de software muestra la confirmación del nombre del usuario en la pantalla móvil en el bloque 729, de forma similar a la descrita con anterioridad. Al escanear la confirmación, la barrera de entrada determina que el usuario tiene los permisos de acceso necesarios y permite al usuario 201 entrar en el recinto.

Como puede constatarse, los sistemas y métodos dados a conocer permiten una verificación de atributos de usuario sencilla, segura y fiable. Un usuario puede hacer uso de una o más aplicaciones de software en el mismo dispositivo informático y puede configurarlas con facilidad, solamente necesitando proporcionar un identificador ID durante el primer registro. Lo que antecede permite una interoperabilidad fluida y sin fricciones entre múltiples aplicaciones para la verificación de atributos. Se pueden verificar varios atributos, tales como la edad y la identidad. No se requiere conexión de red para la verificación, y no es necesario transmitir ninguna información PII sensible a ninguna red o servidor remoto. La incorporación de información espaciotemporal a la confirmación de atributos y/o el uso de procesos antifalsificación

durante la verificación de imágenes pueden garantizar aún más que la verificación de atributos sea segura y que el sistema no pueda ser con facilidad falsificado, lo que proporciona más ventajas técnicas. Estas ventajas las proporciona el sistema dado a conocer con independencia de los datos que se procesen, es decir, con independencia del atributo específico que se verifique. Los métodos y sistemas dados a conocer abordan de este modo varias deficiencias técnicas de los sistemas de la técnica anterior.

Variantes

La descripción detallada que antecede da a conocer diversos sistemas y métodos a modo de ejemplo para la verificación de atributos. Sin embargo, las disposiciones y métodos descritos son meramente a modo de ejemplo, y un experto en esta técnica apreciará que pueden realizarse diversas modificaciones sin desviarse por ello del alcance de las reivindicaciones adjuntas. A continuación se describirán brevemente algunas de estas modificaciones, aunque esta lista de modificaciones no debe considerarse exhaustiva, y otras modificaciones serán evidentes para un experto en esta técnica.

Los diagramas de flujo utilizados en esta invención, concretamente en las Figuras 3, 4, 6 y 7, implican cada uno una secuencia específica de eventos, indicada por las flechas que conducen desde un bloque al siguiente. Sin embargo, cada una de estas figuras representa solamente un ejemplo de puesta en práctica, y en otras puestas en práctica la secuencia de bloques puede cambiar. Por lo tanto, la secuencia mostrada en las Figuras 3, 4, 6 y 7 no debe interpretarse como el único orden posible de las etapas. Al contrario, por poner solamente algunos ejemplos: en algunas formas de realización, el bloque 303 puede preceder al bloque 301; en algunas formas de realización, el bloque 307 puede preceder al bloque 305 y los datos pueden borrarse si la respuesta al bloque 305 es "no"; en algunas formas de realización, el bloque 603 puede preceder o desencadenar el bloque 601; y en algunas formas de realización, el bloque 605 puede preceder o incluir al bloque 603 y/o al bloque 601. A menos que se indique explícitamente que una etapa concreta debe preceder a otra, debe suponerse que es posible cualquier orden de las etapas.

Tal como se ha indicado con anterioridad, puede incorporarse al certificado o a los datos de verificación almacenados, de algún modo, un identificador ID único del dispositivo informático en donde se realiza el registro, para garantizar que la verificación solamente pueda realizarse posteriormente en dicho dispositivo informático. En algunos ejemplos, el identificador ID único se obtiene del identificador del circuito integrado del dispositivo informático, que puede ser un número de serie o un identificador ID único proporcionado al dispositivo informático en el momento de su fabricación.

Tal como ya se ha mencionado, la(s) aplicación(es) de software proporcionada(s) al dispositivo informático para la verificación de atributos puede(n) incluir un SDK concreto, o un subconjunto de activos SDK. El SDK puede ser proporcionado por un proveedor de software de verificación de atributos a terceros e integrarse en aplicaciones de software de terceros, por ejemplo, aplicaciones asociadas a establecimientos o locales comerciales. El SDK puede establecer los criterios de edad mínima o contener una lista de nombres de personas certificadas. El SDK puede ayudar a la aplicación de software a almacenar y/o encriptar los datos biométricos autenticados almacenados y la información de atributos, por ejemplo, tal como un certificado. Posteriormente, el SDK puede proporcionar o permitir el acceso a una clave privada para acceder a los datos encriptados con una aplicación de software diferente que también incluya el SDK, o un subconjunto de los activos del SDK.

En algunos ejemplos, los datos seudonimizados o anonimizados pueden enviarse a un proveedor de software de verificación de atributos que haya proporcionado la aplicación de software de verificación y/o el SDK, para permitir la recopilación de datos de verificación anónimos. Lo que antecede puede permitir que el proveedor de software de verificación de atributos identifique patrones y tendencias que permitan actualizar o mejorar la(s) aplicación(es) de software y/o el SDK. En algunos ejemplos, los datos anonimizados transmitidos pueden incluir datos espaciotemporales, por ejemplo, datos del lugar en donde tuvo lugar la verificación de atributos, y proporcionar de este modo una forma de registro de auditoría de cada verificación individual realizada por el usuario. Lo que antecede puede ayudar en la prevención del fraude al proporcionar un registro verificado y rastreable de las transacciones. El envío de estos datos anonimizados puede realizarse después de la verificación, una vez que la conectividad de red esté disponible. Por ejemplo, los datos pueden almacenarse en una memoria intermedia local del dispositivo informático y transmitirse posteriormente. En algunos casos, se puede pedir al usuario que elija si desea, o no, compartir sus datos con el proveedor de software de verificación de atributos. En algunas puestas en práctica, también se puede pedir al usuario que confirme si permite que el establecimiento (por ejemplo, el minorista) en donde se ha producido la verificación de atributos acceda a determinados datos sobre la verificación y/o la transacción. El establecimiento puede obtener esta información escaneando una confirmación de la verificación mostrada en el dispositivo informático.

La verificación puede formar parte de un proceso total o parcialmente automatizado. En algunos ejemplos en los que el dispositivo informático que realiza la verificación es un dispositivo móvil de un usuario, un dispositivo de consulta (que puede funcionar de forma autónoma o bajo el control del u otro usuario) puede tener su propia aplicación complementaria proporcionada por el mismo proveedor de software de verificación de atributos que la aplicación de verificación del dispositivo móvil del usuario y/o que contenga parte o la totalidad del mismo SDK. Lo que antecede puede permitir a esta aplicación complementaria interactuar con la aplicación de software del dispositivo del usuario e interrogarla.

En un ejemplo, la confirmación de la verificación puede presentarse a un humano, tal como un cajero de una tienda, en cuyo caso la confirmación de la verificación puede incluir elementos legibles por humanos. Además, el humano escanea

o realiza la lectura de una parte legible por máquina de la confirmación de verificación, tal como un código QR dinámico, utilizando un hardware adecuado, tal como un escáner QR. En un caso de uso de este tipo, el método dado a conocer puede utilizarse en el contexto de la entrega a domicilio. Un repartidor puede entregar un paquete a un cliente y realizar una verificación de atributos para asegurarse de que el cliente es el destinatario correcto y/o tiene la edad mínima requerida para recibir el paquete en cuestión. En ese caso, el repartidor puede tener su propio dispositivo informático configurado para escanear una confirmación de verificación presentada por el destinatario en su propio dispositivo de usuario, de la manera comentada con anterioridad.

En una puesta en práctica alternativa, no está presente ningún asistente humano y la confirmación de verificación puede presentarse simplemente a una interfaz de máquina, tal como un escáner QR en una máquina de autopago o en una máquina expendedora automática. De este modo, la verificación de atributos puede estar totalmente automatizada. En un ejemplo particular, en una tienda en donde está habilitada la compra sin pasar por caja, el usuario puede descargar una aplicación host asociada con la tienda. La aplicación host puede entonces comunicarse con la aplicación de verificación de atributos en el dispositivo del usuario para confirmar la verificación de atributos. Por ejemplo, el usuario puede confirmar que es mayor de una edad mínima de la forma habitual, y la confirmación de ello puede transmitirse a la aplicación host asociada con la tienda. Como resultado, se puede permitir al usuario salir de la tienda con un artículo que tenga una edad mínima asociada sin pasar por caja. En una puesta en práctica alternativa, la confirmación de la verificación se presenta o transmite a una máquina expendedora automática. Al recibir esta confirmación, la máquina expendedora automática puede entregar al usuario un artículo, por ejemplo, un artículo de edad restringida. Lo que antecede resuelve un inconveniente del sistema existente, que consiste en que los artículos restringidos por edad no pueden venderse de forma segura a través de máquinas expendedoras.

En algunos ejemplos, la confirmación de la verificación de la edad puede comprender un certificado de prueba digital de edad, DPoA. En algunas puestas en práctica, este certificado sigue los estándares conocidos PASS 5 DPoA. Lo que antecede puede permitir una integración perfecta de los mecanismos de verificación de la edad dados a conocer en los procedimientos existentes ya utilizados en tiendas y establecimientos para la prueba de la edad.

En el ejemplo de uso descrito en relación con la Figura 7, cada establecimiento descrito tiene su propia aplicación de verificación asociada. En otros ejemplos, puede ser posible utilizar una aplicación de verificación asociada con un primer establecimiento o empresa para verificar atributos en un segundo establecimiento o empresa. En algunos ejemplos, una única aplicación puede funcionar para algunos o para la totalidad de los establecimientos.

En algunos ejemplos, la verificación puede activarse mediante una notificación de exigencia. Por ejemplo, un usuario puede escanear un elemento de verificación de atributos en una caja, tal como un código QR. Lo que antecede puede hacer que la aplicación de verificación comience la verificación de atributos.

En algunos ejemplos, la verificación puede estar limitada en el tiempo. Por ejemplo, después de un umbral de tiempo predeterminado, la verificación puede dejar de ser válida o utilizable y/o la aplicación de software puede pedir al usuario que vuelva a verificarse capturando nuevos datos biométricos de verificación. El umbral de tiempo puede ser, por ejemplo, de 10 segundos, 20 segundos, 30 segundos, 40 segundos, 50 segundos, 60 segundos, 2 minutos, 5 minutos, 10 minutos o una hora. Cada uno de estos umbrales de tiempo proporcionaría al menos cierta protección contra la suplantación de identidad.

Se apreciará que la confirmación de verificación mostrada en la Figura 5 es meramente un ejemplo. Algunos elementos pueden omitirse o añadirse a la confirmación mostrada. Por ejemplo, la confirmación puede incluir más o menos elementos de datos legibles por humanos. En una puesta en práctica, la confirmación incluye los datos biométricos autenticados del usuario y/o los datos biométricos de registro del usuario y/o los datos biométricos de verificación del usuario.

Aunque la descripción que antecede se ha centrado en la verificación de atributos del usuario, tal como la edad y la identidad, en el contexto de una tienda o local, se apreciará que pueden existir otros casos de uso. Por ejemplo, la funcionalidad descrita puede utilizarse para permitir el acceso a un dispositivo tal como un ordenador personal, o a sitios web de venta online o restringidos por edad en dicho ordenador. Los sistemas dados a conocer pueden permitir el acceso al domicilio de una persona y, de este modo, proporcionar una funcionalidad de seguridad doméstica. Los sistemas dados a conocer pueden utilizarse en el contexto de la entrega a domicilio para demostrar la identidad de un destinatario de un paquete. Los sistemas dados a conocer pueden utilizarse en el contexto de una máquina expendedora automática.

Por último, aunque la descripción anterior se ha centrado en el uso de datos biométricos tales como imágenes (en particular imágenes faciales), huellas dactilares y datos del iris, será evidente que cualquier dato biométrico adecuado que permita identificar a un usuario puede utilizarse en el contexto de los métodos dados a conocer. Se puede comprobar más de un aspecto biométrico en el mismo procedimiento de verificación o registro. La verificación puede implicar la comprobación de más de un atributo asociado con el usuario, por ejemplo, tanto la edad como el nombre.

Sistema informático

Volviendo por último a la Figura 8, la Figura 8 muestra una representación esquemática y simplificada de un aparato informático o dispositivo informático 800 que puede utilizarse para realizar los métodos aquí descritos. Por ejemplo, el dispositivo informático 800 puede ser el dispositivo de usuario 200, 500 y/o un dispositivo de consulta tal como se ha descrito con anterioridad. El dispositivo informático 800 puede ser un dispositivo informático móvil, tal como un teléfono

móvil o un teléfono inteligente. El dispositivo informático 800 puede ser, de manera alternativa, un terminal o dispositivo de caja proporcionado en una tienda o local.

El aparato informático 800 comprende diversos recursos de procesamiento de datos, tal como un procesador 802 (en particular, un procesador de hardware) acoplado a una estructura de bus central. También están conectados a la estructura de bus otros recursos de procesamiento de datos, tal como la memoria 804. Un adaptador de pantalla 806 conecta un dispositivo de visualización 808 a la estructura de bus. Uno o más adaptadores de dispositivos de entrada de usuario 810 conectan un dispositivo de entrada de usuario 812, tal como un teclado y/o un ratón, a la estructura de bus. En algunos ejemplos, el dispositivo de entrada de usuario 812 forma parte del dispositivo de visualización 808, tal como cuando un teléfono inteligente está provisto de una pantalla táctil. Uno o más adaptadores de comunicaciones 814 también están conectados a la estructura de bus para proporcionar conexiones a otros sistemas informáticos 800 y a otras redes.

En funcionamiento, el procesador 802 del sistema informático 800 ejecuta un programa informático que comprende instrucciones ejecutables por ordenador que pueden almacenarse en la memoria 804. Cuando se ejecutan, las instrucciones ejecutables por ordenador pueden hacer que el sistema informático 800 realice uno o varios de los métodos descritos en este documento. Cuando se ejecutan, las instrucciones ejecutables por ordenador pueden hacer que el sistema informático 800 realice uno o varios de los métodos descritos en el presente documento. Los resultados del procesamiento realizado pueden mostrarse a un usuario a través del adaptador de pantalla 806 y el dispositivo de visualización 808. Las entradas del usuario para controlar el funcionamiento del sistema informático 800 pueden recibirse a través de los adaptadores de dispositivos de entrada de usuario 810 desde los dispositivos de entrada de usuario 812.

Será evidente que algunas características del sistema informático 800 mostrado en la Figura 8 pueden estar ausentes en ciertos casos. Por ejemplo, uno o más de entre la pluralidad de aparatos informáticos 800 pueden no necesitar el adaptador de pantalla 806 ni el dispositivo de visualización 808. Este puede ser el caso, por ejemplo, de determinados aparatos informáticos 800 del lado del servidor que solamente se utilizan por sus capacidades de procesamiento y no necesitan mostrar información a los usuarios. Del mismo modo, el adaptador del dispositivo de entrada de usuario 810 y el dispositivo de entrada de usuario 812 pueden no ser necesarios. En su forma más simple, el aparato informático 800 comprende el procesador 802 y la memoria 804.

Aunque se han descrito varias combinaciones específicas de componentes y etapas del método, se trata de meros ejemplos. Los componentes y las etapas del método pueden combinarse en cualquier disposición o combinación adecuada. También pueden omitirse componentes y etapas del método para dejar cualquier combinación adecuada de componentes o etapas del método.

Los métodos descritos pueden ponerse en práctica mediante instrucciones ejecutables por ordenador. Un producto de programa informático o un medio legible por ordenador puede contener o almacenar las instrucciones ejecutables por ordenador. El producto de programa informático o medio legible por ordenador puede comprender una unidad de disco duro, una memoria instantánea, una memoria de solamente lectura (ROM), un CD, un DVD, una memoria caché, una memoria de acceso aleatorio (RAM) y/o cualquier otro medio de almacenamiento en donde se almacene información durante cualquier periodo de tiempo (por ejemplo, durante periodos de tiempo prolongados, de forma permanente, breves instancias, para almacenamiento temporal y/o para almacenamiento en memoria caché de la información). Un programa informático puede comprender las instrucciones ejecutables por ordenador. El medio legible por ordenador puede ser un medio legible por ordenador tangible o no transitorio. El término "legible por ordenador" engloba "legible por máquina".

Los términos singulares "uno" y "una" no deben entenderse como "uno y solamente uno". Por el contrario, deben entenderse como "al menos uno" o "uno o más", a menos que se indique lo contrario. La palabra "que comprende" y sus derivados, incluidos "comprende" y "comprenden", incluyen cada una de las características indicadas, pero no excluyen la inclusión de una o más características adicionales.

Las puestas en práctica que anteceden se han descrito solamente a modo de ejemplo, y las puestas en práctica descritas deben considerarse en todos los aspectos solamente ilustrativas y no restrictivas. El alcance de la invención queda definido por las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un método puesto en práctica por ordenador para verificar localmente un atributo asociado con un usuario, comprendiendo el método la realización, mediante un dispositivo informático (200), de etapas que incluyen:

capturar (401) datos biométricos de verificación mediante el dispositivo informático;

determinar (403) si los datos biométricos de verificación corresponden al usuario comparando los datos biométricos de verificación con datos biométricos autenticados del usuario obtenidos previamente desde un identificador ID, y almacenados localmente en el dispositivo informático;

en respuesta a la determinación de que los datos biométricos de verificación corresponden al usuario, verificar (405) el atributo asociado con el usuario basándose en la información de atributos asociada con el usuario obtenida previamente del identificador ID y almacenada localmente en el dispositivo informático; y

presentar (715, 729), en una pantalla del dispositivo informático, una confirmación legible por máquina del atributo verificado asociado con el usuario.

2. El método puesto en práctica por ordenador según la reivindicación 1, en donde:

los datos biométricos de verificación comprenden una imagen de verificación capturada mediante una cámara del dispositivo informático y en donde los datos biométricos autenticados comprenden una imagen autenticada del usuario; y/o

los datos biométricos de verificación comprenden una huella dactilar de verificación capturada mediante un escáner de huellas dactilares del dispositivo informático y en donde los datos biométricos autenticados comprenden una huella dactilar autenticada del usuario.

3. El método puesto en práctica por ordenador según cualquier reivindicación anterior, en donde el atributo asociado con el usuario se verifica sin requerir la transmisión de Información de Identificación Personal, PII, desde el dispositivo informático.

4. El método puesto en práctica por ordenador según cualquier reivindicación anterior, en donde la verificación (405) del atributo asociado con el usuario comprende el acceso a un certificado almacenado localmente en el dispositivo informático, comprendiendo dicho certificado la información del atributo asociado con el usuario.

5. El método puesto en práctica por ordenador según cualquier reivindicación anterior, en donde la confirmación comprende un código QR.

6. El método puesto en práctica por ordenador según cualquier reivindicación anterior, en donde la confirmación está limitada en el tiempo.

7. El método puesto en práctica por ordenador según cualquier reivindicación anterior, en donde proporcionar la confirmación comprende transmitir un mensaje que confirma el atributo verificado asociado con el usuario.

8. El método puesto en práctica por ordenador según cualquier reivindicación anterior, en donde las etapas incluyen, además:

obtener información espaciotemporal asociada con la verificación del atributo asociado con el usuario; e

integrar la información espaciotemporal obtenida en la confirmación del atributo verificado.

9. El método puesto en práctica por ordenador según la reivindicación 8, en donde la información espaciotemporal comprende información relativa a uno o más de entre:

una fecha actual;

una hora actual;

una ubicación actual; y

una identidad de un establecimiento en donde se está llevando a cabo la verificación del atributo asociado con el usuario.

10. El método puesto en práctica por ordenador según la reivindicación 8 o 9, en donde el dispositivo informático (200) comprende un dispositivo informático móvil y en donde la obtención de la información espaciotemporal comprende el escaneo, mediante una cámara del dispositivo informático móvil, de un indicador visual o elemento de memoria proporcionado en la ubicación en donde tiene lugar la verificación.

11. El método puesto en práctica por ordenador según cualquier reivindicación anterior, en donde las etapas incluyen, además, antes de capturar los datos biométricos de verificación:

obtener (301), a partir del identificador ID, los datos biométricos autenticados del usuario y la información de atributos asociada con el usuario;

capturar (303) los datos biométricos de registro mediante el dispositivo informático;

determinar (305) si los datos biométricos de registro corresponden al usuario comparando los datos biométricos de registro con los datos biométricos autenticados; y

en respuesta a la determinación de que los datos biométricos de registro corresponden al usuario, almacenar (307) localmente en el dispositivo informático:

a) los datos biométricos autenticados del usuario; y

b) la información de atributos asociada con el usuario.

12. El método puesto en práctica por ordenador según la reivindicación 11, en donde la obtención (301) de los datos biométricos autenticados del usuario y/o de la información de atributos asociada con el usuario comprende:

capturar una imagen del identificador ID, utilizando una cámara del dispositivo informático; y/o

interrogar una memoria del identificador ID.

13. Un dispositivo informático (200) configurado para realizar el método según cualquier reivindicación anterior; o

un medio legible por ordenador que comprenda instrucciones que, al ser ejecutadas por un procesador de un dispositivo informático, hagan que el dispositivo informático realice el método según cualquier reivindicación anterior; o bien

un programa informático que contenga instrucciones que, al ser ejecutadas por un dispositivo informático, hagan que dicho dispositivo realice el método según cualquier reivindicación anterior.

14. Un sistema que comprende:

un dispositivo informático (200) configurado para realizar el método según cualquiera de las reivindicaciones 1 a 12, para la verificación de un atributo asociado con un usuario; y

un dispositivo de consulta (108) configurado para efectuar la lectura de la confirmación legible por máquina del atributo verificado asociado con el usuario presentado en la pantalla del dispositivo informático.

15. Un sistema que comprende:

un programa informático que comprende instrucciones que, cuando el programa es ejecutado por un dispositivo informático (200), hacen que el dispositivo informático realice el método según cualquiera de las reivindicaciones 1 a 12; y

un programa informático que comprende instrucciones que, cuando el programa es ejecutado por un dispositivo de consulta (108), configura el dispositivo de consulta para que efectúe la lectura de la confirmación legible por máquina del atributo verificado asociado con el usuario presentado en la pantalla del dispositivo informático.

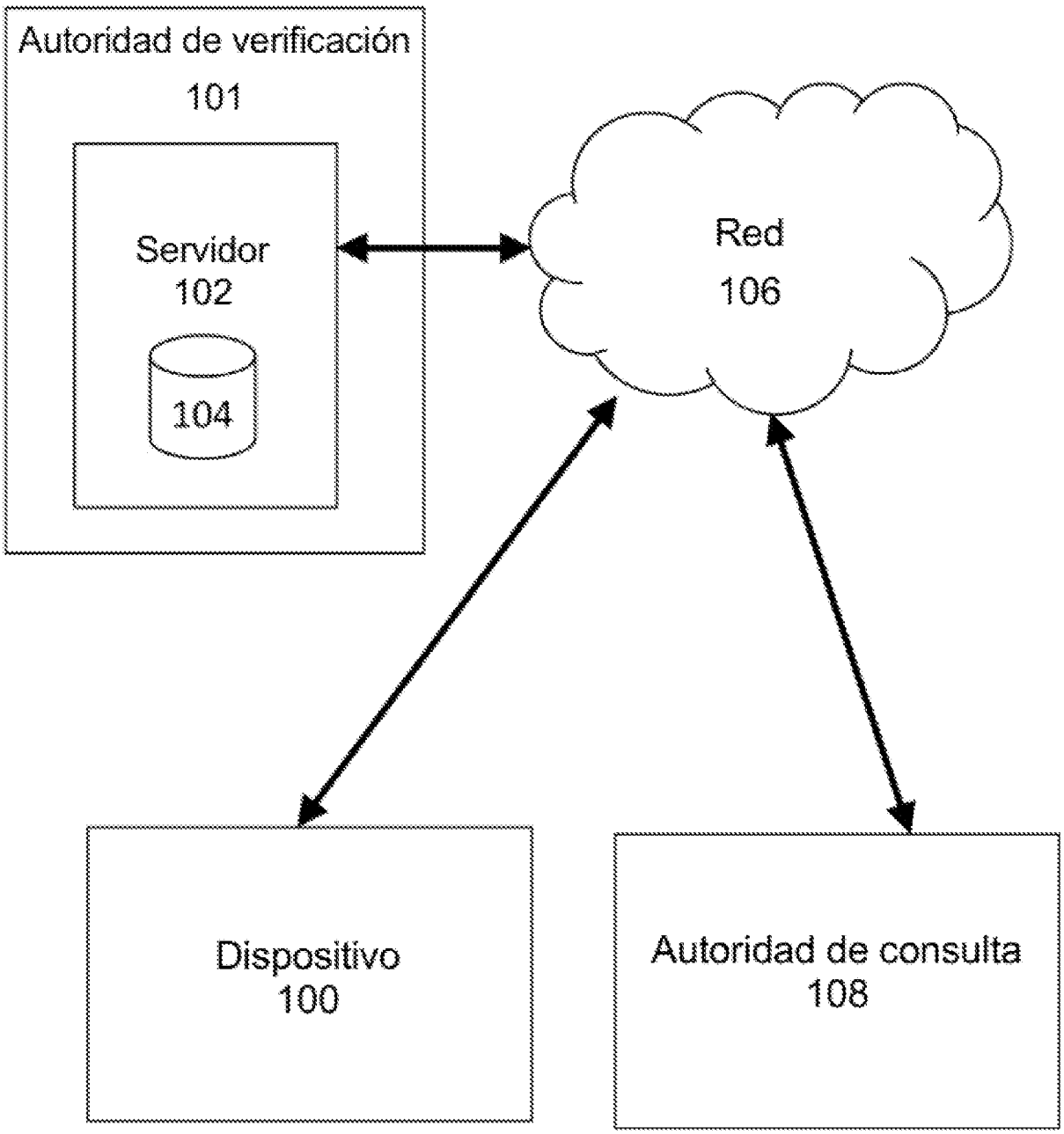

Fig 1

Técnica anterior

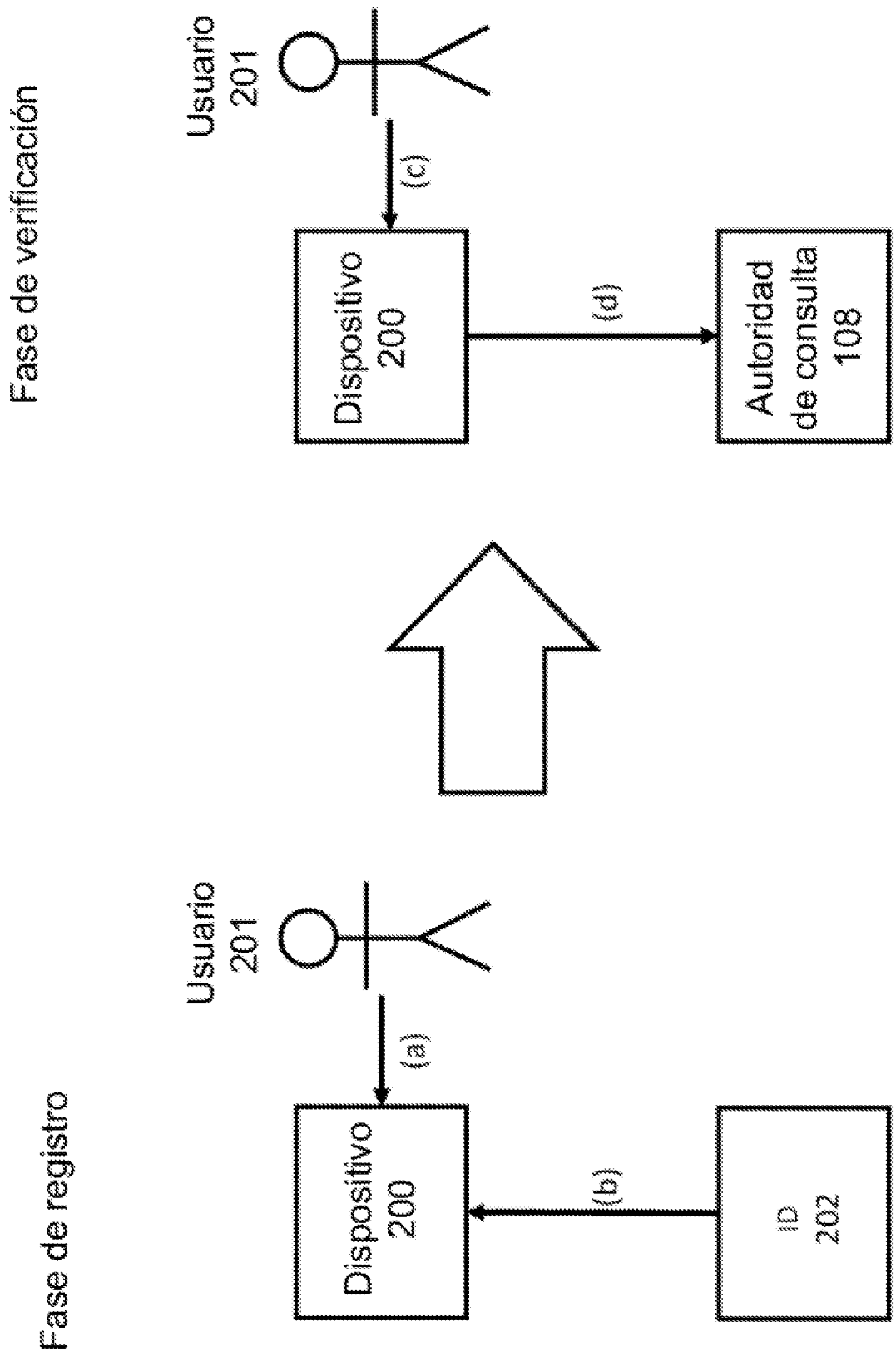
Fase de verificación
Usuario
201
(c)
Dispositivo
200
(d)
Autoridad
de consulta
108
Fase de registro
Usuario
201
(a)
Dispositivo
200
(b)
ID
202

Fig 2

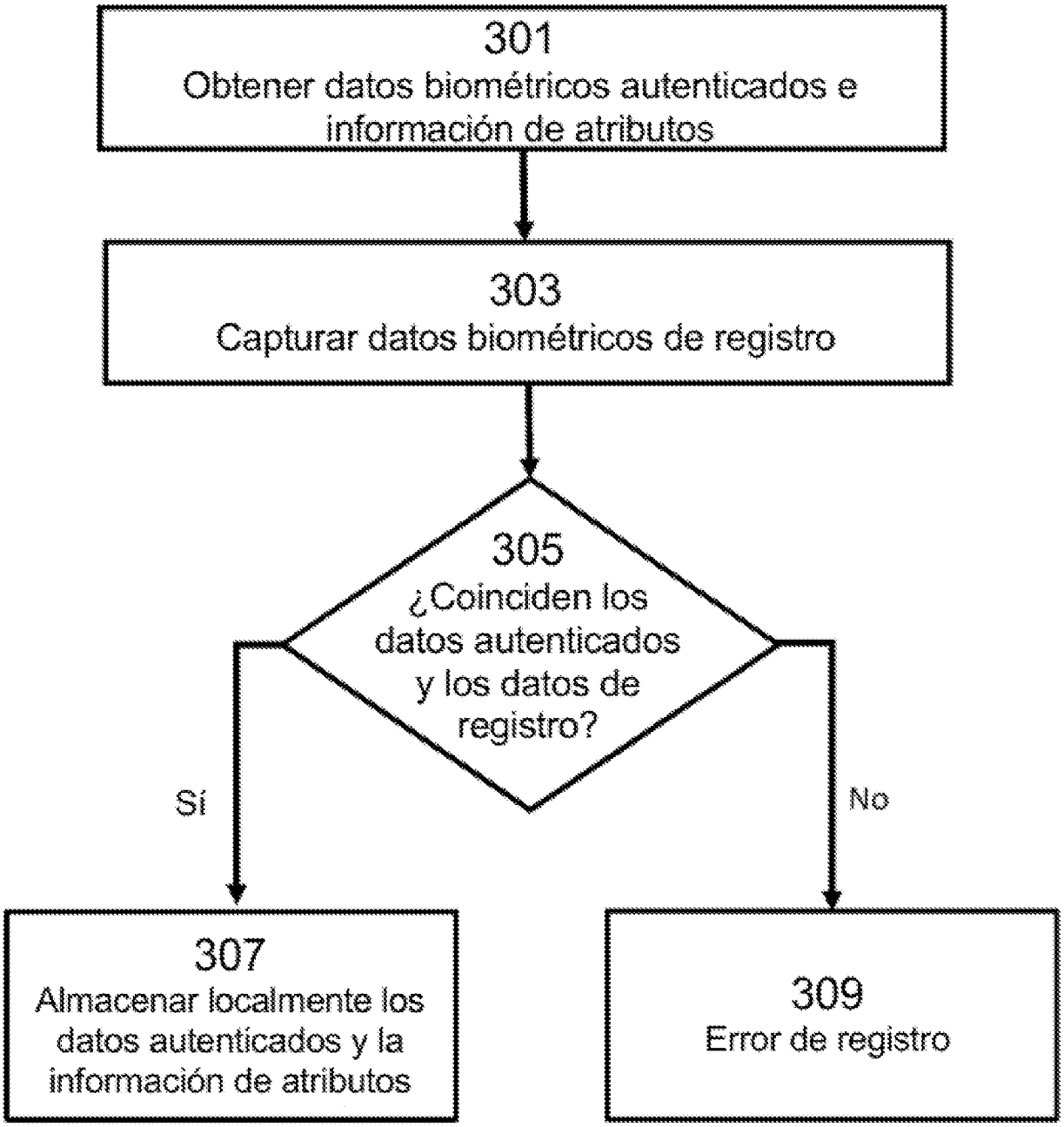
301
Obtener datos biométricos autenticados e información de atributos
303
Capturar datos biométricos de registro
305
¿Coinciden los datos autenticados y los datos de registro?
Sí
No
307
Almacenar localmente los datos autenticados y la información de atributos
309
Error de registro

Fig 3

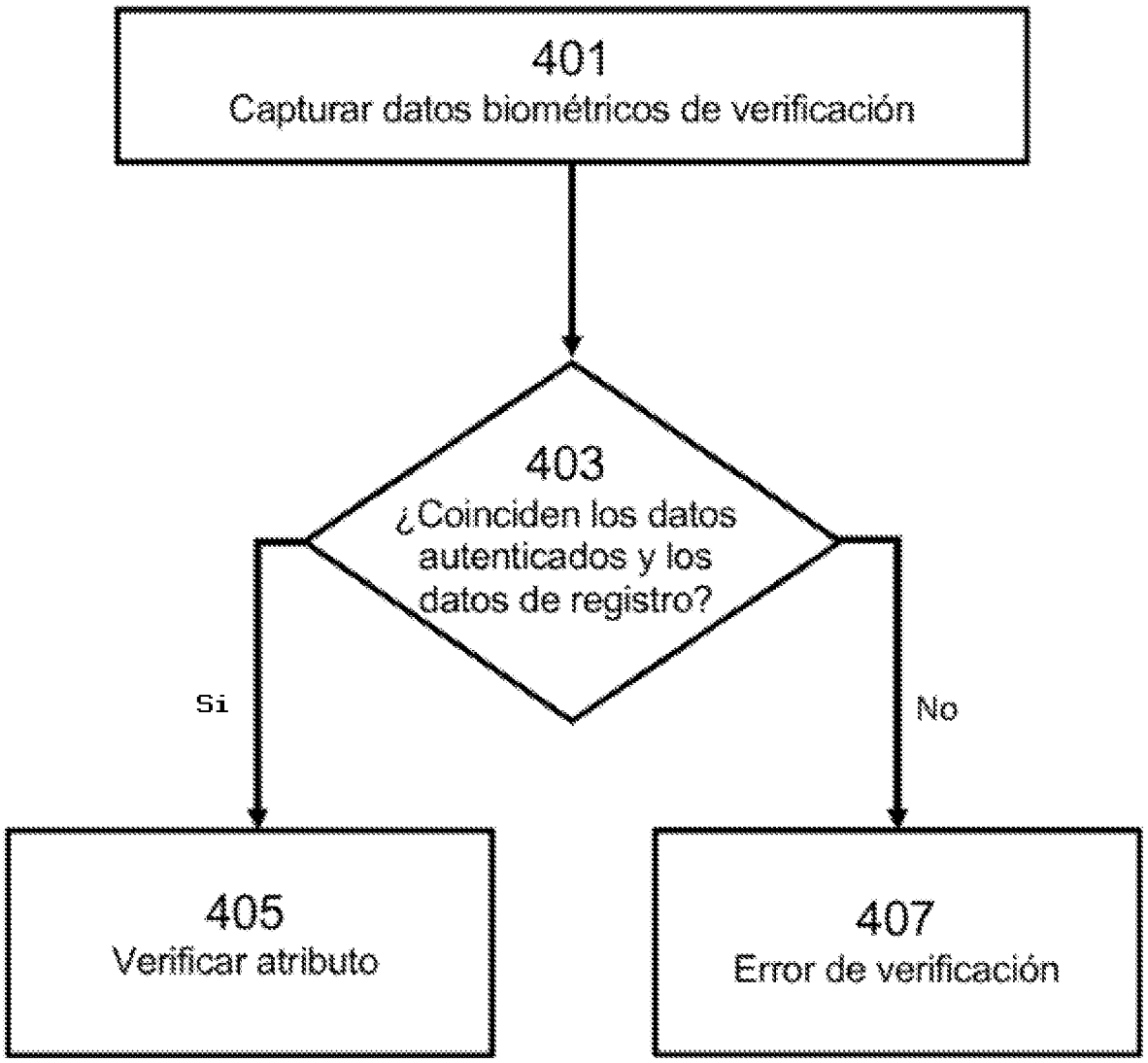
401
Capturar datos biométricos de verificación
403
¿Coinciden los datos autenticados y los datos de registro?
Si
No
405
Verificar atributo
407
Error de verificación

Fig 4

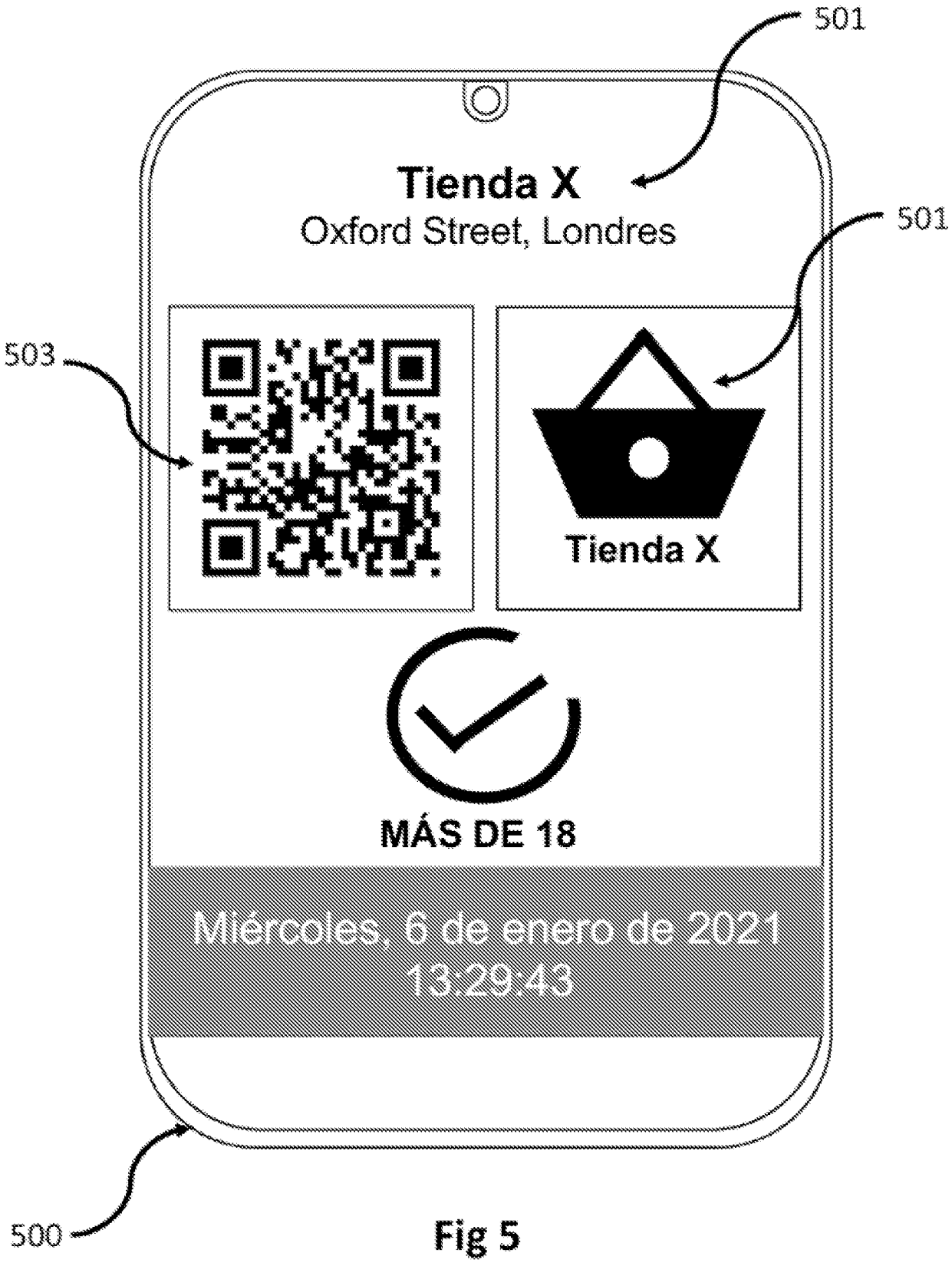
501
Tienda X
Oxford Street, Londres
501
503
Tienda X
MÁS DE 18
Miércoles, 6 de enero de 2021
13:29:43
500

Fig 5

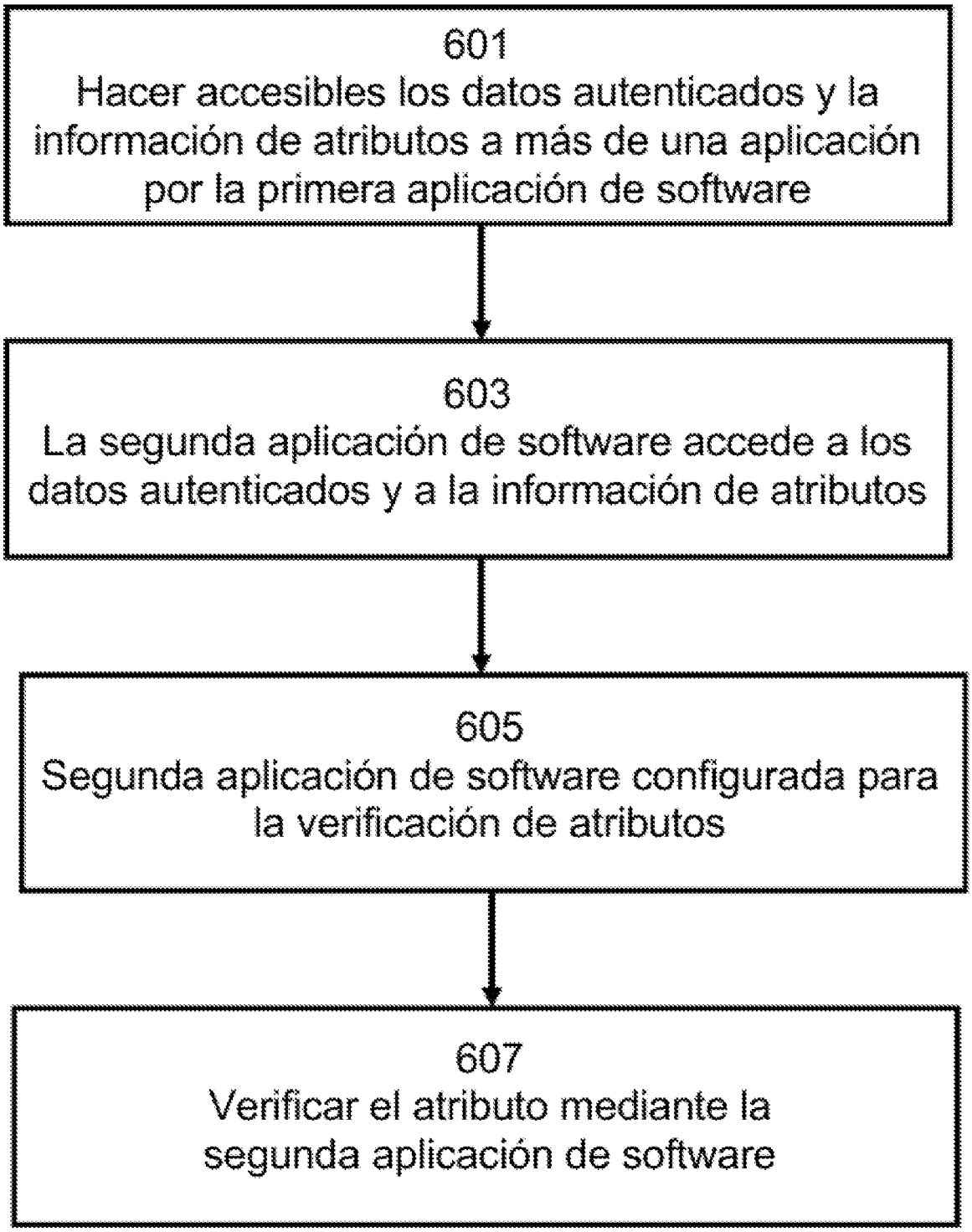
601
Hacer accesibles los datos autenticados y la información de atributos a más de una aplicación por la primera aplicación de software
603
La segunda aplicación de software accede a los datos autenticados y a la información de atributos
605
Segunda aplicación de software configurada para la verificación de atributos
607
Verificar el atributo mediante la segunda aplicación de software

Fig 6

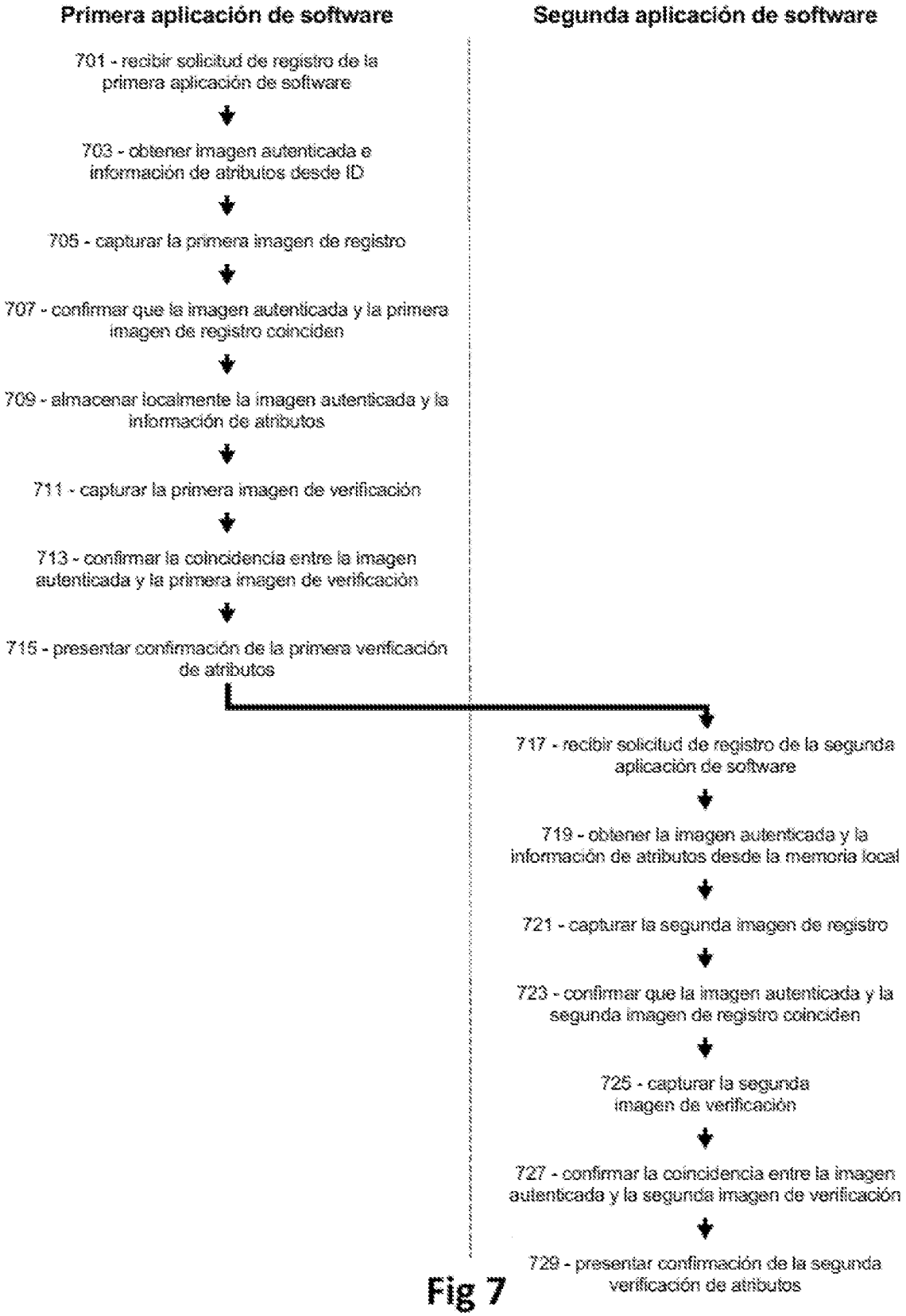
Primera aplicación de software
Segunda aplicación de software
701 - recibir solicitud de registro de la primera aplicación de software
703 - obtener imagen autenticada e información de atributos desde ID
705 - capturar la primera imagen de registro
707 - confirmar que la imagen autenticada y la primera imagen de registro coinciden
709 - almacenar localmente la imagen autenticada y la información de atributos
711 - capturar la primera imagen de verificación
713 - confirmar la coincidencia entre la imagen autenticada y la primera imagen de verificación
715 - presentar confirmación de la primera verificación de atributos
717 - recibir solicitud de registro de la segunda aplicación de software
719 - obtener la imagen autenticada y la información de atributos desde la memoria local
721 - capturar la segunda imagen de registro
723 - confirmar que la imagen autenticada y la segunda imagen de registro coinciden
725 - capturar la segunda imagen de verificación
727 - confirmar la coincidencia entre la imagen autenticada y la segunda imagen de verificación
729 - presentar confirmación de la segunda verificación de atributos

Fig 7

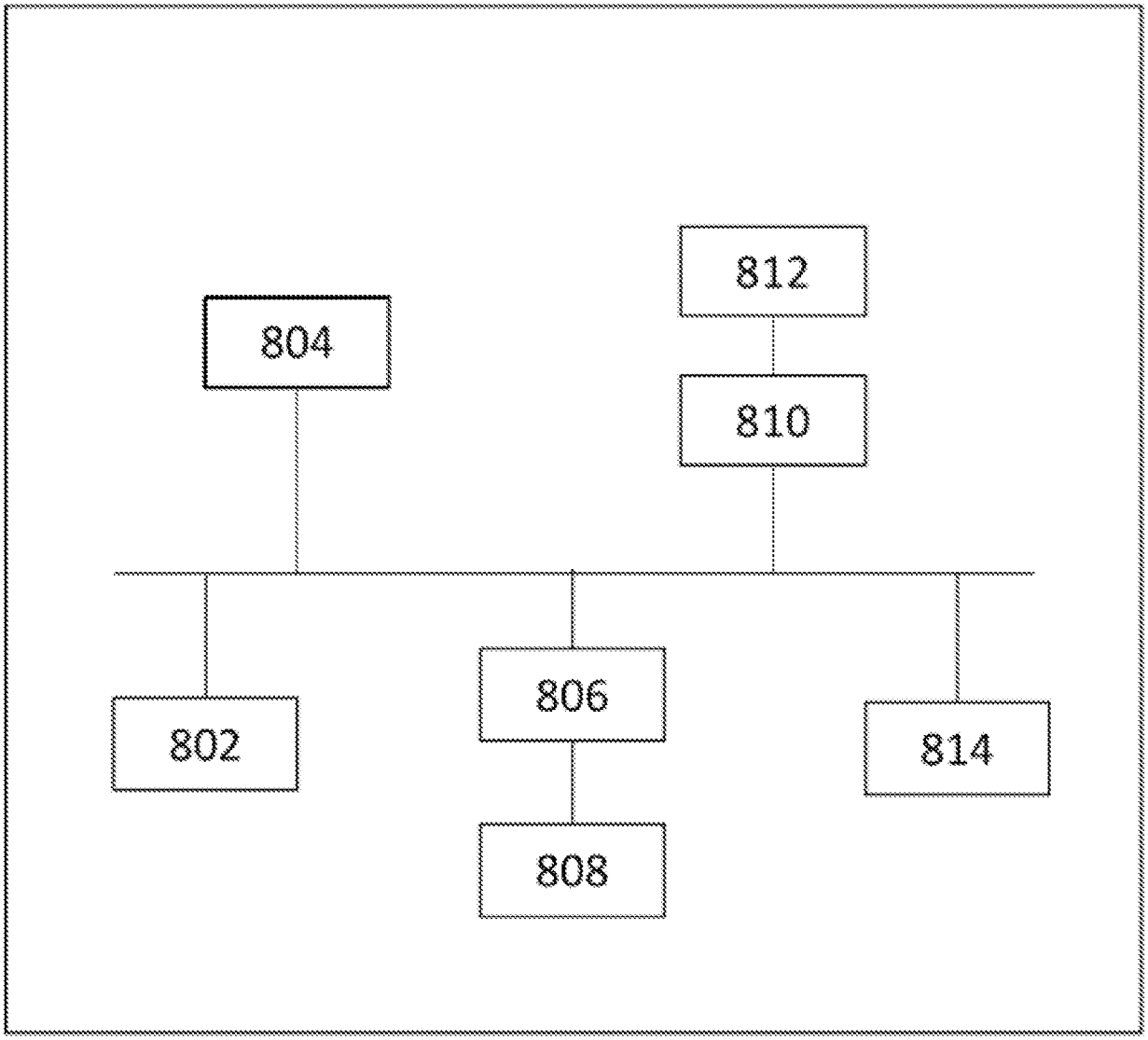

Fig 8