(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 829 916**

(51) Int. CI.:

H04W 12/06 (2009.01)
G06Q 20/32 (2012.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **21.05.2015 PCT/US2015/031976**

(87) Fecha y número de publicación internacional: **26.11.2015 WO15179640**

(96) Fecha de presentación y número de la solicitud europea: **21.05.2015 E 15727784 (9)**

(97) Fecha y número de publicación de la concesión europea: **30.09.2020 EP 3146744**

(54) Título: **Procedimiento, aparato y sistema que proporciona una comprobación de seguridad**

(30) Prioridad:

22.05.2014 CN 201410219868
20.05.2015 US 201514717545

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
02.06.2021

(73) Titular/es:

ADVANCED NEW TECHNOLOGIES CO., LTD. (100.0%)
Cayman Corporate Centre, 27 Hospital Road George Town, Grand Cayman KY1-9008, KY

(72) Inventor/es:

FENG, JINGGANG

(74) Agente/Representante:

PONTI & PARTNERS, S.L.P.

DESCRIPCIÓN

Procedimiento, aparato y sistema que proporciona una comprobación de seguridad

REFERENCIA CRUZADA A OTRAS SOLICITUDES

[0001] La presente solicitud reivindica prioridad a la solicitud de patente de la República Popular China n.º 201410219868.0 titulada A METHOD, A DEVICE, A SERVER AND A TERMINAL FOR SECURITY CHECKS, depositada el 22 de mayo de 2014.

CAMPO DE LA INVENCIÓN

[0002] La presente solicitud se refiere a un campo de la tecnología de seguridad de las comunicaciones en red. En particular, la presente solicitud se refiere a un procedimiento, un dispositivo, un servidor, un sistema y un terminal para verificar la seguridad.

ANTECEDENTES DE LA INVENCIÓN

[0003] Como resultado del desarrollo de terminales inteligentes y aplicaciones de Internet, los usuarios pueden acceder a varias aplicaciones de Internet utilizando varios clientes de aplicaciones instaladas en terminales. En relación con el procedimiento mediante el cual un usuario accede a las diversas aplicaciones de Internet, generalmente se requiere que los usuarios autentiquen identidades, se registren como miembros, participen en transacciones de red o similares. De acuerdo con alguna técnica relacionada, un servidor de aplicaciones envía un mensaje de texto de verificación que incluye un código de verificación dinámico al terminal en posesión del usuario. Por lo general, se requiere que el usuario introduzca el código de verificación dinámico incluido en el mensaje de texto de verificación. En el caso de que el usuario introduzca el código de verificación dinámico, el usuario pasa la comprobación de seguridad del servidor de la aplicación y se le concede acceso a la aplicación de Internet.

[0004] Sin embargo, el código de verificación dinámico que figura en el mensaje de texto de verificación generalmente se compone de números simples. Por ejemplo, en el caso de que se realice una transacción por Internet, un servidor de banca en línea asociado con la transacción por Internet enviará un mensaje de texto de verificación que consiste en un número de seis dígitos al terminal registrado por el usuario. Si el usuario introduce correctamente el número de seis dígitos incluido en el mensaje de texto de verificación, al usuario se le permite completar la transacción bancaria en línea. Sin embargo, debido a que los mensajes de texto de verificación utilizados en alguna técnica relacionada solo incluyen información numérica escrita simple, terceros maliciosos pueden robar los mensajes de texto de verificación o la información numérica incluida en los mensajes de texto de verificación utilizando programas Trojan Horse con relativa facilidad. Los terceros maliciosos pueden introducir la información numérica escrita en interfaces de verificación seguras y, por lo tanto, completar las comprobaciones de seguridad. En consecuencia, los códigos numéricos de verificación transmitidos en los procedimientos de comprobación de seguridad existentes son relativamente poco fiables, lo que da lugar a una seguridad de acceso deficiente para las aplicaciones de Internet.

[0005] Por lo tanto, existe la necesidad de un procedimiento, dispositivo, servidor, sistema y terminal para proporcionar comprobaciones de seguridad más efectivas.

[0006] La presente invención está definida en las reivindicaciones.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

[0007] En la siguiente descripción detallada y los dibujos adjuntos, se describen varias realizaciones de la invención.

[0008] Los dibujos aquí se han incorporado en la descripción y constituyen una parte de la descripción. Representan realizaciones que se ajustan a la presente solicitud y se utilizan junto con la descripción para explicar los principios de la presente solicitud.

La figura 1 es un diagrama de un contexto de solicitud de acuerdo con diversas realizaciones de la presente descripción de la presente solicitud.

La figura 2 es un diagrama de flujo de un procedimiento de comprobación de seguridad de acuerdo con diversas realizaciones de la presente descripción de la presente solicitud.

La figura 3 es un diagrama de flujo de un procedimiento de comprobación de seguridad de acuerdo con varias realizaciones de la presente descripción de la presente solicitud

La figura 4 es un diagrama de flujo de un procedimiento de comprobación de seguridad de acuerdo con diversas

realizaciones de la presente descripción de la presente solicitud.

La figura 5 es un diagrama de bloques de un dispositivo de verificación de seguridad de acuerdo con varias realizaciones de la presente descripción de la presente solicitud.

La figura 6 es un diagrama de bloques de un dispositivo de verificación de seguridad de acuerdo con varias realizaciones de la presente descripción de la presente solicitud.

La figura 7 es un diagrama de bloques de un dispositivo de verificación de seguridad de acuerdo con varias realizaciones de la presente descripción de la presente solicitud.

La figura 8 es un diagrama de bloques de un dispositivo de verificación de seguridad de acuerdo con varias realizaciones de la presente descripción de la presente solicitud.

La figura 9 es un diagrama de bloques de una realización de un servidor de acuerdo con varias realizaciones de la presente descripción de la presente solicitud.

La figura 10 es un diagrama de bloques de un terminal de acuerdo con varias realizaciones de la presente descripción de la presente solicitud.

La figura 11 es un diagrama de bloques estructurales de un sistema para proporcionar seguridad de acuerdo con varias realizaciones de la presente solicitud.

La figura 12 es un diagrama funcional de un sistema informático para proporcionar seguridad de acuerdo con varias realizaciones de la presente solicitud.

DESCRIPCIÓN DETALLADA

[0009] La invención puede implementarse de numerosas maneras, incluyendo como un procedimiento; un aparato; un sistema; una composición de la materia; un producto de programa informático incorporado en un medio de almacenamiento legible por ordenador; y/o un procesador, tal como un procesador configurado para ejecutar instrucciones almacenadas y/o proporcionadas por una memoria acoplada al procesador. En esta memoria descriptiva, estas implementaciones, o cualquier otra forma que la invención pueda adoptar, pueden denominarse técnicas. En general, el orden de las etapas de los procedimientos descritos puede alterarse dentro del alcance de la invención. A menos que se indique lo contrario, un componente como un procesador o una memoria descrita como configurada para realizar una tarea puede implementarse como un componente general que se configura temporalmente para realizar la tarea en un momento dado o un componente específico que se fabrica para realizar la tarea. Como se usa en esta invención, el término "procesador" se refiere a uno o más dispositivos, circuitos y/o núcleos de procesamiento configurados para procesar datos, como las instrucciones del programa informático.

[0010] Aunque la presente solicitud emplea los términos "primero", "segundo", "tercero", y así sucesivamente para describir información diversa, esta información no estará limitada por estos términos. Estos términos simplemente sirven para diferenciar piezas de información de la misma categoría. Por ejemplo, mientras permanezcan dentro del alcance de la presente solicitud, una primera pieza de información podría denominarse una segunda pieza de información. Del mismo modo, una segunda pieza de información podría denominarse primera pieza de información. Depende del contexto, por ejemplo, el término "si" que se usa en esta invención se puede interpretar como "cuando" o "al confirmarse."

[0011] Un termina generalmente se refiere a un dispositivo utilizado (por ejemplo, por un usuario) dentro de un sistema de red y utilizado para comunicarse con uno o más servidores. De acuerdo con diversas realizaciones de la presente descripción, un terminal puede incluir funcionalidad de comunicación. Por ejemplo, un terminal puede ser un teléfono inteligente, una tableta, un teléfono móvil, un teléfono de vídeo, un lector de libros electrónicos, un ordenador personal de escritorio (PC), un ordenador portátil, un ordenador de netbook, un asistente digital personal (PDA), un reproductor multimedia portátil (PMP), un reproductor mp3, un dispositivo médico móvil, una cámara, un dispositivo portátil (por ejemplo, un dispositivo montado en la cabeza (HMD), ropa electrónica, aparatos electrónicos, un collar electrónico, un accesorio electrónico, un tatuaje electrónico o un reloj inteligente) o similares.

[0012] De acuerdo con algunas realizaciones de la presente descripción, un terminal incluye un electrodoméstico inteligente con funcionalidad de comunicación. Un electrodoméstico inteligente puede ser, por ejemplo, un televisor, un reproductor de disco de vídeo digital (DVD), un dispositivo de audio, un refrigerador, un aire acondicionado, una aspiradora, un horno, un horno de microondas, una lavadora, una secadora, un purificador de aire, un decodificador, una caja de TV (por ejemplo, Samsung HomeSync™, Apple TV™ o Google TV™), una consola de juegos, un diccionario electrónico, una llave electrónica, una videocámara, un marco de imagen electrónico o similares.

[0013] De acuerdo con varias realizaciones de la presente descripción, un terminal puede ser cualquier

combinación de los terminales anteriores. Además, será evidente para un experto en la materia que un terminal de acuerdo con varias realizaciones de la presente descripción no se limita al terminal anterior.

[0014] Varias realizaciones de la presente descripción incluyen un procedimiento, un dispositivo, un servidor, un sistema y un terminal para proporcionar seguridad. Por ejemplo, varias realizaciones de la presente descripción incluyen un procedimiento, un dispositivo, un servidor, un sistema y un terminal para proporcionar comprobaciones de seguridad. Las comprobaciones de seguridad se pueden proporcionar en relación con eventos de acceso (por ejemplo, un usuario que intenta acceder a un servicio o aplicación de red, como un servicio basado en la web).

[0015] La figura 1 es un diagrama de un contexto de solicitud de acuerdo con diversas realizaciones de la presente descripción de la presente solicitud.

[0016] Con referencia a la figura 1, se proporciona un contexto (también denominado entorno) 100 para usar una verificación de seguridad. En algunas realizaciones, los procedimientos 200-400 de las figuras 2-4 se pueden implementar en el entorno 100.

[0017] Tal como se ilustra, el contexto 100 incluye un terminal 110 y un servidor 120. Un usuario puede acceder a diversas aplicaciones de Internet a través de los diversos clientes de aplicaciones instaladas en el terminal 110. Por ejemplo, el terminal 110 puede acceder a un sitio web o un servicio alojado por el servidor 120 usando Internet. Durante el procedimiento de acceso, se puede requerir que el usuario autentique la identidad del usuario, se registre como miembro, participe en una transacción en línea o similares. Con el fin de garantizar la seguridad del procedimiento de acceso, el servidor 120 puede realizar una comprobación de seguridad de la identidad del usuario.

[0018] De acuerdo con alguna técnica relacionada, en el caso de que un usuario intente acceder a una aplicación de Internet, un usuario puede realizar una comprobación de seguridad introduciendo información numérica escrita en una interfaz de verificación de seguridad. El usuario puede obtener la información numérica de un mensaje de texto que se transmite al terminal del usuario a través de una red móvil.

[0019] De acuerdo con diversas realizaciones de la presente solicitud, una comprobación de seguridad incluye procedimientos de verificación entre el terminal 110 y el servidor 120 que se basan en Internet. El procedimiento de verificación utiliza una técnica basada en un identificador único de objeto digital (DOUI) (130). Como se describirá con mayor detalle a continuación, el procedimiento de verificación basado en DOUI asociado con un procedimiento de seguridad mejora la fiabilidad y la seguridad de la verificación.

[0020] La figura 2 es un diagrama de flujo de un procedimiento de comprobación de seguridad de acuerdo con diversas realizaciones de la presente descripción de la presente solicitud.

[0021] Con referencia a la figura 2, se proporciona un procedimiento 200 para realizar una comprobación de seguridad. En algunas realizaciones, el procedimiento 200 puede implementarse mediante el dispositivo 500 de la figura 5, el dispositivo 600 de la figura 6 o el dispositivo 900 de la figura 9.

[0022] En 210, se recibe una solicitud de verificación de seguridad. En algunas realizaciones, un servidor recibe la solicitud de verificación de seguridad. La solicitud de verificación de seguridad se puede enviar desde un terminal. El terminal puede enviar la solicitud de verificación de seguridad en relación con un evento de acceso, una transacción en línea o similar. Un usuario puede seleccionar que se realice una comprobación de seguridad en relación con el evento de acceso, la transacción en línea o similar. Por ejemplo, en el caso de que un terminal se utilice para realizar una transacción en línea utilizando una interfaz de usuario (por ejemplo, una página web para un sitio web mostrado por un navegador instalado en el terminal), el terminal puede proporcionar una opción para realizar la solicitud de verificación de seguridad (por ejemplo, a través de un cuadro de diálogo, un cuadro de selección, etc.). El usuario puede seleccionar realizar una opción de solicitud de verificación de seguridad en la interfaz, y en relación con la selección para realizar una opción de solicitud de verificación de seguridad, se comunica una solicitud de verificación de seguridad.

[0023] De acuerdo con algunas realizaciones, se puede proporcionar una comprobación de seguridad en una interfaz de cliente en un terminal. Por ejemplo, en el caso de que un usuario acceda a una aplicación de Internet (por ejemplo, una aplicación que se ejecuta en un servidor) a través de un cliente en un terminal, el usuario puede ingresar a una interfaz de cliente de la aplicación de Internet (por ejemplo, cargar una página específica que comprende la interfaz de cliente a través de un navegador o invocar la interfaz de cliente usando una aplicación del lado cliente) y someterse a una comprobación de seguridad en la interfaz de cliente. Por ejemplo, se puede proporcionar una comprobación de seguridad en relación con (por ejemplo, durante) una transacción en línea. En este caso, el usuario puede seleccionar (por ejemplo, hacer clic) la opción de solicitud de verificación de seguridad en la interfaz del cliente. En el caso de que se seleccione la opción de solicitud de verificación de seguridad, el servidor recibe la solicitud de verificación de seguridad enviada por el terminal.

[0024] En algunas realizaciones, se comunica un identificador en relación con la solicitud de verificación de

seguridad. Por ejemplo, el identificador puede corresponder a un nombre de usuario, un identificador de terminal, similares o cualquier combinación de estos. El identificador se puede incluir en la solicitud de verificación de seguridad. Por ejemplo, el nombre de usuario del usuario que usa el terminal, o que ha iniciado sesión de otro modo en él, se puede comunicar en la solicitud de verificación de seguridad. En algunas realizaciones, el identificador de terminal puede ser una dirección de Control de Acceso a Medios (MAC), un número de teléfono (por ejemplo, un número de teléfono leído desde la tarjeta SIM o tarjeta UIM de un teléfono móvil), un número de tarjeta de Módulo de Identidad de Suscriptor (SIM), una dirección de Protocolo de Internet (IP), Identidad de Equipo de Estación Móvil Internacional (IMEI), Identificador de Equipo Móvil (MEID), un token u otro identificador que identifique el terminal.

[0025] En 220, se obtiene la primera información del elemento de verificación. En algunas realizaciones, el servidor obtiene la primera información del elemento de verificación. Por ejemplo, el servidor puede obtener la primera información del elemento de verificación de acuerdo con la solicitud de verificación de seguridad.

[0026] En algunas realizaciones, el servidor puede almacenar asignaciones entre nombres de usuario e información del terminal. Por ejemplo, el servidor puede almacenar una asociación entre un nombre de usuario y el identificador de terminal del terminal utilizado por el usuario. En el caso de que se reciba la solicitud de verificación de seguridad enviada por el terminal, se puede buscar una asignación guardada entre los nombres de usuario y la información del terminal con el nombre de usuario del propietario del terminal (que se incluye en la solicitud de verificación de seguridad) para obtener el identificador de terminal del terminal correspondiente al usuario del terminal. El identificador de terminal puede denominarse un primer identificador de terminal.

[0027] En algunas realizaciones, el servidor puede generar un primer código de verificación de seguridad y una primera marca de tiempo en relación con la presente comprobación de seguridad en función, al menos en parte, de la solicitud de verificación de seguridad. La primera marca de tiempo se puede utilizar para indicar el límite de tiempo de la presente comprobación de seguridad. El primer código de verificación de seguridad puede ser texto, números, subtítulos, imágenes, enlaces, similares o cualquier combinación de los mismos. El primer identificador de terminal, el primer código de verificación de seguridad y la primera marca de tiempo pueden denominarse colectivamente primera información del elemento de verificación. El primer código de verificación se puede generar aleatoriamente. Por ejemplo, el primer código de verificación se puede generar usando una función de cálculo aleatorizado tal como RandomStringUtils. randomAlphanumeric(int length).

[0028] En 230, se genera un identificador único de objeto digital. En algunas realizaciones, un servidor genera el identificador único de objeto digital. El identificador único de objeto digital se puede generar en función, al menos en parte, de la primera información del elemento de verificación. Por ejemplo, el identificador único de objeto digital puede generarse usando el primer identificador de terminal, el primer código de verificación de seguridad y la primera marca de tiempo.

[0029] En algunas realizaciones, el identificador único de objeto digital es una herramienta utilizada para identificar información numérica. El identificador único de objeto digital puede incluir un código bidimensional, un código de barras, un código de respuesta rápida (QR), similares o cualquier combinación de los mismos. El identificador único de objeto digital se puede configurar de acuerdo con un entorno de aplicación en el que se utilizará el identificador único de objeto digital. Por ejemplo, el identificador único de objeto digital puede configurarse para incluir un código bidimensional, un código de barras, un código QR o similares de acuerdo con el entorno de la aplicación. En algunas realizaciones, el servidor puede usar identificadores únicos de objetos digitales para transportar información de verificación con el fin de aumentar la fiabilidad de una comprobación de seguridad. En el caso de que el servidor haya obtenido la primera información del elemento de verificación, el servidor puede generar una primera cadena de caracteres de combinación. El servidor puede usar el primer identificador de terminal, el primer código de verificación de seguridad y la primera marca de tiempo incluida en este para generar la cadena de caracteres de combinación. Por ejemplo, el servidor puede combinar el primer identificador de terminal, el primer código de verificación de seguridad y la primera marca de tiempo incluida en el mismo para generar una primera cadena de caracteres de combinación. En el caso de que el servidor haya generado la cadena de caracteres de combinación, el servidor puede generar un identificador único de objeto digital utilizando la primera cadena de caracteres de combinación ejecutando una función de generación que recibe la primera cadena de caracteres de combinación como entrada. Se pueden usar varios procedimientos conocidos para generar identificadores únicos de objetos digitales usando cadenas de caracteres (por ejemplo, una función createQRForString proporcionada con la biblioteca iOS) para generar el identificador único digital usando la primera cadena de caracteres de combinación.

[0030] En 240, se comunica el identificador único de objeto digital. En algunas realizaciones, el servidor comunica el identificador único de objeto digital. Por ejemplo, el servidor puede enviar el identificador único de objeto digital al terminal. La imagen correspondiente al identificador de objeto digital (por ejemplo, un código de barras 2D, un código QR o similares) se puede incluir en un mensaje que el servidor envía al terminal.

[0031] En algunas realizaciones, todo el procedimiento de verificación entre el terminal y el servidor está basado en Internet. Por consiguiente, el servidor puede enviar el identificador único de objeto digital mediante transmisión en línea al terminal. El identificador único de objeto digital se puede transmitir al terminal como un archivo

adjunto a un correo electrónico, un archivo adjunto a un mensaje instantáneo, en conexión con una página web, en conexión con una sesión HTTP o similares.

[0032] En 250, se recibe una segunda información del elemento de verificación. En algunas realizaciones, el servidor recibe la segunda información del elemento de verificación. Por ejemplo, el servidor puede recibir la segunda información del elemento de verificación desde el terminal. El terminal incluye código que está configurado para recibir el identificador único de objeto digital, y en respuesta a recibir el identificador único de objeto digital, comunica la segunda información del elemento de verificación al servidor. La segunda información del elemento de verificación puede incluir, o de otro modo corresponder a, información del elemento de verificación obtenida por el terminal a través del identificador único de objeto digital. Por ejemplo, el terminal puede extraer la primera información del elemento de verificación del identificador único de objeto digital y generar la segunda información del elemento de verificación usando la primera información del elemento de verificación extraída del identificador único de objeto digital.

[0033] En algunas realizaciones, el terminal escanea, o procesa de otro modo (por ejemplo, analiza), el identificador único de objeto digital recibido del servidor. Cuando el terminal escanea, o procesa de otro modo, el identificador único de objeto digital recibido, el terminal obtiene una segunda cadena de caracteres de combinación. El terminal puede descomponer, o de otro modo procesar, la segunda cadena de caracteres de combinación. El terminal puede obtener un segundo identificador de terminal, un segundo código de verificación de seguridad y una segunda marca de tiempo mediante la descomposición de la segunda cadena de caracteres de combinación. El segundo identificador de terminal, el segundo código de verificación de seguridad y la segunda marca de tiempo pertenecen a la segunda información del elemento de verificación, o de otro modo corresponden colectivamente a esta. Por ejemplo, la segunda información del elemento de verificación puede incluir el segundo identificador de terminal, el segundo código de verificación de seguridad y la segunda marca de tiempo. En algunas realizaciones, el terminal puede determinar si el segundo identificador de terminal obtenido del identificador único de objeto digital recibido del servidor es el mismo que el identificador de terminal del terminal. En el caso de que el terminal determine que el segundo identificador de terminal obtenido del identificador único de objeto digital recibido del servidor es el mismo que el identificador de terminal del terminal, el terminal puede enviar la segunda información del elemento de verificación al servidor.

[0034] El terminal puede escanear el identificador único de objeto digital procesando una imagen del identificador único de objeto digital que es capturada por una cámara conectada al terminal. En algunas realizaciones, el escaneo del identificador único de objeto digital incluye la captura de la imagen del identificador único de objeto digital con la cámara conectada al terminal.

[0035] En algunas realizaciones, el terminal tiene una aplicación instalada en él que invoca una cámara del terminal para capturar el identificador único de objeto digital (por ejemplo, código 2D o código QR) mostrado por el primer terminal. El terminal incluye un código de procesamiento de imágenes que utiliza el reconocimiento de imágenes para extraer imágenes geométricas de la imagen y decodificar la imagen en consecuencia.

[0036] En algunas realizaciones, el terminal obtiene el identificador único de objeto digital a partir de un mensaje de correo electrónico, un mensaje de Servicio de Mensaje Corto (SMS), un mensaje de Servicio de Mensaje Multimedia (MMS) o similares. El terminal puede extraer el identificador único de objeto digital (por ejemplo, un código 2D o código QR) o una imagen de este de un mensaje de correo electrónico y traducir el identificador único de objeto digital usando (por ejemplo, ejecutando) un código de procesamiento de imágenes. El código de procesamiento de imágenes puede traducir inversamente el identificador único de objeto digital para obtener la información incluida (por ejemplo, incrustada) en este. Las piezas de información (por ejemplo, código de verificación de seguridad, número de teléfono móvil, marca de tiempo o similares) incluidos en el identificador único de objeto digital pueden separarse por un carácter predefinido (por ejemplo, un guion).

[0037] En 260, se comunica la información del pase de comprobación de seguridad. En algunas realizaciones, el servidor comunica la información del pase de comprobación de seguridad al terminal. El servidor puede determinar si la segunda información del elemento de verificación es consistente con la primera información del elemento de verificación. Por ejemplo, el servidor puede determinar si la segunda información del elemento de verificación coincide con la primera información del elemento de verificación. En el caso de que el servidor confirme que la primera información del elemento de verificación y la segunda información del elemento de verificación son consistentes (por ejemplo, el primer código de verificación se compara con el segundo código de verificación y la primera marca de tiempo y la segunda marca de tiempo se comparan con una hora actual de acuerdo con el servidor), el servidor puede enviar información del pase de comprobación de seguridad de vuelta al terminal. La información del pase de comprobación de seguridad puede indicar que el terminal ha pasado la comprobación de seguridad. En el caso de que el servidor determine que la primera información del elemento de verificación y la segunda información del elemento de verificación no son consistentes (por ejemplo, no coinciden), el servidor puede enviar una indicación de que la comprobación de seguridad falló en el terminal, denegar el acceso del terminal a un dominio (por ejemplo, el servidor) o denegar, o de otro modo impedir, una transacción asociada con la comprobación de seguridad.

[0038] En algunas realizaciones, el servidor almacena el primer identificador de terminal, el primer código de

verificación de seguridad y la primera marca de tiempo. Por ejemplo, en el caso de que el servidor obtenga la primera información del elemento de verificación, el servidor puede almacenar las relaciones (por ejemplo, asociaciones) entre el primer identificador de terminal, el primer código de verificación de seguridad y la primera marca de tiempo. Las relaciones se pueden almacenar en una tabla o base de datos. En respuesta a la recepción de la segunda información del elemento de verificación, el servidor puede buscar las relaciones almacenadas de identificadores de terminal, códigos de verificación de seguridad y marcas de tiempo usando el segundo identificador de terminal (por ejemplo, el identificador de terminal incluido en la segunda información del elemento de verificación), con el fin de obtener el código de verificación de seguridad y la marca de tiempo correspondientes al segundo identificador de terminal. En el caso de que el servidor determine (por ejemplo, confirme) que el segundo código de verificación de seguridad y el código de verificación de seguridad obtenido son iguales, que la segunda marca de tiempo y la marca de tiempo obtenida son iguales, y que la segunda marca de tiempo está dentro del límite de tiempo (por ejemplo, 60 segundos) de la presente comprobación de seguridad (por ejemplo, que se puede determinar para que se corresponda a una hora actual del servidor), el servidor envía la información del pase de comprobación de seguridad al terminal.

[0039] El identificador único de objeto digital se puede usar para transmitir información de verificación durante una comprobación de seguridad. Se puede transmitir información de confirmación más rica y fiable en relación con un identificador único de objeto digital que en una comprobación de seguridad de acuerdo con alguna técnica relacionada que implemente un mensaje de texto que solo incluya números. En comparación con los valores numéricos, la información de confirmación transmitida en relación con el identificador único de objeto digital es relativamente difícil de robar y usar. Por consiguiente, la seguridad de acceso de las aplicaciones de Internet puede mejorarse mediante el uso de identificadores únicos de objetos digitales en la comunicación de la información de confirmación en lugar de mensajes de texto en relación con la comunicación de números escritos. De acuerdo con diversas realizaciones, el identificador único de objeto digital se transmite a través del tráfico de Internet y, por lo tanto, evita los cargos de comunicación que surgen cuando los códigos de verificación se transmiten a través de mensajes de texto. Como resultado, en diversas realizaciones, se reducen los recursos de comunicación móvil necesarios para realizar una comprobación de seguridad. De acuerdo con algunas realizaciones, en respuesta a que el terminal reconozca el identificador único de objeto digital o la información incluida en el identificador único de objeto digital, el terminal puede devolver automáticamente información de reconocimiento al servidor. Por consiguiente, el procedimiento de comprobación de seguridad de acuerdo con diversas realizaciones no requiere la entrada manual por parte del usuario y evita la posibilidad de información de confirmación de fraude manual.

[0040] La figura 3 es un diagrama de flujo de un procedimiento de comprobación de seguridad de acuerdo con diversas realizaciones de la presente descripción de la presente solicitud.

[0041] Con referencia a la figura 3, se proporciona un procedimiento 300 para realizar una comprobación de seguridad. En algunas realizaciones, el procedimiento 300 puede implementarse mediante el dispositivo 700 de la figura 7, el dispositivo 800 de la figura 8 o el terminal 1000 de la figura 10.

[0042] En 310, se comunica una solicitud de verificación de seguridad. En algunas realizaciones, un terminal puede enviar la solicitud de verificación de seguridad a un servidor. El terminal puede enviar la solicitud de verificación de seguridad en relación con un evento de acceso, una transacción en línea o similar. Un usuario puede seleccionar que se realice una comprobación de seguridad en relación con el evento de acceso, la transacción en línea o similar. Por ejemplo, en el caso de que un terminal se utilice para realizar una transacción en línea utilizando una interfaz de usuario (por ejemplo, una página web para un sitio web mostrado por un navegador instalado en el terminal), el terminal puede proporcionar una opción para realizar la solicitud de verificación de seguridad (por ejemplo, a través de un cuadro de diálogo, un cuadro de selección, etc.). El usuario puede seleccionar realizar una opción de solicitud de verificación de seguridad en la interfaz, y en relación con la selección para realizar una opción de solicitud de verificación de seguridad, se comunica una solicitud de verificación de seguridad.

[0043] De acuerdo con algunas realizaciones, se puede proporcionar una comprobación de seguridad en una interfaz de cliente en un terminal. Por ejemplo, en el caso de que un usuario acceda a una aplicación de Internet (por ejemplo, una aplicación que se ejecuta en un servidor) a través de un cliente en un terminal, el usuario puede ingresar a una interfaz de cliente de la aplicación de Internet (por ejemplo, cargar una página específica que comprende la interfaz de cliente a través de un navegador o invocar la interfaz de cliente usando una aplicación del lado cliente) y someterse a una comprobación de seguridad en la interfaz de cliente. Por ejemplo, se puede proporcionar una comprobación de seguridad en relación con una transacción en línea. En el caso de que el usuario seleccione (por ejemplo, haga clic) una opción de solicitud en la interfaz del cliente, se puede enviar una solicitud de verificación de seguridad a través del terminal al servidor.

[0044] En algunas realizaciones, se comunica un identificador en relación con la solicitud de verificación de seguridad. Por ejemplo, el identificador puede corresponder a un nombre de usuario, un identificador de terminal, similares o cualquier combinación de estos. El identificador se puede incluir en la solicitud de verificación de seguridad. Por ejemplo, el nombre de usuario del usuario que utiliza, o de otro modo ha iniciado sesión en, el terminal, se comunica en la solicitud de verificación de seguridad.

[0045] En 320, se recibe un identificador único de objeto digital. En algunas realizaciones, el terminal recibe el identificador único de objeto digital. El terminal puede recibir el identificador único de objeto digital desde el servidor. Por ejemplo, el identificador único de objeto digital puede ser enviado de vuelta por el servidor en respuesta al servidor que recibe (y procesa) la solicitud de verificación de seguridad. El identificador único de objeto digital es un identificador generado de acuerdo con la primera información del elemento de verificación después de que el servidor haya obtenido la primera información del elemento de verificación de acuerdo con la solicitud de verificación de seguridad. Por ejemplo, el identificador único de objeto digital puede generarse usando el primer identificador de terminal, el primer código de verificación de seguridad y la primera marca de tiempo. El primer código de verificación de seguridad puede determinarse de acuerdo con un identificador de terminal incluido (por ejemplo, el primer identificador de terminal) en, o comunicarse en relación con, la solicitud de verificación de seguridad. La primera marca de tiempo se puede utilizar para indicar el límite de tiempo de la presente comprobación de seguridad.

[0046] En 330, se obtiene la segunda información del elemento de verificación. En algunas realizaciones, el terminal obtiene la segunda información del elemento de verificación. El terminal puede obtener la segunda información del elemento de verificación usando el identificador único de objeto digital. El terminal puede comunicar la segunda información del elemento de verificación al servidor en respuesta a que el terminal reciba el identificador único de objeto digital. La segunda información del elemento de verificación puede incluir, o de otro modo corresponder a, información del elemento de verificación obtenida por el terminal a través del identificador único de objeto digital. Por ejemplo, el terminal puede extraer información del elemento de verificación del identificador único de objeto digital y generar la segunda información del elemento de verificación usando la información del elemento de verificación extraída del identificador único de objeto digital.

[0047] El identificador único de objeto digital puede ser generado por el servidor. Por ejemplo, el identificador único de objeto digital puede generarse basándose al menos en parte en una primera cadena de caracteres de combinación. La primera cadena de caracteres de combinación se puede generar usando un primer identificador de terminal, un primer código de verificación de seguridad y una primera marca de tiempo. Por ejemplo, el servidor puede generar la primera cadena de caracteres de combinación combinando un primer identificador de terminal, un primer código de verificación de seguridad y una primera marca de tiempo. El primer identificador de terminal, el primer código de verificación de seguridad y la primera marca de tiempo pueden pertenecer a, o incluirse en, una primera información del elemento de verificación. El primer identificador de terminal puede corresponder al identificador de terminal del terminal. El identificador de terminal del terminal se puede determinar en función, al menos en parte, de la información incluida en la solicitud de verificación de seguridad. Por ejemplo, el identificador de terminal del terminal se puede determinar de acuerdo con el nombre de usuario del terminal que se lleva en la solicitud de verificación de seguridad. La primera comprobación de seguridad puede corresponder al código de verificación de seguridad generado por el servidor en relación con la presente comprobación de seguridad y la primera marca de tiempo puede corresponder a una marca de tiempo generada por el servidor en relación con la presente comprobación de seguridad.

[0048] En algunas realizaciones, el terminal escanea, o procesa de otro modo (por ejemplo, analiza), el identificador único de objeto digital recibido del servidor. En el caso de que el terminal escanee, o procese de otro modo, el identificador único de objeto digital recibido, el terminal puede obtener una segunda cadena de caracteres de combinación. Por ejemplo, el terminal puede obtener la segunda cadena de caracteres de combinación escaneando el identificador único de objeto digital. El terminal puede descomponer, o de otro modo procesar, la segunda cadena de caracteres de combinación. El terminal puede obtener un segundo identificador de terminal, un segundo código de verificación de seguridad y una segunda marca de tiempo mediante la descomposición de la segunda cadena de caracteres de combinación. El segundo identificador de terminal, el segundo código de verificación de seguridad y la segunda marca de tiempo pertenecen a la segunda información del elemento de verificación, o de otro modo corresponden colectivamente a esta. Por ejemplo, la segunda información del elemento de verificación puede incluir el segundo identificador de terminal, el segundo código de verificación de seguridad y la segunda marca de tiempo.

[0049] En 340, se comunica la segunda información del elemento de verificación. En algunas realizaciones, el terminal comunica la segunda información del elemento de verificación. Por ejemplo, el terminal puede enviar la segunda información del elemento de verificación al servidor.

[0050] En algunas realizaciones, el terminal puede determinar si el segundo identificador de terminal obtenido del identificador único de objeto digital recibido del servidor es el mismo que el identificador de terminal del terminal. En el caso de que el terminal determine que el segundo identificador de terminal obtenido del identificador único de objeto digital recibido del servidor es el mismo que el identificador de terminal del terminal, el terminal puede enviar la segunda información del elemento de verificación al servidor.

[0051] A 350, se recibe un resultado de una comprobación de seguridad. En algunas realizaciones, el terminal recibe el resultado de la comprobación de seguridad del servidor. Por ejemplo, en el caso de que una comprobación de seguridad tenga éxito, el terminal puede recibir información del pase de comprobación de seguridad del servidor.

[0052] El servidor puede determinar si la segunda información del elemento de verificación es consistente con la primera información del elemento de verificación. Por ejemplo, el servidor puede determinar si la segunda

información del elemento de verificación coincide con la primera información del elemento de verificación. En el caso de que el servidor confirme que la primera información del elemento de verificación y la segunda información del elemento de verificación son consistentes (por ejemplo, coinciden), el servidor puede enviar información del pase de comprobación de seguridad de vuelta al terminal y el terminal puede recibir la información del pase de comprobación de seguridad. La información del pase de comprobación de seguridad puede indicar que el terminal ha pasado la comprobación de seguridad (por ejemplo, que la comprobación de seguridad se ha realizado correctamente). En el caso de que el servidor determine que la primera información del elemento de verificación y la segunda información del elemento de verificación no son consistentes (por ejemplo, no coinciden), el servidor puede enviar una indicación de que la comprobación de seguridad falló en el terminal, denegar el acceso del terminal a un dominio (por ejemplo, el servidor) o denegar, o de otro modo impedir, una transacción asociada con la comprobación de seguridad.

[0053] En algunas realizaciones, el servidor puede almacenar el primer identificador de terminal, el primer código de verificación de seguridad y la primera marca de tiempo. Por ejemplo, en el caso de que el servidor obtenga la primera información del elemento de verificación, el servidor puede almacenar las relaciones entre el primer identificador de terminal, el primer código de verificación de seguridad y la primera marca de tiempo. Las relaciones se pueden almacenar en una tabla o base de datos. En respuesta a la recepción de la segunda información del elemento de verificación, el servidor puede buscar las relaciones almacenadas de identificadores de terminal, códigos de verificación de seguridad y marcas de tiempo para obtener el código de verificación de seguridad y la marca de tiempo correspondientes al segundo identificador de terminal (por ejemplo, un identificador de terminal incluido en la segunda información del elemento de verificación). En el caso de que el servidor determine (por ejemplo, confirme) que el segundo código de verificación de seguridad y el código de verificación de seguridad obtenido son iguales, que la segunda marca de tiempo y la marca de tiempo obtenida son iguales y que la segunda marca de tiempo está dentro del límite de tiempo de la presente comprobación de seguridad, el servidor puede enviar la información del pase de comprobación de seguridad al terminal.

[0054] El identificador único de objeto digital se puede usar para transmitir información de verificación durante una comprobación de seguridad. Se puede transmitir información de confirmación más rica y fiable en relación con un identificador único de objeto digital que en una comprobación de seguridad de acuerdo con alguna técnica relacionada que implemente un mensaje de texto que incluya números escritos. En algunas realizaciones, la información de confirmación transmitida en conexión con el identificador único de objeto digital es relativamente difícil de robar y usar. Por consiguiente, la seguridad de acceso de las aplicaciones de Internet puede mejorarse mediante el uso de identificadores únicos de objetos digitales en la comunicación de la información de confirmación en lugar de mensajes de texto en relación con la comunicación de números escritos. De acuerdo con diversas realizaciones, el identificador único de objeto digital se transmite a través del tráfico de Internet y, por lo tanto, evita los cargos de comunicación que surgen cuando los códigos de verificación se transmiten a través de mensajes de texto. Como resultado, en diversas realizaciones, hay una reducción en los recursos de comunicación móvil necesarios para realizar una comprobación de seguridad. De acuerdo con algunas realizaciones, en respuesta a que el terminal reconozca el identificador único de objeto digital o la información incluida en el identificador único de objeto digital, el terminal puede devolver automáticamente información de reconocimiento al servidor. Por consiguiente, el procedimiento de comprobación de seguridad de acuerdo con diversas realizaciones no requiere la entrada manual por parte del usuario y evita la posibilidad de información de confirmación de fraude manual.

[0055] De acuerdo con diversas realizaciones, el procedimiento de comprobación de seguridad se puede realizar en conexión con intercambios entre un terminal y un servidor. El identificador único de objeto digital utilizado en relación con un procedimiento de comprobación de seguridad puede ser un código bidimensional.

[0056] La figura 4 es un diagrama de flujo de un procedimiento de comprobación de seguridad de acuerdo con diversas realizaciones de la presente descripción de la presente solicitud.

[0057] Con referencia a la figura 4, se proporciona un procedimiento 400 para realizar una comprobación de seguridad. En algunas realizaciones, al menos parte del procedimiento 400 puede implementarse mediante el dispositivo 500, 600, 700, 800, 900 y 1000 de las figuras 5-10.

[0058] En 410, el servidor 402 almacena asignaciones entre identificadores de usuario e identificadores de terminal. Por ejemplo, el servidor 402 almacena correspondencias entre nombres de usuario e identificadores de terminal. El servidor 402 puede almacenar la asignación entre el identificador de usuario y el identificador de terminal en una tabla, una base de datos, similares o cualquier combinación de los mismos.

[0059] En algunas realizaciones, el terminal que se somete a la comprobación de seguridad es un dispositivo móvil (por ejemplo, un teléfono celular) con funciones de comunicación móvil. Por consiguiente, el identificador de terminal puede ser un número de teléfono celular, el número de tarjeta SIM o similar. El servidor puede guardar previamente las correspondencias entre los nombres de usuario de los usuarios y los respectivos identificadores de terminal de los usuarios (por ejemplo, números de teléfono celular) para que las comprobaciones de seguridad se puedan implementar en escenarios de comprobación de seguridad específicos. Por ejemplo, en el caso de que un usuario esté registrado con una determinada aplicación de Internet, generalmente se requiere que un usuario ingrese

las credenciales del usuario (por ejemplo, nombre de usuario, contraseña, número de teléfono celular y otra información). En el caso de que el servidor de aplicaciones reciba las credenciales del usuario, el servidor de aplicaciones puede guardar las correspondencias de dicha información. En otro ejemplo, en el caso de que un usuario comience la banca por Internet, el servidor de transacciones puede guardar las correspondencias de dicha información y puede sincronizar las correspondencias para la información con el servidor de pagos de un sitio web de pago.

[0060] En 412, la terminal 401 envía una solicitud de verificación de seguridad al servidor 402.

[0061] De acuerdo con algunas realizaciones, se puede proporcionar una comprobación de seguridad en una interfaz de cliente en un terminal. Por ejemplo, en el caso de que un usuario acceda a una aplicación de Internet a través de un cliente en el terminal 401 del usuario, el usuario puede ingresar (por ejemplo, cargar) una interfaz de cliente de la aplicación de Internet y someterse a una comprobación de seguridad en la interfaz de cliente. Por ejemplo, se puede proporcionar una comprobación de seguridad en relación con una transacción en línea. En este caso, después de que el usuario seleccione

[0062] (por ejemplo, haga clic) una opción de solicitud en la interfaz del cliente, se puede enviar una solicitud de verificación de seguridad a través del terminal 401 al servidor 402.

[0063] En 414, el servidor 402 obtiene un primer identificador de terminal correspondiente al terminal 401. Por ejemplo, el servidor 402 puede usar el nombre de usuario del terminal transportado o comunicado en relación con la solicitud de verificación de seguridad como base para buscar la correspondencia y obtiene un primer identificador de terminal asociado con el terminal 401 correspondiente al nombre de usuario del terminal 401.

[0064] El servidor puede obtener el nombre de usuario del terminal de la solicitud de verificación de seguridad y usar el nombre de usuario del terminal en una búsqueda de las correspondencias (por ejemplo, la asignación guardada en 410) para obtener el identificador de terminal para el terminal 401 correspondiente a este nombre de usuario. El identificador de terminal para el terminal 401 corresponde al primer identificador de terminal.

[0065] En 416, el servidor 402 genera el primer código de verificación de seguridad y la primera marca de tiempo. En el caso de que el servidor 402 reciba la solicitud de verificación de seguridad, el servidor genera el primer código de verificación de seguridad y la primera marca de tiempo. Por ejemplo, el primer código de verificación de seguridad y la primera marca de tiempo están asociados con la solicitud de verificación de seguridad.

[0066] El servidor puede generar automáticamente un primer código de verificación de seguridad y una primera marca de tiempo en relación con la comprobación de seguridad actual. La primera marca de tiempo se puede utilizar para indicar el límite de tiempo de la presente comprobación de seguridad. El primer código de verificación de seguridad puede ser específicamente texto, números, subtítulos, imágenes, enlaces, similares o cualquier combinación de los mismos. El primer identificador de terminal, el primer código de verificación de seguridad y la primera marca de tiempo pueden denominarse colectivamente primera información del elemento de verificación.

[0067] En 418, el servidor 402 guarda una relación entre el primer identificador de terminal, el primer código de verificación de seguridad y la primera marca de tiempo. El servidor guarda las relaciones entre el primer identificador de terminal, el primer código de verificación de seguridad y la primera marca de tiempo.

[0068] En algunas realizaciones, se configura una tabla relacional en el servidor para guardar las relaciones entre el identificador de terminal, el código de verificación de seguridad y la marca de tiempo de cada comprobación de seguridad.

[0069] En 420, se genera una primera cadena de caracteres de combinación. En algunas realizaciones, el servidor 402 genera la primera cadena de caracteres de combinación. La primera cadena de caracteres de combinación se puede generar en función al menos en parte del primer identificador de terminal, el primer código de verificación de seguridad y la primera marca de tiempo. Por ejemplo, la primera cadena de caracteres de combinación puede generarse combinando el primer identificador de terminal, el primer código de verificación de seguridad y la primera marca de tiempo.

[0070] De acuerdo con varias realizaciones, se pueden usar diferentes modos de combinación para combinar el primer identificador de terminal, el primer código de verificación de seguridad y la primera marca de tiempo. Por ejemplo, suponiendo que el primer identificador de terminal corresponde al número de teléfono celular de usuario de terminal "13000001234", el primer código de verificación de seguridad es "Aj89", y la primera marca de tiempo es "5-12-2014 14:06 189", el primer identificador de terminal, el primer código de verificación de seguridad y la primera marca de tiempo se pueden combinar usando barras dobles u otros caracteres separadores para formar una primera cadena de caracteres de combinación, tal como: 13000001234//5-12-2014 14:06 189//Aj89.

[0071] En 422, se genera un código de verificación. En algunas realizaciones, el servidor 402 genera el código de verificación. El código de verificación se puede generar en función, al menos en parte, de la primera cadena de

caracteres de combinación. A modo de ejemplo, el código de verificación puede configurarse para incluir un código bidimensional, un código de barras, un código QR o similares. En algunas realizaciones, el código de verificación puede corresponder a un identificador único de objeto digital. Por ejemplo, el servidor 402 puede generar un código de verificación bidimensional usando la primera cadena de caracteres de combinación. La primera cadena de caracteres de combinación se puede procesar y utilizar para generar el código de verificación bidimensional.

[0072] En el caso de que se genere un código de verificación bidimensional, la primera cadena de caracteres combinada puede cifrarse para producir una cadena de caracteres cifrada. La cadena de caracteres cifrada se puede usar para generar el código de verificación bidimensional. Debido a que los caracteres en una cadena de caracteres cifrada son típicamente más largos, la cadena de caracteres cifrada se puede convertir en una cadena base 64. La cadena base 64 se puede codificar para producir un código de verificación bidimensional. De acuerdo con diversas realizaciones, la cadena de caracteres cifrada puede convertirse en una cadena *n* base, donde n es un entero positivo. La primera cadena de caracteres combinada se puede cifrar según varios procedimientos de cifrado. Por ejemplo, la primera cadena de caracteres de combinación se puede generar usando una técnica de cifrado conocida, tal como un procedimiento de cifrado hash, un procedimiento de cifrado simétrico, un procedimiento asimétrico, MD5 o similares. En algunas realizaciones, se puede utilizar cualquier cifrado de cadena. Por ejemplo, se puede usar el estándar de cifrado de datos (DES), que utiliza una clave de 64 bits para cifrar una cadena de 64 bits, para generar un valor de 64 bits cifrado.

[0073] En algunas realizaciones, el código de verificación bidimensional es una figura gráfica que comprende alternar blanco y negro distribuido a través del plano de una figura geométrica de acuerdo con un patrón específico. El terminal puede leer (por ejemplo, escanear) la información de código bidimensional con el software de escaneo de código de verificación bidimensional. Por ejemplo, el terminal puede capturar una imagen del código de verificación bidimensional y procesar la imagen capturada para extraer información incrustada o incluida de otro modo en el código bidimensional. Como ejemplo, el terminal puede capturar la imagen del código de verificación bidimensional invocando un código de captura de imagen que utiliza una cámara del terminal para capturar una imagen del código de verificación bidimensional. Como otro ejemplo, el terminal puede capturar la imagen del código de verificación bidimensional al extraer la imagen del código de verificación bidimensional, o el código de verificación bidimensional en sí mismo, de un mensaje tal como un correo electrónico, un mensaje SMS, un mensaje MMS, un mensaje instantáneo o similares. El código de verificación bidimensional puede ser un código QR codificado y generado de acuerdo con las reglas QR. El código QR se puede leer rápidamente y puede guardar un mayor volumen de información, incluyendo texto, imágenes y otros tipos diferentes de datos para la codificación. En algunas realizaciones, el código QR tiene forma cuadrada y solo tiene dos colores: blanco y negro. El código QR puede incluir una figura cuadrada más pequeña impresa en tres de las cuatro esquinas. Estas tres figuras cuadradas permiten al usuario escanear el código QR desde cualquier ángulo. Por ejemplo, la figura cuadrada más pequeña incluida en las tres esquinas permite determinar una posición relativa del código QR de modo que el código QR pueda procesarse de acuerdo con una orientación definida.

[0074] En algunas realizaciones, en el caso de que la primera cadena de caracteres de combinación esté cifrada usando un algoritmo de cifrado simétrico, las mismas claves de cifrado se guardarán por separado en el servidor 402 y en el terminal 401 (por ejemplo, en un programa cliente instalado en el terminal 401). En el caso de que la primera cadena de caracteres de combinación se cifre usando un algoritmo de cifrado asimétrico, la clave de cifrado se puede guardar en el servidor 402 y la clave de descifrado se puede guardar en el terminal 401 (por ejemplo, en un programa cliente instalado en el terminal 401). En algunas realizaciones, independientemente del tipo de algoritmo de cifrado utilizado para cifrar la primera cadena de caracteres de combinación, el servidor 402 cifra la primera cadena de caracteres de combinación usando una clave de cifrado guardada.

[0075] En 424, el servidor 402 envía el código de verificación bidimensional (por ejemplo, el código de verificación) al terminal 401. El servidor 402 puede enviar el código de verificación bidimensional al terminal 401 a través de Internet.

[0076] En algunas realizaciones, todo el procedimiento de verificación entre el terminal y el servidor 402 está basado en Internet. Por lo tanto, el servidor 402 puede enviar el código de verificación bidimensional mediante transmisión en línea al terminal 401.

[0077] En 426, se obtiene una segunda cadena de caracteres de combinación. En algunas realizaciones, el terminal 401 obtiene la segunda cadena de caracteres de combinación. El terminal 401 puede obtener la segunda cadena de caracteres de combinación usando (por ejemplo, de) el código de verificación. Por ejemplo, el terminal 401 obtiene una segunda cadena de caracteres de combinación escaneando (y procesando) el código de verificación bidimensional. En algunas realizaciones, la información utilizada para generar la segunda cadena de caracteres de combinación se puede extraer del código de verificación bidimensional.

[0078] En el caso de que el terminal 401 reciba el código de verificación bidimensional, el código de verificación bidimensional se puede escanear con software de escaneo de código bidimensional para obtener una segunda cadena de caracteres de combinación. Correspondiente al procedimiento mediante el cual el servidor 402 genera un código

bidimensional en 422, el terminal 401 puede, en el procedimiento de escaneo de código bidimensional, decodificar el código de verificación bidimensional de acuerdo con una regla de decodificación QR para generar una cadena de caracteres base 64. La cadena de caracteres base 64 se puede convertir en una cadena de caracteres cifrada, y la cadena de caracteres cifrada se puede descifrar para obtener una segunda cadena de caracteres de combinación. En el caso de que el terminal 401 lleve a cabo el descifrado, el terminal 401 utiliza la clave de descifrado correspondiente a la clave de cifrado guardada por el servidor 402 para descifrar la cadena de caracteres cifrada.

[0079] En 428, se adquieren un segundo identificador de terminal, un segundo código de verificación de seguridad y una segunda marca de tiempo. En algunas realizaciones, el terminal 401 obtiene el segundo identificador de terminal, el segundo código de verificación de seguridad y la segunda marca de tiempo usando (por ejemplo, de) la segunda cadena de caracteres de combinación. Por ejemplo, en algunas realizaciones, el terminal 401 puede descomponer la segunda cadena de caracteres de combinación para obtener el segundo identificador de terminal, el segundo código de verificación de seguridad y la segunda marca de tiempo.

[0080] En algunas realizaciones, el terminal 401 obtiene el segundo identificador de terminal, el segundo código de verificación de seguridad y la segunda marca de tiempo mediante el uso de la regla inversa correspondiente a la regla de combinación aplicada cuando se generó la primera cadena de caracteres de combinación (por ejemplo, por el servidor 402) para descomponer la segunda cadena de caracteres de combinación. El resultado de descomponer la segunda cadena de caracteres de combinación puede ser el segundo identificador de terminal, el segundo código de verificación de seguridad y la segunda marca de tiempo.

[0081] En 430, se determina si el segundo identificador de terminal corresponde al identificador de terminal del terminal 401. En algunas realizaciones, el terminal 401 compara el segundo identificador de terminal con el identificador de terminal del terminal 401 (por ejemplo, el primer identificador de terminal) para determinar si el segundo identificador de terminal y el identificador de terminal del terminal 401 son consistentes (por ejemplo, de acuerdo).

[0082] En algunas realizaciones, se puede completar una primera re-verificación de la comprobación de seguridad en el terminal 401. Por ejemplo, el terminal 401 puede comparar el segundo identificador de terminal (que el terminal 401 obtuvo a través de la descomposición de la segunda cadena de caracteres de combinación) con su propio primer identificador de terminal. Si el segundo identificador de terminal y el primer identificador de terminal son iguales, entonces se puede considerar que la coincidencia del segundo identificador de terminal y el primer identificador de terminal indica que el terminal 401 es el terminal designado del usuario que se está sometiendo a la comprobación de seguridad. Si el segundo identificador de terminal y el primer identificador de terminal no son iguales, entonces se puede considerar que la inconsistencia entre el segundo identificador de terminal y el primer identificador de terminal indica que el terminal 401 no es el terminal designado del usuario. Por ejemplo, el propietario del terminal 401 puede no ser el usuario que desea someterse a una comprobación de seguridad. De este modo, se aumenta la eficacia de detección de las comprobaciones de seguridad.

[0083] En algunas realizaciones, en el caso de que el terminal sea un teléfono celular multimodo con múltiples tarjetas, el terminal 401 puede abarcar cada número de teléfono celular del terminal 401 cuando se compara el número de teléfono celular obtenido a través de la descomposición con los números de teléfono celular del terminal 401. Si cualquier teléfono celular del terminal 401 es el mismo que un número de teléfono celular obtenido a través de la descomposición, entonces ese terminal coincidente 401 puede confirmarse como el teléfono celular designado del usuario.

[0084] En el caso de que el segundo identificador de terminal no sea consistente con (por ejemplo, no coincida) el identificador de terminal del terminal 401, entonces en 432, la comprobación de seguridad falla. El terminal 401 puede proporcionar una indicación al usuario de que la comprobación de seguridad falla. Por ejemplo, el terminal 401 puede proporcionar la indicación en un cuadro de diálogo emergente, mediante una vibración, mediante un sonido, mediante un cambio en el brillo de la pantalla, mediante una luz indicadora, similares o cualquier combinación de estos. En el caso de que el segundo identificador de terminal no sea consistente con (por ejemplo, no coincida) el identificador de terminal del terminal 401, el procedimiento de comprobación de seguridad puede finalizar.

[0085] En el caso de que el segundo identificador de terminal sea consistente con (por ejemplo, coincide con) el identificador de terminal del terminal 401, entonces en 434, se puede comunicar el segundo identificador de terminal, el segundo código de verificación de seguridad y la segunda marca de tiempo. En algunas realizaciones, el terminal 401 envía el segundo identificador de terminal, el segundo código de verificación de seguridad y la segunda marca de tiempo al servidor 402.

[0086] En el caso de que un terminal 401 compare un segundo identificador de terminal con el identificador de terminal del terminal 401 y determine que el segundo identificador de terminal es el mismo que el identificador de terminal del terminal 401 (por ejemplo, el primer identificador de terminal), el terminal 401 puede enviar el segundo identificador de terminal, el segundo código de verificación de seguridad y la segunda marca de tiempo al servidor 402 para que el servidor 402 pueda verificar adicionalmente la autenticidad de la operación de comprobación de seguridad en Internet y llevar a cabo efectivamente una verificación adicional. Por ejemplo, el terminal 401 puede establecer un

canal de comunicación con una interfaz de comunicación de un servidor 402 (por ejemplo, una conexión de protocolo de transferencia de hipertexto (HTTP) o un protocolo de transferencia de hipertexto a través de una conexión de capa de zócalo segura (HTTPS)), y transmitir el segundo identificador de terminal, el segundo código de verificación de seguridad y la segunda marca de tiempo. Por ejemplo, el terminal 401 puede transmitir el segundo identificador de terminal, el segundo código de verificación de seguridad y la segunda marca de tiempo como si el segundo identificador de terminal, el segundo código de verificación de seguridad y la segunda marca de tiempo fueran tres parámetros de la interfaz al servidor 402. Por lo tanto, no es necesaria ninguna operación manual para transmitir el segundo identificador de terminal, el segundo código de verificación de seguridad y la segunda marca de tiempo al servidor 402. En realizaciones, el procedimiento de comprobación de seguridad no requiere ninguna operación manual de un usuario del terminal 401 para completar una comprobación de seguridad.

[0087] En 436, el servidor 402 busca en las relaciones una relación correspondiente al segundo identificador de terminal. Por ejemplo, el servidor 402 busca registros de las asignaciones entre un identificador de terminal, un código de verificación de seguridad y una marca de tiempo (por ejemplo, registros del primer identificador de terminal, el primer código de verificación de seguridad y la primera marca de tiempo). En el caso de que el servidor 402 encuentre un registro correspondiente al segundo identificador de terminal, el servidor 402 obtiene el código de verificación correspondiente (por ejemplo, el primer código de verificación) y la marca de tiempo correspondiente (por ejemplo, la primera marca de tiempo) correspondiente al segundo identificador de terminal.

[0088] El servidor puede, tomando como índice el segundo identificador de terminal recibido, buscar las relaciones guardadas en la etapa 418 y obtener el código de verificación de seguridad y la marca de tiempo correspondientes al segundo identificador de terminal.

[0089] En 438, el servidor determina si el código de verificación de seguridad obtenido y la marca de tiempo obtenida (por ejemplo, el código de verificación de seguridad y la marca de tiempo correspondientes al registro asociado con el segundo identificador de terminal) coinciden con el segundo código de verificación de seguridad (por ejemplo, el segundo código de verificación recibido en 434) y la segunda marca de tiempo (por ejemplo, la segunda marca de tiempo recibida en 434). En algunas realizaciones, el servidor determina si el segundo código de verificación de seguridad y la segunda marca de tiempo son iguales al código de verificación de seguridad y marca de tiempo obtenidos de acuerdo con el segundo identificador de terminal y si la segunda marca de tiempo está dentro del límite de tiempo de la presente comprobación de seguridad.

[0090] En 438, si el servidor 402 determina que el segundo código de verificación de seguridad (por ejemplo, correspondiente al primer código de verificación de seguridad almacenado en 418) y el código de verificación de seguridad obtenido en 434 son iguales, que la segunda marca de tiempo (por ejemplo, correspondiente a la primera marca de tiempo almacenada en 418) y la marca de tiempo obtenida en 434 son iguales, y que la hora actual no está fuera del intervalo de tiempo definido por la segunda marca de tiempo, entonces el servidor 402 puede confirmar que el terminal ha pasado la comprobación de seguridad.

[0091] En el caso de que el servidor 402 determine que el código de verificación de seguridad obtenido y la marca de tiempo obtenida (por ejemplo, el código de verificación de seguridad y la marca de tiempo correspondientes al registro asociado con el segundo identificador de terminal) no coinciden con el segundo código de verificación de seguridad (por ejemplo, el segundo código de verificación recibido en 434) y la segunda marca de tiempo (por ejemplo, la segunda marca de tiempo recibida en 434), la comprobación de seguridad falla. En el caso de que la comprobación de seguridad falle, en 440, el servidor 402 puede enviar información de falla de comprobación de seguridad al terminal 401. En el caso de que el terminal 401 reciba la información de falla de comprobación de seguridad del servidor 402, el terminal 401 puede proporcionar una indicación al usuario de que la comprobación de seguridad falla. Por ejemplo, el terminal 401 puede proporcionar la indicación en un cuadro de diálogo emergente, mediante una vibración, mediante un sonido, mediante un cambio en el brillo de la pantalla, mediante una luz indicadora, similares o cualquier combinación de estos. En caso de que la comprobación de seguridad falle, el procedimiento de comprobación de seguridad puede finalizar.

[0092] En algunas realizaciones, la comprobación de seguridad falla en el caso de que el servidor determine que el segundo código de verificación de seguridad y la segunda marca de tiempo son iguales que el código de verificación de seguridad y la marca de tiempo obtenidos de acuerdo con el segundo identificador de terminal, pero la segunda marca de tiempo no está dentro del límite de tiempo de la presente comprobación de seguridad. Por ejemplo, la comprobación de seguridad puede agotarse (por ejemplo, expirar) si no se determina que el segundo código de verificación de seguridad y la segunda marca de tiempo sean los mismos que el código de verificación de seguridad y la marca de tiempo obtenidos de acuerdo con el segundo identificador de terminal dentro de un límite de tiempo umbral.

[0093] En el caso de que la comprobación de seguridad pase, en 442, el servidor 402 envía información de comprobación de seguridad al terminal. La información del pase de comprobación de seguridad puede indicar que el terminal ha pasado la comprobación de seguridad. En el caso de que la comprobación de seguridad pase, el procedimiento de comprobación de seguridad puede finalizar.

[0094] Como se puede ver en el ejemplo descrito anteriormente, se puede usar un código de verificación bidimensional para transmitir información de verificación durante una comprobación de seguridad. Un código de verificación bidimensional puede transmitir información de confirmación más rica y fiable que alguna técnica relacionada que utiliza una verificación de seguridad implementada a través de un mensaje de texto que contiene números escritos. De acuerdo con diversas realizaciones, la información de confirmación es difícil de robar y usar y, por lo tanto, mejora la seguridad de acceso de las aplicaciones de Internet. En algunas realizaciones, el código de verificación bidimensional se transmite a través del tráfico de Internet y, por lo tanto, evita los cargos de comunicación que surgen cuando los códigos de verificación se transmiten a través de mensajes de texto. Como resultado, en diversas realizaciones, hay una reducción en los recursos de comunicación móvil necesarios para realizar una comprobación de seguridad. De acuerdo con algunas realizaciones, en respuesta a que el terminal reconozca el código de verificación bidimensional, el terminal puede enviar automáticamente información de reconocimiento al servidor. Por consiguiente, el procedimiento de comprobación de seguridad de acuerdo con diversas realizaciones no requiere la entrada manual por parte del usuario y evita la posibilidad de información de confirmación de fraude manual. Además, la eficiencia de la comprobación de seguridad se eleva efectivamente porque el terminal puede implementar una primera re-verificación en el procedimiento de comprobación de seguridad al confirmar el identificador del terminal.

[0095] La figura 5 es un diagrama de bloques de un dispositivo de verificación de seguridad de acuerdo con varias realizaciones de la presente descripción de la presente solicitud.

[0096] Con referencia a la figura 5, se proporciona un dispositivo 500 para realizar una comprobación de seguridad. En algunas realizaciones, el dispositivo 500 puede implementar parte o la totalidad del procedimiento 200 de la figura 2. En algunas realizaciones, el dispositivo 500 puede implementar parte o la totalidad del procedimiento 300 de la figura 3. En algunas realizaciones, el dispositivo 500 puede implementar parte o la totalidad del procedimiento 400 de la figura 4. En algunas realizaciones, el dispositivo 500 puede ser implementado por el terminal 1000 de la figura 10. En algunas realizaciones, el dispositivo 500 puede ser implementado por el sistema 1100 de la figura 11.

[0097] En algunas realizaciones, el dispositivo 500 puede implementarse en un servidor. El dispositivo 500 puede incluir un módulo de recepción 510, un módulo de obtención 520, un módulo de generación 530, un módulo de envío 540 y un módulo de confirmación 550.

[0098] El módulo de recepción 510 se puede configurar para recibir una solicitud de verificación de seguridad enviada desde un terminal.

[0099] El módulo de obtención 520 se puede configurar para obtener una primera información del elemento de verificación de acuerdo con la solicitud de verificación de seguridad recibida por el módulo de recepción 510.

[0100] El módulo de generación 530 puede configurarse para usar la primera información de elemento de verificación obtenida por el módulo de obtención 520 como base para generar un identificador único de objeto digital.

[0101] El módulo de envío 540 se puede configurar para enviar el identificador único de objeto digital generado por el módulo de generación 530. El módulo de envío 540 puede enviar el identificador único de objeto digital al terminal.

[0102] El módulo de recepción 510 se puede configurar adicionalmente para recibir la segunda información del elemento de verificación enviada por el terminal. La segunda información del elemento de verificación puede corresponder a información del elemento de verificación obtenida por el terminal utilizando el identificador único de objeto digital enviado por el módulo de envío 540.

[0103] El módulo de confirmación 550 se puede configurar para enviar un resultado de una comprobación de seguridad. Por ejemplo, al confirmar que la primera información del elemento de verificación obtenida por el módulo de obtención 520 y la segunda información del elemento de verificación recibida por la unidad de recepción están de acuerdo (por ejemplo, consistentes), el módulo de confirmación 550 puede enviar información pasada de comprobación de seguridad de vuelta al terminal.

[0104] La figura 6 es un diagrama de bloques de un dispositivo de verificación de seguridad de acuerdo con varias realizaciones de la presente descripción de la presente solicitud.

[0105] Con referencia a la figura 6, se proporciona un dispositivo 600 para realizar una comprobación de seguridad. En algunas realizaciones, el dispositivo 600 puede implementar parte o la totalidad del procedimiento 200 de la figura 2. En algunas realizaciones, el dispositivo 600 puede implementar parte o la totalidad del procedimiento 300 de la figura 3. En algunas realizaciones, el dispositivo 600 puede implementar parte o la totalidad del procedimiento 400 de la figura 4. En algunas realizaciones, el dispositivo 600 puede ser implementado por el terminal 1000 de la figura 10. En algunas realizaciones, el dispositivo 600 puede ser implementado por el sistema 1100 de la figura 11.

[0106] En algunas realizaciones, el dispositivo 600 puede implementarse en un servidor. El dispositivo 600

puede incluir un módulo de guardado 610, un módulo de recepción 620, un módulo de obtención 630, un módulo de generación 640, un módulo de envío 650 y un módulo de confirmación 660.

[0107] El módulo de guardado 610 se puede configurar para almacenar una asignación entre un identificador de usuario y un identificador de terminal. El módulo de guardado 610 puede almacenar la asignación en una tabla, una base de datos o similar. El módulo de guardado 610 puede actualizar la asignación en caso de que un usuario registre un nombre de usuario o cambie un registro en un registro correspondiente a un nombre de usuario existente.

[0108] El módulo de recepción 620 se puede configurar para recibir una solicitud de verificación de seguridad enviada desde un terminal.

[0109] El módulo de obtención 630 puede incluir un submódulo de búsqueda de identificadores 631 y un submódulo generador de información 632.

[0110] El submódulo de búsqueda de identificadores 631 puede configurarse para usar el nombre de usuario asociado con el terminal como base para buscar las asignaciones guardadas por el módulo de guardado 610 y para obtener un primer identificador de terminal correspondiente a un terminal asociado con el nombre de usuario del terminal. El nombre de usuario asociado con el terminal se puede llevar en la solicitud de verificación de seguridad recibida por el módulo de recepción 620.

[0111] El submódulo generador de información 632 puede configurarse para generar un primer código de verificación de seguridad y una primera marca de tiempo. El submódulo generador de información 632 puede generar el primer código de verificación de seguridad y la primera marca de tiempo en relación con la solicitud de verificación de seguridad recibida por el módulo de recepción 620. La primera marca de tiempo puede indicar el límite de tiempo en la comprobación de seguridad actual. La primera información del elemento de verificación puede incluir el primer identificador de terminal, el primer código de verificación de seguridad y la primera marca de tiempo.

[0112] El módulo de guardado 610 puede configurarse adicionalmente para guardar las relaciones entre el primer identificador de terminal obtenido por el submódulo de búsqueda de identificadores 631 y el primer código de verificación de seguridad y la primera marca de tiempo que se generan por el submódulo generador de información 632.

[0113] El módulo de generación 640 puede incluir un submódulo generador de cadena de caracteres 641 y un submódulo generador de identificadores 642.

[0114] La cadena de caracteres que genera el submódulo 641 se puede configurar para generar una primera cadena de caracteres de combinación. El submódulo generador de cadena de caracteres 641 puede configurarse para generar la primera cadena de caracteres de combinación combinando el primer identificador de terminal obtenido por el submódulo de búsqueda de identificadores 631 y el primer código de verificación de seguridad y la primera marca de tiempo que se generan por el submódulo generador de información 632.

[0115] El submódulo generador de identificadores 642 puede configurarse para usar la primera cadena de caracteres combinada generada por el submódulo generador de cadena de caracteres 641 para generar un identificador único de objeto digital.

[0116] El módulo de envío 650 se puede configurar para enviar el identificador único de objeto digital generado por el submódulo generador de identificadores 642 al terminal.

[0117] El módulo de recepción 620 se puede configurar adicionalmente para recibir la segunda información del elemento de verificación enviada por el terminal. La segunda información del elemento de verificación puede corresponder a información del elemento de verificación obtenida por el terminal utilizando el identificador único de objeto digital enviado por el módulo de envío 650. La segunda información del elemento de verificación recibida por la unidad de recepción 620 puede incluir un segundo identificador de terminal, un segundo código de verificación de seguridad y una segunda marca de tiempo que se obtienen mediante la descomposición de una segunda cadena de caracteres de combinación. El terminal puede obtener la segunda cadena de caracteres de combinación escaneando el identificador único de objeto digital. El terminal puede enviar la segunda información del elemento de verificación en el caso de que el terminal comparara el segundo identificador de terminal con el identificador de terminal del terminal y determinara que el segundo identificador de terminal coincidiera (por ejemplo, fuera el mismo) con el identificador de terminal del terminal.

[0118] El módulo de confirmación 660 puede incluir un submódulo de búsqueda de información 661 y un submódulo de ejecución de confirmación 662.

[0119] El submódulo de búsqueda de información 661 puede configurarse para buscar relaciones (por ejemplo, registros de relaciones) guardadas por el módulo de guardado 610 y para obtener el código de verificación de

seguridad y la marca de tiempo que corresponden respectivamente al segundo identificador de terminal en la segunda información del elemento de verificación recibida por el módulo de recepción 620.

[0120] El submódulo de ejecución de confirmación 662 puede configurarse para enviar una indicación de un resultado del resultado de la comprobación de seguridad. El submódulo de ejecución de confirmación 662 puede determinar si el segundo código de verificación de seguridad y el código de verificación de seguridad obtenidos por la coincidencia del submódulo de búsqueda de información 661 (por ejemplo, son iguales), si la segunda marca de tiempo y la marca de tiempo obtenidas por la coincidencia del submódulo de búsqueda de información 661 (por ejemplo, son iguales), y si la segunda marca de tiempo está dentro del límite de tiempo de la presente comprobación de seguridad. En el caso de que el submódulo de ejecución de confirmación 662 determine que el segundo código de verificación de seguridad y el código de verificación de seguridad obtenidos por la coincidencia del submódulo de búsqueda de información 661 coinciden (por ejemplo, son los mismos), que la segunda marca de tiempo y la marca de tiempo obtenidas por el submódulo de búsqueda de información 661 coinciden (por ejemplo, son los mismos), y que la segunda marca de tiempo está dentro del límite de tiempo de la presente configuración de seguridad, el submódulo de ejecución de confirmación 662 envía información del pase de comprobación de seguridad de vuelta al terminal.

[0121] En algunas realizaciones, el submódulo generador de identificador 642 está configurado para cifrar la primera cadena de caracteres combinada generada por el submódulo generador de cadena de caracteres 641 para generar una cadena de caracteres cifrada y convertir la cadena de caracteres cifrada en una cadena de caracteres base 64. El submódulo generador de identificador 642 puede configurarse para codificar la cadena de caracteres base 64 de acuerdo con una regla de codificación QR y para generar un código de verificación bidimensional, que corresponde al identificador único de objeto digital.

[0122] La figura 7 es un diagrama de bloques de un dispositivo de verificación de seguridad de acuerdo con varias realizaciones de la presente descripción de la presente solicitud.

[0123] Con referencia a la figura 7, se proporciona un dispositivo 700 para realizar una comprobación de seguridad. En algunas realizaciones, el dispositivo 700 puede implementar parte o la totalidad del procedimiento 200 de la figura 2. En algunas realizaciones, el dispositivo 700 puede implementar parte o la totalidad del procedimiento 300 de la figura 3. En algunas realizaciones, el dispositivo 700 puede implementar parte o la totalidad del procedimiento 400 de la figura 4. En algunas realizaciones, el dispositivo 700 puede ser implementado por el terminal 1000 de la figura 10. En algunas realizaciones, el dispositivo 700 puede ser implementado por el sistema 1100 de la figura 11.

[0124] El dispositivo 700 se puede implementar en un terminal. El dispositivo 700 puede incluir un módulo de envío 710, un módulo de recepción 720, un módulo de obtención 730 y un módulo de confirmación 740.

[0125] El módulo de envío 710 puede configurarse para enviar una solicitud de verificación de seguridad a un servidor.

[0126] El módulo de recepción 720 se puede configurar para recibir un identificador único de objeto digital enviado por el servidor. El identificador único de objeto digital puede ser un identificador único generado de acuerdo con (por ejemplo, basado al menos en parte en) la primera información del elemento de verificación después de que el servidor haya obtenido la primera información del elemento de verificación de acuerdo con la solicitud de verificación de seguridad enviada por el módulo de envío 710.

[0127] El módulo de obtención 730 se puede configurar para obtener la segunda información del elemento de verificación usando el identificador único de objeto digital recibido por la unidad de recepción 720.

[0128] El módulo de envío 710 se puede configurar adicionalmente para enviar la segunda información del elemento de verificación obtenida por el módulo de obtención 730 al servidor.

[0129] El módulo de confirmación 740 se puede configurar para recibir un resultado de la comprobación de seguridad. El módulo de confirmación 740 puede recibir información del pase de comprobación de seguridad enviada por el servidor. El servidor puede enviar la información del pase de verificación de seguridad en caso de que el servidor confirme que la primera información del elemento de verificación y la segunda información del elemento de verificación enviada por el módulo de envío 710 están de acuerdo.

[0130] La figura 8 es un diagrama de bloques de un dispositivo de verificación de seguridad de acuerdo con varias realizaciones de la presente descripción de la presente solicitud.

[0131] Con referencia a la figura 8, se proporciona un dispositivo 800 para realizar una comprobación de seguridad. En algunas realizaciones, el dispositivo 800 puede implementar parte o la totalidad del procedimiento 200 de la figura 2. En algunas realizaciones, el dispositivo 800 puede implementar parte o la totalidad del procedimiento 300 de la figura 3. En algunas realizaciones, el dispositivo 800 puede implementar parte o la totalidad del procedimiento 400 de la figura 4. En algunas realizaciones, el dispositivo 800 puede ser implementado por el terminal 1000 de la

figura 10. En algunas realizaciones, el dispositivo 800 puede ser implementado por el sistema 1100 de la figura 11.

[0132] El dispositivo 800 se puede implementar en un terminal. El dispositivo 800 puede incluir un módulo de envío 810, un módulo de recepción 820, un módulo de obtención 830, un módulo de comparación 840 y un módulo de confirmación 850.

[0133] El módulo de envío 810 puede configurarse para enviar una solicitud de verificación de seguridad a un servidor.

[0134] El módulo de recepción 820 se puede configurar para recibir un identificador único de objeto digital enviado por el servidor. El identificador único de objeto digital puede corresponder a un identificador único generado de acuerdo con (por ejemplo, basado al menos en parte en) la primera información del elemento de verificación después de que el servidor haya obtenido la primera información del elemento de verificación de acuerdo con la solicitud de verificación de seguridad enviada por el módulo de envío 810.

[0135] El módulo de obtención 830 puede incluir un submódulo de escaneo de identificador 831 y un submódulo de descomposición de cadena de caracteres 832.

[0136] El submódulo de escaneo de identificador 831 puede obtener una segunda cadena de caracteres de combinación escaneando el identificador único de objeto digital recibido por el módulo de recepción 820. El identificador único de objeto digital puede corresponder a un identificador único de objeto digital generado a partir de una primera cadena de caracteres de combinación. El servidor puede generar la primera cadena de caracteres de combinación combinando un primer identificador de terminal, un primer código de verificación de seguridad y una primera marca de tiempo. La primera información del elemento de verificación puede incluir el primer identificador de terminal, el primer código de verificación de seguridad y la primera marca de tiempo. El primer identificador de terminal puede corresponder al identificador de terminal del terminal. El primer identificador de terminal se puede obtener según el nombre de usuario de terminal que se lleva en la solicitud de verificación de seguridad. El primer código de verificación de seguridad y la primera marca de tiempo pueden corresponder respectivamente al código de verificación de seguridad y la marca de tiempo que genera el servidor en relación con la solicitud de verificación de seguridad.

[0137] El submódulo de descomposición de cadena de caracteres 832 se puede configurar para descomponer la segunda cadena de caracteres de combinación obtenida por el submódulo de escaneo de identificadores 831. El submódulo de descomposición de cadena de caracteres 832 se puede configurar para obtener la segunda información del elemento de verificación mediante la descomposición de la segunda cadena de caracteres de combinación. La segunda información del elemento de verificación puede incluir un segundo identificador de terminal, un segundo código de verificación de seguridad y una segunda marca de tiempo.

[0138] El módulo de comparación 840 puede configurarse para comparar el segundo identificador de terminal obtenido por el submódulo de descomposición de cadena de caracteres 832 y el identificador de terminal del terminal.

[0139] El módulo de envío 810 se puede configurar adicionalmente para enviar la segunda información del elemento de verificación al servidor. Por ejemplo, el módulo de envío puede enviar la segunda información del elemento de verificación al servidor en el caso de que el resultado de comparación del módulo de comparación 840 indique que el segundo identificador de terminal y el identificador de terminal del terminal coinciden (por ejemplo, son los mismos).

[0140] El módulo de confirmación 850 se puede configurar para recibir un resultado de la comprobación de seguridad. El módulo de confirmación 850 puede recibir información del pase de comprobación de seguridad enviada por el servidor. El servidor puede enviar la información del pase de verificación de seguridad en caso de que el servidor confirme que la primera información del elemento de verificación y la segunda información del elemento de verificación enviada por el módulo de envío 810 están de acuerdo.

[0141] En algunas realizaciones, el submódulo de escaneo de identificadores 831 puede configurarse para decodificar, de acuerdo con una regla de decodificación QR, el código de verificación bidimensional que corresponde al identificador único de objeto digital y que fue recibido por la unidad de recepción 820. El submódulo de escaneo de identificadores 831 se puede configurar adicionalmente para generar una cadena de caracteres base 64, para convertir la cadena de caracteres base 64 en una cadena de caracteres cifrada y para descifrar la cadena de caracteres cifrada para obtener la segunda cadena de caracteres de combinación.

[0142] Los módulos descritos anteriormente en relación con las figuras 5-8 pueden ser componentes separados que pueden o no estar físicamente separados. Los módulos se pueden ubicar en un solo lugar, o los módulos se pueden distribuir a través de múltiples unidades de red. Los esquemas de la presente solicitud se pueden realizar seleccionando parte o la totalidad de los módulos de acuerdo con la necesidad real.

[0143] La figura 9 es un diagrama de bloques de una realización de un servidor de acuerdo con varias

realizaciones de la presente descripción de la presente solicitud.

[0144] Con referencia a la figura 9, se proporciona un servidor 900 para realizar una comprobación de seguridad. En algunas realizaciones, el servidor 900 puede implementar parte o la totalidad del procedimiento 200 de la figura 2. En algunas realizaciones, el servidor 900 puede implementar parte o la totalidad del procedimiento 300 de la figura 3. En algunas realizaciones, el servidor 900 puede implementar parte o la totalidad del procedimiento 400 de la figura 4. En algunas realizaciones, el servidor 900 puede ser implementado en el sistema 1000 de la figura 10. En algunas realizaciones, el servidor 900 puede ser implementado en el sistema 1100 de la figura 11.

[0145] El servidor 900 puede incluir un procesador 910, un dispositivo de almacenamiento 920 para almacenar comandos ejecutables por el procesador 910, una interfaz de entrada/salida (no mostrada), una interfaz de Internet (no mostrada) y varios hardware (no mostrado).

[0146] El procesador 910 se puede configurar para recibir una solicitud de verificación de seguridad enviada desde un terminal, para obtener la primera información del elemento de verificación de acuerdo con la solicitud de verificación de seguridad, para usar la primera información del elemento de verificación como base para generar un identificador único de objeto digital, para enviar el identificador único de objeto digital al terminal y para recibir la segunda información del elemento de verificación enviada por el terminal. La segunda información del elemento de verificación puede corresponder a la información del elemento de verificación obtenida por el terminal a través (por ejemplo, usando) el identificador único de objeto digital.

[0147] En algunas realizaciones, el procesador 910 puede configurarse para enviar una indicación de un resultado del resultado de la comprobación de seguridad. El procesador 910 puede determinar si la primera información del elemento de verificación y la segunda información del elemento de verificación están de acuerdo (por ejemplo, coinciden). En el caso de que el procesador 910 determine que la primera información del elemento de verificación y la segunda información del elemento de verificación están de acuerdo (por ejemplo, coinciden), el procesador 910 envía información del pase de verificación de seguridad al terminal.

[0148] El dispositivo de almacenamiento 920 puede almacenar una asignación entre un identificador de usuario y un identificador de terminal. El dispositivo de almacenamiento 920 puede almacenar la asignación entre el identificador de usuario y el identificador de terminal en una tabla, una base de datos, similares o cualquier combinación de los mismos. El dispositivo de almacenamiento 920 puede almacenar una relación entre el primer identificador de terminal, el primer código de verificación de seguridad y la primera marca de tiempo.

[0149] La figura 10 es un diagrama de bloques de un terminal de acuerdo con varias realizaciones de la presente descripción de la presente solicitud.

[0150] Con referencia a la figura 10, se proporciona un terminal 1000 para realizar una comprobación de seguridad. En algunas realizaciones, el terminal 1000 puede implementar parte o la totalidad del procedimiento 200 de la figura 2. En algunas realizaciones, el terminal 1000 puede implementar parte o la totalidad del procedimiento 300 de la figura 3. En algunas realizaciones, el terminal 1000 puede implementar parte o la totalidad del procedimiento 400 de la figura 4. En algunas realizaciones, el terminal 1000 puede ser implementado en el sistema 1100 de la figura 11.

[0151] El terminal 1000 puede incluir un procesador 1010, un dispositivo de almacenamiento 1020 que almacena comandos ejecutables por el procesador 1010, una interfaz de entrada/salida (no mostrada), una interfaz de Internet (no mostrada) y varios hardware (no mostrado).

[0152] El procesador 1010 puede configurarse para enviar una solicitud de verificación de seguridad a un servidor. El procesador 1010 se puede configurar adicionalmente para recibir un identificador único de objeto digital enviado de vuelta por el servidor. El identificador único de objeto digital puede corresponder a un identificador único generado de acuerdo con la información del primer elemento de verificación después de que el servidor haya obtenido la información del primer elemento de verificación de acuerdo con la solicitud de verificación de seguridad. El procesador 1010 se puede configurar adicionalmente para obtener información del segundo elemento de verificación a través del identificador único de objeto digital. El procesador 1010 se puede configurar adicionalmente para enviar la segunda información del elemento de verificación al servidor.

[0153] En algunas realizaciones, el procesador 1010 puede configurarse para recibir un resultado de la comprobación de seguridad. El procesador 1010 puede recibir información del pase de comprobación de seguridad enviada por el servidor. El servidor puede enviar la información del pase de verificación de seguridad en caso de que el servidor confirme que la primera información del elemento de verificación y la segunda información del elemento de verificación están de acuerdo.

[0154] El dispositivo de almacenamiento 1020 puede almacenar un identificador. Por ejemplo, el identificador puede corresponder a un nombre de usuario, un identificador de terminal, similares o cualquier combinación de estos.

[0155] El identificador único de objeto digital se puede usar para transmitir información de verificación durante una comprobación de seguridad. Se puede transmitir información de confirmación más rica y fiable en relación con un identificador único de objeto digital que en una comprobación de seguridad de acuerdo con alguna técnica relacionada que implemente un mensaje de texto que incluya números escritos. En algunas realizaciones, la información de confirmación transmitida en conexión con el identificador único de objeto digital es relativamente difícil de robar y usar. Por consiguiente, la seguridad de acceso de las aplicaciones de Internet puede mejorarse mediante el uso de identificadores únicos de objetos digitales en la comunicación de la información de confirmación en lugar de mensajes de texto en relación con la comunicación de números escritos. De acuerdo con diversas realizaciones, el identificador único de objeto digital se transmite a través del tráfico de Internet y, por lo tanto, evita los cargos de comunicación que surgen cuando los códigos de verificación se transmiten a través de mensajes de texto. Como resultado, en diversas realizaciones, hay una reducción en los recursos de comunicación móvil necesarios para realizar una comprobación de seguridad. De acuerdo con algunas realizaciones, en respuesta a que el terminal reconozca el identificador único de objeto digital o la información incluida en el identificador único de objeto digital, el terminal puede devolver automáticamente información de reconocimiento al servidor. Por consiguiente, el procedimiento de comprobación de seguridad de acuerdo con diversas realizaciones no requiere la entrada manual por parte del usuario y evita la posibilidad de información de confirmación de fraude manual. Además, la eficiencia de la comprobación de seguridad se eleva efectivamente porque el terminal puede implementar una primera re-verificación en el procedimiento de comprobación de seguridad al confirmar el identificador del terminal.

[0156] La figura 11 es un diagrama de bloques estructurales de un sistema para proporcionar seguridad de acuerdo con varias realizaciones de la presente solicitud.

[0157] Con referencia a la figura 11, se proporciona un sistema 1100 para proporcionar seguridad. En algunas realizaciones, el sistema 1100 puede implementar parte o la totalidad del procedimiento 200 de la figura **2.** En algunas realizaciones, el sistema 1100 puede implementar parte o la totalidad del procedimiento 300 de la figura 3. En algunas realizaciones, el sistema 1100 puede implementar parte o la totalidad del procedimiento 400 de la figura 4. En algunas realizaciones, el dispositivo 500 de la figura 5 puede implementarse mediante el sistema 1100. En algunas realizaciones, el dispositivo 600 de la figura 6 puede implementarse mediante el sistema 1100. En algunas realizaciones, el dispositivo 700 de la figura 7 puede implementarse mediante el sistema 1100. En algunas realizaciones, el dispositivo 800 de la figura 8 puede implementarse mediante el sistema 1100. En algunas realizaciones, el servidor 900 de la figura 9 puede implementarse mediante el sistema 1100. En algunas realizaciones, el terminal 1000 de la figura 10 puede implementarse mediante el sistema 1100.

[0158] El sistema 1100 para proporcionar una comprobación de seguridad incluye un terminal 1110 y un servidor 1120. El sistema 1100 puede incluir una red 1130 a través de la cual el terminal 1110 y el servidor 1120 se comunican. En respuesta a la recepción de una solicitud de verificación de seguridad del terminal 1110, el servidor 1120 puede proporcionar una comprobación de seguridad del terminal 1110 (por ejemplo, el usuario que usa, o de otro modo está asociado con, el terminal 1110).

[0159] La figura 12 es un diagrama funcional de un sistema informático para proporcionar seguridad de acuerdo con varias realizaciones de la presente solicitud.

[0160] Con referencia a la figura 12, se proporciona un sistema informático 1200 para proporcionar seguridad. Como será evidente, otras arquitecturas y configuraciones del sistema informático se pueden utilizar para proporcionar seguridad. El sistema informático 1200, que incluye varios subsistemas como se describe a continuación, incluye al menos un subsistema de microprocesador (también denominado procesador o unidad central de procesamiento (CPU)) 1202. Por ejemplo, el procesador 1202 puede implementarse mediante un procesador de chip único o mediante múltiples procesadores. En algunas realizaciones, el procesador 1202 es un procesador digital de propósito general que controla el funcionamiento del sistema informático 1200. Usando instrucciones recuperadas de la memoria 1210, el procesador 1202 controla la recepción y manipulación de datos de entrada, y la salida y visualización de datos en dispositivos de salida (por ejemplo, visualización 1218).

[0161] El procesador 1202 está acoplado bidireccionalmente con la memoria 1210, que puede incluir un primer almacenamiento primario, típicamente una memoria de acceso aleatorio (RAM), y una segunda área de almacenamiento primario, típicamente una memoria de solo lectura (ROM). Como es bien sabido en la técnica, el almacenamiento primario se puede utilizar como un área de almacenamiento general y como memoria scratch-pad, y también se puede utilizar para almacenar datos de entrada y datos procesados. El almacenamiento primario también puede almacenar instrucciones y datos de programación, en forma de objetos de datos y objetos de texto, además de otros datos e instrucciones para procedimientos que operan en el procesador 1202. También, como es bien conocido en la materia, el almacenamiento primario típicamente incluye instrucciones de funcionamiento básicas, código de programa, datos y objetos utilizados por el procesador 1202 para realizar sus funciones (por ejemplo, instrucciones programadas). Por ejemplo, la memoria 1210 puede incluir cualquier medio de almacenamiento legible por ordenador adecuado, descrito a continuación, dependiendo de si, por ejemplo, el acceso a los datos debe ser bidireccional o unidireccional. Por ejemplo, el procesador 1202 también puede recuperar y almacenar directa y rápidamente los datos que se necesitan con frecuencia en una memoria caché (no mostrada). La memoria puede ser un medio de

almacenamiento legible por ordenador no transitorio.

[0162] Un dispositivo de almacenamiento masivo extraíble 1212 proporciona capacidad de almacenamiento de datos adicional para el sistema informático 1200 y se acopla bidireccionalmente (lectura/escritura) o unidireccionalmente (solo lectura) al procesador 1202. Por ejemplo, el almacenamiento 1212 también puede incluir medios legibles por ordenador tales como cinta magnética, memoria flash, PC-CARDS, dispositivos portátiles de almacenamiento masivo, dispositivos de almacenamiento holográfico y otros dispositivos de almacenamiento. Un almacenamiento masivo fijo 1220 también puede, por ejemplo, proporcionar capacidad de almacenamiento de datos adicional. El ejemplo más común de almacenamiento masivo 1220 es una unidad de disco duro. El dispositivo de almacenamiento masivo 1212 y el almacenamiento masivo fijo 1220 generalmente almacenan instrucciones de programación adicionales, datos y similares que típicamente no están en uso activo por el procesador 1202. Se apreciará que la información retenida dentro del dispositivo de almacenamiento masivo 1212 y el almacenamiento masivo fijo 1220 se puede incorporar, si es necesario, de manera estándar como parte de la memoria 1210 (por ejemplo, RAM) como memoria virtual.

[0163] Además de proporcionar acceso al procesador 1202 a los subsistemas de almacenamiento, el bus 1214 también se puede utilizar para proporcionar acceso a otros subsistemas y dispositivos. Tal como se muestra, estos pueden incluir un monitor de visualización 1218, una interfaz de red 1216, un teclado 1204 y un dispositivo apuntador 1206, así como una interfaz de dispositivo auxiliar de entrada/salida, una tarjeta de sonido, altavoces y otros subsistemas según sea necesario. Por ejemplo, el dispositivo apuntador 1206 puede ser un ratón, un lápiz óptico, una bola de seguimiento o una tableta, y es útil para interactuar con una interfaz gráfica de usuario.

[0164] La interfaz de red 1216 permite que el procesador 1202 se acople a otro ordenador, red informática o red de telecomunicaciones usando una conexión de red como se muestra. Por ejemplo, a través de la interfaz de red 1216, el procesador 1202 puede recibir información (por ejemplo, objetos de datos o instrucciones de programa) de otra red o información de salida a otra red en el curso de realizar etapas de procedimiento/proceso. La información, a menudo representada como una secuencia de instrucciones para ser ejecutada en un procesador, puede ser recibida y enviada a otra red. Se puede usar una tarjeta de interfaz o dispositivo similar y software apropiado implementado por (por ejemplo, ejecutado/realizado en) el procesador 1202 para conectar el sistema informático 1200 a una red externa y transferir datos de acuerdo con los protocolos estándar. Por ejemplo, varias realizaciones de procedimiento descritas en esta invención pueden ejecutarse en el procesador 1202, o pueden realizarse a través de una red tal como Internet, redes de intranet o redes de área local, junto con un procesador remoto que comparte una parte del procesamiento. Los dispositivos de almacenamiento masivo adicionales (no mostrados) también se pueden conectar al procesador 1202 a través de la interfaz de red 1216.

[0165] Se puede utilizar una interfaz de dispositivo de E/S auxiliar (no mostrada) junto con el sistema informático 1200. La interfaz de dispositivo de E/S auxiliar puede incluir interfaces generales y personalizadas que permiten que el procesador 1202 envíe y, más típicamente, reciba datos de otros dispositivos tales como micrófonos, pantallas sensibles al tacto, lectores de tarjetas transductoras, lectores de cinta, reconocimientos de voz o escritura a mano, lectores de biometría, cámaras, dispositivos de almacenamiento masivo portátiles y otros ordenadores.

[0166] El sistema informático que se muestra en la figura 12 no es más que un ejemplo de un sistema informático adecuado para su uso con las diversas realizaciones descritas en esta invención. Otros sistemas informáticos adecuados para dicho uso pueden incluir subsistemas adicionales o menos. Además, el autobús 1214 ilustra cualquier esquema de interconexión que sirva para enlazar los subsistemas. También se pueden utilizar otras arquitecturas informáticas que tienen diferentes configuraciones de subsistemas.

[0167] Lo anterior son meramente realizaciones de la presente solicitud y no limitan la presente solicitud. Para un experto en la materia, la presente solicitud puede tener diversos cambios y variaciones.

[0168] Aunque las realizaciones anteriores se han descrito con cierto detalle con fines de claridad de comprensión, la invención no se limita a los detalles proporcionados. Hay muchas formas alternativas de implementar la invención. Las realizaciones descritas son ilustrativas y no restrictivas.

REIVINDICACIONES

1. Un procedimiento, que comprende:

recibir (210), por un servidor, una solicitud de verificación de seguridad enviada desde un terminal (110);
obtener, a partir de un identificador incluido en la solicitud de verificación de seguridad recibida, un primer identificador de terminal que identifica el terminal;
obtener (220), mediante el servidor, una primera información del elemento de verificación en función del primer identificador de terminal, una primera marca de tiempo y un primer código de verificación de seguridad;
generar (230), mediante el servidor, un identificador único de objeto digital (130) en función al menos en parte de la primera información del elemento de verificación;
enviar (240), mediante el servidor, el identificador único de objeto digital (130) al terminal (110);
recibir (250), por el servidor, una segunda información del elemento de verificación desde el terminal (110),
donde la segunda información del elemento de verificación se genera en función al menos en parte de la información extraída del identificador único de objeto digital (130), la segunda información del elemento de verificación comprende un segundo identificador de terminal y una segunda marca de tiempo, y la segunda información del elemento de verificación es enviada por el terminal al servidor en respuesta a que el terminal (110) determine que el segundo identificador de terminal es el mismo que el primer identificador de terminal; y en respuesta a la determinación de que la primera información del elemento de verificación y la segunda información del elemento de verificación son consistentes, enviar (260) una información del pase de comprobación de seguridad al terminal (110), la determinación de que la primera información del elemento de verificación y la segunda información del elemento de verificación son consistentes comprende comparar la primera información del elemento de verificación con la segunda información del elemento de verificación y comparar la primera marca de tiempo con una hora actual y la segunda marca de tiempo con la hora actual.

2. El procedimiento de la reivindicación 1, donde la segunda información del elemento de verificación corresponde a la primera información del elemento de verificación obtenida por el terminal (110) del identificador único de objeto digital (130).

3. El procedimiento de la reivindicación 1, donde el terminal (110) obtiene la segunda información del elemento de verificación mediante el procesamiento del identificador único de objeto digital (130).

4. Un procedimiento, que comprende:

enviar (310), mediante un terminal (110), una solicitud de verificación de seguridad a un servidor;
recibir (320), mediante el terminal (110), un identificador único de objeto digital (130) del servidor (120), donde el identificador único de objeto digital (130) corresponde a un identificador único generado en función al menos en parte de la primera información del elemento de verificación que el servidor (120) obtiene en función de un primer identificador de terminal que identifica el terminal, una primera marca de tiempo y un primer código de verificación de seguridad;
obtener (330), mediante el terminal (110), una segunda información del elemento de verificación en función al menos en parte de la información extraída del identificador único de objeto digital (130), comprendiendo la segunda información del elemento de verificación un segundo identificador de terminal y una segunda marca de tiempo;
enviar (340), mediante el terminal (110), la segunda información del elemento de verificación al servidor (120), donde la segunda información del elemento de verificación es enviada por el terminal (110) al servidor en respuesta a que el terminal (110) determine que el segundo identificador de terminal es el mismo que el primer identificador de terminal; y
en el caso de que la primera información del elemento de verificación y la segunda información del elemento de verificación sean consistentes, recibir (350) información del pase de comprobación de seguridad del servidor, donde una determinación de que la primera información del elemento de verificación y la segunda información del elemento de verificación son consistentes comprende comparar la primera información del elemento de verificación con la segunda información del elemento de verificación, y comparar la primera marca de tiempo con una hora actual y la segunda marca de tiempo con la hora actual.

5. El procedimiento de la reivindicación 4, donde la obtención (330) de la segunda información del elemento de verificación comprende: procesar el identificador único de objeto digital (130) y obtener la segunda información del elemento de verificación en función al menos en parte del procesamiento del identificador único de objeto digital (130).

6. El procedimiento de la reivindicación 1 o 4, que comprende, además: determinar si al menos parte de la primera información del elemento de verificación y al menos parte de la segunda información del elemento de verificación son consistentes.

7. Un dispositivo de comprobación de seguridad, que comprende:
al menos un procesador (1202) configurado para; o un producto de programa informático, estando el producto de programa informático incorporado en un medio de almacenamiento legible por ordenador no transitorio y

comprendiendo instrucciones informáticas para:

recibir (210) una solicitud de verificación de seguridad enviada desde un terminal (110);
obtener, a partir de un identificador incluido en la solicitud de verificación de seguridad recibida, un primer identificador de terminal que identifica el terminal;
obtener (220) una primera información del elemento de verificación en función del primer identificador de terminal, una primera marca de tiempo y un primer código de verificación de seguridad;
generar (230) un identificador único de objeto digital (130) en función al menos en parte de la primera información del elemento de verificación;
enviar (240) el identificador único de objeto digital al terminal (110);
recibir (250) una segunda información del elemento de verificación del terminal (110), donde la segunda información del elemento de verificación se genera en función al menos en parte de una información extraída del identificador único de objeto digital (130), la segunda información del elemento de verificación comprende un segundo identificador de terminal y una segunda marca de tiempo, y la segunda información del elemento de verificación es enviada por el terminal al servidor en respuesta a que el terminal (110) determine que el segundo identificador de terminal es el mismo que el primer identificador de terminal; y
en respuesta a una determinación de que la primera información del elemento de verificación y la segunda información del elemento de verificación son consistentes, enviar (260) una información del pase de comprobación de seguridad al terminal (110), la determinación de que la primera información del elemento de verificación y la segunda información del elemento de verificación son consistentes comprende comparar la primera información del elemento de verificación con la segunda información del elemento de verificación y comparar la primera marca de tiempo con una hora actual y la segunda marca de tiempo con la hora actual; y donde el dispositivo comprende:
una memoria (1210) acoplada al al menos un procesador (1202) y configurada para proporcionar instrucciones al al menos un procesador (1202).

8. El dispositivo de la reivindicación 7, donde el al menos un procesador (1202) está configurado, además para; o el procedimiento de la reivindicación 1, que comprende, además:

almacenar (410) asignaciones entre nombres de usuario e identificadores de terminal,
donde la obtención por parte del al menos un procesador (1202) de la primera información del elemento de verificación en función al menos en parte de la solicitud de verificación de seguridad comprende:

usar un nombre de usuario del terminal como base para buscar las asignaciones de nombres de usuario e identificadores de terminal para obtener (414) el primer identificador de terminal asociado con el terminal (110), donde el nombre de usuario del terminal (110) se incluye en la solicitud de verificación de seguridad; y
generar (416) un primer código de verificación de seguridad asociado con la solicitud de verificación de seguridad y la primera marca de tiempo asociada con la solicitud de verificación de seguridad, donde la primera marca de tiempo indica un límite de tiempo en una presente comprobación de seguridad, y donde la primera información del elemento de verificación incluye el primer identificador de terminal, el primer código de verificación de seguridad y la primera marca de tiempo.

9. El dispositivo de la reivindicación 8, donde el al menos un procesador (1202) está configurado además para; o el procedimiento de la reivindicación 8, donde la generación del identificador único de objeto digital (130) en función al menos en parte de la primera información del elemento de verificación comprende:

generar (420) una primera cadena de caracteres de combinación mediante la combinación del primer identificador de terminal, el primer código de verificación de seguridad y la primera marca de tiempo; y
generar el identificador único de objeto digital (130) en función al menos en parte de la primera cadena de caracteres de combinación.

10. El dispositivo de la reivindicación 9, donde el al menos un procesador (1202) está configurado además para; o el procedimiento de la reivindicación 9, donde la generación del identificador único de objeto digital (130) en función al menos en parte de la primera cadena de caracteres de combinación comprende:

generar una cadena de caracteres cifrada en función al menos en parte de cifrar la primera cadena de caracteres de combinación;
convertir la cadena de caracteres cifrada en una cadena de caracteres base 64;
codificar la cadena de caracteres base 64 de acuerdo con una regla de codificación de respuesta rápida (QR); y
generar un código de verificación bidimensional, donde el código de verificación bidimensional corresponde al identificador único de objeto digital.

11. El dispositivo como se describe en la reivindicación 8, donde al menos un procesador (1202) está configurado, además para; o el procedimiento de la reivindicación 8, que comprende, además:

guardar relaciones entre el primer identificador de terminal, el primer código de verificación de seguridad y la

primera marca de tiempo,
donde la segunda información del elemento de verificación comprende: el segundo identificador de terminal, un segundo código de verificación de seguridad y la segunda marca de tiempo que se obtienen mediante la descomposición de una segunda cadena de caracteres de combinación, donde la segunda cadena de caracteres de combinación se obtiene (426) mediante el escaneo de terminal del identificador único de objeto digital (130), y donde la segunda información del elemento de verificación corresponde a información enviada desde el terminal en el caso de que el terminal haya comparado el segundo identificador de terminal con el primer identificador de terminal del terminal (110) y determinado que el segundo identificador de terminal y el primer identificador de terminal del terminal (110) son iguales; y
donde el envío de la información del pase de comprobación de seguridad al terminal (110) comprende:

buscar, en función al menos en parte del segundo identificador de terminal, las relaciones entre una pluralidad de primeros identificadores de terminal, una pluralidad de primeros códigos de verificación de seguridad y una pluralidad de primeras marcas de tiempo, y obtener el código de verificación de seguridad y la marca de tiempo, respectivamente, correspondientes al segundo identificador de terminal; y
en el caso de que el segundo código de verificación de seguridad y el código de verificación de seguridad obtenido coincidan, la segunda marca de tiempo y la marca de tiempo obtenida coincidan, y la segunda marca de tiempo se encuentre dentro de un límite de tiempo de una verificación de seguridad actual asociada con la solicitud de verificación de seguridad, enviar una información del pase de comprobación de seguridad al terminal.

12. Un dispositivo, que comprende:
al menos un procesador (1202) configurado para; o un producto de programa informático, estando el producto de programa informático incorporado en un medio de almacenamiento legible por ordenador no transitorio y comprendiendo instrucciones informáticas para:

enviar (310) una solicitud de verificación de seguridad a un servidor (120);
recibir (320) un identificador único de objeto digital (130) del servidor (120), donde el identificador único de objeto digital (130) corresponde a un identificador único generado en función al menos en parte de la primera información del elemento de verificación que el servidor (120) obtiene en función de un primer identificador de terminal que identifica el terminal, una primera marca de tiempo y un primer código de verificación de seguridad;
obtener (330) una segunda información del elemento de verificación en función al menos en parte de una información extraída del identificador único de objeto digital (130), comprendiendo la segunda información del elemento de verificación un segundo identificador de terminal y una segunda marca de tiempo;
enviar (340) la segunda información del elemento de verificación al servidor (120), donde la segunda información del elemento de verificación es enviada por el terminal (110) al servidor en respuesta a que el terminal (110) determine que el segundo identificador de terminal es el mismo que el primer identificador de terminal; y
en el caso de que la primera información del elemento de verificación y la segunda información del elemento de verificación sean consistentes, recibir (350) una información del pase de comprobación de seguridad del servidor (120), donde una determinación de que la primera información del elemento de verificación y la segunda información del elemento de verificación son consistentes comprende comparar la primera información del elemento de verificación con la segunda información del elemento de verificación, y comparar la primera marca de tiempo con una hora actual y la segunda marca de tiempo con la hora actual; y
donde el dispositivo comprende:
una memoria (1210) acoplada al al menos un procesador (1202) y configurada para proporcionar instrucciones al al menos un procesador (1202).

13. El dispositivo de la reivindicación 12, donde el al menos un procesador (1202) está configurado además para; o el procedimiento de la reivindicación 4, donde la obtención de la segunda información del elemento de verificación en función al menos en parte del identificador único de objeto digital (130) comprende:

escanear el identificador único de objeto digital (130);
obtener una segunda cadena de caracteres de combinación en función al menos en parte del escaneo del identificador único de objeto digital (130), donde el identificador único de objeto digital (130) se genera en función al menos en parte de una primera cadena de caracteres de combinación, donde la primera cadena de caracteres de combinación es generada por el servidor (120) que combina el primer identificador de terminal, un primer código de verificación de seguridad y la primera marca de tiempo, donde la primera información del elemento de verificación comprende el primer identificador de terminal, el primer código de verificación de seguridad y la primera marca de tiempo, donde el primer identificador de terminal corresponde a un identificador de terminal de un terminal (110) obtenido en función al menos en parte de un nombre de usuario del terminal (110), donde el nombre de usuario del terminal (110) está incluido en la solicitud de verificación de seguridad, y donde una primera comprobación de seguridad y la primera marca de tiempo corresponden respectivamente al primer código de verificación de seguridad y la primera marca de tiempo que son generados por el servidor (120) en relación con la solicitud de verificación de seguridad;
descomponer la segunda cadena de caracteres de combinación; y

obtener la segunda información del elemento de verificación en función al menos en parte de la descomposición de la segunda cadena de caracteres de combinación, donde la segunda información del elemento de verificación incluye el segundo identificador de terminal, un segundo código de verificación de seguridad y la segunda marca de tiempo.

14. El dispositivo de la reivindicación 13, donde el al menos un procesador (1202) está configurado además para; o donde la obtención de la segunda cadena de caracteres de combinación en función al menos en parte del escaneo del identificador único de objeto digital (130) comprende:

decodificar un código de verificación bidimensional utilizando una regla de decodificación de respuesta rápida (QR), donde el código de verificación bidimensional corresponde al identificador único de objeto digital (130);
generar una cadena de caracteres base 64 en función al menos en parte de la decodificación del código de verificación bidimensional;
convertir la cadena de caracteres base 64 en una cadena de caracteres cifrada; y obtener la segunda cadena de caracteres de combinación en función al menos en parte del descifrado de la cadena de caracteres cifrada.

15. El dispositivo de la reivindicación 13, donde el al menos un procesador (1202) está configurado además para; o el procedimiento de la reivindicación 13, que comprende, además:

comparar el segundo identificador de terminal y un identificador de terminal del terminal (110) antes de que la segunda información del elemento de verificación se envíe al servidor (120); y
en el caso de que el segundo identificador de terminal y el identificador de terminal del terminal (110) coincidan, realizar el envío de la segunda información del elemento de verificación al servidor (120).

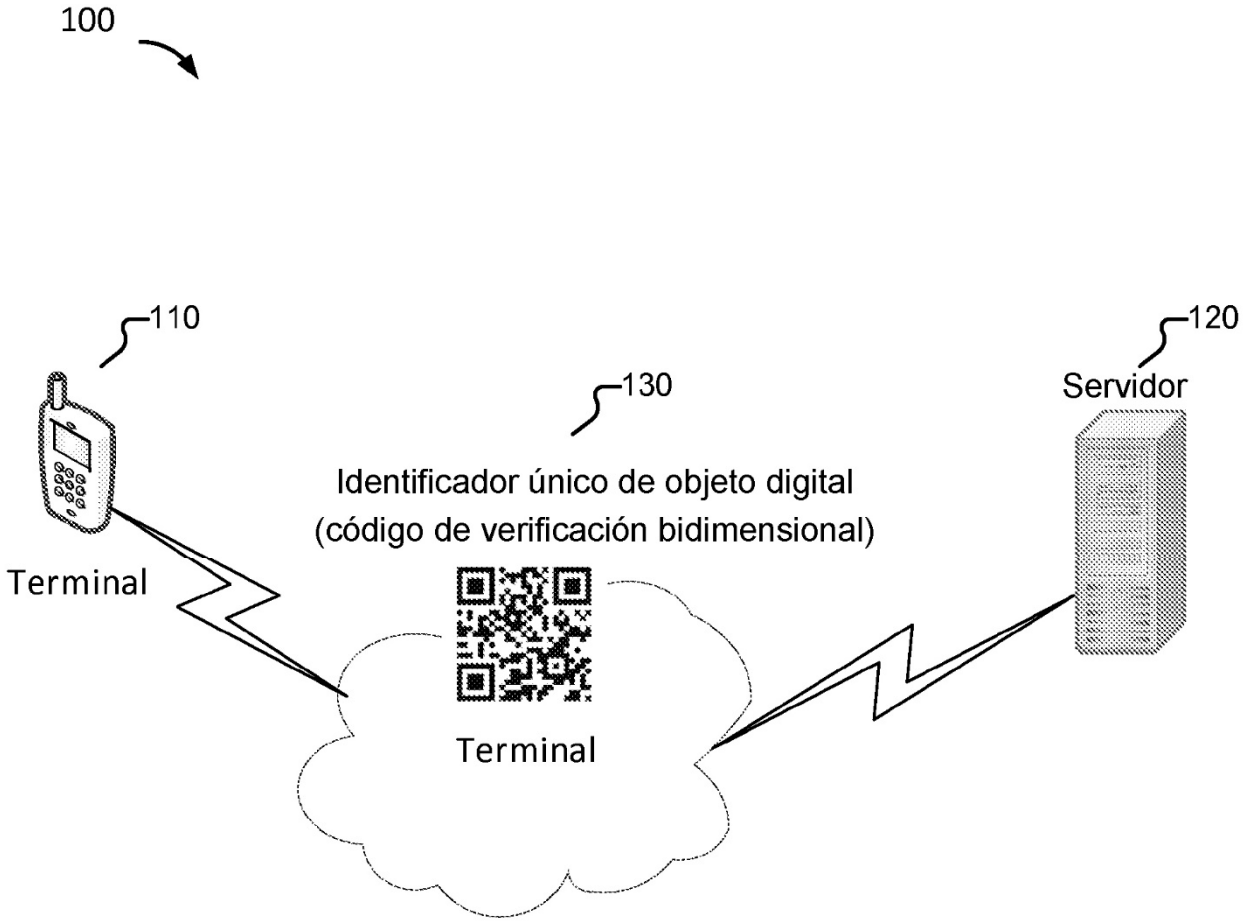
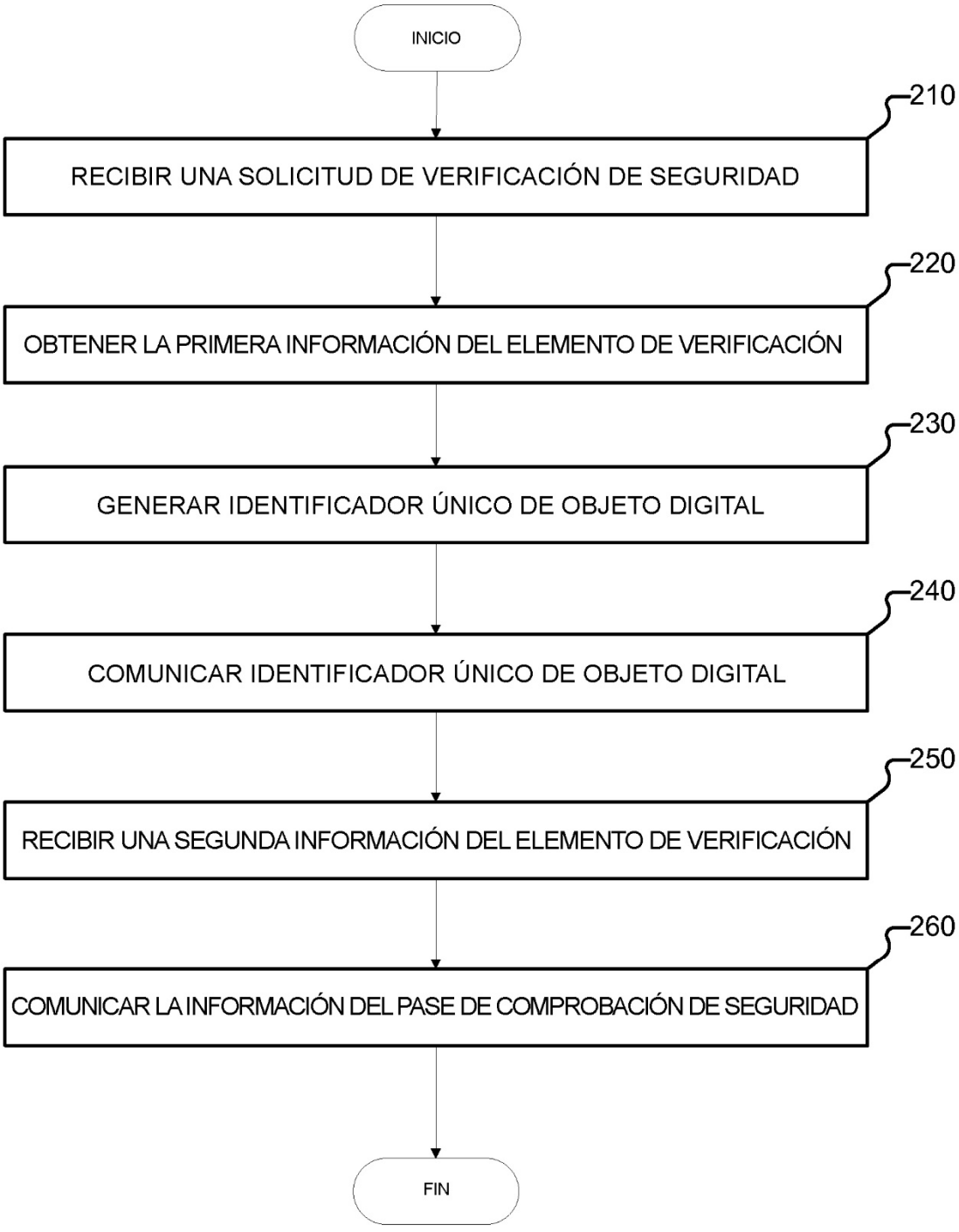
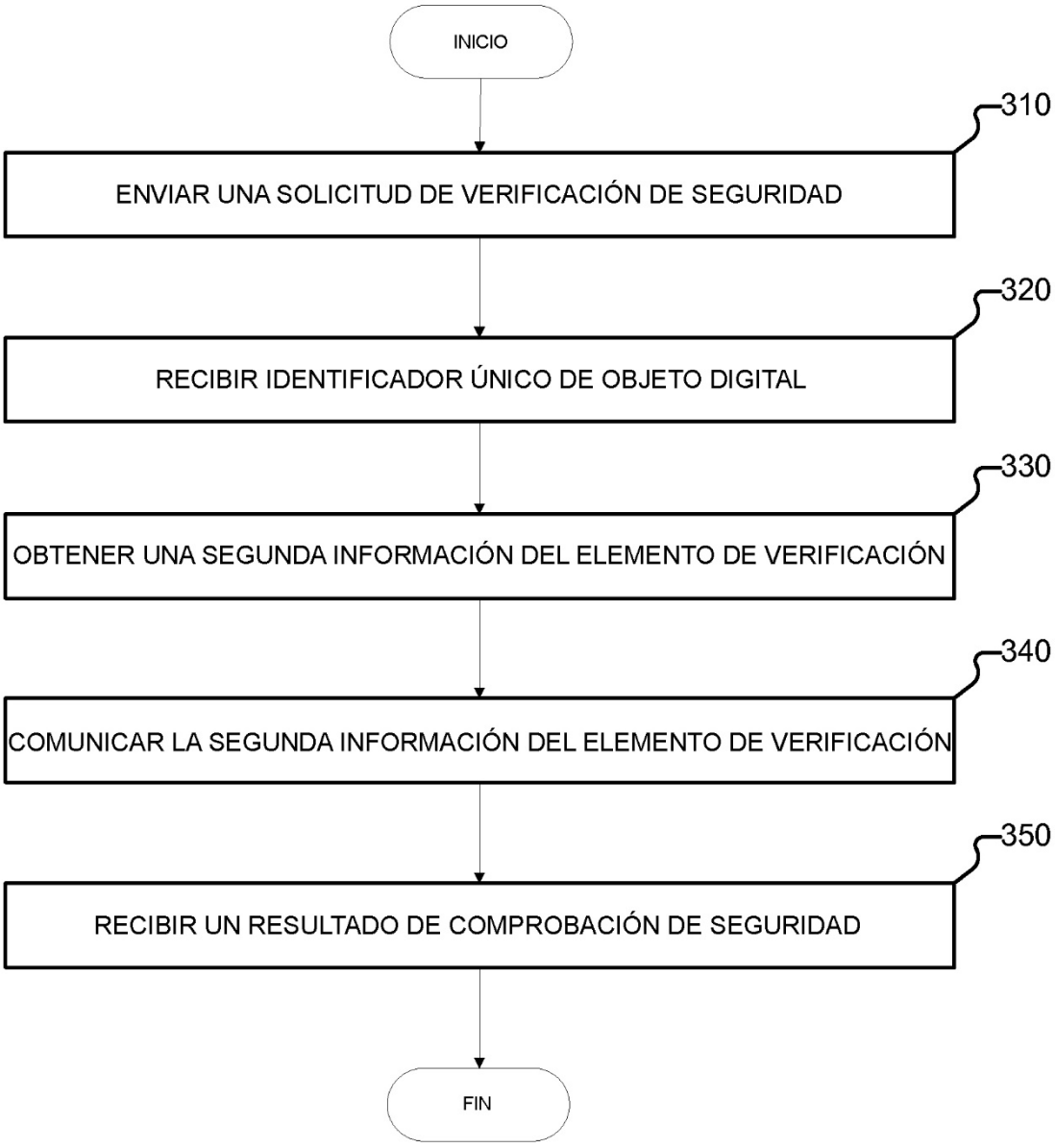

100
110
120
130
Servidor
Identificador único de objeto digital
(código de verificación bidimensional)
Terminal
Terminal

FIG. 1


INICIO
210
RECIBIR UNA SOLICITUD DE VERIFICACIÓN DE SEGURIDAD
220
OBTENER LA PRIMERA INFORMACIÓN DEL ELEMENTO DE VERIFICACIÓN
230
GENERAR IDENTIFICADOR ÚNICO DE OBJETO DIGITAL
240
COMUNICAR IDENTIFICADOR ÚNICO DE OBJETO DIGITAL
250
RECIBIR UNA SEGUNDA INFORMACIÓN DEL ELEMENTO DE VERIFICACIÓN
260
COMUNICAR LA INFORMACIÓN DEL PASE DE COMPROBACIÓN DE SEGURIDAD
FIN

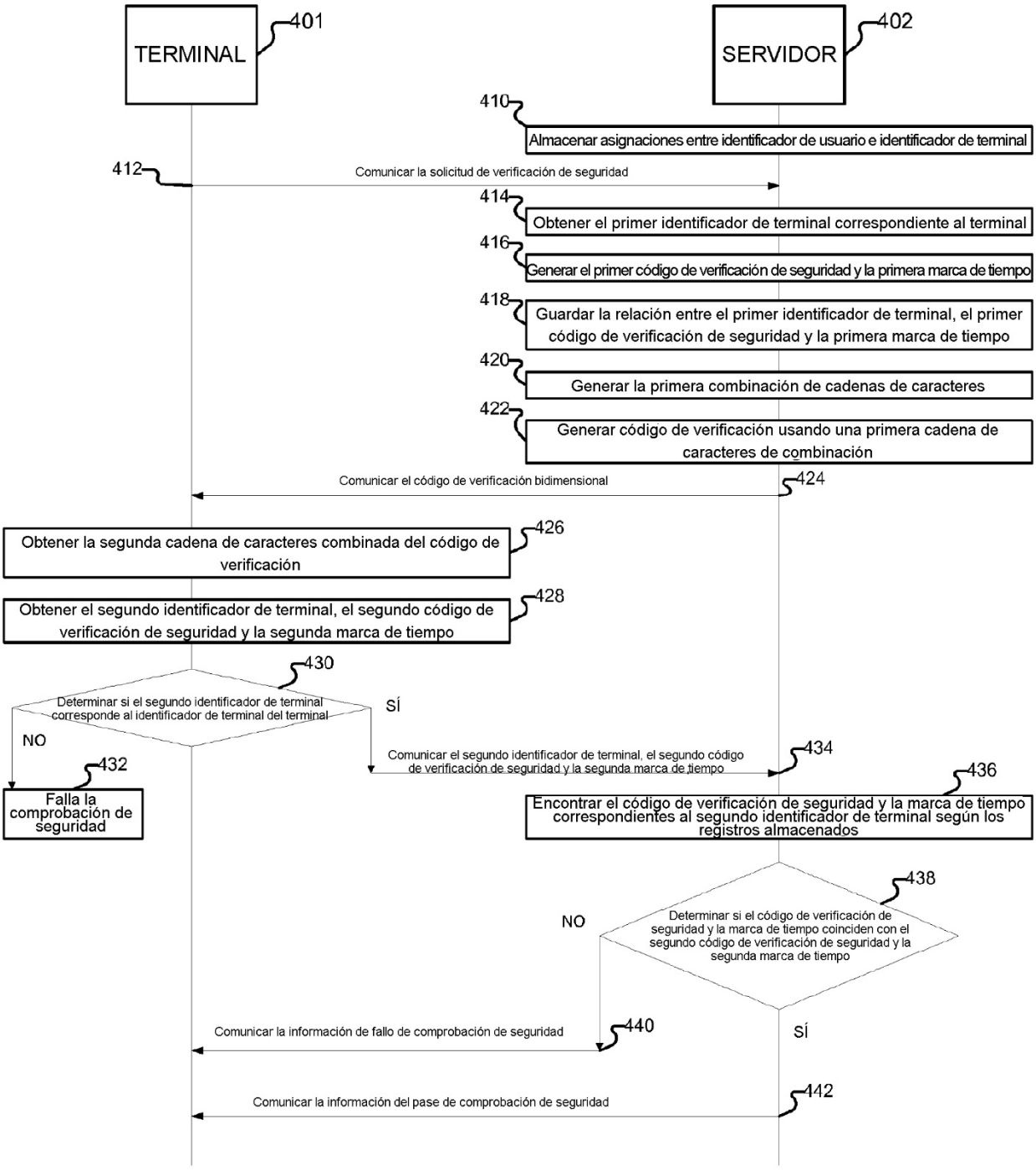
200

FIG. 2


INICIO
310
ENVIAR UNA SOLICITUD DE VERIFICACIÓN DE SEGURIDAD
320
RECIBIR IDENTIFICADOR ÚNICO DE OBJETO DIGITAL
330
OBTENER UNA SEGUNDA INFORMACIÓN DEL ELEMENTO DE VERIFICACIÓN
340
COMUNICAR LA SEGUNDA INFORMACIÓN DEL ELEMENTO DE VERIFICACIÓN
350
RECIBIR UN RESULTADO DE COMPROBACIÓN DE SEGURIDAD
FIN

300

FIG. 3


TERMINAL
401
SERVIDOR
402
410
Almacenar asignaciones entre identificador de usuario e identificador de terminal
412
Comunicar la solicitud de verificación de seguridad
414
Obtener el primer identificador de terminal correspondiente al terminal
416
Generar el primer código de verificación de seguridad y la primera marca de tiempo
418
Guardar la relación entre el primer identificador de terminal, el primer código de verificación de seguridad y la primera marca de tiempo
420
Generar la primera combinación de cadenas de caracteres
422
Generar código de verificación usando una primera cadena de caracteres de combinación
Comunicar el código de verificación bidimensional
424
Obtener la segunda cadena de caracteres combinada del código de verificación
426
Obtener el segundo identificador de terminal, el segundo código de verificación de seguridad y la segunda marca de tiempo
428
430
Determinar si el segundo identificador de terminal corresponde al identificador de terminal del terminal
SÍ
NO
Comunicar el segundo identificador de terminal, el segundo código de verificación de seguridad y la segunda marca de tiempo
434
432
Falla la comprobación de seguridad
436
Encontrar el código de verificación de seguridad y la marca de tiempo correspondientes al segundo identificador de terminal según los registros almacenados
438
NO
Determinar si el código de verificación de seguridad y la marca de tiempo coinciden con el segundo código de verificación de seguridad y la segunda marca de tiempo
Comunicar la información de fallo de comprobación de seguridad
440
SÍ
Comunicar la información del pase de comprobación de seguridad
442

400

FIG. 4

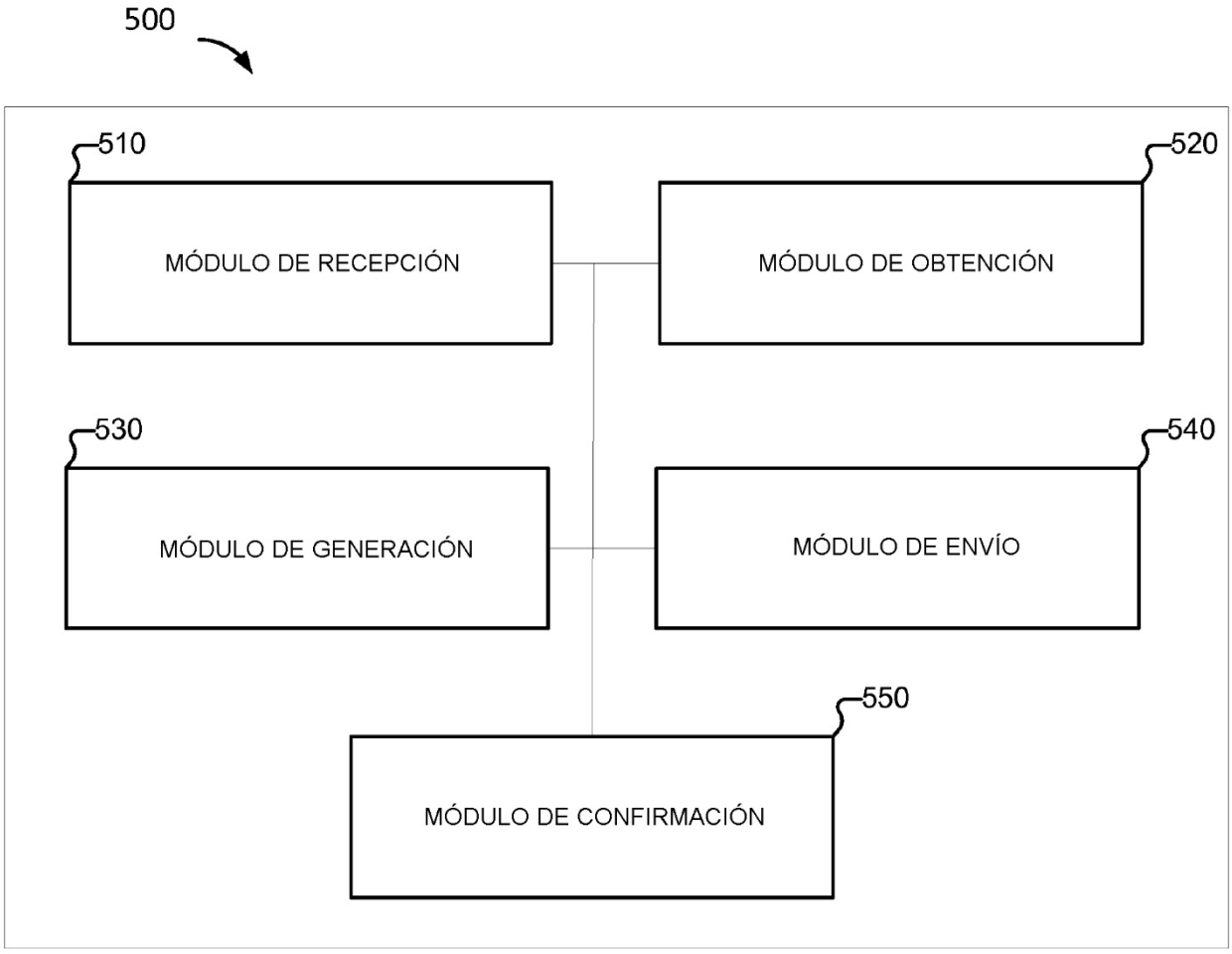

500
510
MÓDULO DE RECEPCIÓN
520
MÓDULO DE OBTENCIÓN
530
MÓDULO DE GENERACIÓN
540
MÓDULO DE ENVÍO
550
MÓDULO DE CONFIRMACIÓN

FIG. 5

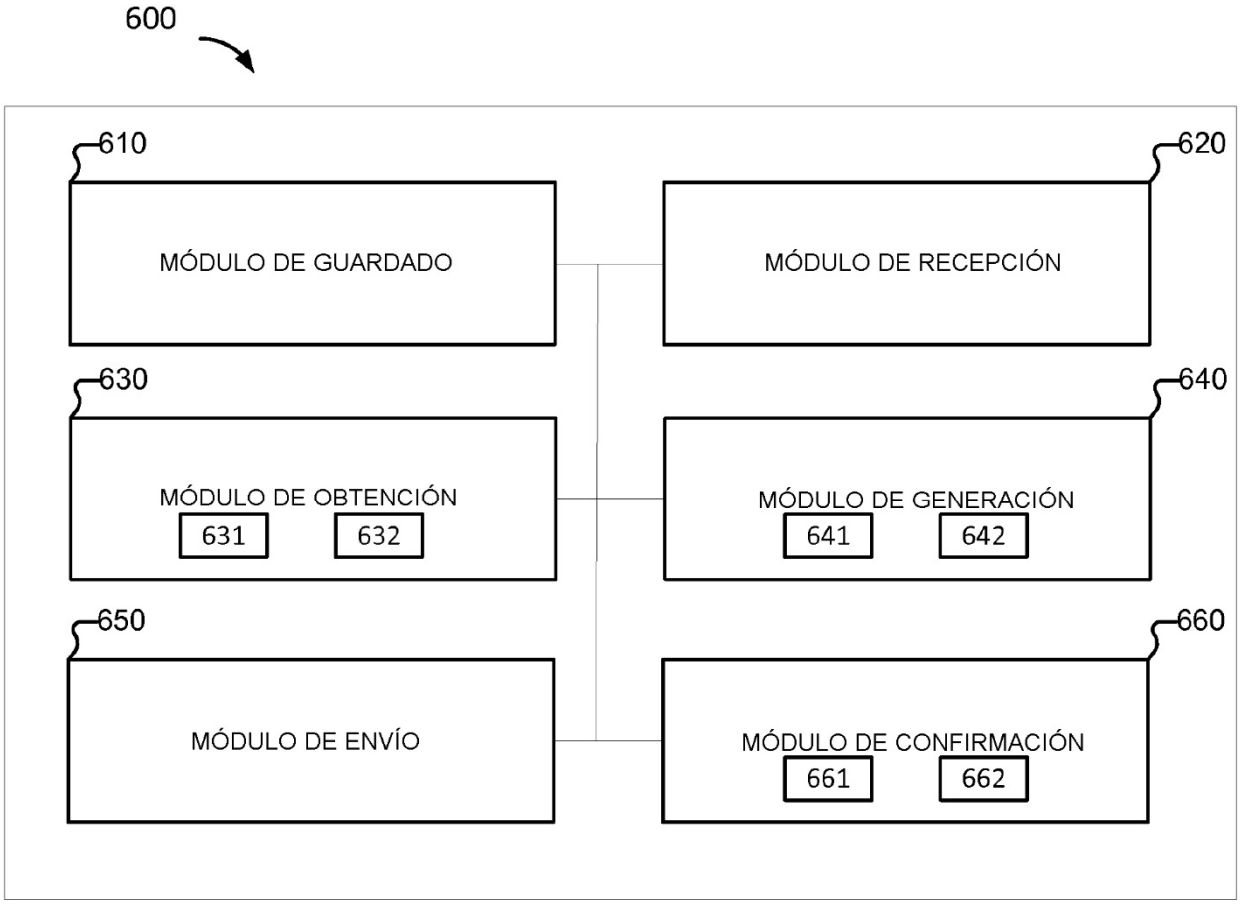

600
610
MÓDULO DE GUARDADO
620
MÓDULO DE RECEPCIÓN
630
MÓDULO DE OBTENCIÓN
631
632
640
MÓDULO DE GENERACIÓN
641
642
650
MÓDULO DE ENVÍO
660
MÓDULO DE CONFIRMACIÓN
661
662

FIG. 6

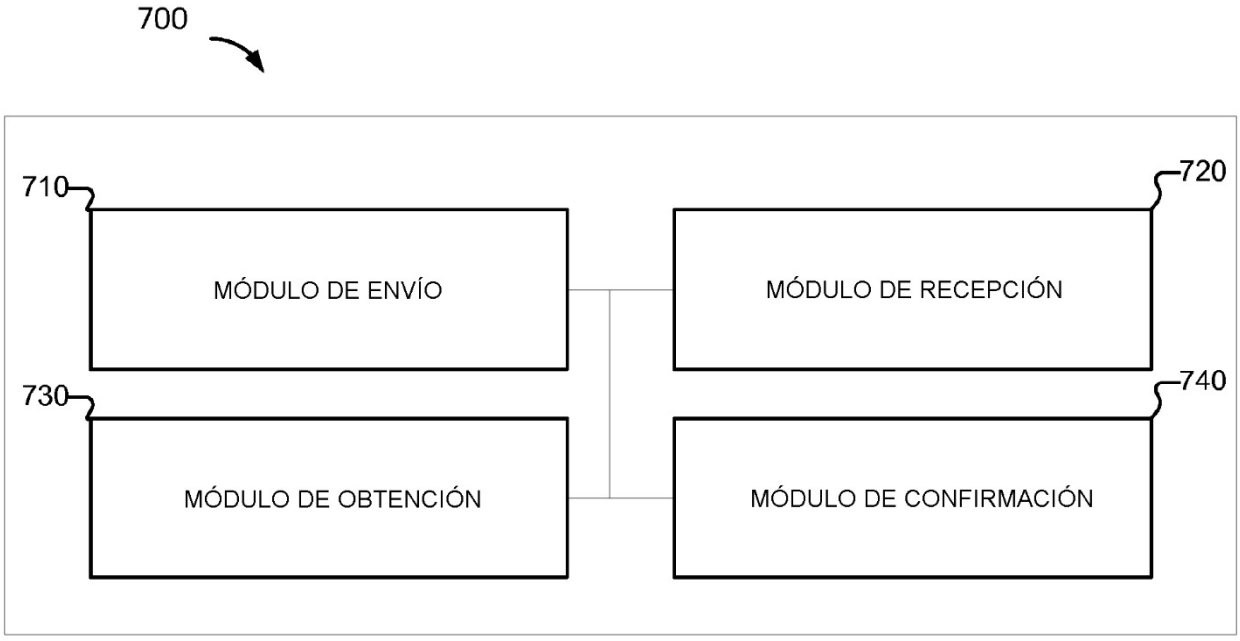

700
710
MÓDULO DE ENVÍO
720
MÓDULO DE RECEPCIÓN
730
MÓDULO DE OBTENCIÓN
740
MÓDULO DE CONFIRMACIÓN

FIG. 7

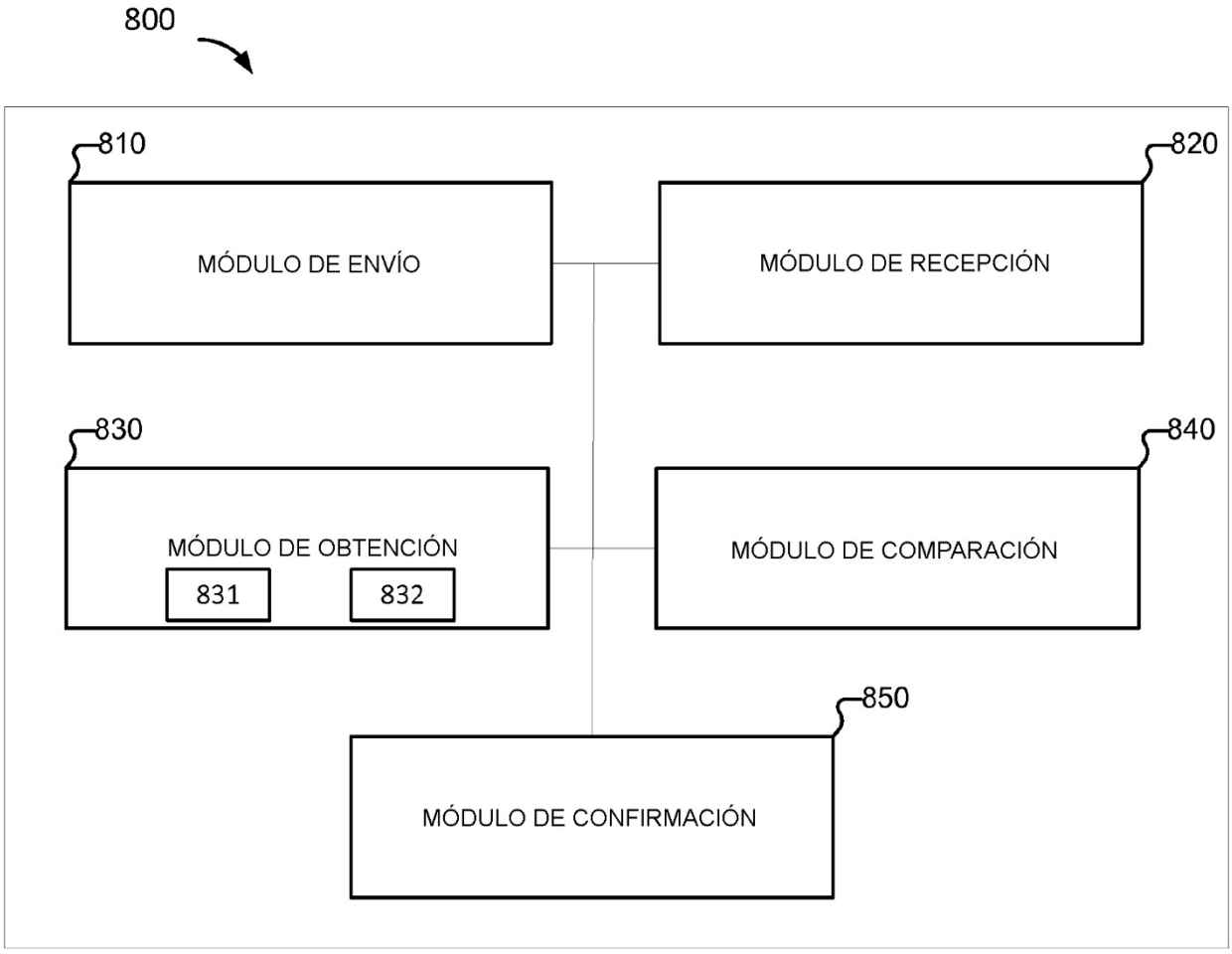

800
810
MÓDULO DE ENVÍO
820
MÓDULO DE RECEPCIÓN
830
MÓDULO DE OBTENCIÓN
831
832
840
MÓDULO DE COMPARACIÓN
850
MÓDULO DE CONFIRMACIÓN

FIG. 8

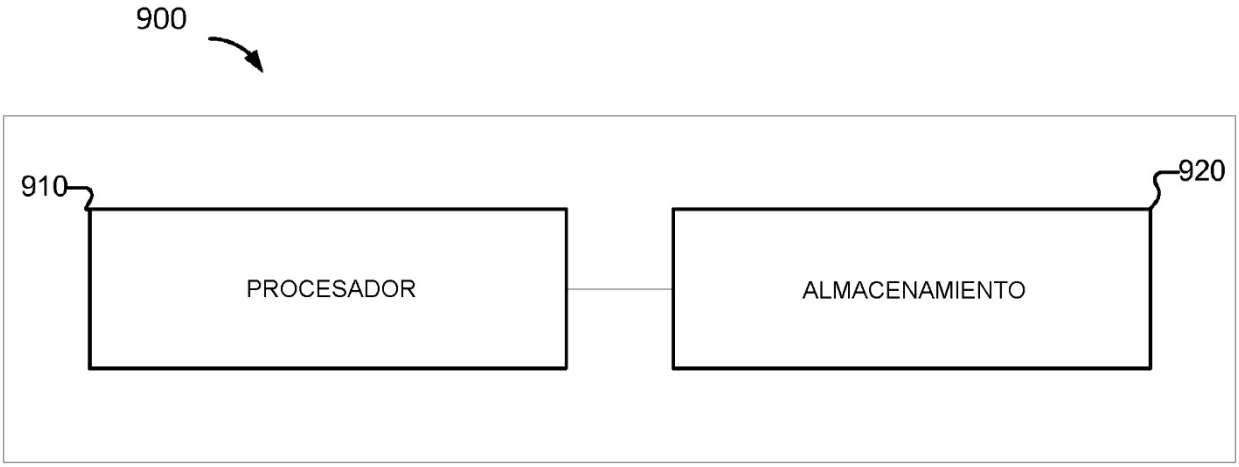


FIG. 9

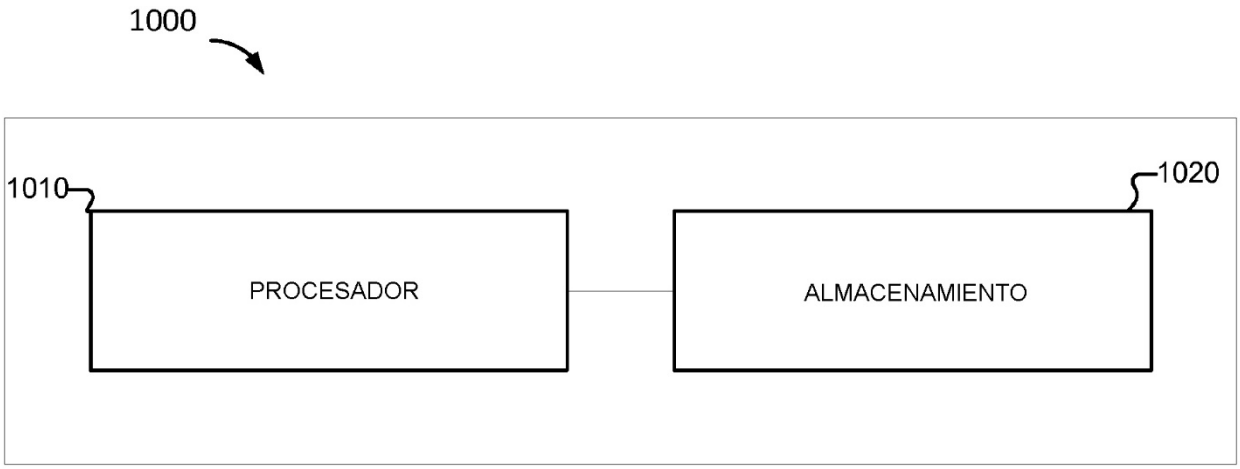


FIG. 10

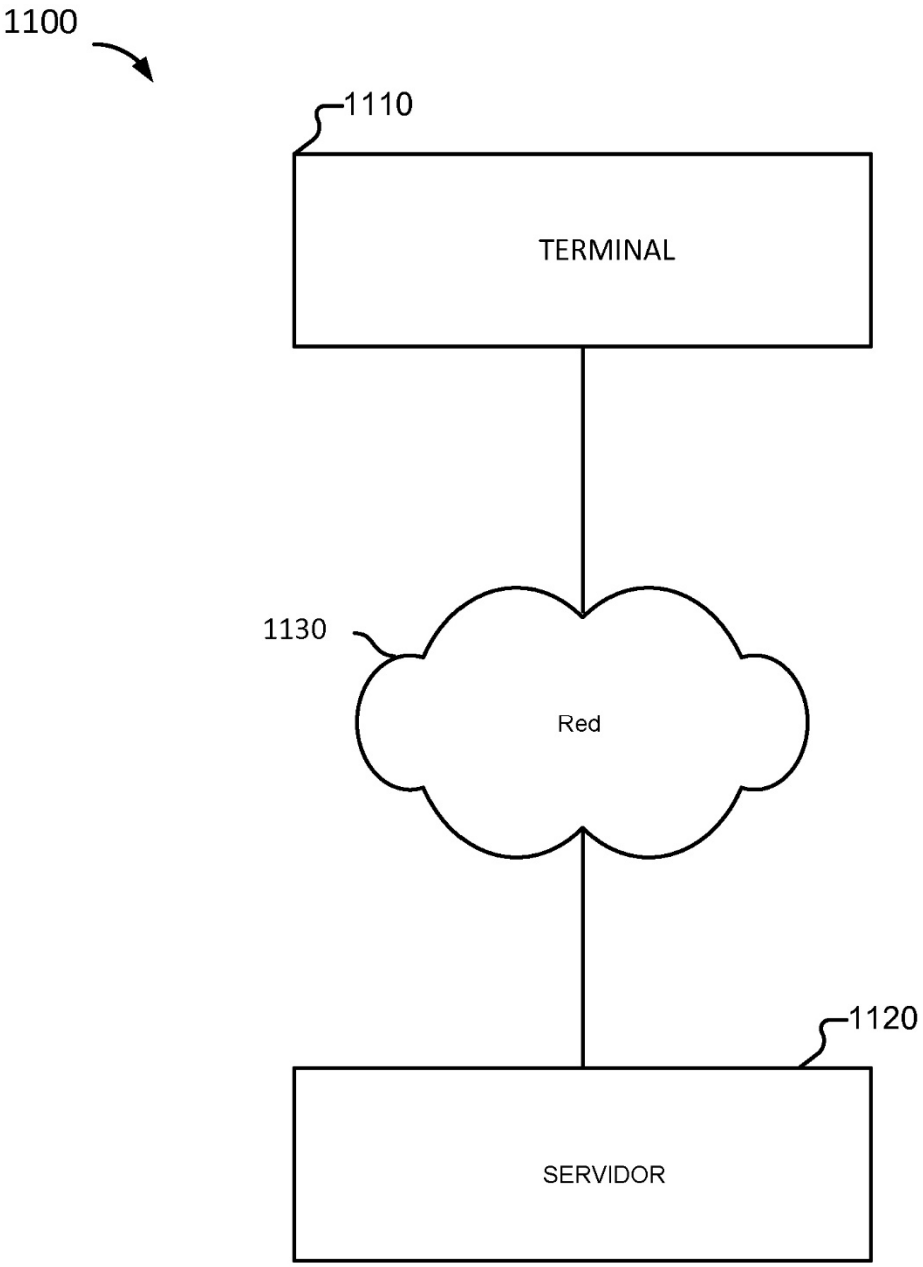


FIG.11

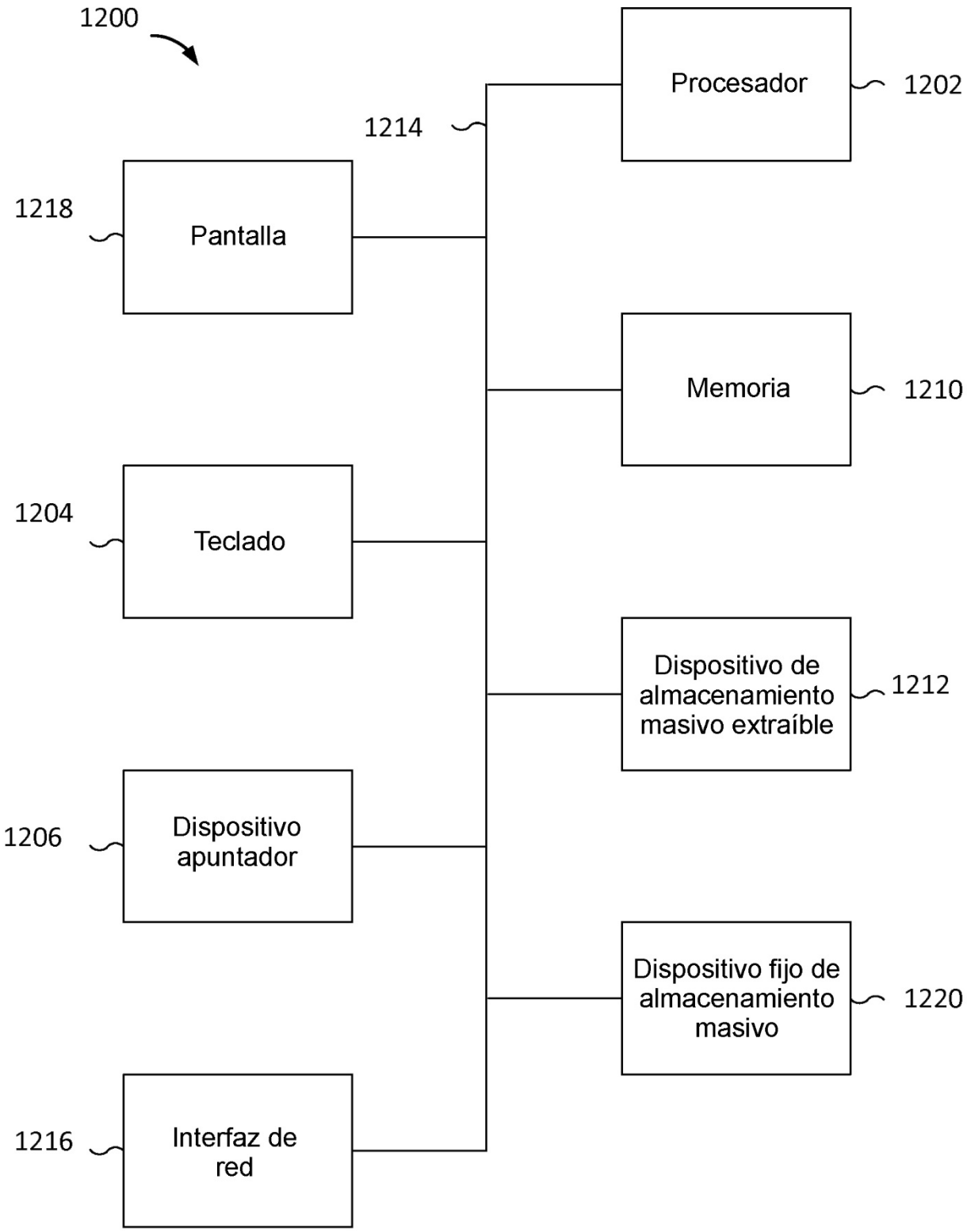

1200
Procesador
1202
1214
1218
Pantalla
Memoria
1210
1204
Teclado
Dispositivo de almacenamiento masivo extraíble
1212
1206
Dispositivo apuntador
Dispositivo fijo de almacenamiento masivo
1220
1216
Interfaz de red

FIG. 12