(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 811 249**

(51) Int. CI.:

***G07C 9/00*** (2010.01)
***G06Q 20/38*** (2012.01)
***G06Q 20/40*** (2012.01)
***G06F 21/31*** (2013.01)
***G06F 21/62*** (2013.01)
***G06Q 20/02*** (2012.01)
***G06F 16/93*** (2009.01)
***G07C 9/22*** (2010.01)
***G07C 9/27*** (2010.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **10.02.2014 PCT/EP2014/052504**

(87) Fecha y número de publicación internacional: **09.04.2015 WO15049065**

(96) Fecha de presentación y número de la solicitud europea: **10.02.2014 E 14703589 (3)**

(97) Fecha y número de publicación de la concesión europea: **03.06.2020 EP 3053146**

(54) Título: **Sistemas y métodos para compartir documentos de identidad verificados**

(30) Prioridad:

**01.10.2013 US 201361885432 P**
**06.12.2013 US 201314099751**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**11.03.2021**

(73) Titular/es:

**TRUNOMI LTD. (50.0%)**
**New Venture House 3rd Floor 3 Mill Creek Road**
**Pembroke HM05, BM y**
**LACEY, STUART H. (50.0%)**

(72) Inventor/es:

**LACEY, STUART H.**

(74) Agente/Representante:

**ROEB DÍAZ-ÁLVAREZ, María**

## DESCRIPCIÓN

Sistemas y métodos para compartir documentos de identidad verificados

**Campo técnico**

Las implementaciones divulgadas se refieren, en general, a la verificación de información y, más específicamente, a compartir documentos de identidad verificados entre entidades.

**Antecedentes**

La verificación de la identidad de un individuo o entidad es un hecho común para muchas transacciones financieras, comerciales y de otro tipo. Por ejemplo, antes de que un individuo pueda abrir una cuenta corriente, habitualmente un banco requiere que el individuo establezca que este es, de hecho, quien dice ser. Tradicionalmente, este requisito es satisfecho por el individuo al presentar un permiso de conducir y una factura de servicios públicos reciente, u otra carta oficial dirigida al individuo. Sin embargo, esto puede ser engorroso para el individuo, que a menudo ha de presentar físicamente los documentos requeridos al solicitante. Asimismo, debido a que, habitualmente, el individuo ha de verificar su identidad ante muchas instituciones diferentes para muchos fines diferentes, se puede volver una molestia tener que localizar repetidamente la información particular que se solicita y proporcionar la misma al solicitante. Esto tampoco es ideal para el solicitante de los documentos, que puede no ser competente para (o puede no desear) verificar que los documentos son legítimos, o puede no desear almacenar los documentos y tratar con cuestiones de seguridad, privacidad, conservación y destrucción de documentos.

Además, las transacciones financieras y de otro tipo se realizan, cada vez más, de forma electrónica y / o a grandes distancias. Esto puede hacer que sea aún menos práctico que los individuos proporcionen copias originales de documentos al solicitante. Asimismo, debido a que puede ser que las partes no lleguen a encontrarse cara a cara, esto le da aún más importancia a una verificación precisa de que el individuo es, o de que al menos es probable que sea, quien este dice ser.

El documento US 8.494.961 B1 divulga realizaciones que están relacionadas con un método y un sistema de autenticación implementado por ordenador para autenticar a un cliente usando un dispositivo electrónico para tomar parte en una transacción que involucra a una institución financiera a través de una red. Algunas realizaciones del método incluyen capturar una imagen del cliente tomando parte en la transacción usando un dispositivo de captura de imágenes integrado con el dispositivo electrónico y recuperar una imagen almacenada del cliente desde una base de datos de autenticación. Algunas realizaciones de la invención incluyen adicionalmente comparar, usando un algoritmo de comparación ejecutado por componentes de procesamiento informático, la imagen almacenada con la imagen capturada para autenticar al cliente y, tras la autenticación, supervisar la imagen capturada durante la transacción en busca de una interrupción usando los componentes de procesamiento informático. El método incluye adicionalmente terminar la transacción si se detecta una interrupción.

El documento US 2009/0132813 A1 divulga aparatos y métodos que realizan transacciones en un entorno seguro entre un individuo y otra parte, tal como un comerciante, en diversas realizaciones. El individuo posee un dispositivo electrónico móvil, tal como un teléfono inteligente, que puede cifrar datos de acuerdo con una infraestructura de clave pública. El individuo autentica la identidad del individuo en el dispositivo, desbloqueando de ese modo unas credenciales que se pueden usar en una transacción segura. El individuo hace que el dispositivo comunique las credenciales, de una forma segura, a un sistema electrónico de una parte de confianza, con el fin de obtener la autorización de la parte de confianza para pasar a formar parte de la transacción. El sistema de parte de confianza determina si conceder la autorización, y comunica la concesión y el resultado de la transacción al dispositivo usando un cifrado de acuerdo con la infraestructura de clave pública.

El documento US 2001/0002485 A1 divulga métodos para manejar objetos electrónicos originales almacenados que se han creado al firmar objetos de información por agentes de transferencia respectivos, presentar objetos de información firmados a una utilidad de custodia de confianza, validar los objetos de información firmados presentados al menos al someter a prueba la integridad de los contenidos de cada objeto de información firmado y la validez de la firma del agente de transferencia respectivo, y aplicar, a cada objeto de información validado, una marca de fecha y de hora y una firma digital y un certificado de autenticación de la utilidad de custodia de confianza.

El documento US 2012/0191614 A1 divulga un sistema para mejorar la seguridad de transacción basándose en información de ubicación. El sistema incluye un centro de procesamiento de transacciones en comunicación con un primer dispositivo de transacción y un segundo dispositivo de transacción. El centro de procesamiento de transacciones incluye un receptor que recibe una identificación y una ubicación respectivas desde al menos uno del primer y el segundo dispositivos de transacción. El centro de procesamiento de transacciones también incluye un procesador de transacciones que valida las identificaciones, valida las ubicaciones y ejecuta una transacción entre el primer y el segundo dispositivos de transacción cuando se validan las identificaciones y las ubicaciones.

El documento WO 03/007538 A1 divulga un sistema, método, aparato y producto de programa informático para la

verificación, la autenticación y el no rechazo de dispositivos, de usuarios y / o de transacciones. La aplicación inalámbrica captura y utiliza datos biométricos procedentes del usuario que posee un teléfono móvil, un PDA u otro ordenador portátil. El aparato de información autentica el dispositivo y / o usuario para reducir o eliminar la probabilidad de que se rechace la transacción. La autenticación y el no rechazo de transacciones se aplican a todo tipo de comercio, incluyendo la compra y venta de productos y servicios, operaciones bancarias, inversiones y otras transacciones financieras, así como en transacciones personales que no involucran directamente el comercio. La autenticación y el no rechazo tienen lugar a través de una red cableada de extremo a extremo o inalámbrica de ordenadores interconectados.

El documento WO 2008/020991 A2 divulga métodos, programas informáticos, aparatos y sistemas que proporcionan una gestión de identidad federada notarizada. Las realizaciones ilustrativas pueden ser útiles, por ejemplo, para soportar una autenticación de usuario eficiente cuando los proveedores son desconocidos entre sí y / o para evitar una comunicación directa entre proveedores de identidad y proveedores de servicios, lo que proporciona una protección de privacidad mejorada para los usuarios. En una realización ilustrativa no limitante, un método incluye: recibir, a través de una red de comunicación de datos, una afirmación generada por una primera entidad; notarizar la afirmación para obtener una afirmación notarizada correspondiente; y, en respuesta a recibir, de una segunda entidad, a través de la misma red de comunicación de datos, o de una diferente, una consulta correspondiente a la afirmación, devolver la afirmación notarizada correspondiente. En una realización ilustrativa adicional, el método incluye adicionalmente: Determinar una clave privada de usuario para una clave pública de usuario correspondiente que consiste en al menos un fragmento de información de identidad de usuario; y devolver la clave privada de usuario al usuario como datos que se van a almacenar en un medio de almacenamiento.

El documento US 2010/0161993 A1 divulga un sistema de procesamiento de documentos notariales, y se describen métodos relacionados. El sistema recibe archivos cargados por usuarios, procesa los mismos al aplicar una ID de documento, una marca de tiempo, etc., a páginas del documento y convierte estos a un formato de solo lectura para su almacenamiento. Una vez que los documentos se han procesado y almacenado en el sistema, estos no pueden ser cambiados por usuario alguno, incluyendo el propietario del documento. El sistema facilita documentos almacenados al propietario o a otros usuarios a solicitud o permiso del propietario. El sistema también procesa archivos generados a partir de mensajes cortos introducidos por usuarios, y versiones anotadas de documentos existentes. El sistema proporciona una forma de conservar versiones originales de documentos que se van a usar más adelante con el fin de evidenciar las fechas y los contenidos de documentos, evidenciar acuerdos entre partes en cuanto a los contenidos de documentos, etc. También se proporcionan funciones de notario electrónico, de firma electrónica, de marca de agua de manipulación indebida, etc.

El documento US 2006/0010323 A1 divulga un método mediante el cual datos privados se almacenan en un repositorio de tal modo que la información no sea accesible, ni siquiera para el propietario del repositorio. El repositorio facilita proporcionar acceso a la información a usuarios arbitrarios. Los datos se protegen al almacenarse de forma cifrada, teniendo lugar el cifrado en el sistema del usuario usando un cifrado de clave pública. Los datos se comparten de una de dos maneras: 1) con cada solicitud, al descifrar, el sistema del propietario, el documento y volver a cifrar el mismo usando la clave pública del solicitante; o 2) a lo largo de un periodo de tiempo, al compartir una clave privada de grupo con el solicitante al cifrar la clave privada de grupo usando la clave pública del solicitante. El repositorio facilita ambos métodos de tal modo que no se requiera una comunicación directa entre el sistema del propietario y los sistemas de los usuarios.

El documento US 6.839.843 B1 se dirige a un sistema seguro de almacenamiento y recuperación de datos electrónicos, que consiste en un repositorio de datos, un gestor de repositorios para gestionar el almacenamiento de datos electrónicos cifrados de un ordenador depositante en el repositorio de datos, y la recuperación de estos fuera del mismo, y un programa de agente del ordenador depositante. El programa de agente es accesible por el gestor de repositorios, tanto si el ordenador depositante está en línea como si está sin conexión. El programa de agente también tiene medios para descifrar, en la autenticación de un ordenador solicitante, los datos electrónicos cifrados del ordenador depositante que se recuperan del repositorio de datos a solicitud del ordenador solicitante. Preferiblemente, el gestor de repositorios puede firmar digitalmente los datos electrónicos cifrados antes del almacenamiento en el repositorio de datos, y reenviar entonces una copia de los datos cifrados firmados al programa de agente, de tal modo que el programa de agente puede verificar, contra los datos cifrados firmados, los datos electrónicos cifrados recuperados a continuación del descifrado.

El documento US 2013/0204786 A1 divulga sistemas, métodos y dispositivos descritos en este documento que posibilitan una verificación de identidad mejorada durante las transacciones financieras en línea. En particular, las características de diversas implementaciones se usan para posibilitar una verificación de identidad de los titulares de cuenta de tarjetas de crédito, tarjetas de débito y otros instrumentos de pago durante las transacciones en línea. Por ejemplo, en algunas implementaciones, son operables sistemas, métodos y dispositivos para comparar una o más imágenes codificadas y / o cifradas de características faciales obtenidas tras la activación del instrumento de pago o medidas de seguridad con una o más imágenes codificadas y / o cifradas de características faciales obtenidas durante una transacción en línea subsiguiente para verificar que el individuo que ofrece el instrumento de pago como forma de pago es el usuario verdadero y autorizado del instrumento de pago. Adicionalmente y / o como alternativa, se puede combinar un registro de impresión de voz y / o información de ubicación con el uso de las imágenes codificadas y / o

cifradas para proporcionar una seguridad adicional.

El documento US 2012/0036081 A1 divulga un método y sistema interactivo basado en web que facilita a un empleado procesar virtual y electrónicamente su verificación y certificación de elegibilidad de empleado con un notario público o agente de terceros autorizado remoto y en vivo; que comprende una funcionalidad a petición que implementa una reserva de citas basada en web, una plataforma de pago en línea, una comunicación por videoconferencia interactiva basada en web segura en tiempo real, una cámara web digital, una autenticación de identificación en tiempo real, un certificado de firma de capa de zócalos seguros de vídeo digital, firma de anotación y digital segura, sistema de entrega de documentos de red y archivo seguro.

**Sumario**

Por consiguiente, sería ventajoso proporcionar sistemas y métodos que mejoren las técnicas existentes para compartir documentos de identidad verificados de individuos o empresas con otros.

La presente invención se define en las reivindicaciones independientes adjuntas, a las que se debería hacer referencia. En las reivindicaciones dependientes adjuntas se exponen algunas características ventajosas. Las realizaciones o ejemplos de la siguiente descripción que no están cubiertos por las reivindicaciones adjuntas se proporcionan con fines simplemente ilustrativos. De acuerdo con algunas realizaciones, se divulga un método para compartir documentos de identidad verificados. El método se realiza en uno o más dispositivos electrónicos (por ejemplo, un dispositivo de cliente y / o un sistema de servidor) con uno o más procesadores y memoria que almacena uno o más programas para su ejecución por los uno o más procesadores. El dispositivo de cliente obtiene información de identidad de un usuario. El dispositivo de cliente también obtiene un documento. El dispositivo de cliente extrae datos a partir del documento, incluyendo los datos extraídos una información de identidad extraída. El dispositivo de cliente determina que la información de identidad del usuario y la información de identidad extraída coinciden sustancialmente, y genera al menos una calificación de verificación para el documento. El dispositivo de cliente envía el documento, los datos extraídos a partir del documento y la al menos una calificación de verificación a un sistema de servidor remoto con respecto al dispositivo de cliente. El sistema de servidor almacena el documento, los datos extraídos a partir del documento y la al menos una calificación de verificación en asociación con una cuenta del usuario, en donde al menos uno del documento, los datos extraídos a partir del documento y la al menos una calificación de verificación se almacena en uno o más contenedores cifrados. El sistema de servidor recibe, de un tercero, una solicitud de información asociada con la cuenta del usuario, incluyendo la información al menos uno del documento, los datos extraídos a partir del documento y la al menos una calificación de verificación. El sistema de servidor envía una solicitud al dispositivo de cliente que solicita una autorización para divulgar la información al tercero. En respuesta a recibir, del dispositivo de cliente, una autorización para divulgar la información al tercero, el sistema de servidor envía la información al tercero.

De acuerdo con algunas implementaciones, un sistema informático (por ejemplo, un sistema de cliente o un sistema de servidor) incluye uno o más procesadores, memoria y uno o más programas; los uno o más programas se almacenan en la memoria y se configuran para ser ejecutados por los uno o más procesadores, y los uno o más programas incluyen instrucciones para realizar las operaciones del método descrito anteriormente. De acuerdo con algunas realizaciones, un medio de almacenamiento legible por ordenador no transitorio ha almacenado en el mismo unas instrucciones que, cuando son ejecutadas por uno o más procesadores, hacen que un sistema informático (por ejemplo, un sistema de cliente o un sistema de servidor) realice las operaciones de los métodos descritos anteriormente.

Los sistemas y métodos divulgados evitan muchas dificultades logísticas tanto para los individuos como para las partes solicitantes. En particular, debido a que los documentos se comparten de forma electrónica, los usuarios no necesitan presentar físicamente, o enviar por correo, copias originales de documentos a un solicitante. De forma similar, el solicitante no necesita almacenar o mantener copias originales de los documentos, reduciendo los riesgos de cumplimiento y gastos generales. Además, debido a que los documentos están sujetos a pruebas de verificación, las entidades solicitantes pueden renunciar a una verificación independiente de los documentos, cuando sea apropiado, y pueden ser alertadas, de una forma rápida y fácil, acerca de notificaciones de identidad potencialmente fraudulentas. Por último, debido a que los documentos se cifran y se almacenan de forma segura, se puede asegurar la privacidad y la seguridad de la información tanto al individuo como al solicitante.

**Breve descripción de los dibujos**

Las implementaciones divulgadas en el presente documento se ilustran a modo de ejemplo, y no a modo de limitación, en las figuras de los dibujos adjuntos. De principio a fin de los dibujos, números de referencia semejantes se refieren a partes correspondientes.

La figura 1 es un diagrama de bloques que ilustra un entorno de cliente - servidor, de acuerdo con algunas implementaciones.

La figura 2 es un diagrama de bloques que ilustra un dispositivo informático de cliente, de acuerdo con algunas

implementaciones.

La figura 3 es un diagrama de bloques que ilustra un dispositivo informático de empresa, de acuerdo con algunas implementaciones.

La figura 4 es un diagrama de bloques que ilustra un dispositivo informático de servidor, de acuerdo con algunas implementaciones.

Las figuras 5A - 5D son diagramas de flujo que ilustran un método para verificar la identidad de un usuario, de acuerdo con algunas implementaciones.

La figura 6 es un diagrama de flujo que ilustra un método de verificación de un documento, de acuerdo con algunas implementaciones.

**Descripción detallada**

La atención se dirige a continuación a las figuras y, en particular, a la figura 1, que es un diagrama de bloques de un entorno de cliente - servidor 100, de acuerdo con algunas implementaciones, en el que es posible un uso compartido eficiente, seguro y conveniente de documentos de identidad verificados.

El entorno de cliente - servidor 100 incluye unos dispositivos de cliente 102-1 ... 102-n, un servidor 104 y unos dispositivos de empresa 108-1 ... 108-n, todos ellos conectados a través de una red 110. La red 110 incluye cualquiera de una diversidad de redes, incluyendo redes de área extensa (WAN), redes de área local (LAN), Redes de Área Personal, redes de área metropolitana, VPN, conexiones locales punto a punto, ad hoc, redes inalámbricas, redes cableadas, Internet o una combinación de tales redes.

En algunas implementaciones, el dispositivo de cliente 102-1 está asociado con un individuo (o cualquier entidad que desee verificar su identidad ante otra parte), y se usa para capturar y / o procesar documentos y otra información de un individuo, como se describe en el presente documento. En algunas implementaciones, el dispositivo de cliente 102-1 incluye una aplicación de cliente 112 que facilita la captura y / o el procesamiento de documentos y otra información (por ejemplo, con una cámara o escáner integrado o acoplado), y se comunica con uno o ambos del servidor 104 y el dispositivo de empresa 108-1. En algunas implementaciones, la aplicación de cliente 112 también genera calificaciones de verificación para documentos, extrae información a partir de los documentos y cifra los documentos (así como las calificaciones de verificación y la información extraída) antes de enviar los documentos al servidor 104. El dispositivo de cliente 102-1 y la aplicación de cliente 112, y las funciones y métodos que realizan los mismos, se analizan en el presente documento. Cualquier descripción o descripciones del dispositivo de cliente 102-1, o de las funciones o métodos realizados por el dispositivo de cliente 102-1, son igualmente de aplicación a cualquiera o todas las instancias de los dispositivos de cliente 102-n (además, en algunas implementaciones, las funciones o métodos descritos como asociados con o realizados por el dispositivo de cliente 102-1 son realizados por el dispositivo de empresa 108-1, tal como cuando un banco u otra institución financiera crea cuentas preliminares para sus clientes). Los dispositivos de cliente ilustrativos incluyen un ordenador de escritorio, un ordenador portátil, un ordenador de tipo tableta, un dispositivo electrónico móvil, un teléfono móvil (por ejemplo, un "teléfono inteligente"), un reproductor de medios digitales o cualquier otro dispositivo electrónico apropiado (o un quiosco que aloje cualquiera de los dispositivos anteriormente mencionados).

En algunas implementaciones, el dispositivo de empresa 108-1 está asociado con una entidad que requiere una verificación de identidad a partir de individuos u otras entidades. En algunas implementaciones, el dispositivo de empresa 108-1 incluye una aplicación de empresa 114 que facilita la solicitud y recepción de información de verificación de identidad a partir de individuos o entidades (por ejemplo, a través del servidor 104). En algunas implementaciones, el dispositivo de empresa 108-1 se comunica con uno o ambos del servidor 104 y el dispositivo de cliente 102-1. El dispositivo de empresa 108-1 y la aplicación de empresa 114, y las funciones y métodos que realizan los mismos, se analizan en el presente documento. Cualquier descripción o descripciones del dispositivo de empresa 108-1, o de las funciones o métodos realizados por el dispositivo de empresa 108-1, son igualmente de aplicación a cualquiera o todas las instancias de los dispositivos de empresa 108-n. Los dispositivos de empresa ilustrativos incluyen un ordenador de escritorio, un ordenador portátil, un ordenador de tipo tableta, un dispositivo electrónico móvil, un ordenador de servidor (o sistema informático de servidor), un teléfono móvil, un reproductor de medios digitales o cualquier otro dispositivo electrónico apropiado (o un quiosco que aloje cualquiera de los dispositivos anteriormente mencionados).

En algunas implementaciones, el servidor 104 está asociado con un proveedor de servicios que se puede comunicar, a través de la red 110 y / u otros medios de comunicación, con múltiples dispositivos de cliente (por ejemplo, 102-n) y múltiples dispositivos de empresa (por ejemplo, 108-n) para proporcionar y / o facilitar un uso compartido de documentos entre entidades. En algunas implementaciones, el servidor 104 incluye y / o se comunica con una base de datos de información de usuario 106. Como se describe en el presente documento, la base de datos de información de usuario 106 almacena información asociada con los usuarios, incluyendo, pero sin limitarse a, documentos (por ejemplo, imágenes u otras representaciones digitales de documentos de identificación, facturas de servicios públicos,

etc.), contenedores de los que se pueden extraer documentos, información extraída a partir de documentos, información de cuenta de usuario, calificaciones de verificación, puntuaciones de usuario, etc. En algunas implementaciones, parte de o toda la información anterior se cifra de tal modo que solo el usuario con el que está asociada la información (y las partes autorizadas por el usuario) pueden acceder a, y / o ver, la información.

Usando el entorno de cliente - servidor 100 ilustrado en la figura 1, se pueden compartir documentos de verificación de identidad de una forma rápida y eficiente entre un individuo y una institución u otra entidad, permitiendo que la identidad del individuo sea verificada de una forma rápida y eficiente. En particular, y como se describe en el presente documento, el dispositivo de cliente 102-1 se usa para capturar imágenes y / o archivos de documentos que se pueden usar para una verificación de identidad, tales como credenciales o tarjetas de identificación con fotografía emitidas por el gobierno (por ejemplo, permisos de conducir, pasaportes, etc.), facturas de servicios públicos y similares. Por ejemplo, en algunas implementaciones, el dispositivo de cliente 102-1 es un teléfono inteligente con una cámara digital, y un individuo usa la cámara para capturar una fotografía de un permiso de conducir y una factura de servicios públicos. El teléfono inteligente extrae entonces información a partir de las fotografías de los documentos, las analiza y genera una calificación de verificación para los documentos. Entonces, las fotografías, la información extraída a partir de las fotografías y las calificaciones de verificación se cifran y se envían al servidor 104, que almacena estos elementos en la base de datos de información de usuario 106 de una forma segura.

Una entidad solicitante solicita entonces información de verificación de identidad a partir de un individuo (por ejemplo, usando el dispositivo de empresa 108-1), y se envía una solicitud al individuo (por ejemplo, a través del servidor 104). El individuo usa entonces el dispositivo de cliente 102-1 y / o la aplicación de cliente 112 para aprobar (o denegar) parcial o totalmente la solicitud. Si la solicitud es aprobada por el individuo (por ejemplo, el individuo autoriza a la entidad solicitante a acceder a toda o parte de la información solicitada), se concede a la entidad solicitante acceso a la información autorizada a través del servidor 104.

El presente análisis se refiere, en general, a la entidad cuya identidad se está verificando como a un individuo o un "usuario". Sin embargo, se contempla asimismo la verificación de identidad para otras entidades, tal como para empresas, fondos fiduciarios, sociedades, negocios, familias, instituciones financieras, etc. Por consiguiente, cualquier análisis relacionado con un individuo o un usuario también es de aplicación a otras entidades o partes cuya identidad y documentos se deban verificar y / o compartir.

La figura 2 es un diagrama de bloques que ilustra un dispositivo de cliente 102-1, de acuerdo con algunas implementaciones. Aunque la figura 2 ilustra una instancia de un dispositivo de cliente (es decir, el dispositivo de cliente 102-1), la figura y la descripción asociada son igualmente de aplicación a cualquier dispositivo de cliente (por ejemplo, 102-1 - 102-n).

En algunas implementaciones, el dispositivo de cliente 102-1 es cualquiera de: un ordenador de escritorio, un ordenador portátil, un ordenador de tipo tableta, un dispositivo electrónico móvil, un teléfono móvil, un reproductor de medios digitales o cualquier otro dispositivo electrónico apropiado (o un quiosco que aloje cualquiera de los dispositivos anteriormente mencionados).

El dispositivo de cliente 102-1 incluye habitualmente una o más CPU 204, una interfaz de usuario 206, al menos una interfaz de comunicaciones de red 212 (cableada y / o inalámbrica), un dispositivo de captura de imágenes 214, un sistema de determinación de posición 216, un dispositivo de captura de biométrica 217, memoria 218 y al menos un bus de comunicación 202 para interconectar estos componentes. Cada bus de comunicación 202 puede incluir un conjunto de circuitos (denominado a veces conjunto de chips) que interconecta y controla las comunicaciones entre componentes de sistema. En algunas implementaciones, la interfaz de usuario 206 incluye un visualizador 208 y un dispositivo o dispositivos de entrada 210 (por ejemplo, un teclado, un ratón, una pantalla táctil, teclados numéricos, etc.).

El dispositivo de captura de imágenes 214 es cualquier dispositivo que sea capaz de capturar una imagen de una escena u objeto del mundo real. En algunas implementaciones, el dispositivo de captura de imágenes 214 es una cámara digital (incluyendo cualquier lente o lentes, sensor o sensores y otros componentes, que sean apropiados). En algunas implementaciones, el dispositivo de captura de imágenes es un escáner (por ejemplo, un escáner de documentos de superficie plana). En algunas implementaciones, el dispositivo de captura de imágenes 214 se incorpora en una carcasa común con el dispositivo de cliente 102-1. Por ejemplo, cuando el dispositivo de cliente 102-1 es un teléfono móvil, el dispositivo de captura de imágenes 214 es una cámara digital integrada en el teléfono móvil. Como otro ejemplo, cuando el dispositivo de cliente 102-1 es un ordenador portátil, el dispositivo de captura de imágenes 214 es una cámara digital integrada en el ordenador portátil (por ejemplo, una "cámara web"). Otros dispositivos de captura de imágenes posibles incluyen escáneres 3D, cámaras 3D, cámaras de distancia, dispositivos de formación de imágenes de detección de movimiento, escáneres ultrasónicos y similares.

En algunas implementaciones, el dispositivo de captura de imágenes 214 está en una carcasa diferente de la del dispositivo de cliente 102-1. En un ejemplo, el dispositivo de cliente 102-1 es un ordenador portátil o de escritorio, y el dispositivo de captura de imágenes 214 es un escáner o cámara separado que se puede acoplar al dispositivo de cliente 102-1 para proporcionar imágenes al dispositivo de cliente (por ejemplo, a través de una conexión cableada,

tal como una conexión de red cableada o una conexión de Bus Serie Universal, o a través de una conexión inalámbrica, tal como WiFi, Bluetooth o similares).

El sistema de determinación de posición 216 incluye dispositivos y / o componentes para determinar la ubicación del dispositivo de cliente 102-1, incluyendo, pero sin limitarse a, sensores del sistema global de determinación de posición (GPS), receptores de radio (por ejemplo, para una triangulación por torres de célula, determinación de posición basada en WiFi, etc.), sensores inerciales y acelerómetros. En algunas implementaciones, el dispositivo de cliente 102-1 no incluye (o no se basa en) un sistema de determinación de posición 216 separado. Por ejemplo, cuando el dispositivo de cliente 102-1 está conectado a Internet (por ejemplo, a través de la interfaz de comunicaciones de red 212), la ubicación del dispositivo de cliente 102-1 se puede determinar usando técnicas de geolocalización de dirección de IP. También se contemplan otras técnicas para determinar la ubicación del dispositivo de cliente, incluyendo las que están basadas en un sistema de determinación de posición integrado o conectado y las que no lo están.

El dispositivo de captura de biométrica 217 (opcional) incluye dispositivos y / o componentes para capturar datos biométricos a partir de una persona. En algunas implementaciones, el dispositivo de captura de biométrica 217 es un escáner de huellas dactilares. En algunas implementaciones, este es un escáner de retina. En algunas implementaciones, este es un escáner facial. En algunas implementaciones, este es un escáner de reconocimiento de voz. En algunas implementaciones, el dispositivo de captura de biométrica 217 es un dispositivo de captura multipropósito que puede capturar múltiples tipos de datos biométricos a partir de un usuario (por ejemplo, huellas de manos, huellas dactilares, imágenes faciales, etc.). En algunas implementaciones, el dispositivo de captura de biométrica 217 se incorpora y / o coopera con el dispositivo de captura de imágenes 214 (por ejemplo, para capturar imágenes de la cara de un usuario para un reconocimiento facial). En algunas implementaciones, las imágenes para un análisis biométrico se capturan usando el dispositivo de captura de imágenes 214, y no es necesario un dispositivo de captura de biométrica separado. En tales casos, el análisis biométrico se puede realizar usando uno o más módulos de software (por ejemplo, el módulo de análisis biométrico 234, analizado posteriormente).

La memoria 218 incluye memoria de acceso aleatorio de alta velocidad, tal como DRAM, SRAM, DDR RAM u otros dispositivos de memoria de estado sólido de acceso aleatorio, y puede incluir memoria no volátil, tal como uno o más dispositivos de almacenamiento en disco magnético, dispositivos de almacenamiento en disco óptico, dispositivos de memoria flash u otros dispositivos de almacenamiento de estado sólido no volátiles. La memoria 218 puede incluir opcionalmente uno o más dispositivos de almacenamiento remotamente ubicados con respecto a la o las CPU 204 (por ejemplo, un dispositivo o servicio de almacenamiento conectado a la red, tal como un servicio de almacenamiento basado en "la nube"). La memoria 218 o, como alternativa, el dispositivo o dispositivos de memoria no volátil dentro de la memoria 218, incluye un medio de almacenamiento legible por ordenador no transitorio. En algunas implementaciones, la memoria 218 o el medio de almacenamiento legible por ordenador de la memoria 218 almacena los siguientes programas, módulos y estructuras de datos, o un subconjunto de los mismos:

- un sistema operativo 220 que incluye procedimientos para manejar diversos servicios de sistema básicos y para realizar tareas dependientes de hardware;
- un módulo de comunicación 222 que se usa para conectar el dispositivo de cliente 102-1 a otros ordenadores a través de las una o más interfaces de comunicación de red 212 (cableadas o inalámbricas) y una o más redes de comunicación, tales como Internet, otras Redes de Área Extensa, Redes de Área Local, Redes de Área Personal, Redes de Área Metropolitana, VPN, conexiones locales punto a punto y / o ad hoc, y así sucesivamente;
- un módulo de interfaz de usuario 224 que recibe órdenes y / o entradas procedentes de un usuario a través de la interfaz de usuario 206 (por ejemplo, a partir del dispositivo o dispositivos de entrada 210, que pueden incluir un teclado o teclados, una pantalla o pantallas táctiles, un micrófono o micrófonos, un dispositivo o dispositivos apuntadores y similares), y proporciona objetos de interfaz de usuario en un visualizador (por ejemplo, el visualizador 208);
- un módulo de dispositivo de captura de imágenes 226 (incluyendo, por ejemplo, aplicaciones, controladores, etc.) que funciona junto con el dispositivo de captura de imágenes 214 para capturar imágenes, tales como imágenes o escaneos de documentos físicos, caras, escenas del mundo real, etc.;
- un módulo de dispositivo de captura de biométrica 227 que funciona junto con el dispositivo de captura de biométrica 217 (y / o el dispositivo de captura de imágenes 214) para capturar datos biométricos de un usuario, incluyendo datos relacionados con cualquier característica física apropiada de un usuario, tal como huellas dactilares, ojos, retinas, características faciales, huellas de voz, huellas de manos, etc.;
- un módulo de sistema de determinación de posición 228 que, junto con el sistema de determinación de posición 216, determina una ubicación actual (por ejemplo, latitud y longitud, dirección postal, ciudad, estado, municipio, etc.) del dispositivo de cliente 102-1; y
- uno o más módulo o módulos de aplicación de cliente 230 para posibilitar que el dispositivo de cliente 102-1 realice los métodos y / o técnicas descritos en el presente documento, incluyendo el módulo o módulos de aplicación de cliente 230, pero sin limitarse a:

    - un módulo de generación / confirmación de cuenta 231 para generar una cuenta con un proveedor de servicios, incluyendo recibir información acerca de un usuario del dispositivo de cliente 102-1 (por ejemplo, nombre, dirección, número de seguridad social, contraseña, preguntas / respuestas de recuperación de

cuenta, datos biométricos, credenciales de inicio de sesión, etc.), proporcionar esta información a un dispositivo remoto (por ejemplo, el servidor 104) con el fin de crear una cuenta de usuario única, e interaccionar con el dispositivo remoto para establecer la cuenta del usuario; el módulo de generación / confirmación de cuenta 231 también facilita la confirmación de usuario de una información de cuenta que fue proporcionada a un dispositivo remoto (por ejemplo, el servidor 104) por otra entidad (por ejemplo, un banco), como se describe en el presente documento;

- un módulo de extracción de datos 232 para extraer información a partir de documentos obtenidos por el dispositivo de cliente 102-1, incluyendo extraer texto legible por ordenador a partir de documentos, usar un reconocimiento óptico de caracteres para reconocer y extraer texto no legible por ordenador a partir de documentos, así como localizar y extraer fotografías, imágenes, hologramas, perforaciones de láser, firmas, códigos de barras, Códigos de Respuesta Rápida (QR), etc., y similares;
- un módulo de análisis biométrico 234 para analizar datos biométricos, incluyendo determinar si unos datos biométricos de muestra coinciden con unos datos biométricos de referencia (por ejemplo, para fines de autenticación de usuario), determinar si una fotografía de un usuario extraída a partir de un documento coincide con una fotografía capturada del usuario (por ejemplo, una fotografía capturada por el dispositivo de captura de imágenes 214), determinar si una muestra de voz coincide con una huella de voz aprobada anterior del usuario, etc.;
- un módulo de análisis de documentos 236 para analizar documentos (y / o información, fotografías u otro contenido extraído a partir de documentos), por ejemplo, para determinar si y / o en qué grado una información extraída a partir del documento coincide con otra información asociada con el usuario (tal como el nombre del usuario, la fecha de nacimiento, la dirección, etc.), la calidad del contenido extraído a partir del documento (por ejemplo, hologramas, perforaciones de láser, etc.) y similares;
- un módulo de calificación de verificación 238 para generar calificaciones de verificación para documentos;
- un módulo de cifrado / carga 240 para cifrar documentos, datos biométricos, calificaciones de verificación, datos extraídos y similares, y cargar tal información (o bien cifrada o bien no cifrada) en un dispositivo remoto (tal como el servidor 104);
- un módulo de gestión de solicitudes 242 para recibir solicitudes de información (por ejemplo, a partir del servidor 104, un dispositivo de empresa 108-n y / u otro dispositivo de cliente 102-n), proporcionar indicaciones a un usuario del dispositivo de cliente 102-1 (por ejemplo, a través de la interfaz de usuario 206), recibir autorizaciones o denegaciones parciales o completas de las solicitudes procedentes del usuario y responder a las solicitudes con unas respuestas apropiadas (por ejemplo, al comunicarse con el servidor 104, un dispositivo de empresa 108-n y / u otro dispositivo de cliente 102-n); y
- un módulo de gestión de autorizaciones 244 para posibilitar que un usuario vea, gestione, conceda, cambie y / o modifique autorizaciones, incluyendo revocar autorizaciones previamente concedidas.

En algunas implementaciones, el dispositivo de cliente 102-1 incluye un subconjunto de los componentes y módulos mostrados en la figura 2. Además, en algunas implementaciones, el dispositivo de cliente 102-1 incluye componentes y / o módulos adicionales no mostrados en la figura 2.

La figura 3 es un diagrama de bloques que ilustra un dispositivo de empresa 108-1, de acuerdo con algunas implementaciones. Aunque la figura 3 ilustra una instancia de un dispositivo de empresa (es decir, el dispositivo de empresa 108-1), la figura y la descripción asociada son igualmente de aplicación a cualquier dispositivo de empresa (por ejemplo, 108-1 - 108-n).

En algunas implementaciones, el dispositivo de empresa 108-1 es cualquiera de: un ordenador de escritorio, un ordenador portátil, un ordenador de tipo tableta, un ordenador de servidor (o un sistema de servidor) un dispositivo electrónico móvil, un teléfono móvil, un reproductor de medios digitales o cualquier otro dispositivo electrónico apropiado (o un quiosco que aloje cualquiera de los dispositivos anteriormente mencionados).

El dispositivo de empresa 108-1 incluye habitualmente una o más CPU 304, una interfaz de usuario 306, al menos una interfaz de comunicaciones de red 312 (cableada y / o inalámbrica), un dispositivo de captura de imágenes 314, memoria 318 y al menos un bus de comunicación 302 para interconectar estos componentes. Cada bus de comunicación 302 puede incluir un conjunto de circuitos (denominado a veces conjunto de chips) que interconecta y controla las comunicaciones entre componentes de sistema. En algunas implementaciones, la interfaz de usuario 306 incluye un visualizador 308 y un dispositivo o dispositivos de entrada 310 (por ejemplo, un teclado, un ratón, una pantalla táctil, teclados numéricos, etc.).

El dispositivo de captura de imágenes 314 es cualquier dispositivo que sea capaz de capturar una imagen de una escena u objeto del mundo real. En algunas implementaciones, el dispositivo de captura de imágenes 314 es una cámara digital (incluyendo cualquier lente o lentes, sensor o sensores u otros componentes, que sean apropiados). En algunas implementaciones, el dispositivo de captura de imágenes es un escáner (por ejemplo, un escáner de superficie plana). En algunas implementaciones, el dispositivo de captura de imágenes 314 se incorpora en una carcasa común con el dispositivo de empresa 108-1.

En algunas implementaciones, el dispositivo de captura de imágenes 314 está en una carcasa diferente de la del dispositivo de empresa 108-1. En un ejemplo, el dispositivo de empresa 108-1 es un ordenador portátil o de escritorio,

y el dispositivo de captura de imágenes 314 es un escáner o cámara separado que se puede acoplar al dispositivo de empresa 108-1 para proporcionar imágenes al dispositivo de empresa (por ejemplo, a través de una conexión cableada, tal como una conexión de red cableada o una conexión de Bus Serie Universal, o a través de una conexión inalámbrica, tal como WiFi, Bluetooth o similares).

La memoria 318 incluye memoria de acceso aleatorio de alta velocidad, tal como DRAM, SRAM, DDR RAM u otros dispositivos de memoria de estado sólido de acceso aleatorio, y puede incluir memoria no volátil, tal como uno o más dispositivos de almacenamiento en disco magnético, dispositivos de almacenamiento en disco óptico, dispositivos de memoria flash u otros dispositivos de almacenamiento de estado sólido no volátiles. La memoria 318 puede opcionalmente incluir uno o más dispositivos de almacenamiento ubicados de manera remota con respecto a la o las CPU 304. La memoria 318 o, como alternativa, el dispositivo o dispositivos de memoria no volátil dentro de la memoria 318, incluye un medio de almacenamiento legible por ordenador no transitorio. En algunas implementaciones, la memoria 318 o el medio de almacenamiento legible por ordenador de la memoria 318 almacena los siguientes programas, módulos y estructuras de datos, o un subconjunto de los mismos:

- un sistema operativo 320 que incluye procedimientos para manejar diversos servicios de sistema básicos y para realizar tareas dependientes de hardware;
- un módulo de comunicación 322 que se usa para conectar el dispositivo de empresa 108-1 a otros ordenadores a través de las una o más interfaces de red 312 (cableadas o inalámbricas) y una o más redes de comunicación, tales como Internet, otras Redes de Área Extensa, Redes de Área Local, Redes de Área Personal, Redes de Área Metropolitana, VPN, conexiones locales punto a punto y / o ad hoc, y así sucesivamente;
- un módulo de interfaz de usuario 324 que recibe órdenes y / o entradas procedentes de un usuario a través de la interfaz de usuario 306 (por ejemplo, a partir del dispositivo o dispositivos de entrada 310, que pueden incluir un teclado o teclados, una pantalla o pantallas táctiles, un micrófono o micrófonos, un dispositivo o dispositivos apuntadores y similares), y proporciona objetos de interfaz de usuario en un visualizador (por ejemplo, el visualizador 308);
- un módulo de dispositivo de captura de imágenes 326 (incluyendo, por ejemplo, aplicaciones, controladores, etc.) que funciona junto con el dispositivo de captura de imágenes 314 para capturar imágenes, tales como imágenes o escaneos de documentos físicos, caras, escenas del mundo real, etc.
- uno o más módulo o módulos de aplicación de empresa 328 para posibilitar que el dispositivo de empresa 108-1 realice los métodos y / o técnicas descritos en el presente documento, incluyendo el módulo o módulos de aplicación de empresa 328, pero sin limitarse a:

    - uno o más módulo o módulos de generación de cuentas 329 para generar cuentas con un proveedor de servicios para uno o más usuarios basándose en información que ya posee la entidad que opera el dispositivo de empresa 108-1 (por ejemplo, información y documentos que un usuario ya ha compartido con una institución), incluyendo el módulo o módulos de generación de cuentas 329, pero sin limitarse a:

        - un módulo de extracción de datos 330 para extraer información a partir de documentos obtenidos por el dispositivo de empresa 108-1, incluyendo extraer texto legible por ordenador a partir de documentos, usar un reconocimiento óptico de caracteres para reconocer y extraer texto no legible por ordenador a partir de documentos, así como localizar y extraer fotografías, imágenes, firmas, hologramas, perforaciones de láser, códigos de barras, Códigos de Respuesta Rápida (QR), etc., y similares;
        - un módulo de análisis de documentos 332 para analizar documentos (y / o información, fotografías u otro contenido extraído a partir de documentos), por ejemplo, para determinar si y / o en qué grado una información extraída a partir del documento coincide con otra información asociada con el usuario (tal como el nombre del usuario, la fecha de nacimiento, la dirección, etc.), la calidad del contenido extraído a partir del documento (por ejemplo, hologramas, perforaciones de láser, etc.) y similares;
        - un módulo de calificación de verificación 334 para generar calificaciones de verificación para documentos; y
        - un módulo de cifrado / carga 336 para cifrar documentos, datos biométricos, calificaciones de verificación, datos extraídos, información de usuario (por ejemplo, nombre, dirección, número de seguridad social, etc.) y similares, y cargar tal información (o bien cifrada o bien no cifrada) en un dispositivo remoto (tal como el servidor 104); y

    - uno o más módulo o módulos de acceso a información 338 para manejar solicitudes de información de usuario y manejar información recibida según esas solicitudes, incluyendo el módulo o módulos de acceso a información 338, pero sin limitarse a:

        - un módulo de manejo de solicitudes 340 para recibir solicitudes a partir de un operador del dispositivo de empresa 108-1 (y / o solicitudes automáticamente generadas) de información de usuario, y para comunicar las solicitudes de información de usuario a dispositivos remotos (por ejemplo, tales como el servidor 104 y / o el dispositivo de cliente 102-n);
        - un módulo de recepción de información 342 para recibir información asociada con un usuario (por ejemplo, a partir del servidor 104), incluyendo, pero sin limitarse a, documentos, datos extraídos a partir de documentos, calificaciones de verificación, etc., y para recibir claves de descifrado (por

ejemplo, a partir del servidor 104 y / o un dispositivo de cliente 102-n); y
- un módulo de seguridad / descifrado 344 para determinar derechos de acceso a información asociada con un usuario y para descifrar información asociada con un usuario; y

- una base de datos de información de usuario 346 para almacenar información de usuario (por ejemplo, recibida del servidor 104), incluyendo, pero sin limitarse a, documentos, datos extraídos a partir de documentos, calificaciones de verificación, claves de descifrado, etc.

En algunas implementaciones, el dispositivo de empresa 108-1 incluye un subconjunto de los componentes y módulos mostrados en la figura 3. Además, en algunas implementaciones, el dispositivo de empresa 108-1 incluye componentes y / o módulos adicionales no mostrados en la figura 3.

La figura 4 es un diagrama de bloques que ilustra un servidor 104, de acuerdo con algunas implementaciones. En algunas implementaciones, el servidor 104 es cualquiera de: un ordenador de escritorio, un ordenador portátil, un ordenador de tipo tableta, un ordenador de servidor (o un sistema de servidor) un dispositivo electrónico móvil, un teléfono móvil, un reproductor de medios digitales o cualquier otro dispositivo electrónico apropiado (o un quiosco que aloje cualquiera de los dispositivos anteriormente mencionados).

El servidor 104 incluye habitualmente una o más CPU 404, una interfaz de usuario 406, al menos una interfaz de comunicaciones de red 412 (cableada y / o inalámbrica), memoria 414 y al menos un bus de comunicación 402 para interconectar estos componentes. Cada bus de comunicación 402 puede incluir un conjunto de circuitos (denominado a veces conjunto de chips) que interconecta y controla las comunicaciones entre componentes de sistema. En algunas implementaciones, la interfaz de usuario 406 incluye un visualizador 408 y un dispositivo o dispositivos de entrada 410 (por ejemplo, un teclado, un ratón, una pantalla táctil, teclados numéricos, etc.).

La memoria 414 incluye memoria de acceso aleatorio de alta velocidad, tal como DRAM, SRAM, DDR RAM u otros dispositivos de memoria de estado sólido de acceso aleatorio, y puede incluir memoria no volátil, tal como uno o más dispositivos de almacenamiento en disco magnético, dispositivos de almacenamiento en disco óptico, dispositivos de memoria flash u otros dispositivos de almacenamiento de estado sólido no volátiles. La memoria 414 puede opcionalmente incluir uno o más dispositivos de almacenamiento ubicados de manera remota con respecto a la o las CPU 404. La memoria 414 o, como alternativa, el dispositivo o dispositivos de memoria no volátil dentro de la memoria 414, incluye un medio de almacenamiento legible por ordenador no transitorio. En algunas implementaciones, la memoria 414 o el medio de almacenamiento legible por ordenador de la memoria 414 almacena los siguientes programas, módulos y estructuras de datos, o un subconjunto de los mismos

- un sistema operativo 416 que incluye procedimientos para manejar diversos servicios de sistema básicos y para realizar tareas dependientes de hardware;
- un módulo de comunicación 418 que se usa para conectar el servidor 104 a otros ordenadores a través de las una o más interfaces de red 412 (cableadas o inalámbricas) y una o más redes de comunicación, tales como Internet, otras Redes de Área Extensa, Redes de Área Local, Redes de Área Personal, Redes de Área Metropolitana, VPN, conexiones locales punto a punto y / o ad hoc, y así sucesivamente;
- un módulo de interfaz de usuario 420 que recibe órdenes y / o entradas procedentes de un usuario a través de la interfaz de usuario 406 (por ejemplo, a partir del dispositivo o dispositivos de entrada 410, que pueden incluir un teclado o teclados, una pantalla o pantallas táctiles, un micrófono o micrófonos, un dispositivo o dispositivos apuntadores y similares), y proporciona objetos de interfaz de usuario en un visualizador (por ejemplo, el visualizador 408);
- uno o más módulo o módulos de aplicación de servidor 422 para posibilitar que el servidor 104 realice los métodos y / o técnicas descritos en el presente documento, incluyendo el módulo o módulos de aplicación de servidor 422, pero sin limitarse a:
    - un módulo de generación de cuentas 424 para generar cuentas para usuarios basándose en información proporcionada (y / o verificada) por los usuarios o por otras entidades, y almacenar las cuentas (e información asociada) en la base de datos de cuentas de usuario 106;
    - un módulo de recepción 426 para recibir información a partir de dispositivos remotos (por ejemplo, dispositivos de cliente 102-n, dispositivos de empresa 108-n), incluyendo, pero sin limitarse a: documentos, calificaciones de verificación, datos extraídos a partir de documentos, información de cuenta (por ejemplo, nombre, dirección, número de seguridad social, contraseña, preguntas / respuestas de recuperación de cuenta, datos biométricos, credenciales de inicio de sesión, etc.), etc.;
    - un módulo de cifrado 428 opcional para cifrar información de usuario (incluyendo, pero sin limitarse a, documentos, calificaciones de verificación, datos extraídos a partir de documentos, información de cuenta) para un almacenamiento seguro en la base de datos de información de usuario 106, si la información de usuario no estaba cifrada antes de que fuera recibida por el servidor 104;
    - un módulo de gestión de solicitudes 430 para recibir y procesar solicitudes de información asociada con unos usuarios respectivos (por ejemplo, a partir de un dispositivo de empresa 108-n), enviar solicitudes de autorización a los usuarios respectivos (por ejemplo, a un dispositivo de cliente 102-n) y recibir autorizaciones a partir de los usuarios respectivos para permitir el acceso a la información solicitada (o a

un subconjunto o superconjunto de la información solicitada);

- un módulo de encapsulación / cifrado de información 432 para recopilar, encapsular y cifrar información de usuario (incluyendo, pero sin limitarse a, documentos, calificaciones de verificación, datos extraídos a partir de documentos, información de cuenta) que se va a enviar a, o a la que va a acceder de otro modo, un solicitante (por ejemplo, un dispositivo de empresa 108-n), y para enviar la información al solicitante;
- un módulo de gestión de acceso 434 para determinar si permitir a entidades solicitantes acceder a información de usuario (por ejemplo, basándose en permisos concedidos y / o denegados por los usuarios respectivos, límites de tiempo impuestos por usuarios y / o agencias reguladoras, o cualquier otro permiso, límite, criterio, etc., apropiado); y
- una base de datos de información de usuario 106 que incluye información asociada con una pluralidad de usuarios.

La figura 4 ilustra adicionalmente una porción de la base de datos de información de usuario 106 relacionada con una cuenta de usuario 436 para un usuario "n" ilustrativo. La cuenta de usuario 436 incluye, pero no se limita a:

- información de cuenta 438 asociada con el usuario (por ejemplo, nombre, dirección, número de seguridad social, contraseña, preguntas / respuestas de recuperación de cuenta, datos biométricos, credenciales de inicio de sesión, etc.);
- un documento o documentos 440 asociados con el usuario, incluyendo cualquier documento, archivo, contenedor, dato / contenido extraído a partir de documentos, etc., así como conjuntos archivados de la información y / o documentos anteriores, conjuntos enriquecidos de documentos (por ejemplo, realizados al actualizar documentos existentes con versiones actualizadas / revisadas subsiguientes del mismo documento);
- una calificación o calificaciones de verificación 442, incluyendo calificaciones de verificación para todos o un subconjunto del documento o documentos 440, calificaciones de verificación compuestas (por ejemplo, calificaciones de verificación basándose en una pluralidad de pruebas), una puntuación de usuario y similares; y
- datos de permisos 444, incluyendo permisos activos e históricos concedidos por un usuario para entidades solicitantes o autorizadas.

En algunas implementaciones, se cifra cualquiera o toda la información de usuario en la base de datos de información de usuario 106. Además, en algunas implementaciones, el proveedor de servicios no posee claves de descifrado para la información de usuario. Por consiguiente, el proveedor de servicios y / o el servidor 104 no puede descifrar, ver, leer o modificar la información de usuario.

En algunas implementaciones, el servidor 104 incluye un subconjunto de los componentes y módulos mostrados en la figura 4. Además, en algunas implementaciones, el servidor 104 incluye componentes y / o módulos adicionales no mostrados en la figura 4.

Las figuras 5A - 5D son diagramas de flujo que ilustran un método 500 para compartir documentos de identidad verificados, de acuerdo con algunas implementaciones. Cada una de las operaciones mostradas en las figuras 5A - 5D puede corresponder a instrucciones almacenadas en una memoria informática o medio de almacenamiento legible por ordenador. En algunas implementaciones, las etapas se realizan en un dispositivo electrónico con uno o más procesadores (o núcleos) y memoria que almacena uno o más programas para su ejecución por los uno o más procesadores (o núcleos). Por ejemplo, en algunas implementaciones, las etapas se realizan en cualquiera (o en cualquier combinación) del dispositivo de cliente 102-1, el servidor 104 y el dispositivo de empresa 108-1. Además, las etapas individuales del método se pueden distribuir entre los múltiples dispositivos electrónicos de cualquier forma apropiada.

En algunas implementaciones, cualquiera o todas las comunicaciones entre los dispositivos descritos con respecto a las figuras 5A - 5D se aseguran y / o se cifran usando cualquier técnica de seguridad y / o cifrado apropiada, incluyendo, pero sin limitarse a, Protocolo Seguro de Transporte de Hipertexto (HTTPS), Capa de Zócalos Seguros (SSL), Seguridad de Capa de Transporte (TLS), Intérprete de Comandos Seguro (SSH), Seguridad de Protocolo de Internet (IPSec), cifrado de clave pública y similares (incluyendo cualquier método de seguridad y / o cifrado aún por desarrollar apropiado).

Se crea una cuenta con un proveedor de servicios (502) (por ejemplo, con el módulo de generación / confirmación de cuenta 231). En algunas implementaciones, como parte de la creación de la cuenta (es decir, la inscripción / registro de cuenta), un usuario proporciona al dispositivo de cliente 102-1 información de identidad, tal como un nombre, un género, una fecha de nacimiento, una dirección, un número de seguridad social, una residencia, etc. En algunas implementaciones, el usuario proporciona información de inicio de sesión, tal como un nombre de usuario, una contraseña y preguntas / respuestas de verificación de identidad (por ejemplo, apellido de soltera de la madre, segundo nombre del padre, ciudad de nacimiento, etc.). En algunas implementaciones, el usuario proporciona asimismo otra información, tal como: una firma (por ejemplo, una fotografía / imagen de una firma, o una entrada de firma directamente en el dispositivo de cliente 102-1, tal como con una pantalla sensible al tacto y un lápiz), una fotografía, un nombre de usuario, una biométrica de huella dactilar, una biométrica de huella vocal, una biométrica facial, un

código postal y un número de cuenta.

El dispositivo de cliente 102-1 se comunica con el servidor 104 para registrar la cuenta de usuario, lo que incluye que el servidor 104 reciba y / o almacene información de cuenta y / o información de identidad proporcionada por el usuario (501) (por ejemplo, con el módulo de generación de cuentas 424).

El dispositivo de cliente 102-1 obtiene un documento (504). Los documentos obtenidos por el dispositivo de cliente 102-1 a partir de un usuario se proporcionan a entidades solicitantes para ayudar a verificar la identidad del usuario. Los documentos ilustrativos incluyen permisos de conducir, carnés de identidad nacionales, certificados de nacimiento, pasaportes, tarjetas de seguridad social, certificados de matrimonio, facturas de servicios públicos, tarjetas de identificación con fotografía emitidas por el gobierno y similares. En el presente análisis, los documentos son cualquier tipo apropiado de archivo digital, incluyendo archivos de texto legibles por ordenador (por ejemplo, archivos de procesamiento de texto, archivos de hoja de cálculo, facturas generadas por ordenador, etc.) o imágenes de documentos físicos (por ejemplo, escaneos, fotografías digitales, etc.), cualquiera de los cuales se puede almacenar o representar en cualquier tipo de archivo, formato de archivo, etc., apropiado (por ejemplo, archivos PDF, archivos JPEG, archivos GIF, archivos TIFF, archivos DOC, etc.). Además, cuando se usa el término "documento", el análisis correspondiente se puede referir a una versión legible por ordenador de un documento, una versión física de un documento, o ambas, dependiendo del contexto del análisis. Un experto en la materia reconocerá cuándo el análisis se refiere a versiones legibles por ordenador de un documento y cuándo se refiere a versiones físicas de un documento.

En algunas implementaciones, el documento se obtiene al capturar una imagen digital de un documento físico (por ejemplo, con el dispositivo de captura de imágenes 214 y / o el módulo de dispositivo de captura de imágenes 226). Por ejemplo, cuando el dispositivo de cliente 102-1 es un teléfono móvil con una cámara integrada, el usuario toma una instantánea de un documento usando la cámara. Como otro ejemplo, cuando el dispositivo de cliente 102-1 es un ordenador portátil o de escritorio conectado a un escáner de superficie plana, el usuario obtiene un escaneo del documento usando el escáner.

En algunas implementaciones, el documento se obtiene al recuperar el mismo de la memoria de un dispositivo electrónico. Por ejemplo, los documentos se pueden almacenar como un archivo digital en una memoria asociada con y / o disponible de otro modo para el dispositivo de cliente 102-1. Por consiguiente, un usuario puede apuntar la aplicación de cliente 230 a un documento particular al navegar hasta el archivo a través de un explorador de archivos, o al introducir directamente una ubicación de memoria (por ejemplo, una ruta de archivo) del archivo. El dispositivo de cliente 102-1 obtiene entonces el documento a partir de la ubicación especificada.

El dispositivo de cliente 102-1 extrae datos a partir del documento (506) (por ejemplo, con el módulo de extracción de datos 232). En algunas implementaciones, los datos extraídos incluyen información de identidad (por ejemplo, nombre, dirección, número de teléfono, número de seguridad social, etc.).

En algunas implementaciones, los datos extraídos incluyen datos de texto. Los datos de texto se extraen directamente a partir de documentos que tienen texto legible por ordenador, o se extraen después de realizar un reconocimiento óptico de caracteres en una imagen de un documento (o ambos). En algunas implementaciones, los datos extraídos incluyen datos biométricos, por ejemplo, a partir de una fotografía contenida en el documento. Se extraen datos biométricos usando técnicas de reconocimiento / extracción de biométrica facial o de otro tipo. Se pueden extraer asimismo otros datos, incluyendo imágenes de una firma, imágenes del usuario, otras imágenes, hologramas, perforaciones de láser, códigos de barras, códigos de QR, etc.

El dispositivo de cliente 102 determina entonces que la información de identidad extraída a partir del documento coincide sustancialmente con la información de identidad asociada con la cuenta del usuario (508) (por ejemplo, con el módulo de análisis de documentos 236). Por ejemplo, la información de identidad extraída (por ejemplo, el nombre extraído a partir de un permiso de conducir) se compara con la cuenta del usuario (por ejemplo, el nombre que el usuario proporcionó cuando se creó la cuenta) para confirmar que el documento está asociado con el titular de la cuenta (es decir, la información en los dos documentos coincide o coincide sustancialmente). Por lo tanto, si un usuario intenta cargar el permiso de conducir de alguna otra persona, el dispositivo de cliente 102-1 reconoce que el documento no está asociado con el usuario y puede rechazar el documento, reducir o ajustar una calificación de verificación para ese documento, marcar el documento, solicitar una información de corroboración o adicional, o emprender otras acciones correctivas.

En algunas implementaciones, el dispositivo de cliente 102-1 realiza una o más pruebas adicionales del documento (por ejemplo, con el módulo de análisis de documentos 236). Por ejemplo, en algunas implementaciones, el dispositivo de cliente 102-1 determina si un documento con fecha (por ejemplo, una factura de servicios públicos o cualquier otro documento que tenga una fecha de emisión, fecha de envío por correo, fecha de caducidad, fecha de vencimiento, etc.) se emitió dentro de un intervalo de antigüedad predeterminado con respecto a la fecha actual (por ejemplo, 30, 60 o 90 días, o cualquier otro intervalo apropiado). Como otro ejemplo, en algunas implementaciones, el dispositivo de cliente 102-1 identifica, a partir de los datos extraídos a partir del documento, una fecha de caducidad del documento, y determina si la fecha de caducidad del documento es posterior a una fecha actual (es decir, el documento

no ha caducado). En estos ejemplos, la fecha actual se puede determinar al hacer referencia a una fecha de sistema del dispositivo de cliente 102-1, o recurrir a un servicio o dispositivo remoto (por ejemplo, el servidor 104, un servicio de telecomunicaciones) y recibir una fecha actual. Tales pruebas pueden ayudar a garantizar que un usuario use, de hecho, documentos antiguos u obsoletos, lo que puede ser un indicador de que la información contenida en los mismos no es precisa. También se pueden realizar otras pruebas.

En algunas implementaciones, el dispositivo de cliente 102-1 determina si una fecha de sistema del dispositivo de cliente coincide sustancialmente con una fecha de referencia proporcionada por un dispositivo remoto. Esta prueba puede ayudar a identificar intentos de manipular indebidamente la fecha de sistema del dispositivo de cliente 102-1, lo que puede ser intentado por usuarios para posibilitar que los mismos carguen un documento que está desactualizado o ha caducado. Si la fecha de sistema del dispositivo de cliente no coincide sustancialmente con la fecha de referencia, se pueden tomar medidas correctivas. Por ejemplo, el dispositivo de cliente 102-1 y / o el servidor 104 evitarán que el usuario cargue el documento, ajuste una calificación de verificación para el documento, marque la cuenta del usuario para una revisión o escrutinio adicional, o similares.

En algunas implementaciones, si el documento cumple con los criterios de las pruebas adicionales, se permite que el documento se cargue en la cuenta del usuario y, si el documento no cumple con los criterios de las pruebas adicionales, el documento se rechaza y no se puede cargar en la cuenta del usuario. En otras implementaciones, el documento se carga en la cuenta del usuario independientemente de si se cumplen los criterios, pero la calificación de verificación (analizada posteriormente) se ajusta a o refleja de otro modo si se satisfacen, o no, los criterios (o el grado en el que se satisfacen los mismos).

El dispositivo de cliente 102-1 genera entonces al menos una calificación de verificación para el documento (510) (por ejemplo, con el módulo de calificación de verificación 238). La calificación de verificación, analizada con mayor detalle posteriormente, indica un grado de confianza de que el documento es auténtico y / o está realmente asociado con el usuario. En particular, la precisión de la verificación de identidad está limitada por el nivel de confianza que se puede depositar en la autenticidad de los documentos. Por ejemplo, no se puede confiar en que un permiso de conducir o pasaporte fraudulento identifique con precisión a la persona que lo está presentando. Por consiguiente, el dispositivo de cliente 102-1 realiza una o más pruebas sobre el documento (es decir, la imagen del documento) para determinar su autenticidad y si este identifica realmente al usuario. Un ejemplo específico de una prueba de este tipo es una comparación entre datos biométricos en una fotografía en el documento y datos biométricos en una fotografía del usuario capturada por el dispositivo de cliente 102-1, que es realizada por el módulo de análisis biométrico 234. Si se determina que una cara en la fotografía a partir del documento coincide con la fotografía del usuario recientemente capturada, existe una probabilidad más alta de que el permiso de conducir esté asociado con la persona en la fotografía, y la calificación de verificación reflejará esta confianza más alta (por ejemplo, con una calificación relativamente más alta). Por otro lado, si las caras no coinciden (o si las mismas coinciden en un grado menor), entonces la calificación de verificación reflejará esta confianza más baja (por ejemplo, con una calificación relativamente más baja).

En algunas implementaciones, las calificaciones de verificación son generadas solo por el dispositivo de cliente 102-1. Por lo tanto, los documentos, que contienen información de identidad sensible, no dejan de ser posesión del usuario. En algunas implementaciones, si se usan otros dispositivos para ayudar a generar calificaciones de verificación (por ejemplo, el servidor), cualquier información enviada a los otros dispositivos se cifra, se ofusca y / o se despoja de cualquier información de identificación, de tal modo que se mantienen la privacidad del usuario y la seguridad de los documentos.

En algunas implementaciones, el dispositivo de cliente 102-1 cifra el documento, los datos extraídos y la calificación de verificación (512) (por ejemplo, con el módulo de cifrado / carga 240). El dispositivo de cliente 102-1 envía entonces el documento, los datos extraídos y la calificación (por ejemplo, uno o más archivos de datos cifrados) al servidor 104 en la etapa (514) (por ejemplo, con el módulo de cifrado / carga 240).

En algunas implementaciones, el dispositivo de cliente 102-1 genera uno o más contenedores (es decir, contenedores), incluyendo cualquier combinación del documento, los datos extraídos y la calificación de verificación, y envía el contenedor o contenedores al servidor 104 en la etapa (514). En algunas implementaciones, los contenedores son colecciones de archivos individuales (por ejemplo, un archivo zip). En algunas implementaciones, los contenedores son estructuras de datos complejas que incluyen información a partir de la cual se pueden extraer o construir uno o más archivos y / o documentos diferentes (incluyendo, por ejemplo, una imagen de un documento, datos extraídos a partir de un documento y similares), incluso si los archivos y / o documentos no están representados en los contenedores como archivos discretos.

En algunas implementaciones, los uno o más contenedores incluyen al menos un primer archivo que incluye el documento y un segundo archivo que incluye la información extraída a partir del documento. En algunas implementaciones, los uno o más contenedores incluyen un tercer archivo que incluye la al menos una calificación de verificación. En algunas implementaciones, la al menos una calificación de verificación incluye una pluralidad de calificaciones de verificación (por ejemplo, incluyendo una calificación de verificación para cada documento en los uno o más contenedores, calificaciones de verificación compuestas, una puntuación de usuario, etc.) (cuando el

contenedor es un tipo de datos complejo, el contenedor incluye datos de los cuales se pueden extraer / construir tales archivos y / o información, como se ha analizado anteriormente).

En algunas implementaciones, el dispositivo de cliente 102-1 realiza las etapas (504) - (514), o un subconjunto de las mismas, para uno o más documentos adicionales. Por ejemplo, se capturan imágenes de múltiples documentos (504) y, para cada documento, el dispositivo de cliente 102-1 extrae datos (506), determina que la información de identidad coincide (508), genera una calificación de verificación (510), cifra el documento, la calificación y los datos extraídos (512), y envía estos elementos al servidor (514). En algunas implementaciones, estos documentos múltiples se combinan en el contenedor para su envío al servidor.

El servidor 104 recibe el documento, los datos extraídos y la calificación (516) (por ejemplo, con el módulo de recepción de información 342, figura 3). En algunas implementaciones, estos elementos se reciben como un contenedor, como se ha descrito anteriormente.

En algunas implementaciones, se asigna un estado a las cuentas de usuario, que refleja información particular acerca de la cuenta, y determina cómo se pueden usar la cuenta y / o la información y los documentos asociados con la cuenta. En algunas implementaciones, el estado de una cuenta refleja si la cuenta incluye una cantidad y / o tipo requerido de documentos e información de usuario, o si la cuenta es deficiente en una o más áreas. En algunas implementaciones, si la cuenta incluye los documentos y / o información requeridos, su estado es "completo" y, si la cuenta es deficiente de una o más formas, su estado es "pendiente". En diversas implementaciones, también se asignan a cuentas otros estados, y otras etiquetas para los estados descritos.

En algunos casos, una cuenta se considera "completa" si la misma incluye un documento de identificación con fotografía emitido por el gobierno y una factura de servicios públicos, así como un nombre y una dirección del usuario. En otras implementaciones, se requieren más o menos documentos o elementos de información con el fin de considerar completa una cuenta. Los documentos y / o información particulares que equivalen a una cuenta "completa" se determinan, en algunos casos, basándose en reglamentos, leyes, directrices o costumbres de una jurisdicción aplicable. En algunas implementaciones, la jurisdicción es una jurisdicción del titular de la cuenta, una jurisdicción de una institución o entidad que está solicitando los documentos / información, una jurisdicción que rige una transacción entre el titular de una cuenta y una institución o entidad solicitante, o cualquier otra jurisdicción o combinación de jurisdicciones apropiada.

En algunos casos, una cuenta se considera "pendiente" si la cuenta carece de documentos o elementos de información particulares que se requieren en una cuenta "completa". También se puede asignar un estado "pendiente" a una cuenta basándose en otras condiciones. Por ejemplo, una cuenta puede estar "pendiente" si un documento o elemento de información ha caducado o está, por lo demás, desactualizado. Como un ejemplo específico, si un pasaporte asociado con una cuenta de usuario caduca después de que este se cargue en la cuenta del usuario, se asigna un estado "pendiente" a la cuenta. Como otro ejemplo, si no hay una factura de servicios públicos reciente (por ejemplo, enviada por correo / emitida dentro de un plazo de 90 días con respecto a una fecha actual) asociada con la cuenta, se asigna un estado "pendiente" a la cuenta. En diversas implementaciones, otras condiciones también pueden hacer que se asigne un estado "pendiente" a una cuenta.

En algunas implementaciones, solo una cuenta "completa" puede ser usada por un usuario para compartir documentos con otras partes. Por lo tanto, si la cuenta de un usuario está "pendiente", el usuario ha de proporcionar la información o el documento o documentos faltantes, o realizar las pruebas requeridas (lo que se analizada en el presente documento) con el fin de completar la cuenta antes de que el usuario pueda autorizar a otras partes a acceder a sus documentos y / o información.

El análisis anterior describe cómo los usuarios crean cuentas y cargan documentos con el dispositivo de cliente 102-1. En particular, el dispositivo de cliente 102-1, junto con uno o más módulos en la memoria 218, realiza las etapas (502) a (514). Sin embargo, en algunos casos, otros usuarios del sistema pueden crear cuentas para otros usuarios. Por ejemplo, una institución puede decidir usar un proveedor de servicios para acceder a información de verificación de identidad para individuos u otras entidades con las que el banco realiza transacciones. Por consiguiente, la institución puede desear crear cuentas para algunos o todos los individuos para los cuales esta ya tiene información de identidad, documentos de identificación y similares. Por consiguiente, en algunas implementaciones, un dispositivo de empresa 108-1 incluye un módulo de generación de cuentas 329 para crear cuentas para múltiples usuarios. En particular, el dispositivo de empresa 108-1 usa el módulo de generación de cuentas 329 para realizar las etapas (502-m) a (514-m). Las etapas (502-m) a (514-m) son análogas a las etapas (502) a (514), y se realizan usando unos módulos análogos a los módulos del dispositivo de cliente 102-1 que realizan esas etapas en el dispositivo de cliente, como se ha descrito anteriormente (por ejemplo, incluyendo el módulo de extracción de datos 330, el módulo de análisis de documentos 332, el módulo de calificación de verificación 334 y el módulo de cifrado / carga 336, figura 3).

Aunque una institución puede crear una cuenta para un usuario, en algunas implementaciones, hasta que la cuenta está completa (es decir, contiene toda la información y / o documentos requeridos para establecer una cuenta completa), o hasta que el usuario ha aprobado la cuenta y la información y / o documentos asociados con la cuenta, se da un estado "pendiente" a la cuenta. Una vez que la institución y / o el usuario han completado la cuenta (por

ejemplo, al proporcionar cualquier información y / o documentos faltantes, y / o al aprobar información y / o documentos cargados por la institución), se da un estado "completo" a la cuenta.

En algunas implementaciones, las cuentas creadas para usuarios por una institución no se cargan en el proveedor de servicios (es decir, el servidor 104) hasta que el usuario asociado con la cuenta haya aprobado y / o completado la cuenta. De esta forma, el servidor 104 no necesita almacenar y / o gestionar cuentas incompletas y / o pendientes que nunca serán completadas y / o aprobadas por un usuario (por ejemplo, debido a que el usuario no desea o no necesita en modo alguno establecer la cuenta, o cualquier otra razón apropiada). En su lugar, la información de cuenta para tales cuentas se almacena en una memoria asociada con el dispositivo de empresa 108-1 (por ejemplo, la base de datos de información de usuario 346).

Pasando a la figura 5B, en implementaciones en donde el documento, la calificación de verificación y los datos extraídos no fueron cifrados por el dispositivo de cliente 102-1 (o el dispositivo de empresa 108-1) antes de enviarse al servidor 104, estos son cifrados por el servidor 104 para su almacenamiento (518) (por ejemplo, con el módulo de cifrado 428).

El servidor 104 almacena el documento, los datos extraídos y la calificación de verificación (520) (por ejemplo, en la base de datos de información de usuario 106). En algunas implementaciones, en donde la información se cifra en el dispositivo de cliente 102-1 antes de enviarse al servidor 104, el servidor 104 no es capaz de descifrar la información. Por consiguiente, se puede asegurar la privacidad y la seguridad de su información a los usuarios, al tiempo que se puede asegurar a las instituciones (y a otras entidades solicitantes) que la información no ha sido manipulada indebidamente o alterada de otro modo (o ni siquiera vista) por el proveedor de servicios.

Cuando una institución desea acceder a la documentación y / o información necesaria con el fin de verificar la identidad de un individuo, un operador usa el dispositivo de empresa 108-1 para solicitar información asociada con el individuo, y el dispositivo de empresa 108-1 recibe esta solicitud (522) (por ejemplo, con el módulo de gestión de solicitudes 340). En algunas implementaciones, el usuario solicita un conjunto particular de documentos e información (es decir, elementos de información distintos asociados con la cuenta de usuario). Por ejemplo, un banco puede solicitar información tal como el nombre del usuario, la dirección de residencia, el número de seguridad social (todo lo cual puede ser almacenado por el proveedor de servicios como parte de la información de cuenta del usuario), así como una imagen del permiso de conducir del usuario y una factura de servicios públicos reciente y calificaciones de verificación para esos documentos.

En algunas implementaciones, la solicitud incluye límites de acceso relacionados con el alcance del acceso que se va a conceder al solicitante, tales como un periodo de tiempo en el que se permitirá al solicitante acceder a la información, la cantidad de veces que se permitirá al solicitante acceder a la información, etc. En algunas implementaciones, el solicitante incluye tal información en su solicitud al servidor 104. Por ejemplo, un banco puede solicitar el permiso de conducir y una factura de servicios públicos reciente de un usuario, y especificar que este necesita acceder a esta información solo una vez. Como alternativa, un banco puede solicitar esta información y especificar que este necesita acceder a copias actualizadas de la misma en cualquier momento (y tantas veces como se desee) mientras la cuenta permanezca abierta y / o durante un periodo de tiempo especificado (por ejemplo, según sea especificado por un usuario). Se prevén asimismo otros límites de acceso o intervalos de tiempo (o cualquier otra restricción al acceso a la información) apropiados.

El dispositivo de empresa 108-1 envía entonces la solicitud de información al servidor 104 en la etapa (524) (por ejemplo, con el módulo de manejo de solicitudes 340).

El servidor 104 recibe la solicitud de información asociada con la cuenta del usuario (incluyendo la información al menos uno de un documento, datos extraídos a partir de un documento y al menos una calificación de verificación) a partir del dispositivo de empresa 108-1 en la etapa (526) (por ejemplo, con el módulo de gestión de solicitudes 430), y envía una solicitud al dispositivo de cliente 102-1 que solicita una autorización para divulgar la información solicitada al solicitante (528) (por ejemplo, con el módulo de gestión de solicitudes 430). En algunas implementaciones, el dispositivo de cliente 102-1 proporciona una notificación o alerta que indica que una solicitud se ha recibido o está disponible para verse. En algunas implementaciones, la notificación o alerta es o se incluye en un correo electrónico, mensaje de texto, alerta de aplicación o cualquier otro mensaje apropiado, usando cualquier protocolo o técnica de mensajería apropiado. En algunas implementaciones, el servidor 104 envía la notificación o alerta al dispositivo de cliente 102-1 antes de enviar la solicitud al dispositivo de cliente 102-1, y la solicitud se envía al dispositivo de cliente 102-1 una vez que el usuario ha iniciado sesión en su cuenta a través del dispositivo de cliente 102-1 (por ejemplo, en respuesta a la notificación o alerta).

El dispositivo de cliente 102-1 recibe la solicitud de autorización (530). El usuario inicia sesión de forma segura en el dispositivo de cliente y puede revisar entonces la solicitud. El dispositivo de cliente 102-1 indica entonces al usuario que autorice o deniegue parcial o totalmente el acceso a la información solicitada (por ejemplo, con el módulo de manejo de solicitudes 242). Si el dispositivo de cliente 102-1 recibe del usuario una autorización para permitir el acceso (532), este envía una autorización al servidor 104 para divulgar la información autorizada al solicitante (534, figura 5C) (por ejemplo, con el módulo de manejo de solicitudes 242). En algunas implementaciones, la solicitud de autorización

que se presenta a un usuario identifica información y / o documentos particulares que se solicitan. Además, en algunas implementaciones, la solicitud de autorización identifica los límites de acceso (o la carencia de los mismos) solicitados por el solicitante. Por ejemplo, como se ha descrito anteriormente, la solicitud puede indicar que un banco ha solicitado acceso al permiso de conducir del usuario y a una factura de servicios públicos, y que este desea poder ver (o descargar una copia actualizada de) los documentos en cualquier momento mientras el usuario tiene una cuenta con el banco, o durante cualquier otro tiempo especificado. Por lo tanto, el usuario puede determinar si permitir, o no, el acceso de acuerdo con la solicitud.

En algunas implementaciones, la información solicitada y / o los límites de acceso son innegociables. Por ejemplo, se puede requerir a un banco, por ley, que mantenga registros de cierta información de las entidades con las que este realiza transacciones. Por consiguiente, en el caso de que el usuario denegara el acceso a esa información, el banco será incapaz de tomar parte en la transacción en cuestión (por ejemplo, abrir una cuenta bancaria, una línea de crédito, etc.).

Por otro lado, en algunas implementaciones, la información solicitada y / o los límites de acceso son negociables y / o seleccionables por el usuario. Por ejemplo, un banco puede solicitar acceso a más información y / o menos límites de acceso de los estrictamente necesarios para una transacción o relación particular. El usuario se puede negar entonces a autorizar el alcance completo de la solicitud y, en su lugar, autorizar el acceso a menos, o diferentes, documentos o información, así como diferentes límites de acceso. En algunas implementaciones, se informa al usuario acerca de los requisitos de acceso mínimos necesarios para una transacción particular, de tal modo que el usuario pueda tomar una decisión informada con respecto a qué límites de acceso permitir.

En algunas implementaciones, una solicitud incluye múltiples paquetes de solicitud de autorización diferentes, incluyendo cada uno una combinación diferente de documentos, información y / o límites de acceso solicitados, y el usuario selecciona qué paquete de solicitud de autorización aprobar. También en el presente caso, se puede informar al usuario acerca de los requisitos de acceso de documentos mínimos necesarios para que la entidad solicitante pueda ser capaz de tomar parte en una transacción particular.

Continuando con la figura 5C, el servidor 104 recibe la autorización para divulgar la información al tercero (536) (por ejemplo, con el módulo de manejo de solicitudes 430).

El servidor 104 crea entonces un paquete de información que incluye la información solicitada (538) (por ejemplo, con el módulo de encapsulado / cifrado de información 432). Por ejemplo, el servidor 104 localiza los documentos solicitados, los datos extraídos, las calificaciones de verificación, etc., y, si es necesario, extrae / construye estos elementos a partir de un contenedor. El paquete de información es cualquier archivo, contenedor, archivo compuesto o grupo de archivos separados, que sea apropiado, que contenga la información solicitada.

En algunas implementaciones, el servidor 104 cifra el paquete de información (540) (por ejemplo, con el módulo de encapsulación / cifrado de información 432). En algunas implementaciones, la información que constituye el paquete de información ya está cifrada (por ejemplo, habiendo sido cifrada por el dispositivo de cliente 102-1, el servidor 104 o el dispositivo de empresa 108-1 antes de almacenarse en la base de datos de información de usuario 106). En algunas implementaciones, un cifrado basado en cliente solo se puede descifrar mediante una clave generada y / o conocida por el dispositivo de cliente 102-1. Por consiguiente, en algunas implementaciones, el servidor 104 no cifra el paquete de información en esta fase.

Sin embargo, en algunas implementaciones, el servidor 104 cifra de nuevo la información ya cifrada en la etapa (540). Este cifrado secundario se puede usar para habilitar y / o imponer límites de acceso al proporcionar una capa de cifrado que es controlada por el servidor 104. Por ejemplo, como se describe en el presente documento, el dispositivo de empresa 108-1 puede tener que recibir una autorización a partir del servidor 104 cada vez que este desea ver la información que recibe el mismo, incluso si la información se almacena localmente en el dispositivo de empresa 108-1. Por consiguiente, el dispositivo de empresa 108-1 se comunica con el servidor 104 con el fin de obtener los permisos (y / o códigos o claves de descifrado) necesarios antes de que este pueda acceder a la información.

Volviendo a la figura 5C, el servidor 104 envía el paquete de información al dispositivo de empresa 108-1 (542) (por ejemplo, con el módulo de encapsulado / cifrado de información 432). En algunas implementaciones en donde el servidor 104 cifró la información (540), el paquete de información se envía con una primera clave de descifrado que es capaz de descifrar el paquete de información. Por otro lado, en algunas implementaciones, la primera clave de descifrado no se incluye con el paquete de información, incluso si este fue cifrado por el servidor en (540). En tales casos, el dispositivo de empresa 108-1 recibe la clave de descifrado en un momento posterior, tal como cuando un operador del dispositivo de empresa intenta acceder a y / o ver la información.

El dispositivo de empresa 108-1 recibe el paquete de información y la primera clave de descifrado opcional (544) (por ejemplo, con el módulo de recepción de información 342). En algunas implementaciones, el dispositivo de empresa 108-1 almacena el paquete de información en una base de datos local 346, por ejemplo, para satisfacer reglamentos y requisitos de mantenimiento de registros. Incluso cuando la información se almacena en una base de datos local, en algunas implementaciones, el dispositivo de empresa 108-1 no puede ver la información sin comunicarse en primer

lugar con el servidor 104 para determinar si está permitido hacer esto, como se analiza en el presente documento.

Como se ha hecho notar anteriormente, si el usuario aprueba una solicitud de información, el dispositivo de cliente 102-1 envía un mensaje de autorización al servidor 104 (534). En algunas implementaciones, si el usuario aprueba la solicitud de información (o un subconjunto o superconjunto de la información), este también genera una segunda clave de descifrado para descifrar la información solicitada (546) (por ejemplo, con el módulo de cifrado / carga 240). En algunas implementaciones, la clave de descifrado se genera antes de recibir la solicitud de autorización.

En algunas implementaciones, el dispositivo de cliente 102-1 ha de generar la clave de descifrado, debido a que este es el único dispositivo que puede hacer tal cosa. De esa manera, ver el acceso a la información permanece bajo el control del usuario, y solo el usuario y las entidades autorizadas por el usuario pueden descifrar y ver la información.

El dispositivo de cliente 102-1 envía la segunda clave de descifrado al dispositivo de empresa 108-1 (por ejemplo, con el módulo de cifrado / carga 240). El dispositivo de empresa 108-1 recibe la segunda clave de descifrado (550) (por ejemplo, con el módulo de recepción de información 342).

El dispositivo de empresa 108-1 descifra entonces el paquete de información (552) (por ejemplo, con el módulo de seguridad / descifrado 344). En algunas implementaciones, descifrar la información incluye en primer lugar descifrar el paquete de información usando la primera clave de descifrado (para eliminar el cifrado aplicado por el servidor 104) y, entonces, descifrar la información contenida en el paquete de información con la segunda clave de descifrado (para eliminar el cifrado aplicado por el dispositivo de cliente 102-1).

Pasando a la figura 5D, el dispositivo de empresa 108-1 recibe, de un operador, una solicitud subsiguiente del paquete de información (554) (por ejemplo, con el módulo de gestión de solicitudes 338), y envía la solicitud subsiguiente del paquete de información al servidor 104 (556) (por ejemplo, con el módulo de gestión de solicitudes 338). En algunas implementaciones, la solicitud subsiguiente del paquete de información es una solicitud de toda la información que estaba en la solicitud original. En otras implementaciones, la solicitud subsiguiente incluye una solicitud de solo un subconjunto de la información en la solicitud original.

Además, las solicitudes también pueden especificar que la información debería incluir las versiones más actualizadas de la información solicitada. Por lo tanto, si el usuario ha cargado un nuevo permiso de conducir o factura de servicios públicos desde que previamente se recibió la información, se proporcionará la nueva información (dependiendo de los permisos de acceso asociados con la solicitud original). Por otro lado, la solicitud también puede especificar que la información debería incluir la información tal cual estaba la misma en el momento de la solicitud original. En algunas implementaciones, si se permite que una entidad solicitante acceda a versiones actualizadas de documentos e información (o si solo se permite que las mismas accedan a las versiones disponibles en el momento de la solicitud original) se especifica en los permisos de acceso analizados con respecto a las etapas (524) - (532).

El servidor 104 recibe la solicitud subsiguiente del paquete de información (558) (por ejemplo, con el módulo de manejo de solicitudes 430), y determina unos permisos de acceso (560) (por ejemplo, con el módulo de gestión de acceso 434). Por ejemplo, el servidor 104 determina si la solicitud subsiguiente es permitida por la autorización original del usuario. Los permisos de acceso incluyen permisos de contenido (por ejemplo, si se permite al solicitante acceder a un documento, calificación u otra información particular) y / o permisos de tiempo / frecuencia (por ejemplo, si la solicitud satisface un intervalo de tiempo y / o unos límites de frecuencia de acceso impuestos por el usuario).

Si se permite el acceso (562, Sí), entonces el servidor 104 proporciona acceso a la información solicitada (564). En algunas implementaciones, proporcionar acceso (564) incluye encapsular, cifrar y enviar la información solicitada al dispositivo de empresa 108-1 como en las etapas (538) - (544). En algunas implementaciones, proporcionar acceso (564) incluye proporcionar una clave de descifrado (u otro testigo de acceso) para posibilitar que el dispositivo de empresa 108-1 descifre o acceda de otro modo a información que ya ha sido almacenada por el dispositivo de empresa 108-1 (por ejemplo, en la base de datos de información de usuario 346). El dispositivo de empresa 108-1 accede entonces al paquete de información (566).

Si no se permite el acceso (563, No), entonces el servidor 104 deniega el acceso a la información solicitada (568) (por ejemplo, con el módulo de gestión de acceso 434).

Como se ha hecho notar anteriormente, se generan calificaciones de verificación para documentos obtenidos por el dispositivo de cliente 102-1 o por el dispositivo de empresa 108-1. Las calificaciones de verificación se basan en, se derivan de o reflejan de otro modo los resultados de una o más pruebas. Las calificaciones de verificación, en algunas implementaciones, indican el grado en el que un documento es auténtico y / o realmente se refiere a un usuario particular. Como un ejemplo, un documento que parece ser una falsificación tendrá probablemente una calificación más baja que un documento que no parece ser una falsificación. Como otro ejemplo, un documento que parece haber caducado probablemente tendrá una calificación más baja que uno que sigue siendo válido. Como otro ejemplo más, un documento que parece indicar una dirección que es diferente de la ubicación actual del usuario probablemente tendrá una calificación más baja que uno que tiene una dirección que cae en o cerca de la ubicación actual del usuario. Debido a que las calificaciones de verificación pueden reflejar los resultados de diversas pruebas y / o características

diferentes, las descripciones anteriores de cómo los resultados de prueba afectan a la calificación de verificación son meramente ilustrativas y no son necesariamente preceptivas con respecto a cómo cualquier calificación de verificación particular se verá afectada por los diversos resultados. Por ejemplo, un documento que tiene una alta probabilidad de ser una falsificación, pero toda la información en el documento es, por lo demás, correcta (por ejemplo, un nombre y una dirección en el documento coinciden con la información de cuenta del usuario, y una fotografía en el documento es una coincidencia biométrica con una fotografía del usuario) puede tener, en realidad, una calificación más alta que un documento que no parece fraudulento, pero incluye información que no coincide con la de la cuenta del usuario (por ejemplo, el nombre, la dirección y la información biométrica indica que el documento no está relacionado en absoluto con el usuario).

En algunas implementaciones, cada una de una pluralidad de pruebas realizadas en o para un documento da como resultado una calificación de verificación distinta, y todas las calificaciones de verificación para el documento se combinan para crear una calificación de verificación compuesta para el documento. La calificación de verificación compuesta se genera de cualquier forma apropiada, incluyendo el uso de un promedio (por ejemplo, una media aritmética, una media ponderada, etc.) de las calificaciones de verificación generadas por cada prueba de verificación respectiva, un algoritmo o cualquier otra combinación apropiada de calificaciones de verificación y / u otra información (por ejemplo, sumando los resultados de cada prueba).

Las calificaciones de verificación para cada prueba emplean cualquier escala de calificación o de puntuación apropiada. Por ejemplo, en algunas implementaciones, las calificaciones de verificación usan una escala numérica, tal como 1 - 100, 1 - 10, 1 - 5, o cualquier otro rango apropiado (por ejemplo, un rango de calificación literal, tal como A - F, A - Z, etc.). Tales escalas se usan para pruebas que producen un rango de resultados y / o indican un nivel o grado de satisfacción de uno o más criterios. Como un ejemplo específico, una prueba que determina el grado en el que una fotografía extraída a partir de un documento coincide con una fotografía de referencia de un usuario se puede calificar usando una escala (por ejemplo, basándose en el algoritmo de coincidencia, una calificación de un 100 % indica una coincidencia buena, un 70 % indica una coincidencia parcial, un 0 % indica una probabilidad de coincidencia baja o nula).

En algunas implementaciones, las calificaciones de verificación son binarias o de "aprobado / suspenso" (lo que se puede indicar de cualquier forma, tal como con una marca de verificación o un círculo de color verde para un aprobado, y una "X" o un círculo de color rojo para un suspenso). En tales casos, si se asigna una calificación de aprobado o de suspenso a un documento se basa en una o más pruebas cualesquiera del documento y / o sus contenidos. En el presente documento se describen algunos ejemplos específicos de pruebas.

En algunas implementaciones, las pruebas dan como resultado tanto una calificación de "aprobado / suspenso" como una calificación numérica (por ejemplo, entre 1 y 100). En algunas implementaciones, si una prueba da como resultado una calificación de aprobado o de suspenso se basa en la calificación numérica (por ejemplo, menos de 50 de 100 da como resultado un suspenso).

Además, en algunas implementaciones, se generan calificaciones de verificación compuestas para los documentos. La calificación de verificación compuesta se basa al menos parcialmente en una pluralidad de calificaciones de verificación a partir de una pluralidad de pruebas (como se describe en el presente documento). Se crean calificaciones de verificación compuestas a partir de cualquier combinación apropiada de las calificaciones de verificación a partir de pruebas individuales. Por ejemplo, una calificación de verificación compuesta puede ser un promedio de calificaciones de verificación individuales, o una calificación aditiva (por ejemplo, cada calificación individual se basa en una escala de 0 - 10, y la calificación compuesta es la suma de todas las calificaciones individuales).

En algunas implementaciones, se genera una "puntuación de usuario" para la cuenta de un usuario, basándose al menos en parte en las calificaciones de verificación (y / o calificaciones de verificación compuestas) de los documentos asociados con un usuario. En algunas implementaciones, la puntuación de usuario se basa también, o en su lugar, en otra información, tal como la completitud de una cuenta de usuario, verificaciones / corroboraciones de identidad de terceros, etc.

En algunas implementaciones, la puntuación de usuario también refleja los diversos tipos de documentos que han sido proporcionados por un usuario. Por ejemplo, si un usuario proporciona documentos que no fueron emitidos por un gobierno (por ejemplo, facturas de servicios públicos, tarjetas de identificación de estudiante, tarjetas de crédito, etc.), la puntuación de usuario será menor que si el usuario ha proporcionado documentos emitidos por el gobierno (por ejemplo, un pasaporte, un permiso de conducir, etc.).

Como se ha hecho notar anteriormente, se pueden aplicar diversas pruebas en diversas implementaciones para generar calificaciones de verificación. Posteriormente se analizan algunas pruebas ilustrativas. Cada prueba puede afectar a la calificación de verificación de diversas formas. Por ejemplo, algunas pruebas dan como resultado un análisis cualitativo de un documento, tal como un valor de confianza, un valor de calidad, una calificación o similar. En tales casos, las calificaciones de verificación se pueden basar al menos parcialmente en, y / o reflejar, los resultados del análisis cualitativo. Por ejemplo, en algunas implementaciones, una calificación de verificación se ajusta a escala basándose en los resultados del análisis cualitativo, de tal modo que un resultado más bajo reduce la calificación de

verificación para un documento y un resultado más alto aumenta (o no afecta a) la calificación de verificación.

Algunas pruebas dan como resultado un resultado cuantitativo y / o discreto, tal como si se determina, o no, una coincidencia, si se halla, o no, un resultado esperado, o similar. De forma similar, en algunos casos, se comparan resultados de análisis cualitativo frente a condiciones umbral, lo que produce un resultado discreto (por ejemplo, la condición umbral o bien se satisface, o bien no se satisface). En algunas implementaciones, unos resultados discretos reducen y / o aumentan una calificación de verificación, dependiendo del resultado (por ejemplo, una prueba fallida reduce una calificación de verificación en una cantidad predeterminada). En algunas implementaciones, unos resultados discretos actúan como un umbral para la aceptación del documento. Por ejemplo, si un documento no satisface un umbral particular (por ejemplo, una marca de agua esperada está ausente), el documento se rechaza y no se proporciona calificación de verificación alguna para el documento (por ejemplo, debido a que es probable que el documento sea fraudulento).

Las pruebas descritas en el presente documento se pueden combinar de cualquier forma apropiada. Por ejemplo, en algunas implementaciones, algunas pruebas se usan para generar una calificación de verificación numérica, mientras que otras se usan para determinar si aceptar o rechazar un documento (por ejemplo, unas condiciones de aprobado / suspenso). Además, a veces se describen calificaciones de verificación para documentos como que se "basan en" los resultados de una o más de las siguientes pruebas. Tal como se usa en el presente documento, "basándose en" significa "basándose exclusivamente en" (es decir, basándose solo en) o "basándose al menos parcialmente en".

Confirmación de dirección

En algunas implementaciones, la información de residencia y / o dirección extraída a partir de documentos se compara con información de ubicación del usuario. En particular, con el fin de confirmar que un usuario reside realmente en la dirección mostrada en un documento, la dirección a partir del documento se compara con la ubicación actual del dispositivo del usuario (por ejemplo, según sea determinado por GPS, triangulación por torres de célula, geolocalización de dirección de IP, o similares). En tales casos, la calificación de verificación del documento se basa, al menos parcialmente, en si, o en el grado en el que, la dirección coincide con la ubicación actual del dispositivo del usuario.

Se pueden usar diferentes niveles de precisión para la confirmación de dirección, dependiendo de la aplicación o caso de uso particular. Por ejemplo, en algunos casos, se desea determinar el país de residencia de un usuario. Por consiguiente, no es necesario que la dirección del usuario coincida exactamente con la ubicación actual del usuario. Más bien, es suficiente que la ubicación actual del usuario esté en cualquier lugar dentro del país identificado por la dirección del usuario. En otros casos, se desea determinar que el usuario vive realmente en la ubicación identificada por la dirección del usuario. En tales casos, es necesario determinar que la ubicación actual del usuario está a no más de una distancia predeterminada de la dirección del usuario, de tal modo que es probable que el usuario viva realmente en esa dirección. Por ejemplo, en algunas implementaciones, se determina que la ubicación actual de un usuario coincide con una supuesta dirección si la ubicación actual está a no más de 30,48 m (100 pies) de una ubicación asociada con la dirección del usuario (por ejemplo, valores de latitud y de longitud asociados con la dirección). También se contemplan otras distancias (por ejemplo, 152,4 m (500 pies), 304,8 m (1000 pies), 1,609 km (1 milla), 8,047 km (5 millas), 16,093 km (10 millas) o cualquier otra distancia apropiada).

Además de comparar la ubicación real del usuario con la ubicación a partir de un documento determinado, en algunas implementaciones, una puntuación de usuario se basa en la coherencia de las direcciones de múltiples documentos de un usuario. En particular, si todos los documentos del usuario están asociados con una misma ubicación (por ejemplo, una misma dirección, ciudad, estado, región, país, etc.), la puntuación de usuario será más alta. Además, en algunas implementaciones, las calificaciones de verificación de documentos individuales reflejan si la dirección de ese documento coincide con direcciones de otros documentos. Por ejemplo, si el pasaporte y el permiso de conducir de un usuario especifican una dirección, y la factura de servicios públicos de un usuario especifica una dirección diferente, entonces la calificación de verificación para la factura de servicios públicos (y / o el pasaporte o el permiso de conducir) reflejará la discrepancia (por ejemplo, al bajar la calificación para ese documento o rechazar por completo ese documento). En algunas implementaciones, el dispositivo de cliente 102-1 también consulta una dirección asociada con el usuario en una base de datos separada con el fin de comparar la misma con una dirección en uno o más documentos y / o una ubicación actual del dispositivo de cliente 102-1. Por ejemplo, el dispositivo de cliente 102-1 recupera una dirección para un usuario a partir de una base de datos de puntuaciones de crédito, a partir de recursos de direcciones en línea (por ejemplo, páginas amarillas o blancas), a partir de un portal de redes sociales, etc.

La figura 6 es un diagrama de flujo que ilustra un método 600 para verificar un documento basándose en la ubicación actual del usuario, de acuerdo con algunas implementaciones. Cada una de las operaciones mostradas en la figura 6 puede corresponder a instrucciones almacenadas en una memoria informática o medio de almacenamiento legible por ordenador. En algunas implementaciones, las etapas se realizan en un dispositivo electrónico con uno o más procesadores (o núcleos) y memoria que almacena uno o más programas para su ejecución por los uno o más procesadores (o núcleos). Por ejemplo, en algunas implementaciones, las etapas se realizan en cualquiera (o en cualquier combinación) del dispositivo de cliente 102-1, el servidor 104 y el dispositivo de empresa 108-1. Además, las etapas individuales del método se pueden distribuir entre los múltiples dispositivos electrónicos de cualquier forma

apropiada.

El dispositivo de cliente 102-1 obtiene un documento (602) (por ejemplo, con el módulo de dispositivo de captura de imágenes 226). Anteriormente se han analizado detalles adicionales relacionados con la obtención de documentos con respecto a la etapa (504) de la figura 5A.

El dispositivo de cliente 102-1 extrae datos a partir del documento, incluyendo los datos extraídos una información de ubicación extraída (604) (por ejemplo, con el módulo de extracción de datos 232). La información de ubicación extraída incluye, por ejemplo, una dirección incluida en el documento (por ejemplo, una etiqueta de envío por correo, un campo de dirección de un documento de identificación, etc.), información de país de residencia (por ejemplo, extraída a partir de un permiso de conducir o número de pasaporte o código de país, etc.) y similares.

El dispositivo de cliente 102-1 determina una ubicación actual del dispositivo de cliente (606) (por ejemplo, con el módulo de sistema de determinación de posición 228). En algunas implementaciones, la ubicación actual del dispositivo del usuario se determina usando GPS, triangulación por torres de célula, geolocalización de dirección de IP o similares.

El dispositivo de cliente 102-1 compara la ubicación actual del dispositivo de cliente con la información de ubicación extraída (608) (por ejemplo, con el módulo de análisis de documentos). El dispositivo de cliente 102-1 determina un grado en el que la ubicación actual del dispositivo de cliente coincide con la información de ubicación extraída (610) (por ejemplo, con el módulo de análisis de documentos).

En algunas implementaciones, como se ha descrito anteriormente, el grado en el que la ubicación actual del dispositivo de cliente coincide con la información de ubicación extraída es un resultado de aprobado / suspenso: si la ubicación actual está a no más de una distancia predeterminada de la información de ubicación extraída, se determina que las ubicaciones coinciden; si la ubicación actual está más allá de la distancia predeterminada, se determina que las ubicaciones no coinciden. Asimismo, la resolución de la información de ubicación extraída se selecciona de acuerdo con la aplicación particular. Por ejemplo, en algunos casos, solo es necesario o se desea determinar que el usuario está en el estado, región o país indicado por una dirección extraída a partir de un documento. En otros casos, es necesario o se desea determinar que el usuario está a no más de una distancia predeterminada de la dirección real extraída a partir del documento.

En algunas implementaciones, el dispositivo de cliente 102-1 genera una calificación de verificación basándose en el grado en el que la ubicación actual del dispositivo de cliente coincide con la información de ubicación extraída (612) (por ejemplo, con el módulo de calificación de verificación 238). En algunas implementaciones, en lugar (o además) de determinar el grado en el que la ubicación actual del dispositivo de cliente coincide con la información de ubicación extraída, el dispositivo de cliente 1021 determina el grado en el que un registro histórico de ubicaciones del dispositivo de cliente 102-1 coincide con la información de ubicación extraída. Por ejemplo, el dispositivo de cliente 102-1 indica a un usuario que permita el acceso a información de ubicación histórica (por ejemplo, durante un cierto periodo de tiempo, tal como 1 año) y, si el usuario permite el acceso, el dispositivo de cliente 102-1 determina cuánto tiempo o con qué frecuencia el dispositivo de cliente 102-1 estuvo en o cerca de la ubicación identificada por la información de ubicación extraída, y genera o ajusta la calificación de verificación basándose en ello.

En algunas implementaciones, el dispositivo de cliente 102-1 genera una calificación de verificación basándose en el grado en el que la ubicación actual del dispositivo de cliente coincide con un conjunto histórico de información de ubicación extraída (por ejemplo, el grado en el que la ubicación actual coincide con la información de dirección extraída a partir de una pluralidad de documentos previamente cargados).

Comparación de fotografías

Los documentos que incluyen fotografías (por ejemplo, permisos de conducir, pasaportes, tarjetas de identificación con fotografía emitidas por el gobierno, etc.) se analizan para determinar si la fotografía en el documento coincide con una fotografía del usuario. En algunas implementaciones, un usuario proporciona una o más fotografías de referencia de sí mismo. Las fotografías de referencia pueden ser capturadas por un dispositivo de formación de imágenes asociado con un dispositivo de cliente (por ejemplo, una cámara de teléfono inteligente, una cámara web o un escáner acoplado a un ordenador, etc.), o cargarse en el dispositivo de cliente (por ejemplo, recibirse como un archivo de imagen digital de alguna otra forma). En algunas implementaciones, se capturan fotografías de referencia desde diferentes ángulos, con diferentes expresiones faciales y con diferente iluminación, con el fin de aumentar la calidad del análisis fotográfico.

La fotografía a partir del documento se compara entonces con la fotografía o fotografías de referencia para determinar si las mismas coinciden sustancialmente. La comparación usa técnicas de reconocimiento facial, tales como comparar, entre la fotografía a partir del documento y la biométrica de fotografía de referencia, información tal como: la estructura, la forma y las proporciones de la cara; la ubicación absoluta y / o relativa de la nariz y de los ojos; la distancia entre los ojos, la nariz, la boca y la mandíbula; los contornos superiores de las cuencas oculares; los lados de la boca; y el área que rodea el pómulo. Se extrae información biométrica a partir de la fotografía de documento y la fotografía de

referencia.

En algunas implementaciones, el usuario captura una fotografía que incluye tanto su cara como el documento que contiene una fotografía. La cara del usuario se compara entonces con la fotografía en el documento usando una o más de las técnicas anteriores (o una técnica no enumerada) para determinar si la fotografía coincide con el usuario, y la calificación de verificación se basa, al menos en parte, en un grado de coincidencia entre la información biométrica a partir de la fotografía del usuario y la información biométrica a partir de la fotografía de referencia.

En algunas implementaciones, se calcula el valor de confianza de que los individuos en ambas fotografías son iguales basándose en una o más técnicas de análisis fotográfico, incluyendo, pero sin limitarse a, las enumeradas anteriormente. En algunas implementaciones, el valor de confianza se refleja en una calificación de verificación para un documento que contiene la fotografía.

En algunas implementaciones, se capturan múltiples fotografías de referencia de un usuario. Por ejemplo, se puede pedir a un cliente que capture fotografías de sí mismo desde diferentes ángulos, bajo diferentes condiciones de iluminación, con o sin gafas u otras obstrucciones, con diferentes expresiones faciales o similares. En algunas implementaciones, un dispositivo guía al usuario a través del proceso de obtención de un cierto conjunto de fotografías, por ejemplo, usando indicaciones visuales y / o de audio (por ejemplo, mostrando imágenes o gráficos de fotografías ilustrativas, etc.).

En algunas implementaciones, con el fin de facilitar la comparación entre fotografías, un dispositivo incluye componentes y / o módulos de aplicación para realizar técnicas de formación de imágenes, tales como rectificación de imágenes, creación / cálculo de mapas de profundidad, cálculo de reflectividad, y similares.

Análisis de características de seguridad

Algunos documentos incluyen características de seguridad tales como marcas de agua, hologramas, fotos / imágenes fantasma, tintas ópticamente variables, y / o pigmentos que son sensibles y / o reflejan ciertos tipos de iluminación y / o radiación. Por ejemplo, muchos documentos de identificación con fotografía emitidos por el gobierno (por ejemplo, permisos de conducir, pasaportes, etc.) incluyen tales características de seguridad. Con el fin de detectar y / o capturar una fotografía adecuada de estos elementos, es necesario exponer los documentos a tipos apropiados de radiación mientras se captura la fotografía. En algunas implementaciones, se indica a los usuarios que capturen una o más fotografías de tales documentos mientras se expone a un tipo particular de radiación o fuente de radiación.

En algunas implementaciones, los usuarios capturan una imagen de un documento mientras se expone el documento a una fuente de radiación infrarroja (por ejemplo, un control remoto para un televisor, un equipo estéreo, un reproductor de DVD o similar). En algunas implementaciones, los usuarios capturan una imagen de un documento mientras exponen el documento a una fuente de radiación ultravioleta (por ejemplo, bombillas de luz diurna ultravioleta, linternas de luz ultravioleta, "luces negras", etc.).

Para documentos que incluyen hologramas, los usuarios capturan una serie de fotografías o un vídeo corto mientras el flash de una cámara está encendido (por ejemplo, un flash incorporado con una cámara de teléfono celular). En algunas implementaciones, el flash es controlado (por ejemplo, por un módulo de aplicación) de tal modo que se usan diferentes salidas de flash para diferentes fotografías. Los valores de reflectividad para el holograma a través de la serie de fotografías o vídeos cortos se analizan para determinar que los mismos satisfacen una condición particular (por ejemplo, que la diferencia en la reflectividad entre unas imágenes dadas se ajusta sustancialmente a un valor esperado).

Algunos documentos incluyen texto y / o imágenes que se han de ver a través de un filtro de polarización con el fin de analizarse con éxito. En tales casos, los usuarios capturan una imagen del documento a través de un filtro de polarización, tal como gafas de sol polarizadas o un filtro fotográfico polarizado.

Algunos documentos incluyen perforaciones de láser. Con el fin de detectar tales perforaciones (que a menudo son tan pequeñas que las mismas no se pueden detectar cuando el documento está iluminado frontalmente), el usuario captura una fotografía del documento en condiciones de retroiluminación (por ejemplo, sostenido a la altura de una bombilla) de tal modo que se pueden detectar las perforaciones de láser. Las perforaciones de láser se analizan entonces para determinar su calidad y / o si estas coinciden con un patrón o contenido esperado. En algunas implementaciones, el contenido esperado de una perforación de láser depende de la autoridad emisora del documento (por ejemplo, el país que emitió un pasaporte).

Algunas características de seguridad no requieren radiación y / o iluminación especial para un análisis fotográfico preciso, tal como una impresión en iris y / o guilloché. En algunas implementaciones, un usuario captura una fotografía de un documento que incluye una impresión en iris y / o guilloché, y se analiza la impresión para determinar su presencia y / o calidad. En algunas implementaciones, la calidad de una impresión en iris y / o guilloché se basa en la resolución, los colores, los detalles, la forma o el tamaño de la impresión, o si esta coincide con un patrón y / o contenido esperado (y / o cualquier otra métrica apropiada). En algunas implementaciones, las calificaciones de

verificación se basan en y / o reflejan la calidad y / o presencia de las características de seguridad descritas anteriormente.

Comparación de zonas

Algunos documentos incluyen múltiples zonas diferentes, en donde una zona incluye la misma información, y / o un subconjunto de esta, en otras una o más zonas. Por ejemplo, los pasaportes incluyen una "zona visual" y una "zona legible por máquina". La "zona visual" enumera cierta información, tal como el nombre, la dirección, el número de pasaporte y similares del usuario en un formato que es fácilmente legible por un ser humano. La "zona legible por máquina" incluye información tal como el nombre, el número de pasaporte, la fecha de nacimiento, el país, etc., del usuario, en un formato que es fácilmente legible por una máquina.

En algunas implementaciones, se analizan fotografías de documentos que tienen múltiples zonas para determinar si coincide la información en las diversas zonas. Por ejemplo, un usuario captura una fotografía de un documento que incluye múltiples zonas. Se realiza entonces un reconocimiento óptico de caracteres ("OCR") (usando cualquier técnica de OCR adecuada) en todas o un subconjunto de las zonas (por ejemplo, la "zona visual" y la "zona legible por máquina" de un pasaporte), y se compara la información contenida en las zonas. En algunas implementaciones, las calificaciones de verificación se basan en y / o reflejan el grado en el que coincide una información en cada una de las múltiples zonas.

En algunas implementaciones, una "zona legible por máquina" incluye un código de barras u otro contenido basado en caracteres no alfanuméricos y, por lo tanto, no es adecuado para las técnicas de OCR. En tales casos, el contenido de la "zona legible por máquina" se analiza usando cualquier técnica apropiada, tal como descodificar un código de barras usando técnicas de lectura de código apropiadas.

Pruebas de presencia de documento

Algunas pruebas están diseñadas para confirmar que el usuario está en presencia del documento real en cuestión. Por ejemplo, un usuario captura una serie de fotografías de diferentes páginas de un documento (por ejemplo, un pasaporte) dentro de un determinado plazo de tiempo. Proporcionar con éxito las imágenes solicitadas de las páginas solicitadas dentro del plazo de tiempo corrobora que el usuario está en presencia del documento real.

Como otro ejemplo, un usuario captura una fotografía del usuario sosteniendo el documento frente a un espejo. Como otro ejemplo más, un usuario captura una grabación de vídeo que muestra al usuario sosteniendo el documento. Como otro ejemplo más, un usuario captura una fotografía de un sello que es el más reciente en un pasaporte. La capacidad del usuario para proporcionar tales imágenes / vídeos corrobora que el usuario está en presencia del documento real (por ejemplo, en contraposición a una copia del documento o solo una única página del documento).

Como otro ejemplo más, se indica al usuario que capture fotografías de un documento de acuerdo con ciertos criterios. Específicamente, se indica al usuario que capture fotografías de un documento en ciertas orientaciones, posiciones, ángulos y similares. La capacidad del usuario para capturar las imágenes solicitadas sugiere si el usuario está en presencia del documento real.

En algunas implementaciones, se muestra una retícula en el visor de un dispositivo de formación de imágenes (por ejemplo, en una pantalla de un teléfono inteligente o cámara digital) que especifica una orientación del documento. El usuario ha de capturar entonces una imagen de acuerdo con la orientación especificada. Por ejemplo, la retícula es un trapecio, y el usuario debe orientar el documento y / o la cámara de tal modo que el documento se ajuste y / o coincida sustancialmente con la forma de la retícula. En algunas implementaciones, las orientaciones, posiciones o ángulos específicos solicitados se determinan de una manera pseudoaleatoria, de tal modo que un usuario no puede predecir fácilmente qué fotografías se solicitarán.

En algunas implementaciones, un usuario captura fotografías de documentos en papel contra una superficie sustancialmente transparente (por ejemplo, una ventana de vidrio). Para documentos de papel, la luz que ilumina la superficie posterior hace que el documento parezca traslúcido, permitiendo que cualquier impresión o contenido en la parte posterior de la página se vuelva al menos parcialmente visible. Por consiguiente, la fotografía se analiza para determinar el contenido y / o la calidad del contenido en la superficie posterior del documento (es decir, la superficie del documento que está contra la superficie transparente), y / o para evaluar el nivel, la consistencia o la calidad de traslucidez del propio papel.

Pruebas de confirmación de parte emisora

Algunas pruebas confirman si un documento particular incorpora o incluye parámetros o patrones esperados de un documento emitido por una parte emisora particular. Por ejemplo, los números de pasaporte para un determinado país se pueden ajustar a un patrón detectable. Si los parámetros o patrones no coinciden con los esperados (por ejemplo, basándose en información notifica por el propio usuario o basándose en otra información extraída a partir del documento), entonces se puede sospechar de la autenticidad del documento.

En algunas implementaciones, un usuario captura una fotografía de las páginas centrales de un pasaporte, y el patrón de enhebrado de la encuadernación de pasaporte (visible en las páginas centrales) se compara con un patrón de enhebrado conocido para el supuesto país o parte / jurisdicción emisora del pasaporte.

En algunas implementaciones, un usuario captura una fotografía de una porción de un documento que contiene un identificador único (por ejemplo, un número de pasaporte, un número de permiso de conducir, etc.), y el número se compara con un patrón conocido para el supuesto país, estado o parte / jurisdicción emisora del documento.

Análisis de profundidad

En algunas implementaciones, también se usa un análisis tridimensional de un documento (y / o un documento junto con otros uno o más objetos) para determinar que el documento es auténtico. Por ejemplo, en algunas implementaciones, un usuario captura varias fotografías de punto de vista direccional de un documento. Como otro ejemplo, un usuario captura una o más fotografías de un documento con objetos extraños colocados sobre el mismo. Las calificaciones de verificación para estos documentos reflejan un cálculo de profundidad basándose en técnicas de rectificación de imágenes.

Pruebas de rasgos físicos

Algunos documentos están hechos de materiales que tienen propiedades únicas. Por ejemplo, los permisos de conducir están hechos, habitualmente, de un plástico o material compuesto que tiene una cierta rigidez y / o resistencia a la flexión. Por consiguiente, algunas pruebas están diseñadas para determinar si es probable que el documento esté hecho de un material esperado. Específicamente, en algunas implementaciones, un usuario captura una fotografía en la que este está doblando un documento (por ejemplo, un permiso de conducir). La fotografía se puede analizar para determinar si el documento cumple con una curvatura esperada, o parece, por lo demás, estar hecho de un material esperado (por ejemplo, una tarjeta de plástico en lugar de una cédula de papel).

Pruebas de corroboración de información

En algunas implementaciones, una calificación de verificación para un documento también se basa en si, o en el grado en el que, una información a partir del documento coincide con una información a partir de otra fuente. Por ejemplo, como se ha hecho notar anteriormente, la otra fuente de información puede ser información introducida por el usuario (por ejemplo, información proporcionada por un usuario durante un proceso de inscripción de cuenta). En algunas implementaciones, la otra fuente de información es otro documento. Por ejemplo, una calificación de verificación para un permiso de conducir se basa, al menos en parte, en el grado en el que la información en el permiso de conducir coincide con información extraída a partir de un pasaporte.

Como un ejemplo específico, ciertos permisos de conducir se emiten tanto con una tarjeta de plástico como con una cédula de papel (por ejemplo, los permisos de conducir en el Reino Unido y la Unión Europea). En estos casos, la calificación de verificación para un permiso de conducir se basa en si, o en el grado en el que, la información en la tarjeta de plástico coincide con la información en la cédula de papel. Además, para tales documentos en dos partes, la calificación de verificación también se basa en si se puede proporcionar, o no, la cédula de papel. En algunas implementaciones, no se proporciona calificación de verificación alguna para tal documento si no se puede fotografiar la segunda parte del documento.

Comparación de firma

En algunas implementaciones, se requiere o se solicita que los usuarios firmen documentos antes de capturar fotografías de los mismos. Tales firmas se comparan entonces con una firma de referencia asociada con el usuario. La calificación de verificación se basa entonces en si, o en el grado en el que, la firma coincide con la firma de referencia. Unas firmas de referencia son, por ejemplo, proporcionadas por el usuario durante un proceso de inscripción de cuenta (por ejemplo, son introducidas por un usuario a través de una pantalla táctil o dispositivo de entrada de panel táctil), o son extraídas a partir de otro documento (por ejemplo, un permiso de conducir, un pasaporte, etc.). En algunas implementaciones, los documentos que se han de firmar incluyen facturas de servicios públicos.

En algunas implementaciones, se captura un vídeo de un usuario que firma un documento. El vídeo se analiza entonces para determinar si el usuario firmó el documento dentro de un plazo de tiempo aceptable (por ejemplo, menos de 5 segundos, o cualquier otro plazo de tiempo apropiado), y si la firma resultante coincide suficientemente con una firma de referencia. Esto puede ayudar a detectar firmas fraudulentas o falsificadas, debido a que puede ser difícil que un usuario produzca rápidamente una falsificación convincente.

Revisión por terceros

En algunas implementaciones, terceros pueden verificar y / o corroborar información y / o documentos de otros usuarios. Por ejemplo, notarios, abogados u otros individuos autorizados pueden revisar información presentada por

un usuario y proporcionar un análisis y / u opinión acerca de los documentos y / o el usuario. En algunas implementaciones, tal análisis y / u opinión se refleja en una calificación de verificación de un documento o una puntuación de usuario. En otras implementaciones, este es independiente de una calificación de verificación o puntuación de usuario (por ejemplo, este es una indicación separada de que la cuenta ha sido verificada por un tercero). En algunas implementaciones, al tercero se le proporcionan unas versiones físicas de documentos para su revisión (por ejemplo, al tercero se le entregan copias u originales).

En algunas implementaciones, los terceros son otros usuarios del servicio que corroboran personalmente las notificaciones de identidad de otros usuarios. Por ejemplo, un primer usuario que conoce personalmente a un segundo usuario puede corroborar la identidad del segundo usuario, lo que puede aumentar una calificación de verificación y / o puntuación de usuario del segundo usuario, o aparecer como una indicación separada de que la cuenta ha sido corroborada por otro usuario. En algunas implementaciones, la calificación o calificaciones de verificación, el estado de cuenta y / o la puntuación de usuario del primer usuario se ven afectados si los usuarios y / o cuentas que estos corroboran resultan estar falsificados o ser fraudulentos, o son sospechosos de alguna otra forma. Por ejemplo, se puede reducir una puntuación de usuario del usuario que corrobora, su cuenta se puede degradar a un estado "pendiente" o su cuenta puede ser rechazada por completo por el proveedor de servicios.

Asimismo, cuando la corroboración por un primer usuario afecta a una calificación de verificación o puntuación de usuario de un segundo usuario, las calificaciones de verificación y / o el historial de corroboración del primer usuario pueden afectar a la cantidad en la que se cambia la calificación de verificación o puntuación de usuario del segundo usuario. Por ejemplo, si un usuario con una puntuación de usuario alta (el primer usuario) corrobora la identidad del segundo usuario, la puntuación del segundo usuario se puede aumentar más de lo que lo sería si el primer usuario tuviera una puntuación de usuario más baja.

Cualquiera de las pruebas descritas anteriormente se puede realizar en cualquier dispositivo apropiado, dependiendo de la implementación. Por ejemplo, en algunas implementaciones, estas se realizan en un dispositivo de cliente 102-1 (por ejemplo, como parte de un proceso de carga de documentos realizado por un usuario). En algunas implementaciones, estas se realizan en un dispositivo de empresa 108-1 (por ejemplo, como parte de un proceso de generación de cuentas realizado en nombre de individuos por una institución, usando documentos que ya están en posesión de la institución). En algunas implementaciones, estas se realizan en un servidor 104 (por ejemplo, después de que las mismas hayan sido cargadas por un dispositivo de cliente 102-n o un dispositivo de empresa 108-n).

No todas las pruebas descritas anteriormente se aplican necesariamente a todos los documentos. Más bien, un experto en la materia reconocerá que algunas pruebas no son aplicables a ciertos documentos o tipos de documentos. Por ejemplo, una prueba de comparación de fotografías (por ejemplo, comparar una fotografía a partir de un documento con una fotografía de referencia de un usuario) no sería de aplicación a documentos que no incluyan fotografías del usuario. De forma similar, las pruebas de análisis de hologramas no serían de aplicación a documentos que no incluyan hologramas. En algunas implementaciones, las pruebas que se pueden realizar en un documento particular dependen del tipo de documento.

Además, no todas las pruebas que son adecuadas para un documento particular se realizan necesariamente en ese documento. Más bien, en algunas implementaciones, cuando se carga un documento, se selecciona un cierto subconjunto de las pruebas adecuadas para ese documento. Entonces se indica al usuario que capture las fotografías y / o imágenes requeridas para las pruebas seleccionadas.

En algunas implementaciones, cuando se obtiene de un usuario un documento, el subconjunto de pruebas se selecciona de una forma pseudoaleatoria, de tal modo que es difícil para un usuario predecir qué pruebas se requerirán para un documento particular. Por consiguiente, es más difícil para los usuarios crear u obtener documentos fraudulentos (o capturar fotografías de los documentos de alguna otra persona) con antelación si estos no pueden predecir qué fotografías particulares se les indicará capturar y / o qué análisis se realizará en el documento.

En algunas implementaciones, un usuario puede aumentar la calificación de verificación para un documento particular al elegir realizar una o más pruebas adicionales. La calificación de verificación se ajusta entonces basándose en los resultados de las pruebas adicionales. Específicamente, si los resultados son positivos (por ejemplo, soportan la validez y / o autenticidad del documento), se aumenta la calificación de verificación. Por otro lado, si los resultados son negativos (por ejemplo, refutan la validez y / o autenticidad del documento), se disminuye la calificación de verificación.

En algunas implementaciones, el número de pruebas realizadas en un documento se refleja y / o se incluye en la propia calificación de verificación. Por ejemplo, un documento puede ser apto para 10 pruebas diferentes, y los resultados de cada prueba se puntúan en una escala de 0 - 10. Por lo tanto, si un documento se somete a 3 pruebas y recibe un resultado perfecto para cada prueba, la calificación de verificación global es de 30, de un 100 posible. Someter el documento a pruebas adicionales puede aumentar entonces la calificación de verificación, dependiendo de los resultados de esas pruebas.

Por otro lado, en algunas implementaciones, el número de pruebas realizadas en un documento se refleja por separado

de la calificación de verificación. Por ejemplo, una calificación de verificación para un documento puede ser un cierto valor (por ejemplo, un 80 %) basándose en los resultados de un cierto número de pruebas (por ejemplo, un 3 de un 10 posible), y el número de pruebas se notifica por separado de la calificación de verificación. Por lo tanto, en este ejemplo, la calificación de un 80 % refleja un resultado combinado de las 3 pruebas que se realizaron (por ejemplo, una calificación promedio), y no indica el número de pruebas que se realizaron.

Para cualquiera de las pruebas descritas anteriormente, a los usuarios se les indican instrucciones paso a paso, ejemplos, imágenes de muestra y / o cualquier otra información para ayudar a completar con éxito las pruebas solicitadas. Asimismo, cualquier análisis usado en cualquiera de las pruebas descritas anteriormente puede ser completamente automático (sin intervención humana), completamente manual o una combinación de automático y manual. Un análisis de reconocimiento facial, por ejemplo, puede ser realizado por un ordenador (por ejemplo, usando un algoritmo de reconocimiento y / o comparación facial), o por un ser humano (por ejemplo, un operador humano que revisa una fotografía de referencia y una fotografía de documento y que determina si las mismas coinciden). En algunas implementaciones, un operador humano revisa los resultados de un proceso de análisis automático para confirmar, rechazar y / o modificar los resultados del análisis.

Los métodos ilustrados en las figuras 5A - 6 se pueden regir por instrucciones que se almacenan en un medio de almacenamiento legible por ordenador y que son ejecutadas por al menos un procesador de al menos un dispositivo electrónico (por ejemplo, uno o más dispositivos de cliente 102-n, uno o más dispositivos de empresa 108-n, o un servidor 104). Cada una de las operaciones mostradas en las figuras 5A - 6 puede corresponder a instrucciones almacenadas en una memoria informática o medio de almacenamiento legible por ordenador no transitorio. En diversas implementaciones, el medio de almacenamiento legible por ordenador no transitorio incluye un dispositivo de almacenamiento de disco magnético u óptico, dispositivos de almacenamiento de estado sólido, tales como memoria Flash u otro dispositivo o dispositivos de memoria no volátil. Las instrucciones legibles por ordenador almacenadas en el medio de almacenamiento legible por ordenador no transitorio pueden estar en código fuente, código de lenguaje ensamblador, código objeto u otro formato de instrucciones que sea interpretado y / o ejecutable por uno o más procesadores (o núcleos).

Se puede proporcionar una pluralidad de instancias para los componentes, operaciones o estructuras descritos en el presente documento como una única instancia. Por último, los límites entre diversos componentes, operaciones y almacenes de datos son un tanto arbitrarios, y se ilustran operaciones particulares en el contexto de configuraciones ilustrativas específicas. En general, las estructuras y la funcionalidad presentadas como componentes separados en las configuraciones de ejemplo se pueden implementar como una estructura o componente combinado. De forma similar, las estructuras y la funcionalidad presentadas como un único componente se pueden implementar como componentes separados.

Se apreciará también que, aunque los términos "primero", "segundo", etc., se pueden usar en el presente documento para describir diversos elementos, estos elementos no deberían estar limitados por estos términos. Estos términos solo se usan para distinguir un elemento de otro. Por ejemplo, un primer contacto se podría denominar un segundo contacto y, de forma similar, un segundo contacto se podría denominar un primer contacto, sin cambiar el significado de la descripción, siempre que se cambien de nombre coherentemente todas las apariciones del "primer contacto" y siempre que se cambien de nombre coherentemente todas las apariciones del segundo contacto. Tanto el primer contacto como el segundo contacto son contactos, pero no son el mismo contacto.

La terminología usada en el presente documento es únicamente para el fin de describir implementaciones particulares y no se pretende que limite las reivindicaciones. Como se usa en la descripción de las implementaciones y las reivindicaciones adjuntas, se pretende que las formas singulares "un", "una" y "el / la" incluyan asimismo las formas plurales, a menos que el contexto indique claramente lo contrario. También se ha de entender que la expresión "y / o" usada en el presente documento se refiere a, y abarca, cualesquiera y todas las combinaciones posibles de uno o más de los elementos enumerados asociados. Se entenderá adicionalmente que los términos "comprende" y / o "comprendiendo / que comprende", cuando se usan en la presente memoria descriptiva, especifican la presencia de características, elementos integrantes, etapas, operaciones, elementos y / o componentes indicados, pero no excluyen la presencia o adición de otras una o más características, elementos integrantes, etapas, operaciones, elementos, componentes y / o grupos de los mismos.

Como se usa en el presente documento, se puede interpretar que el término "si" significa "cuando" o "al" o "en respuesta a determinar" o "de acuerdo con una determinación de" o "en respuesta a detectar", que un precedente de condición establecida es verdadero, dependiendo del contexto. De forma similar, se puede interpretar que la frase "si se determina (que un precedente de condición establecida es verdadero)" o "si (un precedente de condición establecida es verdadero)" o "cuando (un precedente de condición establecida es verdadero)" significa "al determinar" o "en respuesta a determinar" o "de acuerdo con una determinación de" o "al detectar" o "en respuesta a detectar" que el precedente de condición establecida es verdadero, dependiendo del contexto.

La descripción anterior incluía sistemas, métodos, técnicas, secuencias de instrucciones y productos de programas de máquina informática ilustrativos que materializan implementaciones ilustrativas. Para fines de explicación, se expusieron numerosos detalles específicos con el fin de proporcionar una comprensión de diversas implementaciones

de la materia objeto inventiva. Sin embargo, será evidente para los expertos en la materia que las implementaciones de la materia objeto inventiva se pueden poner en práctica sin estos detalles específicos. En general, no se han mostrado con detalle instancias, protocolos, estructuras y técnicas bien conocidos.

La descripción anterior, con fines de la explicación, se ha descrito con referencia a implementaciones específicas. Sin embargo, no se pretende que los análisis ilustrativos anteriores sean exhaustivos o que limiten las implementaciones a las formas precisas divulgadas. A la vista de las enseñanzas anteriores, son posibles muchas modificaciones y variaciones, dentro del alcance de las reivindicaciones adjuntas. Las implementaciones se eligieron y describieron con el fin de explicar del mejor modo los principios y sus aplicaciones prácticas, para posibilitar de ese modo que otros expertos en la materia utilicen del mejor modo las implementaciones y diversas implementaciones con diversas modificaciones según sean adecuadas para el uso particular contemplado.

**REIVINDICACIONES**

1. Un método para autorizar una divulgación de información de identidad, que comprende:

en un dispositivo de cliente (102-1, 102-n) con uno o más procesadores y memoria que almacena uno o más programas para su ejecución por los uno o más procesadores:

obtener información de identidad de un usuario;

obtener un documento;

extraer datos a partir del documento, incluyendo los datos extraídos una información de identidad extraída;

determinar que la información de identidad del usuario y la información de identidad extraída coinciden sustancialmente;

generar al menos una calificación de verificación para el documento, en donde la calificación de verificación se basa, al menos en parte, en un grado de coincidencia entre la información de identidad del usuario y la información de identidad extraída; y

enviar el documento, los datos extraídos a partir del documento y la al menos una calificación de verificación a un sistema de servidor (104) remoto con respecto al dispositivo de cliente (102-1, 102-n) para su almacenamiento en uno o más contenedores cifrados;

en el sistema de servidor (104) con uno o más procesadores de servidor y memoria de servidor que almacena uno o más programas de servidor para su ejecución por los uno o más procesadores de servidor:

almacenar el documento, los datos extraídos a partir del documento y la al menos una calificación de verificación en asociación con una cuenta del usuario, en donde al menos uno del documento, los datos extraídos a partir del documento y la al menos una calificación de verificación se almacena en los uno o más contenedores cifrados;

en un dispositivo de empresa (108-1, 108n) distinto tanto del dispositivo de cliente (102-1, 102-n) como del sistema de servidor (104):

recibir, de un operador, una solicitud de información asociada con la cuenta del usuario, incluyendo la información al menos uno del documento, los datos extraídos a partir del documento y la al menos una calificación de verificación; y
enviar la solicitud de la información asociada con la cuenta del usuario al sistema de servidor (104);

en el sistema de servidor (104)

recibir, del dispositivo de empresa (108-1, 108n), la solicitud de información asociada con la cuenta del usuario; y

enviar una solicitud al dispositivo de cliente que solicita una autorización para divulgar la información al dispositivo de empresa (108-1, 108n);

en el dispositivo de cliente (102-1, 102-n):

recibir la solicitud que solicita una autorización para divulgar la información asociada con la cuenta del usuario; recibir, del usuario, una autorización de la solicitud;

enviar una autorización al sistema de servidor (104) para divulgar la información al dispositivo de empresa (108-1, 108-n) para almacenar la información en el dispositivo de empresa (108-1, 108n);

generar una clave de descifrado; y

enviar, al dispositivo de empresa (108-1, 108n), la clave de descifrado;

en el sistema de servidor (104):

en respuesta a recibir, del dispositivo de cliente, la autorización para divulgar la información al dispositivo de empresa (108-1, 108n), enviar la información al dispositivo de empresa (108-1, 108n)

en el dispositivo de empresa (108-1, 108n):

recibir, del servidor (104), la información divulgada;

recibir, del dispositivo de cliente (102-1, 102-n), la clave de descifrado;

y

descifrar la información divulgada recibida.

2. El método de la reivindicación 1,

en donde la al menos una calificación de verificación comprende una pluralidad de calificaciones de verificación, en particular una calificación de verificación compuesta para el documento, en donde la calificación de verificación compuesta se basa al menos parcialmente en cada una de la pluralidad de calificaciones de verificación.

3. El método de cualquiera de las reivindicaciones 1 - 2, que comprende adicionalmente generar los uno o más contenedores cifrados, en particular como un único archivo, en el dispositivo de cliente (102-1, 102-n).

4. El método de la reivindicación 3, en donde los uno o más contenedores cifrados incluyen al menos un primer archivo que incluye el documento y un segundo archivo que incluye la información extraída a partir del documento, en particular en donde los uno o más contenedores cifrados incluyen un tercer archivo que incluye la al menos una calificación de verificación.

5. El método de cualquiera de las reivindicaciones 1 - 4, que comprende adicionalmente, en el dispositivo de cliente (102-1, 102-n):

obtener uno o más documentos adicionales; y

para cada uno respectivo de los uno o más documentos adicionales:

extraer datos a partir del documento respectivo;

generar al menos una calificación de verificación respectiva para el documento respectivo;

enviar el documento respectivo, los datos extraídos a partir del documento respectivo y la al menos una calificación de verificación respectiva al sistema de servidor (104).

6. El método de la reivindicación 5, que comprende adicionalmente, en el dispositivo de cliente (102-1, 102-n):

generar una puntuación de usuario para la cuenta de usuario basándose al menos en parte en:

la al menos una calificación de verificación para el documento; y

la al menos una calificación de verificación respectiva para cada uno de los uno o más documentos adicionales.

7. El método de cualquiera de las reivindicaciones 1 - 6, en donde la solicitud de información asociada con la cuenta del usuario identifica uno o más elementos de información distintos asociados con la cuenta de usuario, en particular en donde la solicitud de información asociada con la cuenta del usuario especifica uno o más límites de acceso solicitados para la información.

8. El método de la reivindicación 7, en donde la autorización para divulgar la información al dispositivo de empresa (108-1, 108n) incluye uno o más límites de acceso, especificados por el usuario, para la información.

9. El método de cualquiera de las reivindicaciones 7 - 8, en donde los uno o más límites de acceso se seleccionan de entre el grupo que consiste en: un límite a un número de veces que el dispositivo de empresa (108-1, 108n) puede acceder a la información; y un límite a la duración en la que el dispositivo de empresa (108-1, 108n) puede acceder a la información.

10. El método de cualquiera de las reivindicaciones 1 - 9, en donde obtener el documento incluye capturar una imagen del documento con una de una cámara o un escáner, y / o

en donde el dispositivo de cliente (102-1, 102-n) es un dispositivo de comunicación móvil, en particular un teléfono móvil; un ordenador portátil; un ordenador de escritorio; y un ordenador de tipo tableta y en donde obtener el documento incluye capturar una imagen del documento con una cámara asociada con el dispositivo de comunicación móvil.

11. El método de cualquiera de las reivindicaciones 1 - 10, en donde generar la al menos una calificación de verificación incluye:

capturar una fotografía de un usuario;

extraer una fotografía de referencia a partir del documento;

extraer información biométrica a partir de la fotografía del usuario;

extraer información biométrica a partir de la fotografía de referencia; y

generar la al menos una calificación de verificación basándose al menos en parte en un grado de coincidencia entre la información biométrica a partir de la fotografía del usuario y la información biométrica a partir de la fotografía de referencia.

12. El método de cualquiera de las reivindicaciones 1 - 11, en donde extraer los datos a partir del documento incluye al menos uno de realizar un reconocimiento óptico de caracteres en el documento y

extraer datos biométricos a partir de una fotografía contenida en el documento y

extraer una firma a partir de una fotografía contenida en el documento.

13. El método de cualquiera de las reivindicaciones 1 - 12, en donde obtener la información de identidad del usuario incluye obtener información de cuenta asociada con el usuario, en donde la información de cuenta asociada con el usuario se obtiene durante un proceso de inscripción de cuenta, y / u

obtener una firma del usuario; y / o

en donde la información de identidad se selecciona de entre uno o más del grupo que consiste en: un nombre de usuario; una dirección; un número de seguridad social; una fecha de nacimiento; una biométrica de huella dactilar; una biométrica facial; un código postal; y un número de cuenta.

14. El método de cualquiera de las reivindicaciones 1 - 13, que comprende adicionalmente, en el dispositivo de cliente (102-1, 102-n):

antes de generar la al menos una calificación de verificación para el documento:

identificar, a partir de los datos extraídos a partir del documento, una fecha del documento; y

(i) determinar que la fecha extraída del documento es posterior a una fecha actual, y / o

determinar que la fecha extraída del documento está dentro de un intervalo de antigüedad predeterminado, en donde el intervalo de antigüedad se determina de acuerdo con una fecha actual.

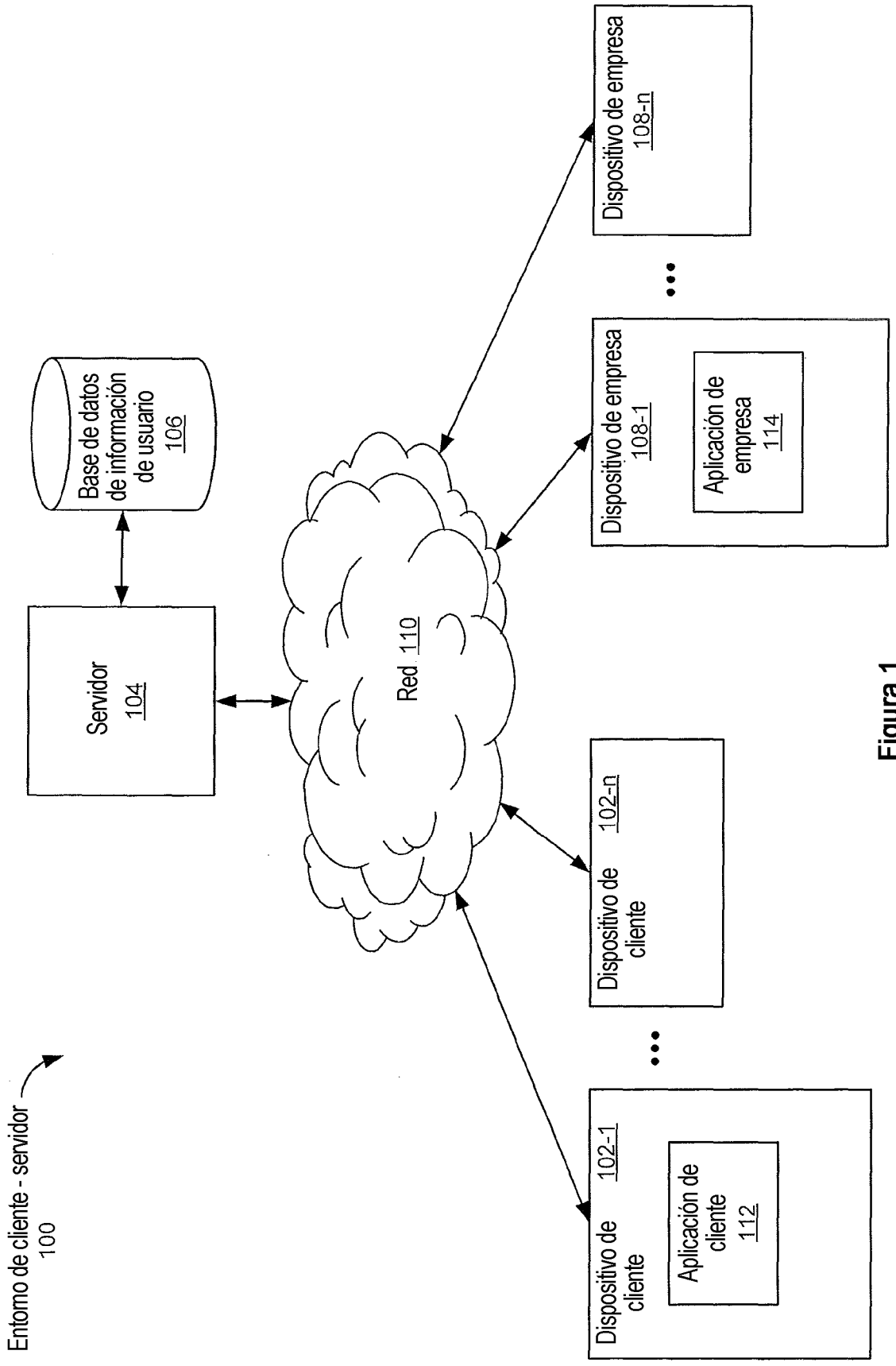
Entorno de cliente - servidor
100
Base de datos de información de usuario
106
Servidor
104
Red 110
Dispositivo de empresa
108-n
Dispositivo de empresa
108-1
Aplicación de empresa
114
Dispositivo de cliente
102-n
Dispositivo de cliente
102-1
Aplicación de cliente
112

Figura 1

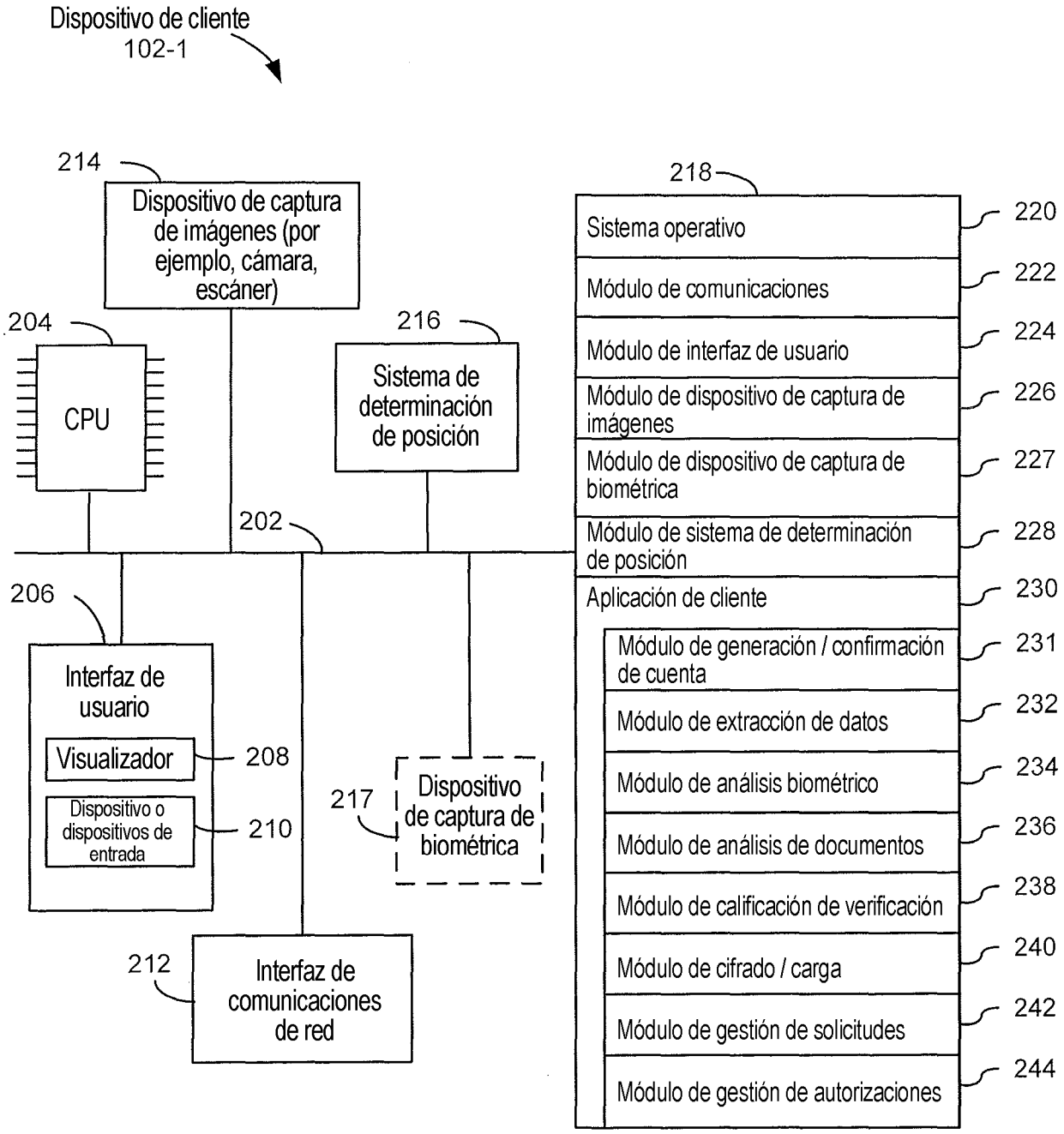
Dispositivo de cliente
102-1
214
Dispositivo de captura de imágenes (por ejemplo, cámara, escáner)
204
CPU
216
Sistema de determinación de posición
202
206
Interfaz de usuario
Visualizador
208
Dispositivo o dispositivos de entrada
210
217
Dispositivo de captura de biométrica
212
Interfaz de comunicaciones de red
218
Sistema operativo
220
Módulo de comunicaciones
222
Módulo de interfaz de usuario
224
Módulo de dispositivo de captura de imágenes
226
Módulo de dispositivo de captura de biométrica
227
Módulo de sistema de determinación de posición
228
Aplicación de cliente
230
Módulo de generación / confirmación de cuenta
231
Módulo de extracción de datos
232
Módulo de análisis biométrico
234
Módulo de análisis de documentos
236
Módulo de calificación de verificación
238
Módulo de cifrado / carga
240
Módulo de gestión de solicitudes
242
Módulo de gestión de autorizaciones
244

**Figura 2**

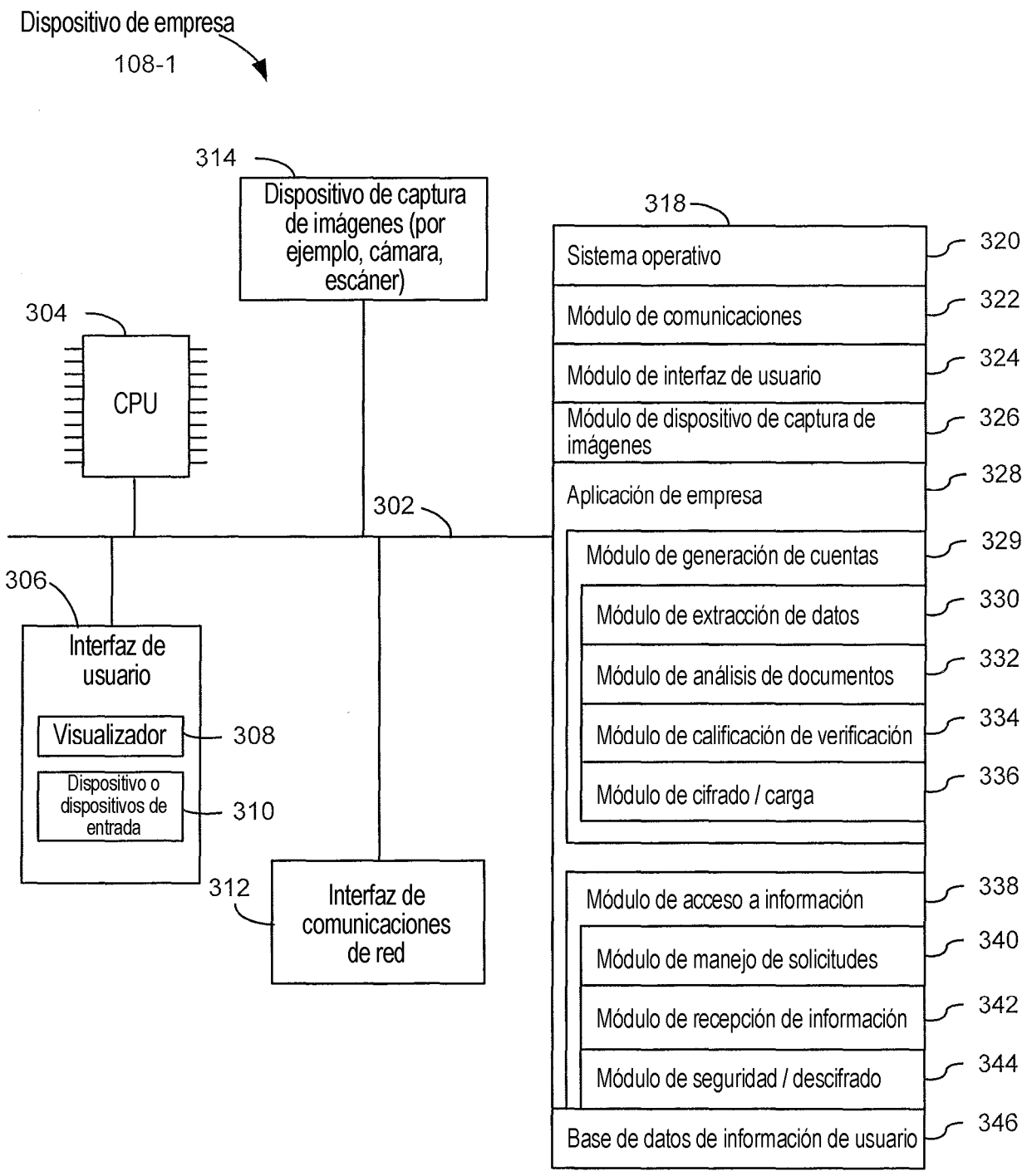
Dispositivo de empresa
108-1
314
Dispositivo de captura de imágenes (por ejemplo, cámara, escáner)
304
CPU
302
306
Interfaz de usuario
Visualizador
308
Dispositivo o dispositivos de entrada
310
312
Interfaz de comunicaciones de red
318
Sistema operativo
320
Módulo de comunicaciones
322
Módulo de interfaz de usuario
324
Módulo de dispositivo de captura de imágenes
326
Aplicación de empresa
328
Módulo de generación de cuentas
329
Módulo de extracción de datos
330
Módulo de análisis de documentos
332
Módulo de calificación de verificación
334
Módulo de cifrado / carga
336
Módulo de acceso a información
338
Módulo de manejo de solicitudes
340
Módulo de recepción de información
342
Módulo de seguridad / descifrado
344
Base de datos de información de usuario
346

**Figura 3**

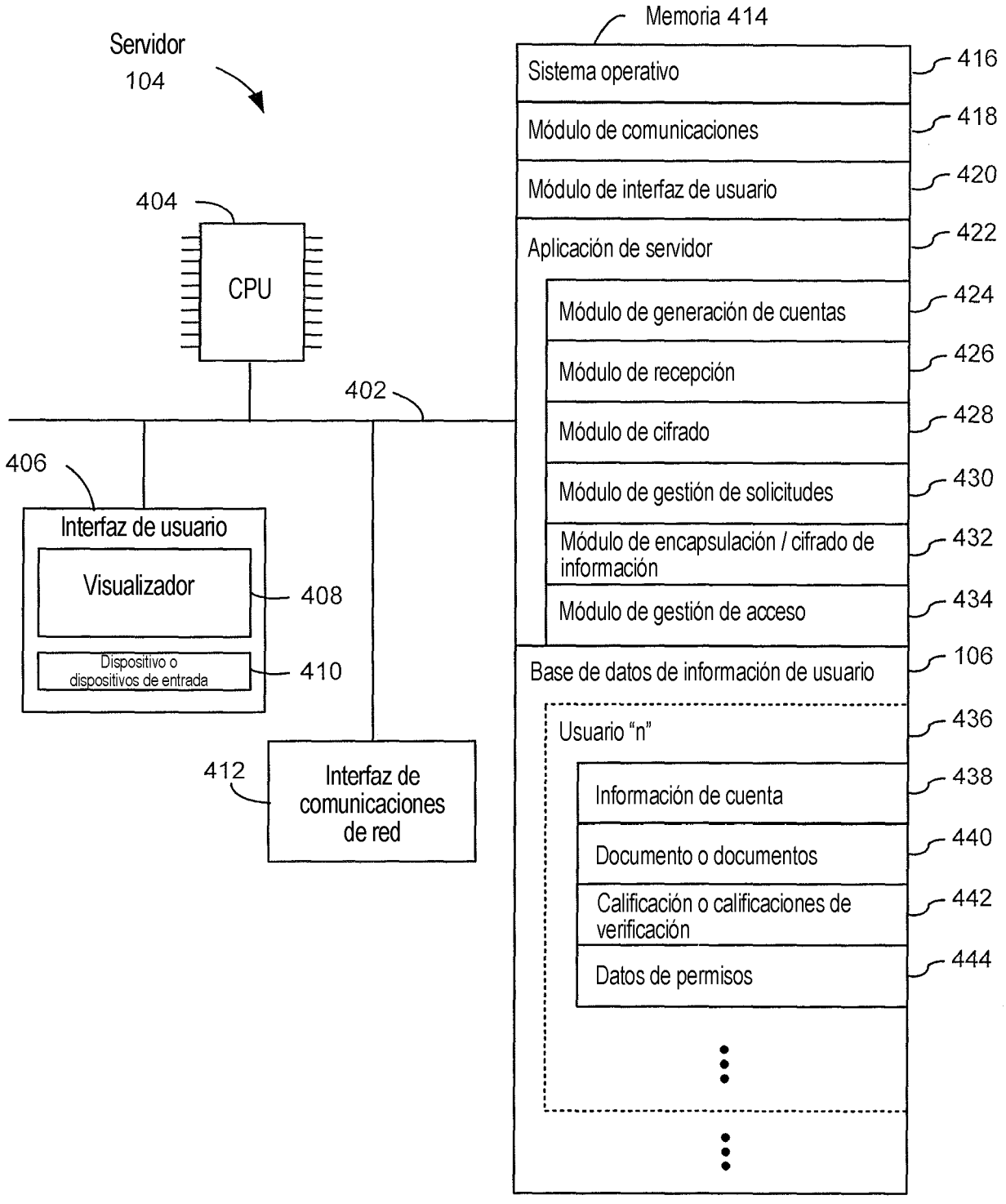
Servidor
104
404
CPU
402
406
Interfaz de usuario
Visualizador
408
Dispositivo o dispositivos de entrada
410
412
Interfaz de comunicaciones de red
Memoria 414
Sistema operativo
416
Módulo de comunicaciones
418
Módulo de interfaz de usuario
420
Aplicación de servidor
422
Módulo de generación de cuentas
424
Módulo de recepción
426
Módulo de cifrado
428
Módulo de gestión de solicitudes
430
Módulo de encapsulación / cifrado de información
432
Módulo de gestión de acceso
434
Base de datos de información de usuario
106
Usuario "n"
436
Información de cuenta
438
Documento o documentos
440
Calificación o calificaciones de verificación
442
Datos de permisos
444

**Figura 4**

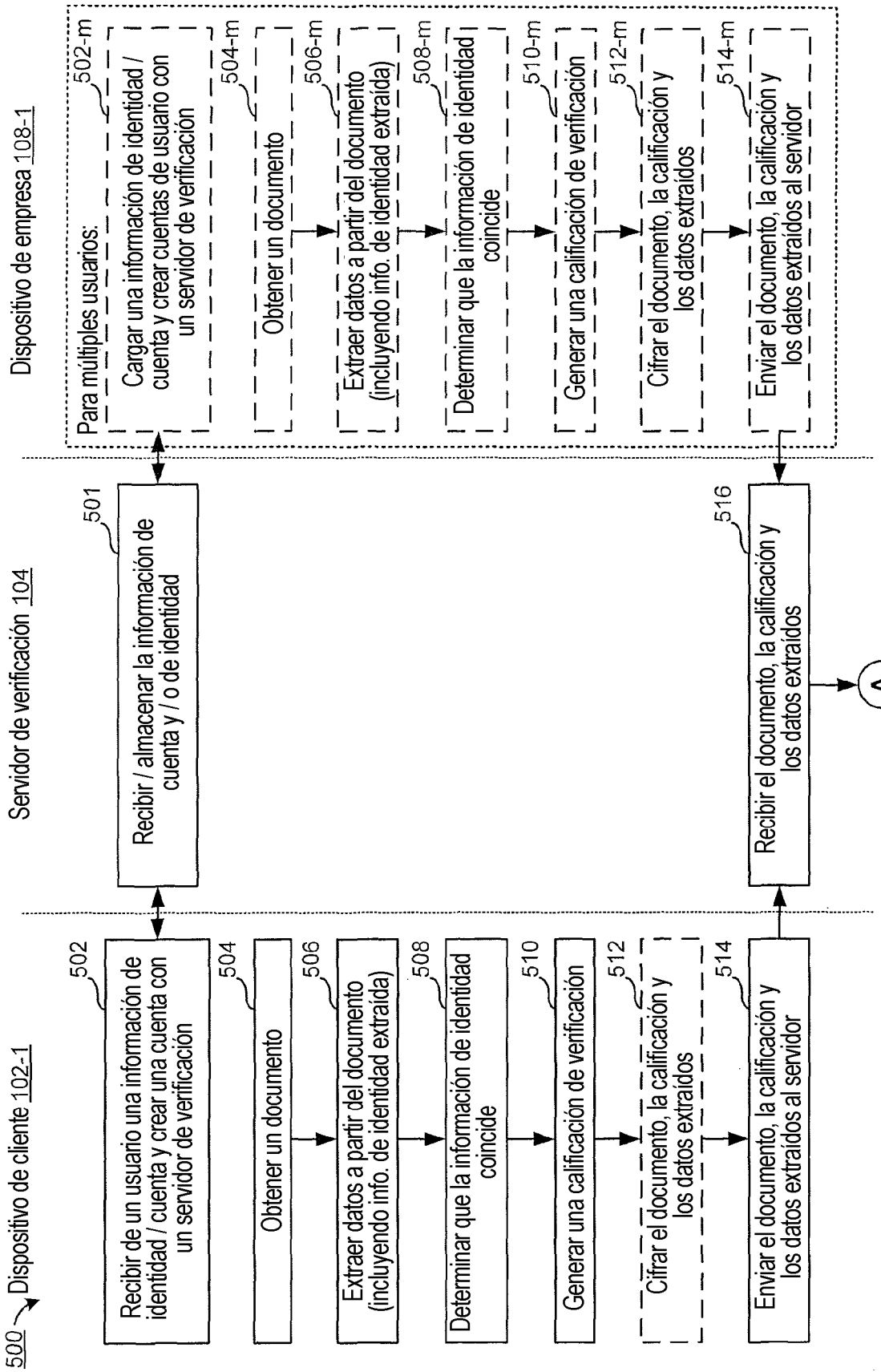
500
Dispositivo de cliente 102-1
Servidor de verificación 104
Dispositivo de empresa 108-1
Recibir de un usuario una información de identidad / cuenta y crear una cuenta con un servidor de verificación
502
Obtener un documento
504
Extraer datos a partir del documento (incluyendo info. de identidad extraida)
506
Determinar que la información de identidad coincide
508
Generar una calificación de verificación
510
Cifrar el documento, la calificación y los datos extraídos
512
Enviar el documento, la calificación y los datos extraídos al servidor
514
Recibir / almacenar la información de cuenta y / o de identidad
501
Recibir el documento, la calificación y los datos extraídos
516
A
Para múltiples usuarios:
Cargar una información de identidad / cuenta y crear cuentas de usuario con un servidor de verificación
502-m
Obtener un documento
504-m
Extraer datos a partir del documento (incluyendo info. de identidad extraida)
506-m
Determinar que la información de identidad coincide
508-m
Generar una calificación de verificación
510-m
Cifrar el documento, la calificación y los datos extraídos
512-m
Enviar el documento, la calificación y los datos extraídos al servidor
514-m

Figura 5A

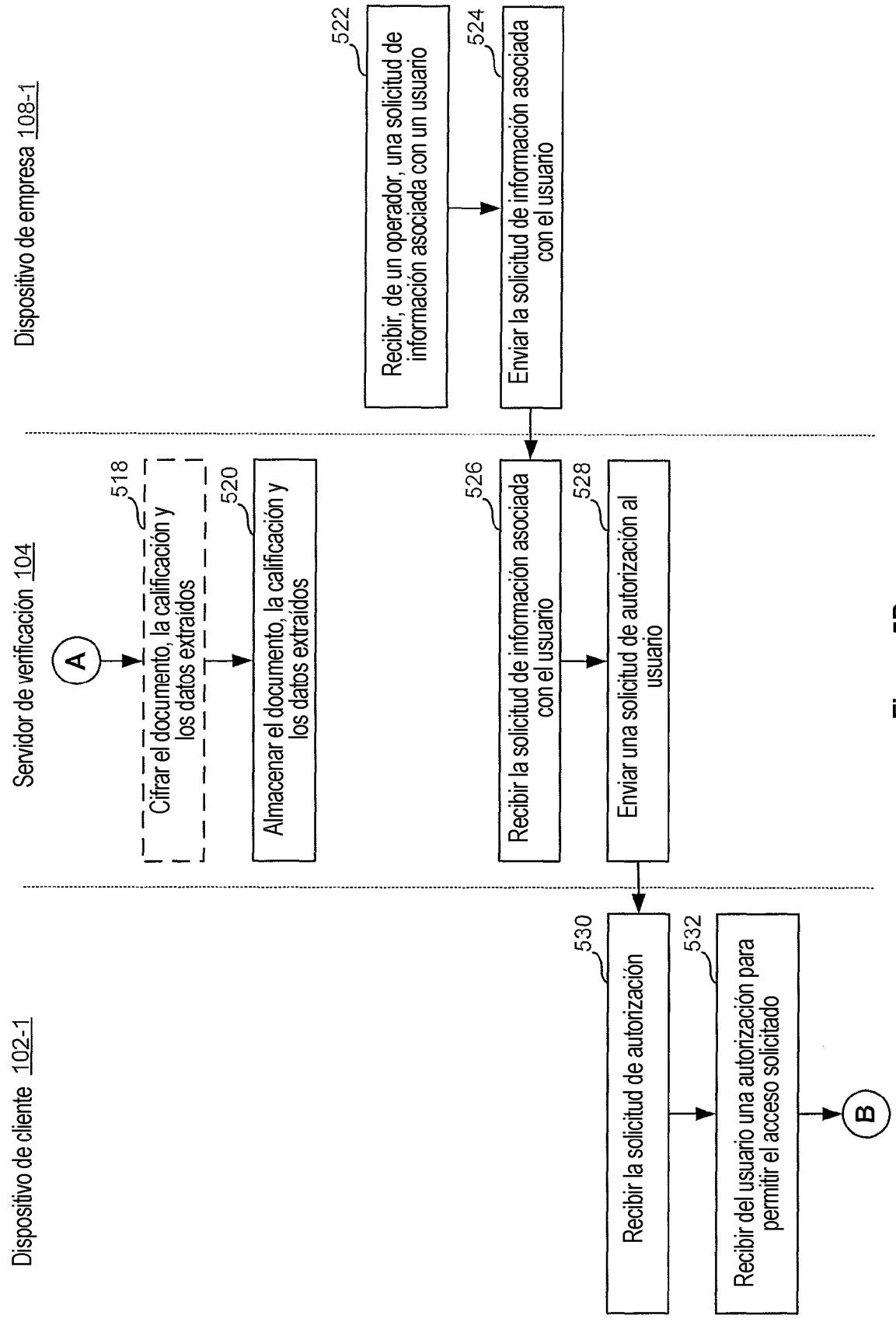
Dispositivo de cliente 102-1
Servidor de verificación 104
Dispositivo de empresa 108-1
A
518
Cifrar el documento, la calificación y los datos extraídos
520
Almacenar el documento, la calificación y los datos extraídos
522
Recibir, de un operador, una solicitud de información asociada con un usuario
524
Enviar la solicitud de información asociada con el usuario
526
Recibir la solicitud de información asociada con el usuario
528
Enviar una solicitud de autorización al usuario
530
Recibir la solicitud de autorización
532
Recibir del usuario una autorización para permitir el acceso solicitado
B

Figura 5B

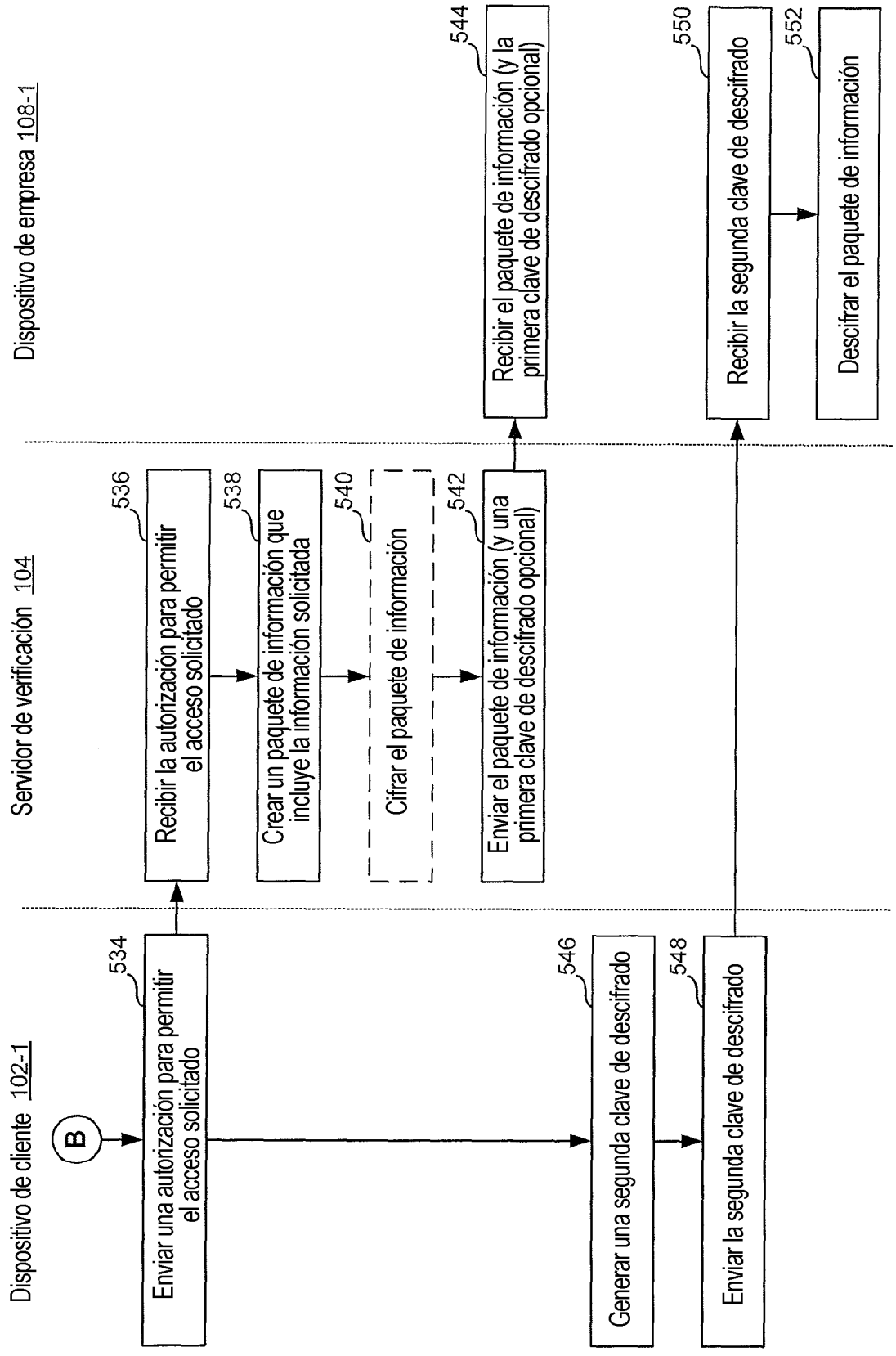
Dispositivo de cliente 102-1
Servidor de verificación 104
Dispositivo de empresa 108-1
B
534
Enviar una autorización para permitir el acceso solicitado
536
Recibir la autorización para permitir el acceso solicitado
538
Crear un paquete de información que incluye la información solicitada
540
Cifrar el paquete de información
542
Enviar el paquete de información (y una primera clave de descifrado opcional)
544
Recibir el paquete de información (y la primera clave de descifrado opcional)
546
Generar una segunda clave de descifrado
548
Enviar la segunda clave de descifrado
550
Recibir la segunda clave de descifrado
552
Descifrar el paquete de información

Figura 5C

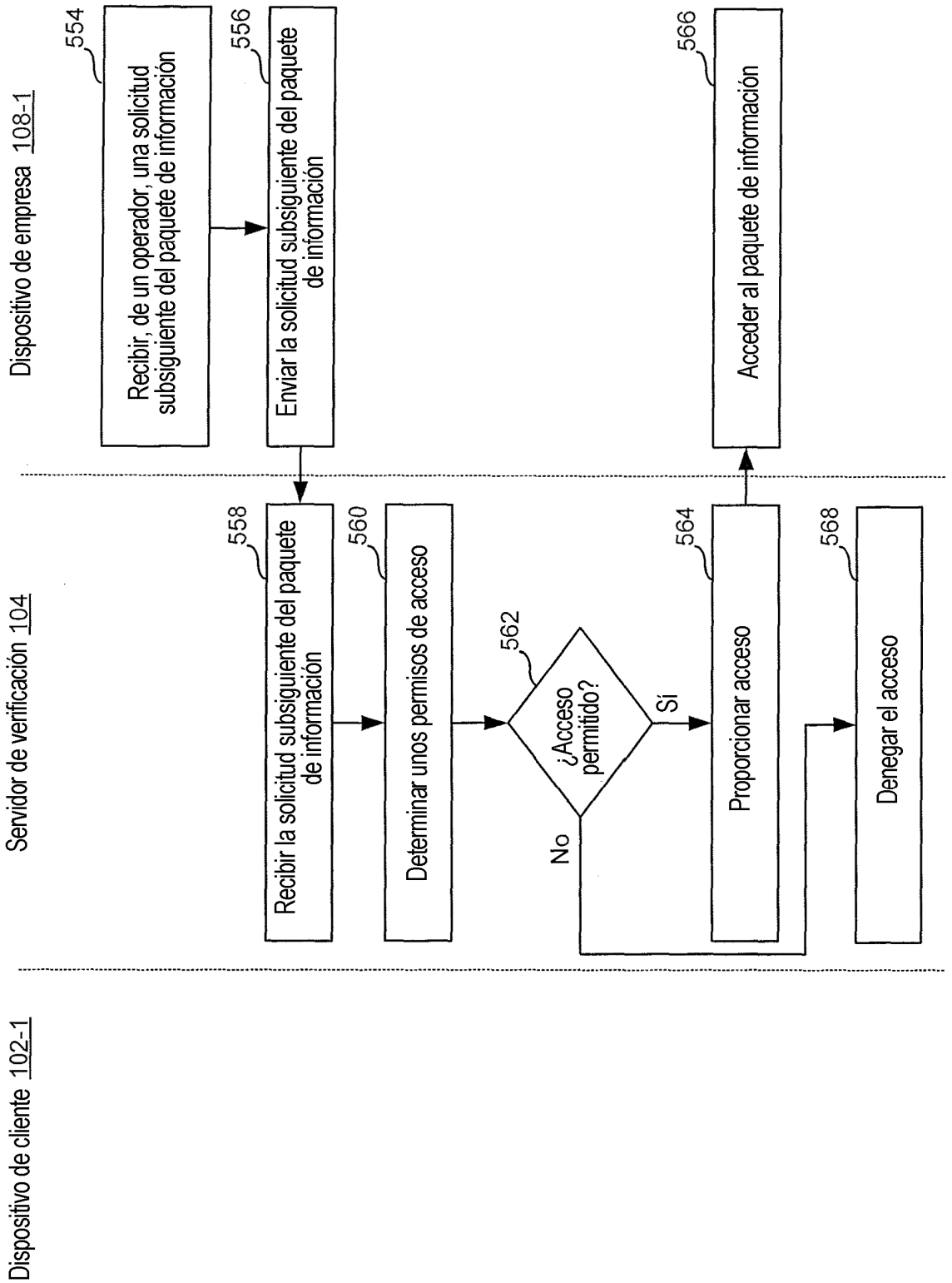
Dispositivo de empresa 108-1
Servidor de verificación 104
Dispositivo de cliente 102-1
554
Recibir, de un operador, una solicitud subsiguiente del paquete de información
556
Enviar la solicitud subsiguiente del paquete de información
566
Acceder al paquete de información
558
Recibir la solicitud subsiguiente del paquete de información
560
Determinar unos permisos de acceso
562
¿Acceso permitido?
Sí
No
564
Proporcionar acceso
568
Denegar el acceso

Figura 5D

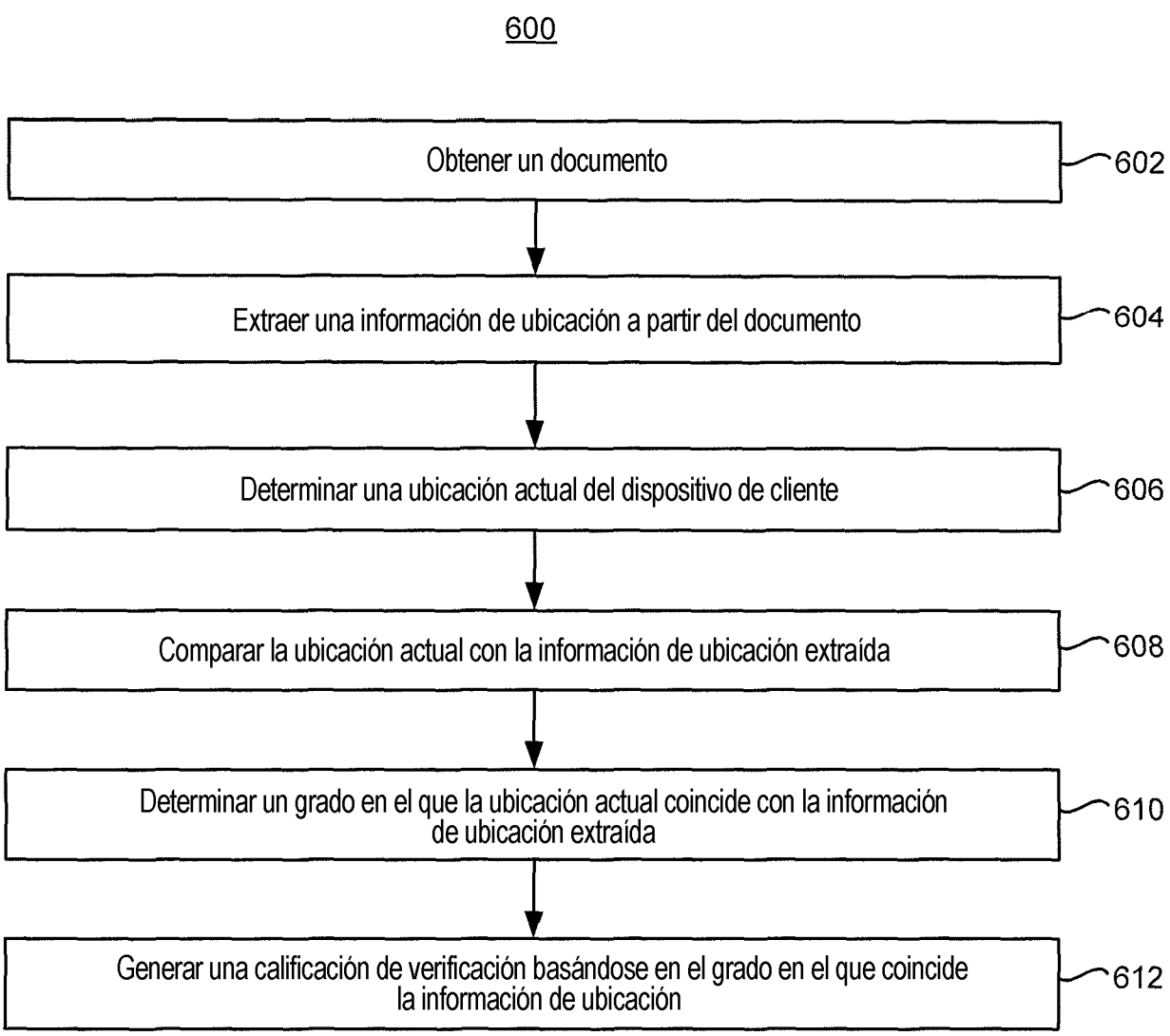
600
Obtener un documento
602
Extraer una información de ubicación a partir del documento
604
Determinar una ubicación actual del dispositivo de cliente
606
Comparar la ubicación actual con la información de ubicación extraída
608
Determinar un grado en el que la ubicación actual coincide con la información de ubicación extraída
610
Generar una calificación de verificación basándose en el grado en el que coincide la información de ubicación
612

**Figura 6**