(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **3 010 167**

(51) Int. Cl.:

H04L 9/40 (2012.01)
H04W 12/065 (2011.01)
H04W 12/71 (2011.01)
H04W 12/68 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **23.02.2022 PCT/US2022/017507**

(87) Fecha y número de publicación internacional: **01.09.2022 WO22182748**

(96) Fecha de presentación y número de la solicitud europea: **23.02.2022 E 22710467 (6)**

(97) Fecha y número de publicación de la concesión europea: **18.12.2024 EP 4298761**

(54) Título: **Establecimiento de persistencia de autenticación**

(30) Prioridad:

24.02.2021 US 202117183888

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
01.04.2025

(73) Titular/es:

CAPITAL ONE SERVICES, LLC (100.00%)
1680 Capital One Drive
McLean, Virginia 22102, US

(72) Inventor/es:

RULE, JEFFREY;
MORETON, PAUL y
POOLE, THOMAS

(74) Agente/Representante:

SÁEZ MAESO, Ana

DESCRIPCIÓN

Establecimiento de persistencia de autenticación

Referencia cruzada con solicitudes relacionadas

Esta solicitud reivindica prioridad de la Solicitud de patente estadounidense con número de serie 17/183,888, titulada “ESTABLISHING AUTHENTICATION PERSISTENCE” presentada el 24 de febrero de 2021.

Antecedentes

La autenticación puede ser el acto de probar o verificar una afirmación, como la identidad de un usuario de un dispositivo informático. Las formas en que se autentica al usuario pueden dividirse en tres categorías según lo que se conoce como factores de autenticación: algo que el usuario sabe, algo que el usuario tiene y algo que el usuario es. Cada factor de autenticación puede cubrir una variedad de elementos utilizados para autenticar o verificar la identidad del usuario antes de otorgarle acceso, aprobar una solicitud, firmar un documento u otro producto de trabajo, otorgar autoridad a otros, establecer una cadena de autoridad, etc.

El documento WO2021/011354A1 describe proporcionar autenticación continua a un servicio digital cuando una tarjeta sin contacto se coloca cerca de un dispositivo informático.

El documento US2020/304310A1 describe un sistema y un método para la autenticación previa de llamadas de soporte al cliente.

El documento US2018/083963A1 describe la autenticación del usuario a través de las características del dispositivo.

Resumen

Varias realizaciones están generalmente dirigidas a realizar una comprobación de persistencia de autenticación y, en función de la comprobación, permitir que una autenticación previamente exitosa persista en un aparato de usuario. La comprobación podrá implicar una comprobación de la estabilidad del aparato del usuario. Si el aparato del usuario es estable, se puede tomar la huella digital del dispositivo en el aparato, cuyo resultado se puede comparar con una captura del aparato tomada en el momento de la autenticación exitosa. Si la comparación revela cambios o desviaciones que estén dentro de un umbral predeterminado, entonces se podrá permitir la persistencia de la autenticación.

De acuerdo con un primer aspecto de la presente divulgación se proporciona un aparato de acuerdo con la reivindicación 1.

De acuerdo con un segundo aspecto de la presente divulgación se proporciona un método de acuerdo con la reivindicación 8.

De acuerdo con un tercer aspecto de la presente divulgación, se proporciona un medio de almacenamiento legible por ordenador no transitorio de acuerdo con la reivindicación 15.

Breve descripción de los dibujos

La Fig. 1A ilustra un sistema de transmisión de datos de ejemplo de acuerdo con una o más realizaciones.

La Fig. 1B ilustra un diagrama de secuencia de ejemplo para proporcionar acceso autenticado de acuerdo con una o más realizaciones.

La Fig. 2 ilustra un sistema de ejemplo que utiliza una tarjeta sin contacto de acuerdo con una o más realizaciones.

La Fig. 3A ilustra un ejemplo de tarjeta sin contacto de acuerdo con una o más realizaciones.

La Fig. 3B ilustra un ejemplo de panel de contacto de una tarjeta sin contacto de acuerdo con una o más realizaciones.

La Fig. 4 ilustra un diagrama de tiempo de ejemplo de acuerdo con una o más realizaciones.

La Fig. 5 ilustra ejemplos de autenticaciones de primer factor y segundo factor de acuerdo con una o más realizaciones.

La Fig. 6 ilustra una captura de ejemplo de la configuración del dispositivo y la biometría del comportamiento del usuario de acuerdo con una o más realizaciones.

La Fig. 7 ilustra un ejemplo de comprobación de estabilidad de un aparato de usuario de acuerdo con una o más realizaciones.

La Fig. 8 ilustra un ejemplo de caracterización de un dispositivo de acuerdo con una o más realizaciones.

La Fig. 9 ilustra un ejemplo de análisis de deriva de acuerdo con una o más realizaciones.

La Fig. 10 ilustra un diagrama de flujo de ejemplo de acuerdo con una o más realizaciones.

Descripción detallada

Varias realizaciones están generalmente dirigidas a realizar una comprobación de persistencia de autenticación en un aparato de usuario (por ejemplo, un dispositivo informático móvil) y, en base a una comprobación de persistencia positiva, permitir que una autenticación previamente exitosa (por ejemplo, autenticación de primer factor, autenticación de segundo factor) persista durante un período de tiempo predeterminado. Por ejemplo, la comprobación de persistencia de la autenticación puede ser activada o causada por uno o más factores, como el transcurso de una cantidad específica de tiempo después de una primera instancia de autenticación o cuando ocurre un evento de autenticación, que puede incluir cualquier acción o instancia que normalmente requeriría que se realice o procese una autenticación, por ejemplo, una acción o comportamiento de alto riesgo, nivel de riesgo de la acción del usuario.

De acuerdo con realizaciones, la comprobación de persistencia de la autenticación puede considerarse positiva si: (i) el aparato del usuario es estable según una comprobación de estabilidad y (ii) la configuración del dispositivo del aparato del usuario y/o la biometría del comportamiento asociada con el usuario están dentro de un umbral de deriva predeterminado. En base a una comprobación de persistencia positiva, la autenticación exitosa anterior puede persistir durante el período de tiempo predeterminado y, por lo tanto, no requiere que el usuario se vuelva a autenticar. Sin embargo, si la comprobación de persistencia es negativa, se solicitará al usuario que vuelva a autenticarse.

Una vez transcurrido el período de tiempo predeterminado desde la comprobación de persistencia de autenticación positiva o cuando ocurre un evento de autenticación posterior, se puede realizar una comprobación de persistencia posterior para determinar si la autenticación puede continuar persistiendo. En algunos casos, la cantidad de comprobaciones de persistencia positivas consecutivas puede ser limitada y, por lo tanto, es posible que se requiera que el usuario vuelva a autenticarse una vez alcanzado ese límite.

De acuerdo con realizaciones, los tipos de autenticación que pueden persistir pueden incluir autenticación de primer factor y autenticación de segundo factor, donde las autenticaciones de primer factor y de segundo factor pueden ser diferentes entre sí. Por ejemplo, el proceso de autenticación de primer factor puede requerir que el usuario que se autentica sepa algo, como un ID de inicio de sesión y una contraseña. La autenticación de segundo factor puede requerir que el usuario que se autentica posea y utilice algo, como una tarjeta inteligente sin contacto.

En algunos ejemplos, la autenticación del segundo factor puede implicar que el usuario toque una tarjeta sin contacto con el aparato del usuario de modo que se establezca una comunicación de campo cercano (NFC) entre el aparato y la tarjeta sin contacto. El aparato de usuario puede recibir información de autenticación cifrada de la tarjeta sin contacto a través de un lector NFC, enviar la información de autenticación a uno o más servidores de autenticación remotos y recibir de los servidores de autenticación una indicación de que el usuario está verificado y autenticado.

En el momento de una autenticación exitosa, se pueden determinar una o más configuraciones del dispositivo del aparato del usuario y/o uno o más datos biométricos del comportamiento del usuario asociados con el uso o la interacción con el aparato del usuario. Esto puede denominarse o describirse aquí como tomar una “captura” de una “constelación” de las distintas configuraciones del dispositivo y datos biométricos del comportamiento del usuario. Como se describirá más adelante, la captura se puede utilizar como punto de referencia para determinar en qué medida las configuraciones del dispositivo y/o los datos biométricos del comportamiento del usuario se han desviado o cambiado en el momento de la comprobación de persistencia de la autenticación. El grado asignado de deriva, desviación o cambio puede denominarse en este documento umbral de deriva predeterminado.

Cuando se activa la comprobación de persistencia de la autenticación, se puede realizar una comprobación de estabilidad en el dispositivo del usuario. Por ejemplo, la comprobación de estabilidad puede ser una verificación del operador de red móvil (MNO), que puede implicar verificar o comprobar con el o los MNO(s) adecuados que el aparato del usuario no ha cambiado sustancialmente (por ejemplo, no ha cambiado las tarjetas SIM, no ha cambiado los números de teléfono, no ha cambiado los propietarios, etc.) de modo de al menos confirmar que el aparato del usuario todavía pertenece y está asociado con el usuario.

En respuesta a que el aparato del usuario haya pasado la comprobación de estabilidad o sea estable, se puede realizar una caracterización del dispositivo del aparato del usuario. La caracterización del dispositivo puede ser

un proceso en el que se determina una constelación actual de configuraciones del dispositivo y/o datos biométricos del comportamiento del usuario correspondientes al aparato del usuario. Al menos en ese sentido, la caracterización del dispositivo puede ser similar al proceso de tomar una captura en el momento de una autenticación exitosa, como se describió anteriormente.

De acuerdo con otras realizaciones, se puede determinar si la constelación actual de configuraciones del dispositivo y/o biometría del comportamiento del usuario proporcionada por la caracterización del dispositivo está dentro del umbral de deriva predeterminado. Si se encuentra dentro del umbral de deriva, se puede permitir que la autenticación persista. Si está fuera del umbral de desviación, es posible que se le solicite al usuario que se vuelva a autenticar y, en algunos ejemplos, que se vuelva a autenticar mediante la autenticación de primer y segundo factor.

En soluciones anteriores, cada instancia de autenticación requería que el usuario realizara manualmente actos relacionados con la autenticación para completar el proceso, lo que causaba molestias al usuario y fricción entre este y la plataforma. Las realizaciones y ejemplos descritos en este documento son ventajosos con respecto a las soluciones convencionales de diversas maneras. Por ejemplo, se puede permitir que la autenticación persista automáticamente en función de una comprobación de persistencia de autenticación positiva de una manera altamente segura, lo que hace que el proceso de autenticación sea conveniente para el usuario y mejora la calidad general de la experiencia del usuario.

A continuación se hace referencia a los dibujos, donde se utilizan números de referencia iguales para referirse a elementos iguales en todos ellos. En la siguiente descripción, a efectos explicativos, se exponen numerosos detalles específicos para facilitar una comprensión completa de la misma. Puede ser evidente, sin embargo, que las nuevas realizaciones pueden practicarse sin estos detalles específicos. En otros casos, se muestran estructuras y dispositivos bien conocidos en forma de diagrama de bloques para facilitar su descripción. La intención es cubrir todas las modificaciones, equivalentes y alternativas dentro del alcance de las reivindicaciones.

La Fig. 1A ilustra un sistema de transmisión de datos de ejemplo de acuerdo con una o más realizaciones. Como se analiza más adelante, el sistema 100 puede incluir una tarjeta sin contacto 105, un dispositivo cliente 110, una red 115 y un servidor 120. Aunque la Fig. 1A ilustra instancias individuales de los componentes, el sistema 100 puede incluir cualquier número de componentes.

El sistema 100 puede incluir una o más tarjetas sin contacto 105, que se explican con más detalle a continuación con referencia a la Fig. 3A y Fig. 3B. En algunas realizaciones, la tarjeta sin contacto 105 puede estar en comunicación inalámbrica, utilizando NFC en un ejemplo, con el dispositivo cliente 110.

El sistema 100 puede incluir el dispositivo cliente 110, que puede ser un ordenador habilitado para red. Como se hace referencia en este documento, un ordenador con conexión a red puede incluir, pero no se limita a, un dispositivo informático o un dispositivo de comunicaciones que incluye, por ejemplo, un servidor, un dispositivo de red, un ordenador personal, una estación de trabajo, un teléfono, un teléfono inteligente, una PC de mano, un asistente digital personal, un cliente ligero, un cliente pesado, un navegador de Internet u otro dispositivo. El dispositivo cliente 110 también puede ser un dispositivo informático móvil, por ejemplo, un iPhone, iPod, iPad de Apple® o cualquier otro dispositivo adecuado que ejecute el sistema operativo iOS® de Apple, cualquier dispositivo que ejecute el sistema operativo Windows® Mobile de Microsoft, cualquier dispositivo que ejecute el sistema operativo Android® de Google y/o cualquier otro dispositivo informático móvil adecuado, como un teléfono inteligente, una tableta o un dispositivo móvil portátil similar.

El dispositivo cliente 110 puede incluir un procesador y una memoria, y se entiende que los circuitos de procesamiento pueden contener componentes adicionales, incluidos procesadores, memorias, comprobadores de errores y paridad/CRC, codificadores de datos, algoritmos anticolisión, controladores, decodificadores de comandos, primitivos de seguridad y hardware a prueba de manipulaciones, según sea necesario para realizar las funciones descritas en este documento. El dispositivo cliente 110 puede incluir además una pantalla y dispositivos de entrada. La pantalla puede ser cualquier tipo de dispositivo para presentar información visual, como un monitor de ordenador, una pantalla plana y una pantalla de dispositivo móvil, incluidas pantallas de cristal líquido, pantallas de diodos emisores de luz, paneles de plasma y pantallas de tubos de rayos catódicos. Los dispositivos de entrada pueden incluir cualquier dispositivo para ingresar información en el dispositivo del usuario que esté disponible y sea compatible con el dispositivo del usuario, como una pantalla táctil, un teclado, un mouse, un dispositivo de control del cursor, una pantalla táctil, un micrófono, una cámara digital, una grabadora de vídeo o una videocámara. Estos dispositivos pueden usarse para ingresar información e interactuar con el software y otros dispositivos aquí descritos.

En algunos ejemplos, el dispositivo cliente 110 del sistema 100 puede ejecutar una o más aplicaciones, tales como aplicaciones de software, que permiten, por ejemplo, comunicaciones de red con uno o más componentes del sistema 100 y transmitir y/o recibir datos.

El dispositivo cliente 110 puede estar en comunicación con uno o más servidores 120 a través de una o más redes 115 y puede funcionar como un par front-end a backend respectivo con el servidor 120. El dispositivo cliente 110 puede transmitir, por ejemplo desde una aplicación de dispositivo móvil que se ejecuta en el dispositivo cliente 110, una o más solicitudes al servidor 120. La una o más solicitudes pueden estar asociadas con la recuperación de datos del servidor 120. El servidor 120 puede recibir una o más solicitudes del dispositivo cliente 110. En función de una o más solicitudes del dispositivo cliente 110, el servidor 120 puede configurarse para recuperar los datos solicitados de una o más bases de datos (no se muestran). En función de la recepción de los datos solicitados de una o más bases de datos, el servidor 120 puede configurarse para transmitir los datos recibidos al dispositivo cliente 110, siendo los datos recibidos una respuesta a una o más solicitudes.

El sistema 100 puede incluir una o más redes 115. En algunos ejemplos, la red 115 puede ser una o más de una red inalámbrica, una red cableada o cualquier combinación de red inalámbrica y red cableada y puede estar configurada para conectar el dispositivo cliente 110 al servidor 120. Por ejemplo, la red 115 puede incluir una o más de una red de fibra óptica, una red óptica pasiva, una red de cable, una red de Internet, una red satelital, una red de área local inalámbrica (LAN), un Sistema Global para Comunicación Móvil, un Servicio de Comunicación Personal, una Red de Área Personal, un Protocolo de Aplicación Inalámbrica, un Servicio de Mensajería Multimedia, un Servicio de Mensajería Mejorado, un Servicio de Mensajes Cortos, Sistemas Basados en Multiplexación por División de Tiempo, Sistemas Basados en Acceso Múltiple por División de Código, D-AMPS, Wi-Fi, Datos Inalámbricos Fijos, IEEE 802.11b, 802.15.1, 802.11n y 802.11g, Bluetooth, NFC, identificación por radiofrecuencia (RFID), Wi-Fi y/o similares.

Además, la red 115 puede incluir, sin limitación, líneas telefónicas, fibra óptica, IEEE Ethernet 802.3, una red de área amplia, una red de área personal inalámbrica, una LAN o una red global como Internet. Además, la red 115 puede soportar una red de Internet, una red de comunicación inalámbrica, una red celular o similar, o cualquier combinación de las mismas. La red 115 puede incluir además una red, o cualquier número de los tipos de redes ejemplares mencionados anteriormente, que funcionan como una red independiente o en cooperación entre sí. La red 115 puede utilizar uno o más protocolos de uno o más elementos de red a los que están acoplados comunicativamente. La red 115 puede traducir hacia o desde otros protocolos a uno o más protocolos de dispositivos de red. Aunque la red 115 se representa como una red única, debe apreciarse que, según uno o más ejemplos, la red 115 puede incluir una pluralidad de redes interconectadas, tales como, por ejemplo, Internet, la red de un proveedor de servicios, una red de televisión por cable, redes corporativas, tales como redes de asociaciones de tarjetas de crédito, y redes domésticas.

El sistema 100 puede incluir uno o más servidores 120. En algunos ejemplos, el servidor 120 puede incluir uno o más procesadores, que están acoplados a la memoria. El servidor 120 puede configurarse como un sistema, servidor o plataforma central para controlar y llamar a diversos datos en diferentes momentos para ejecutar una pluralidad de acciones de flujo de trabajo. El servidor 120 puede configurarse para conectarse a una o más bases de datos. El servidor 120 puede estar conectado a al menos un dispositivo cliente 110.

La Fig. 1B ilustra un diagrama de secuencia de ejemplo para proporcionar acceso autenticado de acuerdo con una o más realizaciones. El diagrama puede incluir una tarjeta sin contacto 105 y un dispositivo cliente 110, que puede incluir una aplicación 122 y un procesador 124. La Fig. 1B puede hacer referencia a componentes similares a los ilustrados en la Fig. 1A.

En la etapa 102, la aplicación 122 se comunica con la tarjeta sin contacto 105 (por ejemplo, después de acercarse a la tarjeta sin contacto 105). La comunicación entre la aplicación 122 y la tarjeta sin contacto 105 puede implicar que la tarjeta sin contacto 105 esté lo suficientemente cerca de un lector de tarjetas (no mostrado) del dispositivo cliente 110 para permitir la transferencia de datos NFC entre la aplicación 122 y la tarjeta sin contacto 105.

En la etapa 104, después de que se ha establecido la comunicación entre el dispositivo cliente 110 y la tarjeta sin contacto 105, la tarjeta sin contacto 105 genera un criptograma de código de autenticación de mensaje (MAC). En algunos ejemplos, esto puede ocurrir cuando la aplicación 122 lee la tarjeta sin contacto 105. En particular, esto puede ocurrir durante una lectura, como una lectura NFC, de una etiqueta de intercambio de datos de campo cercano (NDEF), que puede crearse de acuerdo con el formato de intercambio de datos NFC.

Por ejemplo, un lector, tal como la aplicación 122, puede transmitir un mensaje, tal como un mensaje de selección de subprograma, con el ID de subprograma de un subprograma productor de NDEF. Tras la confirmación de la selección, se puede transmitir una secuencia de mensajes de selección de archivo seguidos de mensajes de lectura de archivo. Por ejemplo, la secuencia puede incluir “Seleccionar archivo de capacidades”, “Leer archivo de capacidades” y “Seleccionar archivo NDEF”. En este punto, se puede actualizar o incrementar un valor de contador mantenido por la tarjeta sin contacto 105, lo que puede ser seguido por “Leer archivo NDEF”. En este punto, se puede generar el mensaje que puede incluir un encabezado y un secreto compartido. Luego se podrán generar claves de sesión. El criptograma MAC puede crearse a partir del mensaje, que puede incluir el encabezado y el secreto compartido. Luego, el criptograma MAC puede concatenarse con uno o más bloques de datos aleatorios, y el criptograma MAC y un número aleatorio (RND) pueden cifrarse con la clave de sesión. Posteriormente, el criptograma y el encabezado se pueden concatenar

y codificar como hexadecimal ASCII y devolver en formato de mensaje NDEF (en respuesta al mensaje “Leer archivo NDEF”).

En algunos ejemplos, el criptograma MAC puede transmitirse como una etiqueta NDEF y, en otros ejemplos, el criptograma MAC puede incluirse con un indicador de recurso uniforme (por ejemplo, como una cadena formateada).

En algunos ejemplos, la aplicación 122 puede estar configurada para transmitir una solicitud a la tarjeta sin contacto 105, la solicitud comprende una instrucción para generar un criptograma MAC.

En la etapa 106, la tarjeta sin contacto 105 envía el criptograma MAC a la aplicación 122. En algunos ejemplos, la transmisión del criptograma MAC ocurre a través de NFC, sin embargo, la presente divulgación no se limita a ello. En otros ejemplos, esta comunicación puede ocurrir a través de Bluetooth, Wi-Fi u otros medios de comunicación inalámbrica de datos.

En la etapa 108, la aplicación 122 comunica el criptograma MAC al procesador 124. En la etapa 112, el procesador 124 verifica el criptograma MAC de acuerdo con una instrucción de la aplicación 122. Por ejemplo, el criptograma MAC puede verificarse, como se explica a continuación.

En algunos ejemplos, la verificación del criptograma MAC puede ser realizada por un dispositivo distinto del dispositivo cliente 110, tal como un servidor 120 en comunicación de datos con el dispositivo cliente 110 (como se muestra en la Fig. 1A). Por ejemplo, el procesador 124 puede emitir el criptograma MAC para su transmisión al servidor 120, que puede verificar el criptograma MAC.

En algunos ejemplos, el criptograma MAC puede funcionar como una firma digital para fines de verificación. Se pueden utilizar otros algoritmos de firma digital, como algoritmos asimétricos de clave pública, por ejemplo, el algoritmo de firma digital y el algoritmo RSA, o protocolos de conocimiento cero, para realizar esta verificación.

Se puede entender que en algunos ejemplos, la tarjeta sin contacto 105 puede iniciar la comunicación después de que la tarjeta sin contacto se acerca al dispositivo cliente 110. A modo de ejemplo, la tarjeta sin contacto 105 puede enviar al dispositivo cliente 110 un mensaje, por ejemplo, indicando que la tarjeta sin contacto ha establecido comunicación. Posteriormente, la aplicación 122 del dispositivo cliente 110 puede proceder a comunicarse con la tarjeta sin contacto en la etapa 102, como se describió anteriormente.

La Fig. 2 ilustra un sistema de ejemplo 200 que utiliza una tarjeta sin contacto. El sistema 200 puede incluir una tarjeta sin contacto 205, uno o más dispositivos cliente 210, una red 215, servidores 220, 225, uno o más módulos de seguridad de hardware 230 y una base de datos 235. Aunque la Fig. 2 ilustra instancias individuales de los componentes, el sistema 200 puede incluir cualquier número de componentes.

El sistema 200 puede incluir una o más tarjetas sin contacto 205, que se explican con más detalle a continuación con respecto a la Fig. 3A y Fig. 3B. En algunos ejemplos, la tarjeta sin contacto 205 puede estar en comunicación inalámbrica, por ejemplo NFC, con el dispositivo cliente 210. Por ejemplo, la tarjeta sin contacto 205 puede incluir uno o más chips, como un chip de identificación por radiofrecuencia, configurado para comunicarse a través de NFC u otros protocolos de corto alcance. En otras realizaciones, la tarjeta sin contacto 205 puede comunicarse con el dispositivo cliente 210 a través de otros medios que incluyen, entre otros, Bluetooth, satélite, Wi-Fi, comunicaciones por cable y/o cualquier combinación de conexiones inalámbricas y por cable. De acuerdo con algunas realizaciones, la tarjeta sin contacto 205 puede configurarse para comunicarse con el lector de tarjetas 213 (al que de otro modo se puede denominar en este documento lector NFC, lector de tarjetas NFC o lector) del dispositivo cliente 210 a través de NFC cuando la tarjeta sin contacto 205 está dentro del alcance del lector de tarjetas 213. En otros ejemplos, las comunicaciones con la tarjeta sin contacto 205 pueden realizarse a través de una interfaz física, por ejemplo, una interfaz de bus serie universal o una interfaz de deslizamiento de tarjeta.

El sistema 200 puede incluir el dispositivo cliente 210, que puede ser un ordenador habilitada para red. Como se hace referencia en este documento, un ordenador con conexión a red puede incluir, pero no se limita a: por ejemplo, un dispositivo informático o un dispositivo de comunicaciones que incluye, por ejemplo, un servidor, un dispositivo de red, un ordenador personal, una estación de trabajo, un dispositivo móvil, un teléfono, una PC de mano, un asistente digital personal, un cliente ligero, un cliente pesado, un navegador de Internet u otro dispositivo. Uno o más dispositivos cliente 210 también pueden ser un dispositivo móvil; por ejemplo, un dispositivo móvil puede incluir un iPhone, iPod, iPad de Apple® o cualquier otro dispositivo móvil que ejecute el sistema operativo iOS de Apple®, cualquier dispositivo que ejecute el sistema operativo Windows® Mobile de Microsoft, cualquier dispositivo que ejecute el sistema operativo Android de Google® y/o cualquier otro teléfono inteligente o dispositivo móvil portátil similar. En algunos ejemplos, el dispositivo cliente 210 puede ser el mismo o similar a un dispositivo cliente 110 como se describe con referencia a la Fig. 1A o Fig. 1B.

El dispositivo cliente 210 puede estar en comunicación con uno o más servidores 220 y 225 a través de una o más redes 215. El dispositivo cliente 210 puede transmitir, por ejemplo desde una aplicación 211 que se ejecuta en el dispositivo cliente 210, una o más solicitudes a uno o más servidores 220 y 225. La una o más solicitudes

pueden estar asociadas con la recuperación de datos de uno o más servidores 220 y 225. Los servidores 220 y 225 pueden recibir una o más solicitudes del dispositivo cliente 210. En función de una o más solicitudes del dispositivo cliente 210, uno o más servidores 220 y 225 pueden configurarse para recuperar los datos solicitados de una o más bases de datos 235. Con base en la recepción de los datos solicitados de una o más bases de datos 235, uno o más servidores 220 y 225 pueden configurarse para transmitir los datos recibidos al dispositivo cliente 210, siendo los datos recibidos en respuesta a una o más solicitudes.

El sistema 200 puede incluir uno o más módulos de seguridad de hardware (HSM) 230. Por ejemplo, uno o más HSMs 230 pueden configurarse para realizar una o más operaciones criptográficas como se divulga en este documento. En algunos ejemplos, uno o más HSMs 230 pueden configurarse como dispositivos de seguridad de propósito especial que están configurados para realizar una o más operaciones criptográficas. Los HSMs 230 pueden configurarse de manera que las claves nunca se revelen fuera del HSM 230, y en cambio se mantengan dentro del HSM 230. Por ejemplo, uno o más HSM 230 pueden configurarse para realizar al menos una de las siguientes operaciones: derivación de clave, descifrado y MAC. El uno o más HSM 230 pueden estar contenidos dentro de, o pueden estar en comunicación de datos con, los servidores 220 y 225.

El sistema 200 puede incluir una o más redes 215. En algunos ejemplos, la red 215 puede ser una o más de una red inalámbrica, una red cableada o cualquier combinación de red inalámbrica y red cableada, y puede estar configurada para conectar el dispositivo cliente 210 a los servidores 220 y/o 225. Por ejemplo, la red 215 puede incluir una o más de una red de fibra óptica, una red óptica pasiva, una red de cable, una red celular, una red de Internet, una red satelital, una LAN inalámbrica, un Sistema Global para Comunicación Móvil, un Servicio de Comunicación Personal, una Red de Área Personal, un Protocolo de Aplicación Inalámbrica, un Servicio de Mensajería Multimedia, un Servicio de Mensajería Mejorada, un Servicio de Mensajes Cortos, sistemas basados en Multiplexación por División de Tiempo, sistemas basados en Acceso Múltiple por División de Código, D-AMPS, Wi-Fi, Datos Inalámbricos Fijos, IEEE 802.11b, 802.15.1, 802.11n y 802.11g, Bluetooth, NFC, RFID, Wi-Fi, y/o cualquier combinación de redes de los mismos. Como ejemplo no limitativo, las comunicaciones entre la tarjeta sin contacto 205 y el dispositivo cliente 210 pueden incluir comunicación basada en NFC, red celular entre el dispositivo cliente 210 y un operador, e Internet entre el operador y un backend.

Además, la red 215 puede incluir, sin limitación, líneas telefónicas, fibra óptica, IEEE Ethernet 802.3, una red de área amplia, una red de área personal inalámbrica, una red de área local o una red global como Internet. Además, la red 215 puede soportar una red de Internet, una red de comunicación inalámbrica, una red celular o similar, o cualquier combinación de las mismas. La red 215 puede incluir además una red, o cualquier número de los tipos de redes ejemplares mencionados anteriormente, que funcionan como una red independiente o en cooperación entre sí. La red 215 puede utilizar uno o más protocolos de uno o más elementos de red a los que están acoplados comunicativamente. La red 215 puede traducir hacia o desde otros protocolos a uno o más protocolos de dispositivos de red. Aunque la red 215 se representa como una red única, debe apreciarse que, de acuerdo con uno o más ejemplos, la red 215 puede incluir una pluralidad de redes interconectadas, tales como, por ejemplo, Internet, la red de un proveedor de servicios, una red de televisión por cable, redes corporativas, tales como redes de asociaciones de tarjetas de crédito, y redes domésticas.

En varios ejemplos de acuerdo con la presente divulgación, el dispositivo cliente 210 del sistema 200 puede ejecutar una o más aplicaciones 211, e incluir uno o más procesadores 212, y uno o más lectores de tarjetas 213. Por ejemplo, una o más aplicaciones 211, tales como aplicaciones de software, pueden configurarse para permitir, por ejemplo, comunicaciones de red con uno o más componentes del sistema 200 y transmitir y/o recibir datos. Se entiende que aunque en la Fig. solo se ilustran instancias individuales de los componentes del dispositivo cliente 210. La Fig. 2, se puede utilizar cualquier número de dispositivos 210. El lector de tarjetas 213 puede configurarse para leer y/o comunicarse con la tarjeta sin contacto 205. En conjunto con una o más aplicaciones 211, el lector de tarjetas 213 puede comunicarse con la tarjeta sin contacto 205. En los ejemplos, el lector de tarjetas 213 puede incluir circuitos o componentes de circuitos, por ejemplo, una bobina de lector NFC, que genera un campo magnético para permitir la comunicación entre el dispositivo cliente 210 y la tarjeta sin contacto 205.

La aplicación 211 de cualquiera de los dispositivos cliente 210 puede comunicarse con la tarjeta sin contacto 205 mediante comunicación inalámbrica de corto alcance (por ejemplo, NFC). La aplicación 211 puede configurarse para interactuar con un lector de tarjetas 213 del dispositivo cliente 210 configurado para comunicarse con una tarjeta sin contacto 205. Como debe tenerse en cuenta, los expertos en la materia entenderán que una distancia de menos de veinte centímetros es consistente con el alcance NFC.

En algunas realizaciones, la aplicación 211 se comunica a través de un lector asociado (por ejemplo, el lector de tarjetas 213) con la tarjeta sin contacto 205.

En algunas realizaciones, la activación de la tarjeta puede ocurrir sin autenticación del usuario. Por ejemplo, una tarjeta sin contacto 205 puede comunicarse con la aplicación 211 a través del lector de tarjetas 213 del dispositivo cliente 210 a través de NFC. La comunicación (por ejemplo, un toque de la tarjeta cerca del lector de tarjetas 213 del dispositivo cliente 210) permite que la aplicación 211 lea los datos asociados con la tarjeta y realice una activación. En algunos casos, el toque puede activar o iniciar la aplicación 211 y luego iniciar una

o más acciones o comunicaciones con un servidor de cuenta 225 para activar la tarjeta para su uso posterior. En algunos casos, si la aplicación 211 no está instalada en el dispositivo cliente 210, un toque de la tarjeta contra el lector de tarjetas 213 puede iniciar una descarga de la aplicación 211 (por ejemplo, navegación a una página de descarga de aplicaciones). Posteriormente a la instalación, un toque en la tarjeta puede activar o iniciar la aplicación 211 y luego iniciar (por ejemplo, a través de la aplicación u otra comunicación de back-end) la activación de la tarjeta. Después de la activación, la tarjeta podrá utilizarse en diversas transacciones, incluidas las comerciales.

De acuerdo con algunas realizaciones, la tarjeta sin contacto 205 puede incluir una tarjeta de pago virtual. En esas realizaciones, la aplicación 211 puede recuperar información asociada con la tarjeta sin contacto 205 accediendo a una billetera digital implementada en el dispositivo cliente 210, en la que la billetera digital incluye la tarjeta de pago virtual. En algunos ejemplos, los datos de la tarjeta de pago virtual pueden incluir uno o más números de tarjeta virtual generados estáticamente o dinámicamente.

El servidor 220 puede incluir un servidor web en comunicación con la base de datos 235. El servidor 225 puede incluir un servidor de cuentas. En algunos ejemplos, el servidor 220 puede estar configurado para validar una o más credenciales de la tarjeta sin contacto 205 y/o del dispositivo cliente 210 mediante comparación con una o más credenciales en la base de datos 235. El servidor 225 puede configurarse para autorizar una o más solicitudes, tales como pagos y transacciones, desde la tarjeta sin contacto 205 y/o el dispositivo cliente 210.

La Fig. 3A ilustra una o más tarjetas sin contacto 300, que pueden incluir una tarjeta de pago, como una tarjeta de crédito, una tarjeta de débito o una tarjeta de regalo, emitida por un proveedor de servicios 305 que se muestra en el frente o el reverso de la tarjeta 300. En algunos ejemplos, la tarjeta sin contacto 300 no está relacionada con una tarjeta de pago y puede incluir, sin limitación, una tarjeta de identificación. En algunos ejemplos, la tarjeta de pago puede incluir una tarjeta de pago sin contacto de interfaz dual. La tarjeta sin contacto 300 puede incluir un sustrato 310, que puede incluir una sola capa, o una o más capas laminadas compuestas de plásticos, metales y otros materiales. Los materiales de sustrato ejemplares incluyen cloruro de polivinilo, acetato de cloruro de polivinilo, acrilonitrilo butadieno estireno, policarbonato, poliésteres, titanio anodizado, paladio, oro, carbono, papel y materiales biodegradables. En algunos ejemplos, la tarjeta sin contacto 300 puede tener características físicas compatibles con el formato ID-1 del estándar ISO/IEC 7810, y la tarjeta sin contacto puede, de otro modo, ser compatible con el estándar ISO/IEC 14443. Sin embargo, se entiende que la tarjeta sin contacto 300 de acuerdo con la presente divulgación puede tener características diferentes, y la presente divulgación no requiere que se implemente una tarjeta sin contacto en una tarjeta de pago.

La tarjeta sin contacto 300 también puede incluir información de identificación 315 mostrada en el frente y/o el reverso de la tarjeta, y un panel de contacto 320. El panel de contacto 320 puede configurarse para establecer contacto con otro dispositivo de comunicación, como un dispositivo de usuario, un teléfono inteligente, un ordenador portátil, un ordenador de escritorio o una tableta. La tarjeta sin contacto 300 también puede incluir circuitos de procesamiento, antena y otros componentes no mostrados en la Fig. 3A. Estos componentes pueden estar ubicados detrás del panel de contacto 320 o en otra parte del sustrato 310. La tarjeta sin contacto 300 también puede incluir una tira o cinta magnética, que puede estar ubicada en la parte posterior de la tarjeta (no se muestra en la Fig. 3A).

Como se ilustra en La Fig. 3B, la almohadilla de contacto 320 de la Fig. 3A puede incluir un circuito de procesamiento 325 para almacenar y procesar información, incluyendo un microprocesador 330 y una memoria 335. Se entiende que los circuitos de procesamiento 325 pueden contener componentes adicionales, incluidos procesadores, memorias, comprobadores de errores y paridad/CRC, codificadores de datos, algoritmos anticolisión, controladores, decodificadores de comandos, primitivos de seguridad y hardware a prueba de manipulaciones, según sea necesario para realizar las funciones descritas en este documento.

La memoria 335 puede ser una memoria de sólo lectura, una memoria de escritura única y lectura múltiple o una memoria de lectura/escritura, por ejemplo, RAM, ROM y EEPROM, y la tarjeta sin contacto 300 puede incluir una o más de estas memorias. Una memoria de solo lectura puede ser programable de fábrica como de solo lectura o programable una sola vez. La programabilidad única brinda la oportunidad de escribir una vez y luego leer muchas veces. Se puede programar una memoria de escritura única/lectura múltiple en un momento determinado después de que el chip de memoria haya salido de fábrica. Una vez programada la memoria no se podrá reescribir, pero sí se podrá leer muchas veces. Una memoria de lectura/escritura puede programarse y reprogramarse muchas veces después de salir de fábrica. También puede leerse muchas veces.

La memoria 335 puede estar configurada para almacenar uno o más applets 340, uno o más contadores 345, una o más claves diversificadas 347, uno o más identificadores de cliente 350 y otros tipos de datos o información adecuados. Los uno o más applets 340 pueden incluir una o más aplicaciones de software configuradas para ejecutarse en una o más tarjetas sin contacto, como por ejemplo el applet Java Card. Sin embargo, se entiende que los applets 340 no se limitan a los applets de Java Card, y en su lugar pueden ser cualquier aplicación de software que funcione en tarjetas sin contacto u otros dispositivos que tengan memoria limitada. El o los contadores 345 pueden incluir un contador numérico suficiente para almacenar un número

entero. Como se describirá más adelante, las una o más claves diversificadas 347 se pueden usar para cifrar diversa información, como información sobre el usuario o cliente (por ejemplo, identificador de cliente 450) para generar criptogramas que se pueden enviar, por ejemplo, a un dispositivo móvil al menos para fines de autenticación. El identificador de cliente 350 puede incluir un identificador alfanumérico único asignado a un usuario de la tarjeta sin contacto 300, y el identificador puede distinguir al usuario de la tarjeta sin contacto de otros usuarios de tarjetas sin contacto. En algunos ejemplos, el identificador de cliente 350 puede identificar tanto a un cliente como a una cuenta asignada a ese cliente y puede identificar además la tarjeta sin contacto asociada con la cuenta del cliente.

Los elementos de procesador y de memoria de las realizaciones ejemplares anteriores se describen con referencia al panel de contacto, pero la presente divulgación no se limita a ello. Se entiende que estos elementos pueden implementarse fuera del panel 320 o totalmente separados de él, o como elementos adicionales además de los elementos del microprocesador 330 y de la memoria 335 ubicados dentro del panel de contacto 320.

En algunos ejemplos, la tarjeta sin contacto 300 puede incluir una o más antenas 355. La una o más antenas 355 pueden colocarse dentro de la tarjeta sin contacto 300 y alrededor del circuito de procesamiento 325 del panel de contacto 320. Por ejemplo, una o más antenas 355 pueden ser integrales con el circuito de procesamiento 325 y una o más antenas 355 pueden usarse con una bobina amplificadora externa. Como otro ejemplo, una o más antenas 355 pueden ser externas al panel de contacto 320 y al circuito de procesamiento 325.

En una realización, la bobina de la tarjeta sin contacto 300 puede actuar como secundario de un transformador de núcleo de aire. El terminal puede comunicarse con la tarjeta sin contacto 300 mediante corte de energía o modulación de amplitud. La tarjeta sin contacto 300 puede inferir los datos transmitidos desde el terminal utilizando los espacios en la conexión de energía de la tarjeta sin contacto, que pueden mantenerse funcionalmente a través de uno o más capacitores. La tarjeta sin contacto 300 puede comunicarse de nuevo conmutando una carga en la bobina de la tarjeta sin contacto o modulando la carga. La modulación de carga puede detectarse en la bobina del terminal a través de interferencias.

Como se explicó anteriormente, las tarjetas sin contacto 300 pueden construirse sobre una plataforma de software operable en tarjetas inteligentes u otros dispositivos que tengan memoria limitada, como JavaCard, y una o más aplicaciones o applets pueden ejecutarse de forma segura. Se pueden agregar applets a las tarjetas sin contacto para proporcionar una contraseña de un solo uso (OTP) para la autenticación multifactor (MFA) en varios casos de uso basados en aplicaciones móviles. Los applets pueden configurarse para responder a una o más solicitudes, como solicitudes de intercambio de datos de campo cercano, desde un lector, como un lector NFC móvil, y producir un mensaje NDEF que incluye un OTP criptográficamente seguro codificado como una etiqueta de texto NDEF.

En ejemplos, cuando se prepara para enviar datos (por ejemplo, a un dispositivo móvil, a un servidor, etc.), la tarjeta sin contacto 300 puede incrementar un valor de contador de un contador de uno o más contadores 345. La tarjeta sin contacto 300 puede entonces proporcionar una clave maestra, que puede ser una clave distinta almacenada en la tarjeta 300, y el valor del contador como entrada a un algoritmo criptográfico, que también puede estar almacenado en la tarjeta 300 y produce una clave diversificada como salida, que puede ser una de las claves diversificadas 347. Se entiende que la clave maestra y el valor del contador también se almacenan de forma segura en la memoria de un dispositivo o componente que recibe datos de la tarjeta sin contacto 300 para descifrar los datos utilizando la clave diversificada que fue utilizada por la tarjeta para cifrar los datos transmitidos. El algoritmo criptográfico puede incluir algoritmos de cifrado, algoritmos de código de autenticación de mensajes basado en hash (HMAC), algoritmos de código de autenticación de mensajes basado en cifrado (CMAC) y similares. Los ejemplos no limitativos del algoritmo criptográfico pueden incluir un algoritmo de cifrado simétrico como 3DES o AES128; un algoritmo HMAC simétrico, como HMAC-SHA-256; y un algoritmo CMAC simétrico como AES-CMAC. La tarjeta sin contacto 300 puede entonces cifrar los datos (por ejemplo, el identificador de cliente 350 y cualquier otro dato) utilizando la clave diversificada en forma de uno o más criptogramas que pueden enviarse a un dispositivo móvil, por ejemplo, como mensajes de formato de intercambio de datos NFC (NDEF). La tarjeta sin contacto 300 puede luego transmitir los datos cifrados (por ejemplo, criptogramas) al dispositivo móvil, que luego puede descifrar los criptogramas utilizando la clave diversificada (por ejemplo, la clave diversificada generada por el dispositivo móvil utilizando el valor del contador y la clave maestra almacenada en la memoria del mismo).

La Fig. 4 ilustra un diagrama de tiempo de ejemplo 400 de acuerdo con una o más realizaciones. El diagrama de tiempo 400 muestra al menos las diversas características relacionadas con el tiempo asociadas con una comprobación de persistencia de autenticación y la comunicación entre un aparato de usuario (por ejemplo, un dispositivo informático móvil de usuario como un teléfono inteligente, un ordenador portátil, etc.) y uno o más dispositivos informáticos de back-end remotos (por ejemplo, servidores). En los ejemplos, la comprobación de persistencia de la autenticación puede ser para la autenticación de segundo factor, que de otro modo puede denominarse comprobación de persistencia de la autenticación de segundo factor.

Como se muestra, en el momento 402 puede requerirse y realizarse una autenticación de primer factor. Como se describirá con más detalle a continuación, la autenticación del primer factor puede implicar la autenticación mediante ID de usuario y contraseña. Por ejemplo, un usuario puede ingresar un ID de usuario y una contraseña, que pueden proporcionarse a los servidores back-end para verificar que el ID de usuario y la contraseña ingresados sean correctos.

En el momento 404, después de una autenticación de primer factor exitosa, es posible que se requiera y realice una autenticación de segundo factor. La autenticación de segundo factor puede ser un tipo de autenticación diferente a la autenticación de primer factor. Por ejemplo, la autenticación de segundo factor puede implicar que el usuario toque una tarjeta sin contacto en el aparato del usuario, lo que de otro modo podría conocerse como autenticación de un toque o de un solo toque. El aparato del usuario, a través de NFC, recibe información de autenticación de usuario cifrada de la tarjeta sin contacto, por ejemplo, uno o más criptogramas que contienen un identificador de usuario, un identificador de autenticación, etc. El aparato del usuario puede enviar el(los) criptograma(s) a dispositivos informáticos remotos, que pueden ser los servidores respaldados, donde esos servidores descifran los criptogramas para verificar si el identificador de usuario contenido en ellos corresponde o coincide con el usuario. Los dispositivos informáticos remotos pueden entonces enviar una indicación al aparato del usuario de que el usuario ha sido autenticado exitosamente.

En el momento de la autenticación de segundo factor exitosa (momento 406) o cerca de ese momento, se puede capturar una captura de una o más configuraciones del dispositivo (por ejemplo, cantidad de aplicaciones instaladas en el teléfono, tipos de aplicaciones) del aparato del usuario e información sobre uno o más datos biométricos de comportamiento del usuario (por ejemplo, comportamientos o patrones únicos relacionados con el uso o las interacciones con el aparato del usuario). El resultado capturado puede considerarse una constelación de las configuraciones del dispositivo y la biometría del comportamiento del usuario. La captura se puede enviar o compartir con uno o más servidores back-end para realizar comparaciones posteriores con las huellas digitales del dispositivo durante futuras comprobaciones de persistencia. Mientras que la Fig. 4 muestra una captura que ocurre después de la autenticación del segundo factor en el momento 404, se puede entender que la captura puede ocurrir al mismo tiempo o cerca del mismo tiempo que la autenticación del segundo factor. La captura se puede proporcionar a uno o más dispositivos informáticos back-end remotos en el momento 408.

Posteriormente se podrá realizar la comprobación de persistencia de la autenticación del segundo factor. La comprobación puede activarse por al menos uno de los siguientes motivos: el transcurso de un período de tiempo específico o un evento específico de autenticación de segundo factor. La cantidad de tiempo específica puede ser predeterminada o preestablecida, por ejemplo, un tiempo máximo que puede transcurrir antes de que se requiera que el usuario realice nuevamente la autenticación de segundo factor. El evento de autenticación de segundo factor puede ser cualquier acción o evento, causado o desencadenado por el usuario, que requiera la autenticación de segundo factor, como transacciones de alto riesgo.

En el momento 410, se puede realizar una verificación o comprobación de estabilidad en el aparato del usuario. El aparato de usuario puede solicitar y hacer que uno o más dispositivos informáticos remotos de back-end realicen la comprobación de estabilidad comunicándose con uno o más servidores de operadores móviles asociados con una red de operadores móviles (MNO), por ejemplo, a través de llamadas de interfaz de programación de aplicaciones (API). En otros casos, uno o más servidores backend remotos inician automáticamente o pueden ser obligados a realizar automáticamente la comprobación de estabilidad en respuesta a la comprobación de persistencia de autenticación de segundo factor, una indicación de la cual puede ser proporcionada a los servidores back-end remotos por el aparato del usuario. Un ejemplo de la comprobación de estabilidad es una comprobación de estabilidad de MNO, que implica que los dispositivos informáticos back-end soliciten y reciban indicación de los servidores del operador móvil de que el aparato del usuario no ha cambiado sustancialmente, por ejemplo, la tarjeta SIM del aparato del usuario sigue siendo la misma, el número de teléfono asociado con el aparato del usuario sigue siendo el mismo, etc.

En el momento 412, en respuesta a una determinación de que el aparato del usuario es estable, uno o más dispositivos informáticos respaldados pueden solicitar que el aparato del usuario realice la caracterización del dispositivo. Como alternativa, en el momento 412, en respuesta a una determinación de que el aparato del usuario es inestable, uno o más servidores back-end pueden devolver un resultado negativo para la comprobación de persistencia y requerir que el usuario se vuelva a autenticar a través de la autenticación de segundo factor (no se muestra).

En el momento 414, el aparato del usuario puede realizar la caracterización del dispositivo. Como se describirá más adelante, la caracterización del dispositivo puede ser un proceso en el que se determina una constelación actual de las configuraciones del dispositivo del aparato del usuario y una o más biometrías de comportamiento del usuario asociadas con el uso o la interacción con el aparato del usuario. La constelación actual se puede proporcionar a uno o más dispositivos informáticos back-end en el momento 416.

En el momento 418, los dispositivos informáticos back-end pueden realizar un análisis de deriva. Por ejemplo, el análisis de deriva puede implicar al menos determinar si la constelación actual del aparato de usuario que

se proporcionó en el momento 416 está dentro de un umbral de deriva predeterminado en relación con la captura tomada en el momento 406. Como se describirá en detalle más adelante, el umbral de deriva es una cantidad máxima de desviación o deriva entre la constelación actual y la captura que se puede permitir. Si la constelación actual está dentro del umbral de deriva predeterminado, los dispositivos informáticos back-end pueden proporcionar una indicación en el momento 420 al aparato de usuario de que se puede permitir que persista la autenticación del segundo factor. Si la constelación actual está fuera del umbral de deriva, los dispositivos informáticos backend pueden devolver un resultado de comprobación de persistencia negativo y el usuario deberá volver a autenticarse a través de la autenticación de segundo factor.

La Fig. 5 ilustra ejemplos de autenticaciones de primer factor y segundo factor de acuerdo con una o más realizaciones. Como se muestra, un ejemplo de la autenticación del primer factor 501 puede implicar que un usuario ingrese un ID de usuario y una contraseña. Como se muestra además, un ejemplo de la autenticación de segundo factor 511 puede implicar que un usuario coloque o toque una tarjeta sin contacto en el aparato del usuario, lo que puede denominarse autenticación de tarjeta sin contacto de un toque o de un solo toque.

En algunos ejemplos, es posible que se requiera que un usuario se autentique a través de la autenticación de primer factor para iniciar sesión en una app de transacciones. El usuario puede abrir la interfaz de la app de transacciones 502, que muestra una pantalla de bienvenida 504 y un icono de inicio de sesión 506. Cuando se selecciona el icono de inicio de sesión 506, se presentan al usuario campos para el ID de usuario y la contraseña para la entrada del ID de usuario y la contraseña. La interfaz también puede mostrar un icono 508 para iniciar sesión en la app de transacciones a través de autenticación biométrica, como la autenticación de huellas dactilares del usuario.

Cuando el usuario ingresa el ID de inicio de sesión y la contraseña, el aparato del usuario puede enviar la información de inicio de sesión a uno o más dispositivos informáticos remotos (por ejemplo, servidores de autenticación de back-end) que están al menos configurados para determinar y verificar que la combinación de ID de inicio de sesión y contraseña es válida y está asociada con el usuario. Si es válido, el usuario podrá obtener acceso a la app de transacciones 502. Se puede entender que la autenticación del primer factor puede ser cualquier tipo de autenticación, como biométrica, código de acceso, PIN, etc., y no limitarse únicamente a la autenticación de ID de usuario y contraseña.

Una vez que el usuario ha iniciado sesión en la app de transacciones 502, es posible que desee realizar una transacción específica, por ejemplo, transferir dinero a una cuenta. La suma de dinero que se transfiere puede ser lo suficientemente grande como para activar una indicación o advertencia de alto riesgo por parte de la app de transacciones 502. Como se describió anteriormente, esta indicación o advertencia de alto riesgo puede considerarse el evento de autenticación (específicamente, en este ejemplo, puede considerarse el evento de autenticación de segundo factor ya que las transferencias de fondos de alto riesgo pueden requerir autenticación de segundo factor).

Como se muestra, por ejemplo, el usuario puede seleccionar el icono de transferencia de fondos 512 para iniciar y realizar la transferencia. Posteriormente, un gráfico 514 puede mostrar que se requiere que el usuario realice una autenticación de un toque o de un solo toque. La app de transacciones 502 puede mostrar un cuadro discontinuo 516 que indica dónde el usuario debe colocar o acercar la tarjeta sin contacto 520 al aparato del usuario. Cuando la tarjeta sin contacto 520 se acerca al aparato del usuario a una distancia de comunicación requerida, se puede establecer NFC y el lector NFC del aparato del usuario puede leer o recibir al menos uno o más criptogramas de la tarjeta 520. Los criptogramas pueden contener varios tipos de información cifrada, como información de autenticación de usuario, que puede ser cualquier indicador o identificador (por ejemplo, identificador alfanumérico único, código, información de identificación personal, etc.) o el identificador único de cliente descrito anteriormente con respecto a la Fig. 3B que identifica al usuario autorizado de la tarjeta.

En algunas realizaciones, el aparato de usuario puede recibir y enviar uno o más criptogramas a uno o más dispositivos informáticos remotos, tales como servidores de autenticación de backend. En el lado del servidor back-end, los ordenadores servidor pueden descifrar los criptogramas y determinar si la información de autenticación del usuario contenida en ellos corresponde realmente al usuario. Un ejemplo de este proceso de coincidencia puede implicar que los servidores back-end correlacionen la información del usuario que ha iniciado sesión en la app de transacciones con la información de autenticación del usuario contenida en los criptogramas. Posteriormente, los ordenadores del servidor back-end pueden enviar al aparato del usuario una indicación de autenticación exitosa. En otros casos, se puede entender que uno o más criptogramas de la tarjeta sin contacto se pueden descifrar en el lado del aparato del usuario para determinar si el usuario es un usuario autorizado de la tarjeta sin contacto.

La Fig. 6 ilustra una captura de ejemplo 600 de la configuración del dispositivo y la biometría del comportamiento del usuario en el momento de la autenticación del segundo factor de acuerdo con una o más realizaciones. En el momento de la autenticación de segundo factor exitosa o cerca de ese momento, una captura de una constelación de las configuraciones del dispositivo del usuario y la biometría del comportamiento del usuario. Se puede entender que la captura 600 puede incluir solo las configuraciones del dispositivo, solo

la biometría del comportamiento del usuario o los datos biométricos, o tanto las configuraciones del dispositivo como la biometría del comportamiento.

En los ejemplos, una o más configuraciones del dispositivo pueden incluir: (i) una o más aplicaciones instaladas en el aparato, (ii) uno o más dispositivos inalámbricos conectados al aparato a través de una conexión inalámbrica, (iii) una lista de dispositivos inalámbricos guardados que se pueden conectar al aparato, (iv) una red a la que está conectado el aparato, (v) una lista de redes guardadas a las que se puede conectar el aparato, (vi) la versión de un sistema operativo en el aparato, (vii) una o más preferencias de configuración, etc.

Como se muestra, la subconstelación 602 indica que, en el momento de la autenticación de segundo factor exitosa, la configuración del dispositivo era que había ocho aplicaciones instaladas, tres de las cuales eran aplicaciones de redes sociales, tres eran aplicaciones de entretenimiento, una era una aplicación de comida y una era una aplicación de mapas. Además, había dos dispositivos inalámbricos conectados al aparato del usuario (por ejemplo, auriculares inalámbricos, reloj inteligente) y había cinco tipos diferentes de dispositivos guardados en la lista de conexión de dispositivos inalámbricos. El dispositivo del usuario no estaba conectado a Wi-Fi en el momento de la captura, pero había cuatro tipos diferentes de redes inalámbricas guardadas en la lista de redes Wi-Fi. Además, la versión del sistema operativo era 2.0 y la configuración de visualización estaba establecida de tal manera que el modo de hibernación se activaba después de tres minutos y la configuración de notificaciones estaba establecida en vibración.

En otros ejemplos, los uno o más datos o biometría de comportamiento del usuario pueden recibirse a través de uno o más sensores (por ejemplo, giroscopio, acelerómetro, cámara, micrófono, etc.) o una o más interfaces del aparato del usuario y pueden ser analizados por el aparato del usuario. Los uno o más datos biométricos o biométricos del comportamiento del usuario pueden incluir: (i) cómo el usuario sostiene físicamente el aparato, (ii) cómo el usuario desliza o interactúa con una interfaz de visualización, (iii) cómo el usuario utiliza el teclado o atajos gestuales, (iv) cómo el usuario escribe palabras, (v) una duración de tiempo para que el usuario escriba palabras, (vi) cómo el usuario hace la transición entre dos o más íconos, (vii) la velocidad de escritura del usuario, (viii) la cadencia de escritura del usuario, etc.

Como se ilustra, la subconstelación 604 indica que, en el momento de una autenticación de segundo factor exitosa, varios aspectos del comportamiento o interacción únicos del usuario con el aparato del usuario son que el usuario rara vez sostiene el aparato del usuario horizontalmente, siempre desliza el dedo de izquierda a derecha, no tiene atajos gestuales, escribe aproximadamente 55 palabras por minuto en el aparato del usuario, el usuario presiona el botón de inicio para realizar la transición entre apps y rara vez usa las pestañas de la app para realizar la transición, y selecciona la app 606 antes que la app 608 la mayoría del tiempo.

Se puede entender que la biometría del comportamiento del usuario se refiere en términos generales a la identificación de un individuo en función de la forma única en que el individuo interactúa o usa un dispositivo informático, como medir cómo el usuario sostiene el dispositivo, cómo el individuo desliza la pantalla, qué atajos de teclado o gestuales se utilizan y construir un perfil de comportamiento único del individuo, etc. La biometría del comportamiento del usuario se basa en patrones de comportamiento humano que consisten en una variedad de acciones o comportamientos distintivos (o semicomportamientos) que conforman al individuo y pueden reflejar los hábitos y microhábitos observables de ese individuo.

La Fig. 7 ilustra un ejemplo de comprobación de estabilidad 700 de un aparato de usuario de acuerdo con una o más realizaciones. Como se describió anteriormente, la comprobación de estabilidad del aparato del usuario se puede realizar para al menos confirmar que el usuario asociado con el aparato del usuario no ha cambiado. En algunos ejemplos, la comprobación de estabilidad puede ser una verificación del operador de red móvil (MNO).

En algunas realizaciones, el aparato de usuario 702 puede hacer que se inicie la verificación MNO. La verificación de MNO puede iniciarse o activarse (de lo contrario, puede denominarse “activador de verificación de MNO”), por ejemplo, cuando se ha realizado la primera instancia de la autenticación de segundo factor y (i) cuando ocurre o se solicita un evento de autenticación (por ejemplo, transacción de alto riesgo, transferencia de monto alto en la aplicación de transacción) o (ii) si ha transcurrido una cantidad específica de tiempo después de la primera instancia de la autenticación de segundo factor, por ejemplo, que puede basarse en o ajustarse de acuerdo con varios procedimientos o protocolos de seguridad de back-end.

Como se muestra, el aparato de usuario 702 puede comunicar o proporcionar información a uno o más servidores back-end 704 a través de la red 705 de que se debe realizar la verificación MNO en base al activador de verificación MNO descrito anteriormente. Los servidores back-end 704 pueden entonces establecer comunicación y comunicarse con uno o más dispositivos informáticos MNO 706, por ejemplo, servidores MNO, que pueden estar comunicándose de forma inalámbrica con una o más torres de telefonía celular 708 o cualquier tipo de dispositivos de comunicación inalámbrica (por ejemplo, estaciones base). Debido a que el aparato de usuario 702 también puede estar conectado y comunicarse de forma inalámbrica con una o más torres de telefonía celular 708, los dispositivos informáticos MNO 706 pueden recibir varios tipos de información basada en la red móvil acerca del aparato de usuario 702 a través de las torres de telefonía celular 708, como

por ejemplo qué (por ejemplo, número de modelo, identificador) tarjeta de módulo de identidad (o identificación) de suscriptor (SIM) del aparato de usuario 702 se está utilizando para comunicarse con las torres de telefonía celular 708, si la tarjeta SIM ha sido cambiada o reemplazada, número(s) de teléfono o cualquier otra información de usuario asociada con la tarjeta SIM, si el(los) número(s) de teléfono o la otra información de usuario ha cambiado, etc.

El uno o más dispositivos informáticos MNO 706 pueden proporcionar estos tipos de información a los servidores back-end 704, que pueden determinar, en función de esta información, si el aparato de usuario 702 es "estable" y permanece sin cambios en términos de las características basadas en MNO. Si se ha cambiado o reemplazado la tarjeta SIM, o si se ha cambiado el número de teléfono, etc., se presume que el aparato de usuario 702 ha cambiado de usuario y, por lo tanto, los servidores back-end 704 pueden determinar que el aparato de usuario 702 es inestable. El resultado de la comprobación de estabilidad se envía luego al aparato de usuario 702 para que éste pueda realizar la caracterización del dispositivo.

Se puede entender que los dispositivos informáticos MNO 706 y las torres de telefonía celular 708 son componentes externos al sistema en el que residen los servidores back-end 704 y pueden ser propiedad de un operador de red móvil de terceros o estar operados por él. Un operador de red móvil puede entenderse como un proveedor de servicios inalámbricos, operador, compañía celular, operador de red móvil, etc. que proporciona servicios de comunicaciones inalámbricas y puede poseer o controlar todos los elementos necesarios para vender y entregar servicios a los usuarios finales, incluida la asignación de espectro radioeléctrico, la infraestructura de red inalámbrica, la infraestructura de backhaul, etc.

La Fig. 8 ilustra un ejemplo de caracterización de un dispositivo de acuerdo con una o más realizaciones. Como se describió anteriormente, un aparato de usuario puede recibir una solicitud o una indicación de uno o más servidores back-end para realizar la caracterización del dispositivo. La caracterización del dispositivo implica que el aparato del usuario capture la constelación actual 800 de las configuraciones del dispositivo del usuario y la biometría del comportamiento del usuario. Se puede entender que la caracterización del dispositivo y la captura de la constelación actual 800 pueden ser similares al proceso de tomar la captura 600 descrito anteriormente con respecto a la Fig. 6.

Como se muestra, la subconstelación 802 indica que, en el momento de la caracterización del dispositivo, la configuración del dispositivo era que había diez aplicaciones instaladas, tres de las cuales eran aplicaciones de redes sociales, tres eran aplicaciones de entretenimiento, una era una app de comida, una era una app de mapas, una era una app de TV y una era una app de fotos. Además, había un dispositivo inalámbrico conectado al aparato del usuario (por ejemplo, un reloj inteligente) y había seis tipos diferentes de dispositivos guardados en la lista de conexión de dispositivos inalámbricos. El aparato del usuario no estaba conectado a Wi-Fi en el momento de la caracterización del dispositivo, pero había cinco tipos diferentes de redes inalámbricas guardadas en la lista de redes Wi-Fi. Además, la versión del sistema operativo era 2.0 y la configuración de visualización estaba establecida de tal manera que el modo de hibernación se activaba después de tres minutos y la configuración de notificaciones estaba establecida en silencio.

Como se muestra además, la subconstelación 804 indica que, en el momento de la caracterización del dispositivo, varios aspectos del comportamiento o la interacción únicos del usuario con el aparato del usuario son que el usuario rara vez sostiene el aparato del usuario horizontalmente, siempre desliza el dedo de izquierda a derecha, no tiene atajos gestuales, escribe aproximadamente 50 palabras por minuto en el aparato del usuario, el usuario presiona el botón de inicio para realizar la transición entre aplicaciones y rara vez usa las pestañas de la app para realizar la transición, selecciona la app 606 antes que la app 608 la mayoría de las veces y, de manera similar, selecciona la app 806 antes que la app 808. Como se describió anteriormente, la constelación capturada 800 de la huella digital del dispositivo se puede proporcionar a uno o más servidores back-end para el análisis de desviación.

La Fig. 9 ilustra un ejemplo de análisis de deriva 900 de acuerdo con una o más realizaciones. Por ejemplo, el análisis de deriva 900 puede implicar al menos (i) comparar el resultado capturado de la constelación actual 800 en el momento de la caracterización del dispositivo y la captura 600 tomada en el momento de la autenticación exitosa del segundo factor y (ii) determinar si las diferencias entre la constelación actual 800 y la captura 600 están dentro de umbrales de deriva predeterminados. El límite de umbral de deriva predeterminado puede ser un límite de desviación de umbral de una o más configuraciones del dispositivo y/o una o más biometrías de comportamiento del usuario desde el momento de la autenticación del segundo factor hasta el momento de la caracterización del dispositivo, por ejemplo, un límite sobre cuánto de las configuraciones del dispositivo y/o de las biometrías de comportamiento del usuario pueden cambiar o desviarse dentro de ese lapso de tiempo.

De acuerdo con realizaciones, los ejemplos de los tipos de desviaciones analizadas pueden incluir cambios en la cantidad de aplicaciones, cambios en los tipos de apps, cambios en la cantidad de dispositivos inalámbricos conectados al aparato del usuario, cambios en los tipos de dispositivos inalámbricos conectados al aparato del usuario, cambios en la red a la que está conectado el aparato del usuario, cambios en la lista guardada de

redes a las que se puede conectar el aparato, cambios en la versión del sistema operativo, cambios en la configuración de visualización, cambios en la configuración de notificaciones, etc.

Por ejemplo, el umbral de deriva predeterminado puede establecerse de tal manera que la diferencia en el número de aplicaciones modificadas no pueda exceder de tres, la diferencia en el número de dispositivos conectados modificados no pueda exceder de tres, la diferencia en el número de redes inalámbricas modificadas a las que el aparato del usuario puede conectarse no pueda exceder de tres, la versión del sistema operativo no pueda cambiar. También se pueden analizar otros factores, como por ejemplo, si los tipos de aplicaciones que se han agregado, eliminado, modificado o si la visualización, notificación u otras configuraciones modificadas son total o ampliamente diferentes de la captura 600 a la constelación actual 800, entonces dichas diferencias pueden exceder y violar el umbral de desviación predeterminado. Un tipo de análisis similar se puede aplicar a las diferencias en la biometría del comportamiento del usuario. Por ejemplo, si los tipos de comportamiento siguen siendo similares o sustancialmente iguales, entonces los cambios caerían dentro del umbral de deriva predeterminado. Se puede entender que se puede utilizar un modelo de aprendizaje automático o una red neuronal para realizar el análisis de deriva, donde el modelo de aprendizaje automático o la red neuronal se pueden entrenar utilizando datos de entrenamiento o conjuntos de datos que contienen ejemplos de varias violaciones de deriva o ejemplos de deriva aceptable, etc.

Como se ilustra, los cambios de configuración del dispositivo entre la captura 600 y la constelación actual 800 se muestran subrayados en la constelación actual 800, por ejemplo, la cantidad de apps aumentó de ocho a diez (diferencia de dos), la cantidad de dispositivos inalámbricos conectados al aparato del usuario disminuyó de dos a uno (diferencia de uno), la cantidad de dispositivos inalámbricos guardados en la lista de dispositivos inalámbricos aumentó de cinco a seis (diferencia de uno), la cantidad de redes Wi-Fi guardadas aumentó de cuatro a cinco (diferencia de uno) y la configuración de notificaciones cambió de vibración a silente.

Además, los cambios de comportamiento del usuario entre la captura 600 y la constelación actual 800 se muestran subrayados, por ejemplo, la velocidad de escritura disminuyó de 55 palabras por minuto a 50 palabras por minuto, y que el usuario selecciona la app 806 antes de seleccionar la app 808, lo que es una nueva métrica de comportamiento. El análisis de deriva 900 puede revelar que todos los cambios de configuración del dispositivo están dentro de los umbrales de deriva definidos anteriormente. Es importante destacar que la versión del sistema operativo sigue siendo la misma. El análisis puede revelar además que todos los cambios de comportamiento del usuario permanecen sustancialmente sin cambios y que la adición del nuevo comportamiento es similar o está en línea con el comportamiento observado previamente.

De acuerdo con lo anterior, con base en el análisis de deriva 900, se puede determinar que los cambios entre la captura 600 y la constelación actual 800 están dentro del umbral de deriva predeterminado. De este modo, se puede permitir que la autenticación del segundo factor descrita anteriormente (por ejemplo, la autenticación de un toque o de un solo toque) persista durante un período de tiempo predeterminado hasta una comprobación de persistencia de autenticación posterior.

Se puede entender que las desviaciones en el comportamiento del usuario pueden tener más peso que las desviaciones en la configuración del dispositivo al determinar las violaciones de desviación. Por ejemplo, si el usuario siempre desliza el dedo de izquierda a derecha (por ejemplo, el 99 por ciento del tiempo), pero ahora desliza el dedo con más frecuencia de derecha a izquierda, eso puede indicar que el usuario puede no ser el usuario autenticado originalmente. En otras situaciones, los cambios en la configuración del dispositivo pueden tener más peso, por ejemplo, si las apps cambian completamente de tipo (las apps que en su mayoría no son redes sociales cambian a apps que en su mayoría son redes sociales). Puede entenderse además que el umbral de deriva predeterminado puede depender al menos del nivel de riesgo de la acción del usuario, por ejemplo, un nivel de riesgo más alto puede justificar umbrales más estrictos o más ajustados, mientras que un nivel de riesgo más bajo puede justificar umbrales laxos o más flexibles.

La Fig. 10 ilustra un diagrama de flujo de ejemplo 1000 de acuerdo con una o más realizaciones. El diagrama de flujo 1000 está relacionado con al menos realizar una comprobación de persistencia de autenticación y, en función de la comprobación, permitir o no permitir que persista una autenticación exitosa previa. Se puede entender que no es necesario ejecutar los bloques del diagrama de flujo 1000 y las características descritas en el mismo en ningún orden particular. Además, se puede entender que el diagrama de flujo 1000 y las características descritas en el mismo pueden ser ejecutados por uno o más procesadores o cualquier dispositivo informático o arquitectura informática adecuada descrita en este documento.

En el bloque 1002, se pueden realizar autenticaciones de primer y segundo factor. La autenticación del primer factor puede basarse en algo que el usuario sabe, por ejemplo, el ingreso de su identificación y contraseña. La autenticación de segundo factor puede activarse mediante un evento de autenticación de segundo factor, como la transferencia de una gran cantidad de dinero. El segundo factor de autenticación puede ser un solo toque de la tarjeta inteligente sin contacto del usuario, como se describió anteriormente.

En el bloque 1004, se puede tomar una captura de la constelación de las configuraciones del dispositivo del aparato del usuario y/o uno o más datos biométricos del comportamiento del usuario en el momento de la

autenticación de segundo factor exitosa (o autenticación de primer factor dependiendo de qué autenticación persistirá) en el bloque 1002. La captura se puede proporcionar a uno o más dispositivos informáticos back-end remotos (por ejemplo, servidores back-end asociados con una plataforma de app de transacciones), que luego pueden ser utilizados por los dispositivos informáticos back-end como un punto de referencia para determinar cuánto han cambiado las configuraciones del dispositivo y las métricas de comportamiento.

En el bloque 1006, se puede provocar que se realice una comprobación de estabilidad en el aparato del usuario. La comprobación puede ser causada por el aparato o puede ser iniciada automáticamente por los dispositivos informáticos back-end. La comprobación de estabilidad puede activarse: cuando haya transcurrido un período de tiempo específico desde la primera instancia de autenticación exitosa o en función de la ocurrencia de un evento de autenticación (por ejemplo, solicitar transferir una gran cantidad de fondos a través de la app de transacciones). La comprobación de estabilidad puede ser una verificación de MNO, que implica que un MNO proporcione verificación de que el aparato del usuario no ha cambiado significativamente, por ejemplo, la tarjeta SIM no ha cambiado. El resultado de la verificación del MNO puede proporcionarse a uno o más dispositivos informáticos back-end.

En el bloque 1008, en respuesta a una comprobación de estabilidad exitosa, los dispositivos informáticos back-end pueden solicitar al aparato del usuario que realice la caracterización del dispositivo. Como se describió anteriormente, la caracterización del dispositivo puede ser similar a la captura tomada en el bloque 1004, excepto que se realiza en el momento de la caracterización del dispositivo. El resultado de la caracterización del dispositivo es una constelación actual de las configuraciones del dispositivo del usuario y/o uno o más datos biométricos del comportamiento del usuario. La constelación actual se puede proporcionar a los dispositivos informáticos backend para el análisis de deriva, como se describió en detalle anteriormente.

En el bloque 1010, el aparato de usuario puede recibir el resultado del análisis de desviación de los dispositivos informáticos back-end, lo que indica que la autenticación (por ejemplo, la autenticación de segundo factor) puede o no persistir. Si puede persistir, el usuario no necesita realizar nuevamente la autenticación de un solo toque y la transferencia de fondos puede continuar. Si no puede persistir, se le solicita al usuario que se vuelva a autenticar mediante la autenticación de un solo toque o de una cinta.

Los componentes y características de los dispositivos descritos anteriormente pueden implementarse utilizando cualquier combinación de circuitos discretos, circuitos integrados de aplicación específica (ASICs), puertas lógicas y/o arquitecturas de un solo chip. Además, las características de los dispositivos pueden implementarse utilizando microcontroladores, matrices lógicas programables y/o microprocesadores o cualquier combinación de los anteriores cuando sea adecuadamente apropiado. Se observa que los elementos de hardware, firmware y/o software pueden denominarse colectiva o individualmente en el presente documento “lógica” o “circuito”.

Al menos un medio de almacenamiento legible por ordenador puede incluir instrucciones que, cuando se ejecutan, hacen que un sistema realice cualquiera de los métodos implementados por ordenador descritos en este documento.

Algunas realizaciones pueden describirse utilizando la expresión “una realización” o “una realización” junto con sus derivados. Estos términos significan que una característica, estructura o característica particular descrita en relación con la realización está incluida en al menos una realización. Las apariciones de la frase “en una realización” en varios lugares de la especificación no necesariamente se refieren todas a la misma realización. Además, a menos que se indique lo contrario, se reconoce que las características descritas anteriormente se pueden utilizar juntas en cualquier combinación. Por lo tanto, cualquier característica discutida por separado puede emplearse en combinación con otras, a menos que se observe que las características son incompatibles entre sí.

Con referencia general a las notaciones y nomenclatura utilizadas en este documento, las descripciones detalladas aquí pueden presentarse en términos de procedimientos de programa ejecutados en un ordenador o red de ordenadores. Estas descripciones y representaciones de procedimientos son utilizadas por los expertos en la materia para transmitir de la forma más eficaz la esencia de su trabajo a otros expertos en la materia.

Un procedimiento se concibe aquí, y en general, como una secuencia de operaciones coherente que conduce a un resultado deseado. Estas operaciones son aquellas que requieren manipulaciones físicas de cantidades físicas. Generalmente, aunque no necesariamente, estas cantidades toman la forma de señales eléctricas, magnéticas u ópticas capaces de ser almacenadas, transferidas, combinadas, comparadas y manipuladas de otro modo. A veces resulta conveniente, principalmente por razones de uso común, referirse a estas señales como bits, valores, elementos, símbolos, caracteres, términos, números o similares. Cabe señalar, sin embargo, que todos estos términos y otros similares deben asociarse con las cantidades físicas apropiadas y son simplemente etiquetas convenientes que se aplican a esas cantidades.

Además, las manipulaciones realizadas a menudo se mencionan en términos como sumar o comparar, que comúnmente se asocian con operaciones mentales realizadas por un operador humano. No es necesaria ni

deseable en la mayoría de los casos dicha capacidad de un operador humano en ninguna de las operaciones descritas en este documento, que forman parte de una o más realizaciones. Más bien, las operaciones son operaciones de máquina.

Algunas realizaciones pueden describirse utilizando la expresión “acoplado” y “conectado” junto con sus derivados. Estos términos no necesariamente deben ser sinónimos entre sí. Por ejemplo, algunas realizaciones pueden describirse utilizando los términos “conectado” y/o “acoplado” para indicar que dos o más elementos están en contacto físico o eléctrico directo entre sí. Sin embargo, el término “acoplado” también puede significar que dos o más elementos no están en contacto directo entre sí, pero aun así cooperan o interactúan entre sí.

Diversas realizaciones también se refieren a aparatos o sistemas para realizar estas operaciones. Este aparato puede construirse especialmente para el propósito requerido y puede activarse o reconfigurarse selectivamente mediante un programa de ordenador almacenado en el ordenador. Los procedimientos aquí presentados no están relacionados inherentemente con un ordenador u otro aparato en particular. La estructura requerida para una variedad de estas máquinas aparecerá en la descripción dada.

Se enfatiza que el Resumen de la Divulgación se proporciona para permitir que el lector determine rápidamente la naturaleza de la divulgación técnica. Se presenta con el entendimiento de que no se utilizará para interpretar o limitar el alcance o significado de las reivindicaciones. Además, en la Descripción Detallada anterior, se puede observar que varias características se agrupan en una única realización con el fin de agilizar la divulgación. Este método de divulgación no debe interpretarse como un reflejo de una intención de que las realizaciones reivindicadas requieran más características que las que se mencionan expresamente en cada reivindicación. Más bien, como reflejan las siguientes reivindicaciones, el objeto inventivo reside en menos que todas las características de una única realización divulgada. Por lo tanto, las siguientes reivindicaciones se incorporan a la Descripción detallada, y cada reivindicación se considera por sí sola una realización separada. En las reivindicaciones adjuntas, los términos “que incluyen” y “en el cual” se utilizan como equivalentes en inglés simple de los términos respectivos “que comprende” y “en el que”, respectivamente. Además, los términos «primero», «segundo», «tercero», etc., se utilizan simplemente como etiquetas y no pretenden imponer requisitos numéricos a sus objetos.

Lo descrito anteriormente incluye ejemplos de la arquitectura divulgada. Por supuesto, no es posible describir cada combinación concebible de componentes y/o metodologías, pero una persona con conocimientos medios en la materia puede reconocer que son posibles muchas otras combinaciones y permutaciones. De acuerdo con lo anterior, la nueva arquitectura pretende abarcar todas las alteraciones, modificaciones y variaciones que caen dentro del alcance de las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un aparato (210) que comprende:

un lector de comunicación de campo cercano (NFC) (213);

uno o más procesadores (212) capaces de ejecutar instrucciones almacenadas que, cuando se ejecutan, hacen a uno o más procesadores:

autenticar a un usuario a través de la autenticación de primer factor;

autenticar al usuario a través de una autenticación de segundo factor diferente de la autenticación de primer factor, en la que la autenticación de segundo factor comprende: acercar una tarjeta sin contacto (205) al aparato (210) de manera que se establezca una comunicación NFC, recibir información de autenticación de usuario desde la tarjeta sin contacto (205) a través del lector NFC (213), enviar la información de autenticación de usuario a uno o más dispositivos informáticos remotos, y recibir una indicación desde uno o más dispositivos informáticos remotos de que el usuario está autenticado;

determinar una captura que incluye una o más configuraciones del dispositivo del aparato y uno o más datos biométricos del comportamiento del usuario en un primer momento de la autenticación del segundo factor;

hacer que se realice una comprobación de estabilidad del aparato: (i) en una segunda ocasión después de la primera vez o (ii) cuando se produce un evento de autenticación después de la primera vez;

en respuesta a que el aparato esté estable, realizar una caracterización del dispositivo en el aparato para determinar si el aparato se encuentra dentro de un umbral de deriva predeterminado con respecto a la captura;

en respuesta a que el aparato se encuentre dentro del umbral de deriva predeterminado, permitir que la autenticación del segundo factor persista durante un período de tiempo predeterminado; y

en respuesta a que el aparato no se encuentre dentro del umbral de deriva predeterminado, vuelva a autenticar al usuario a través de la autenticación de segundo factor.

2. El aparato (210) de la reivindicación 1, en el que los uno o más ajustes del dispositivo incluyen: (i) una o más aplicaciones (211) instaladas en el aparato (210), (ii) uno o más dispositivos inalámbricos conectados al aparato a través de una conexión inalámbrica, (iii) una lista de dispositivos inalámbricos guardados que se pueden conectar al aparato, (iv) una red a la que está conectado el aparato, (v) una lista de redes guardadas a las que se puede conectar el aparato, (vi) una versión de un sistema operativo en el aparato, y/o (vii) una o más preferencias de configuración.

3. El aparato (210) de la reivindicación 1, en el que la determinación de uno o más datos biométricos del comportamiento del usuario comprende uno o más procesadores (212) para:

recibir, a través de uno o más sensores o una o más interfaces, datos de comportamiento del usuario, y

determinar en función de los datos de comportamiento del usuario: (i) cómo el usuario sostiene físicamente el aparato, (ii) cómo el usuario desliza o interactúa con una interfaz de visualización, (iii) cómo el usuario utiliza el teclado o atajos gestuales, (iv) cómo el usuario escribe palabras, (v) una duración de tiempo para que el usuario escriba palabras, (vi) cómo el usuario hace la transición entre dos o más íconos, (vii) la velocidad de escritura del usuario, y/o (viii) la cadencia de escritura del usuario.

4. El aparato (210) de la reivindicación 1, en el que la comprobación de estabilidad en el aparato comprende una verificación del operador de red móvil (MNO).

5. El aparato (210) de la reivindicación 1, en la que una o más configuraciones del dispositivo del aparato y una o más biometrías de comportamiento del usuario asociadas con el aparato son únicas para el usuario en el primer momento de la autenticación del segundo factor,

en la que la caracterización del dispositivo captura una constelación actual de una o más configuraciones del dispositivo del aparato y una o más biometrías de comportamiento del usuario asociadas con el aparato en un tercer momento de la caracterización del dispositivo, y

en la que el umbral de deriva predeterminado es un límite de desviación del umbral de una o más configuraciones del dispositivo y una o más biometrías de comportamiento del usuario desde la captura en el primer momento de la autenticación del segundo factor hasta el tercer momento de la caracterización del dispositivo.

6. El aparato (210) de la reivindicación 1, en el que se hace además que los uno o más procesadores (212), en respuesta a que el aparato no es estable, vuelvan a autenticar al usuario a través de las autenticaciones de primer y segundo factor.

7. El aparato (210) de la reivindicación 1, en el que se hace que los uno o más procesadores (212) además:

determine un nivel de riesgo de una acción del usuario que se va a procesar o realizar; y

procese o realizar la acción del usuario, y

en el que el umbral de deriva predeterminado depende al menos del nivel de riesgo de la acción del usuario.

8. Un método que comprende:

autenticar (402), a través de uno o más procesadores, a un usuario basándose en la autenticación de primer factor;

autenticar (404), a través de uno o más procesadores, al usuario basándose en una autenticación de segundo factor diferente de la autenticación de primer factor, en la que la autenticación de segundo factor comprende: acercar una tarjeta sin contacto a un aparato de manera que se establezca una comunicación de campo cercano (NFC), recibir información de autenticación de usuario desde la tarjeta sin contacto a través de un lector NFC, enviar la información de autenticación de usuario a uno o más dispositivos informáticos remotos, y recibir una indicación desde uno o más dispositivos informáticos remotos de que el usuario está autenticado;

determinar (406), a través de uno o más procesadores, una captura que incluye una o más configuraciones del dispositivo del aparato y una o más biometrías de comportamiento del usuario en un primer momento de la autenticación del segundo factor;

provocar (410), a través de uno o más procesadores, una comprobación de estabilidad del aparato a realizar: (i) en una segunda ocasión después de la primera vez o (ii) cuando se produce un evento de autenticación después de la primera vez;

realizar (414), a través de uno o más procesadores, la caracterización del dispositivo en el aparato para determinar si el aparato se encuentra dentro de un umbral de deriva predeterminado con respecto a la captura en respuesta a que el aparato sea estable;

permitir, a través de uno o más procesadores, que la autenticación del segundo factor persista durante un período de tiempo predeterminado en respuesta a que el aparato se encuentre dentro del umbral de deriva predeterminado; y

volver a autenticar, a través de uno o más procesadores, al usuario basándose en la autenticación de segundo factor en respuesta a que el aparato no se encuentra dentro del umbral de deriva predeterminado.

9. El método de la reivindicación 8, en el que uno o más ajustes del dispositivo incluyen: (i) una o más aplicaciones instaladas en el aparato, (ii) uno o más dispositivos inalámbricos conectados al aparato a través de una conexión inalámbrica, (iii) una lista de dispositivos inalámbricos guardados que se pueden conectar al aparato, (iv) una red a la que está conectado el aparato, (v) una lista de redes guardadas a las que se puede conectar el aparato, (vi) la versión de un sistema operativo en el aparato, y/o (vii) una o más preferencias de configuración.

10. El método de la reivindicación 8, en el que la determinación de uno o más datos biométricos del comportamiento del usuario comprende además:

recibir, a través de uno o más sensores o una o más interfaces, datos de comportamiento del usuario, y

determinar, a través de uno o más procesadores, en función de los datos de comportamiento del usuario: (i) cómo el usuario sostiene físicamente el aparato, (ii) cómo el usuario desliza o interactúa con una interfaz de visualización, (iii) cómo el usuario utiliza el teclado o atajos gestuales, (iv) cómo el usuario escribe palabras, (v) una duración de tiempo para que el usuario escriba palabras, (vi) cómo el usuario hace la transición entre dos o más íconos, (vii) la velocidad de escritura del usuario, y/o (viii) la cadencia de escritura del usuario.

11. El método de la reivindicación 8, en el que la comprobación de estabilidad del aparato comprende una verificación del operador de red móvil (MNO).

12. El método de la reivindicación 8, en el que una o más configuraciones del dispositivo del aparato y una o más biometrías de comportamiento del usuario asociadas con el aparato son únicas para el usuario en el primer momento de la autenticación del segundo factor,

en la que la caracterización del dispositivo captura una constelación actual de una o más configuraciones del dispositivo del aparato y una o más biometrías de comportamiento del usuario asociadas con el aparato en un tercer momento de la caracterización del dispositivo, y

en el que el umbral de deriva predeterminado es un límite de desviación del umbral de una o más configuraciones del dispositivo y una o más biometrías de comportamiento del usuario desde la captura en el primer momento de la autenticación del segundo factor hasta el tercer momento de la caracterización del dispositivo.

13. El método de la reivindicación 8, que comprende además volver a autenticar, a través de uno o más procesadores, al usuario basándose en las autenticaciones de primer y segundo factor en respuesta a que el aparato no es estable.

14. El método de la reivindicación 8, que comprende además:

determinar, a través de uno o más procesadores, un nivel de riesgo de una acción del usuario que se procesará o realizará; y

procesar o realizar, a través de uno o más procesadores, la acción del usuario, y

en el que el umbral de deriva predeterminado depende al menos del nivel de riesgo de la acción del usuario.

15. Al menos un medio de almacenamiento legible por ordenador no transitorio que almacena código de programa legible por ordenador ejecutable por al menos un procesador para:

autenticar (402) a un usuario a través de la autenticación de primer factor;

autenticar (404) al usuario a través de una autenticación de segundo factor diferente de la autenticación de primer factor, en la que la autenticación de segundo factor comprende: acercar una tarjeta sin contacto a un aparato de manera que se establezca una comunicación de campo cercano (NFC), recibir información de autenticación de usuario desde la tarjeta sin contacto a través de un lector NFC, enviar la información de autenticación de usuario a uno o más dispositivos informáticos remotos y recibir una indicación de uno o más dispositivos informáticos remotos de que el usuario está autenticado;

determinar (406) una captura que incluye una o más configuraciones del dispositivo del aparato y una o más biometrías de comportamiento del usuario en un primer momento de la autenticación del segundo factor;

hacer que se realice una comprobación de estabilidad del aparato (410): (i) en una segunda ocasión después de la primera vez o (ii) cuando se produce un evento de autenticación después de la primera vez;

en respuesta a que el aparato esté estable, realizar una caracterización del dispositivo (414) en el aparato para determinar si el aparato está dentro de un umbral de deriva predeterminado en función de la captura;

en respuesta a que el aparato se encuentre dentro del umbral de deriva predeterminado, permitir que la autenticación del segundo factor persista durante un período de tiempo predeterminado; y

en respuesta a que el aparato no se encuentre dentro del umbral de deriva predeterminado, vuelva a autenticar al usuario a través de la autenticación de segundo factor.

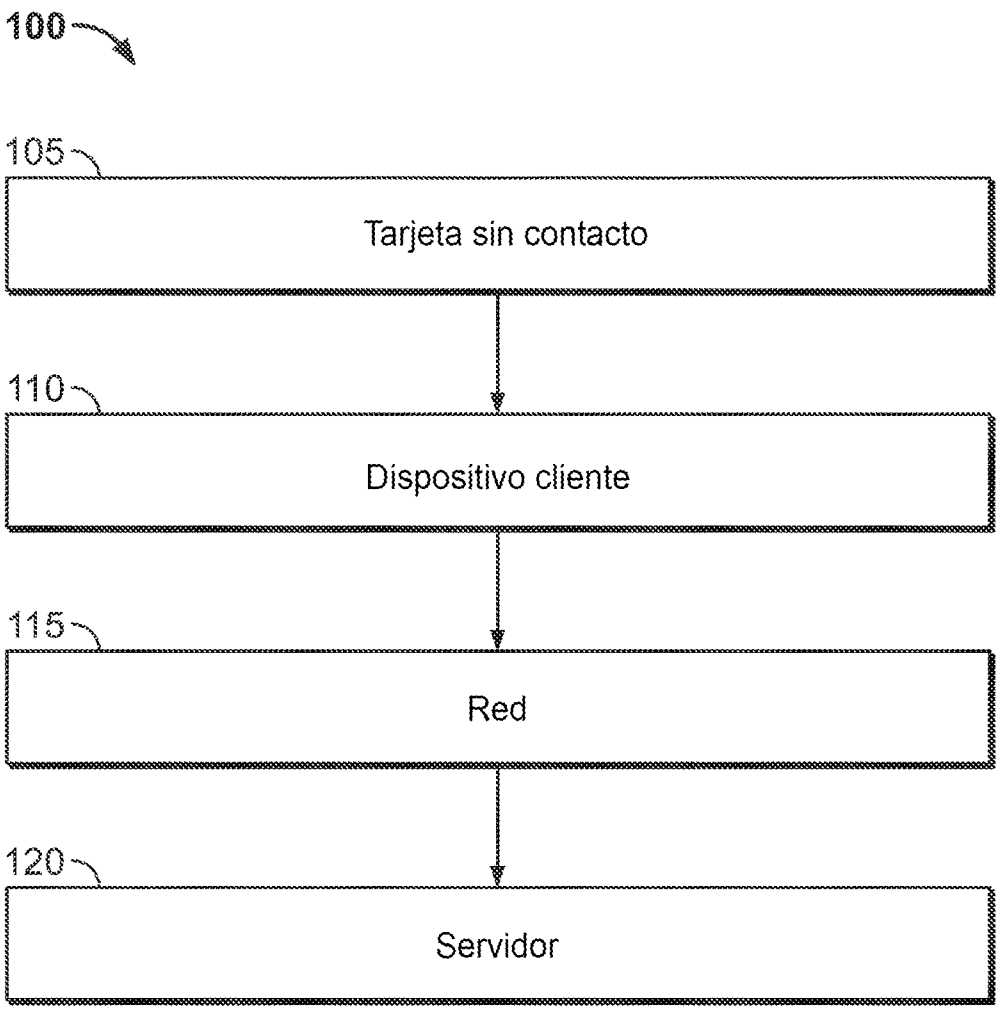
100
105
Tarjeta sin contacto
110
Dispositivo cliente
115
Red
120
Servidor

FIG. 1A

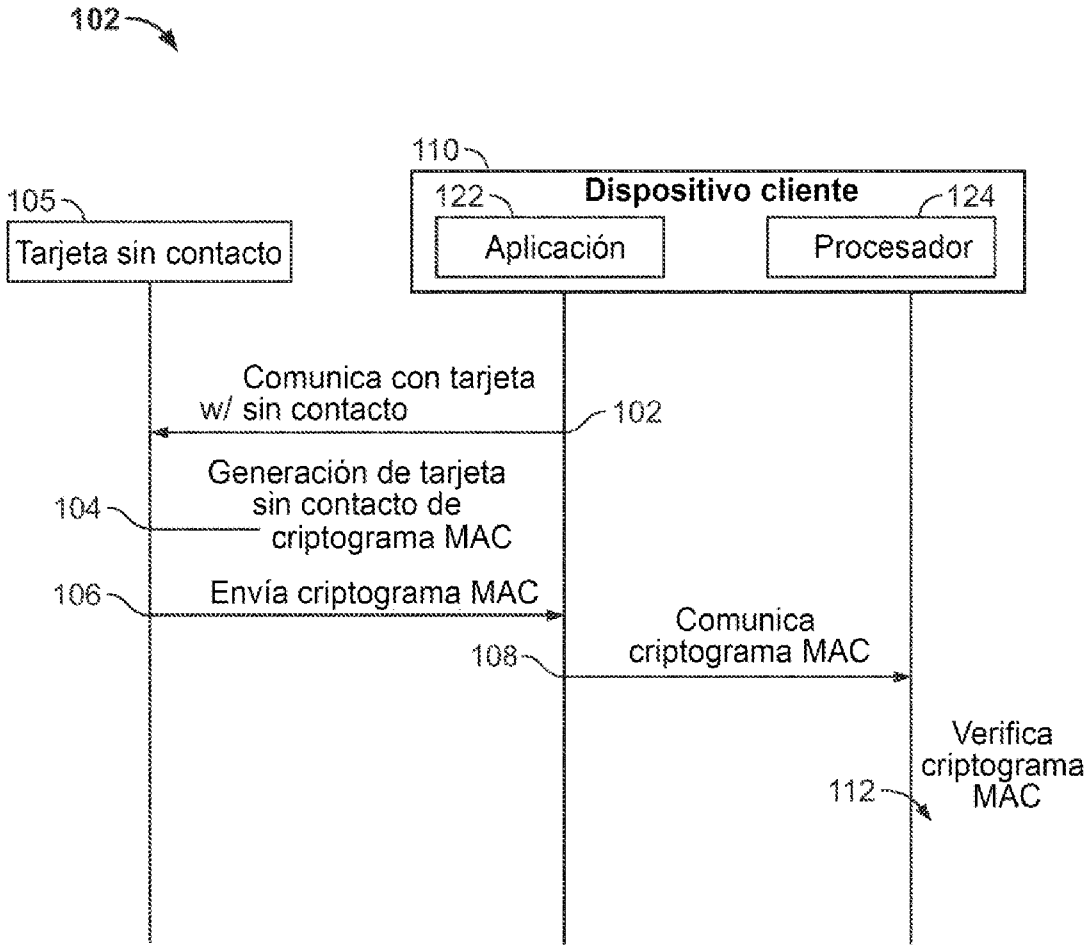
102
110
Dispositivo cliente
122
Aplicación
124
Procesador
105
Tarjeta sin contacto
Comunica con tarjeta w/ sin contacto
102
Generación de tarjeta sin contacto de criptograma MAC
104
Envía criptograma MAC
106
Comunica criptograma MAC
108
Verifica criptograma MAC
112

FIG. 1B

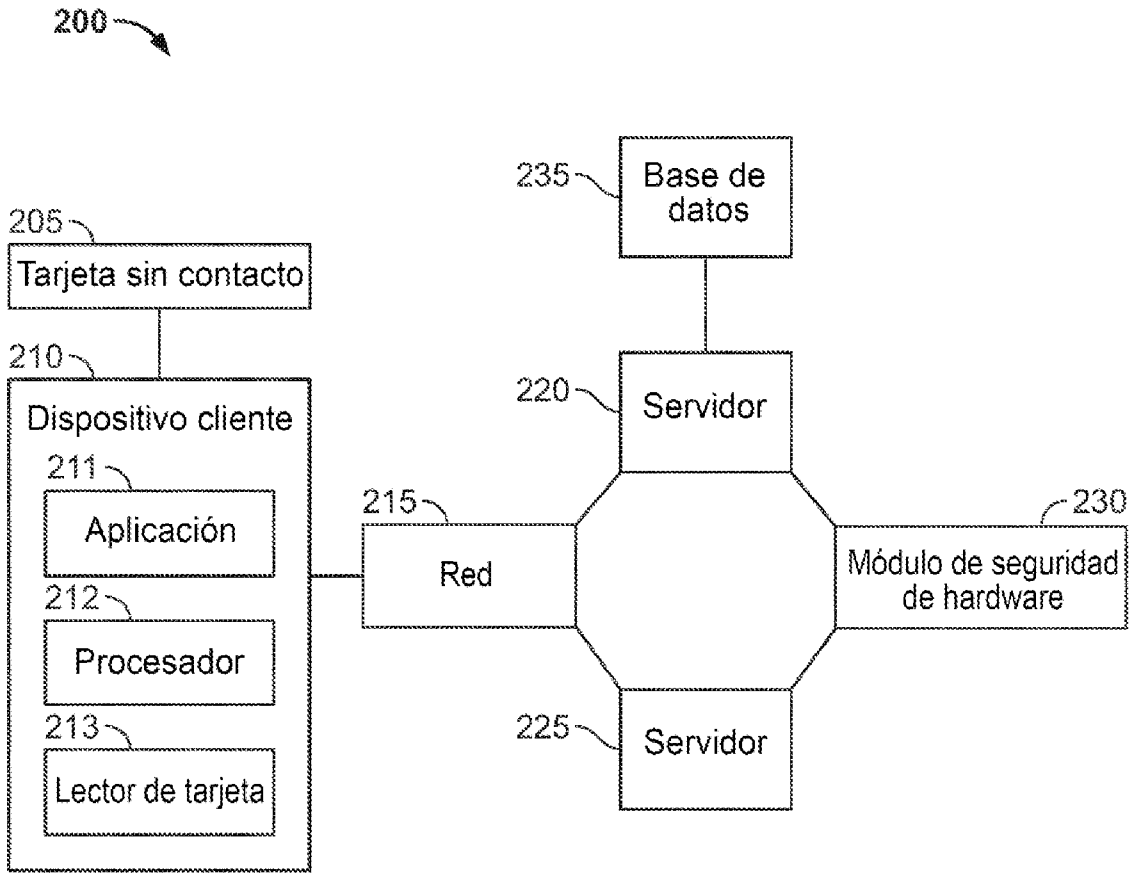
200
235
Base de datos
205
Tarjeta sin contacto
210
Dispositivo cliente
211
Aplicación
212
Procesador
213
Lector de tarjeta
220
Servidor
215
Red
230
Módulo de seguridad de hardware
225
Servidor

FIG. 2

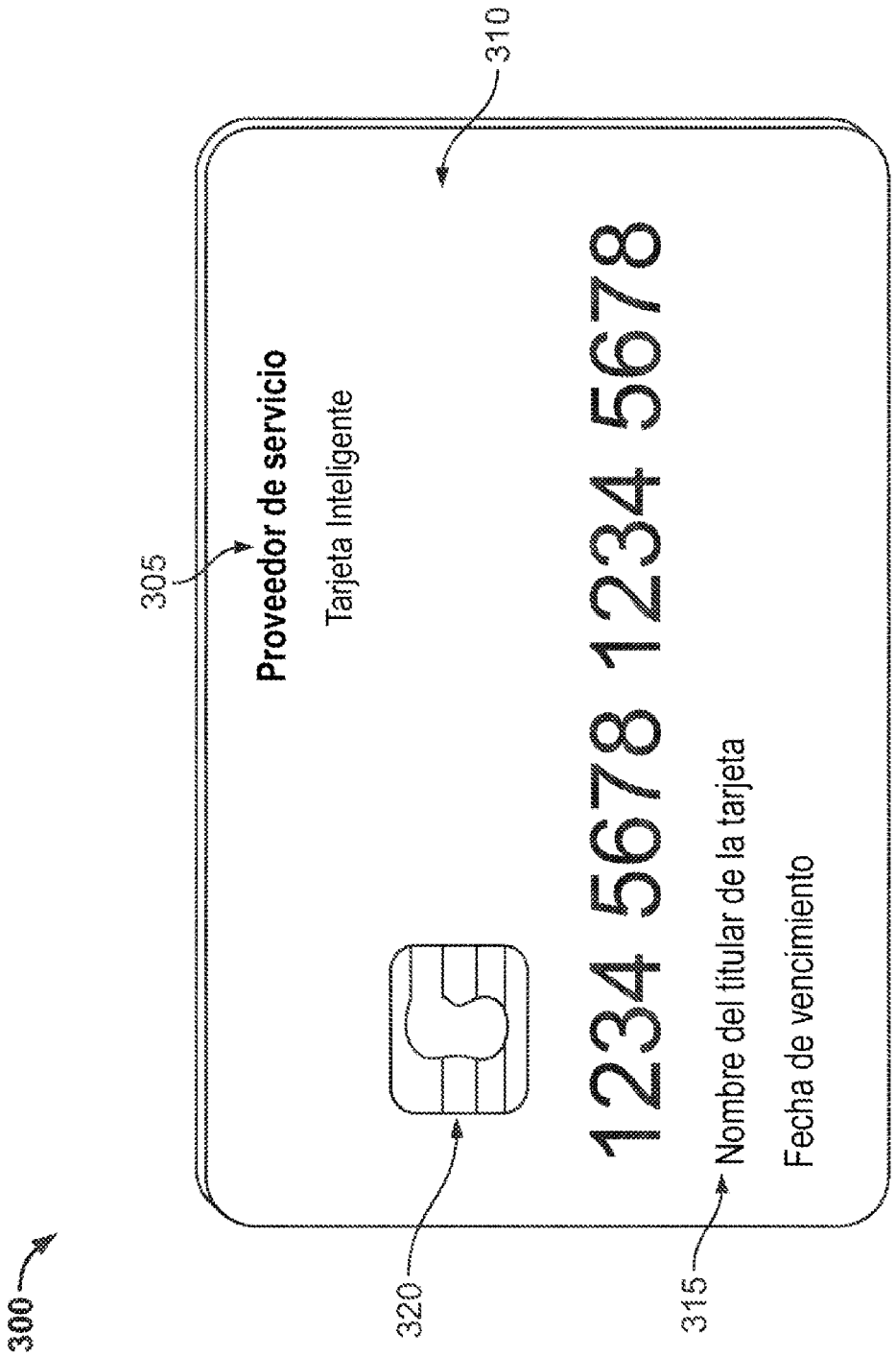
300
305
Proveedor de servicio
Tarjeta Inteligente
310
1234 5678 1234 5678
Nombre del titular de la tarjeta
Fecha de vencimiento
315
320

FIG. 3A

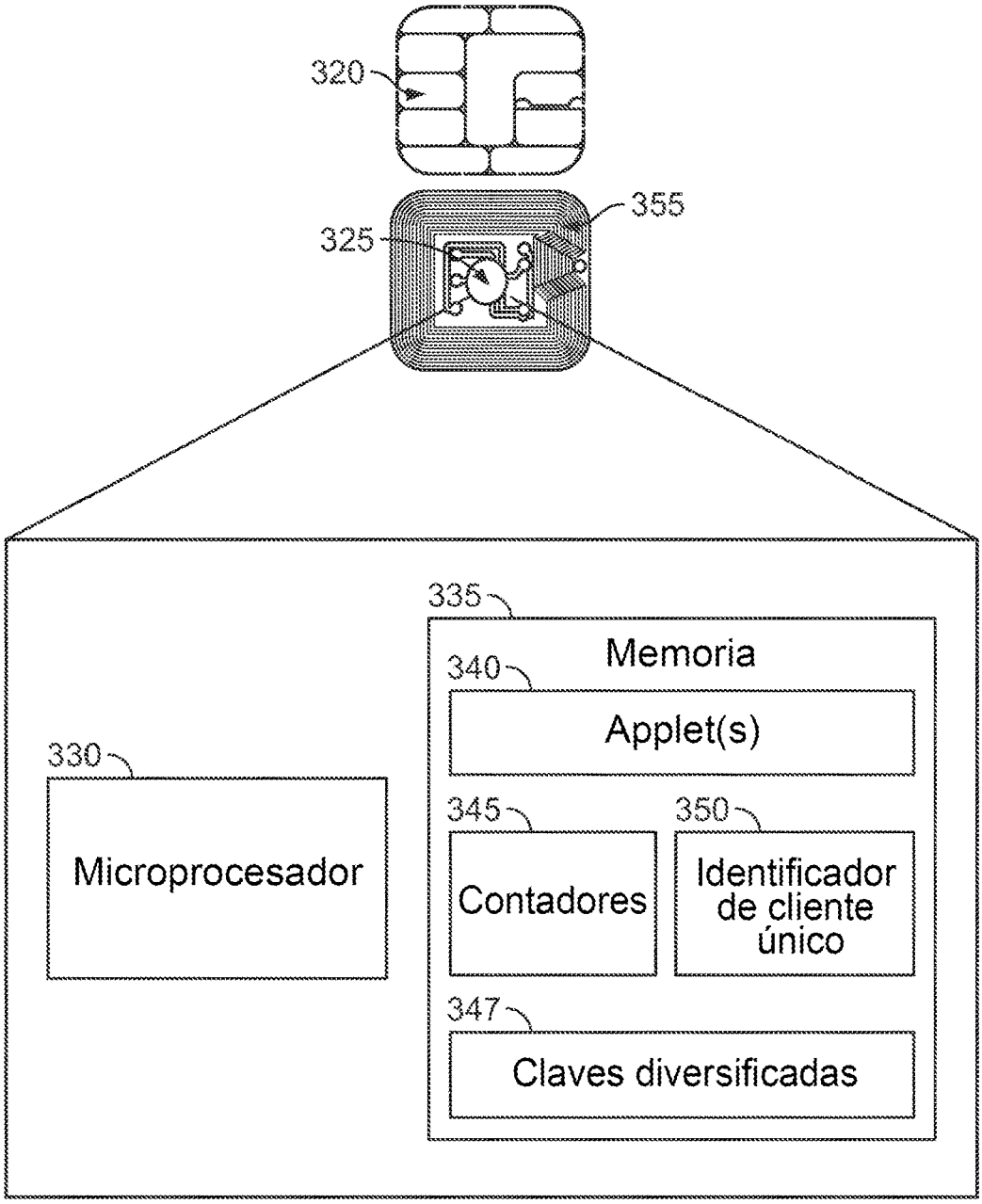
320
325
355
335
Memoria
340
Applet(s)
330
Microprocesador
345
Contadores
350
Identificador de cliente único
347
Claves diversificadas

FIG. 3B

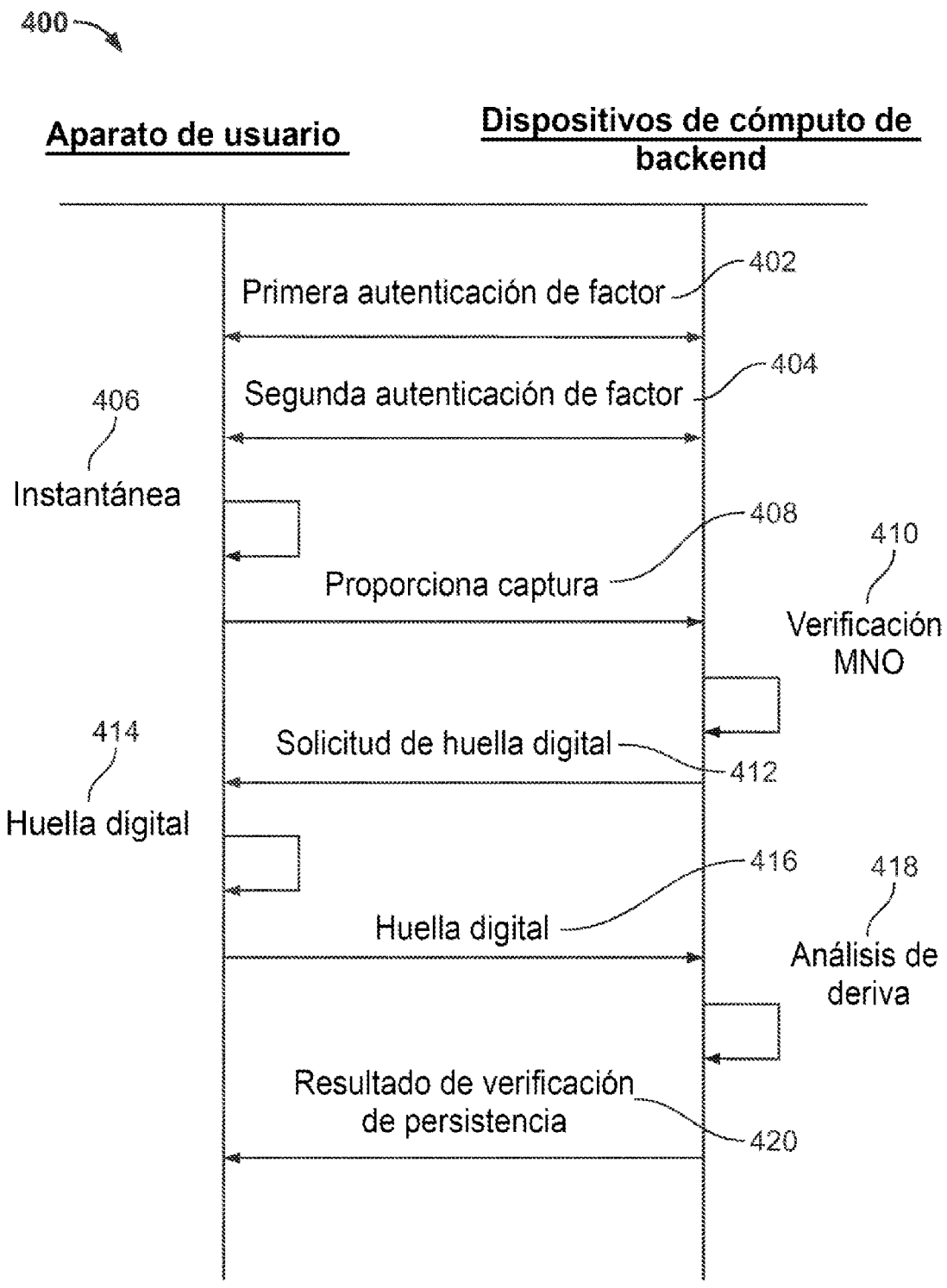
400
Aparato de usuario
Dispositivos de cómputo de backend
Primera autenticación de factor
402
Segunda autenticación de factor
404
406
Instantánea
408
Proporciona captura
410
Verificación MNO
414
Solicitud de huella digital
412
Huella digital
416
Huella digital
418
Análisis de deriva
Resultado de verificación de persistencia
420

FIG. 4

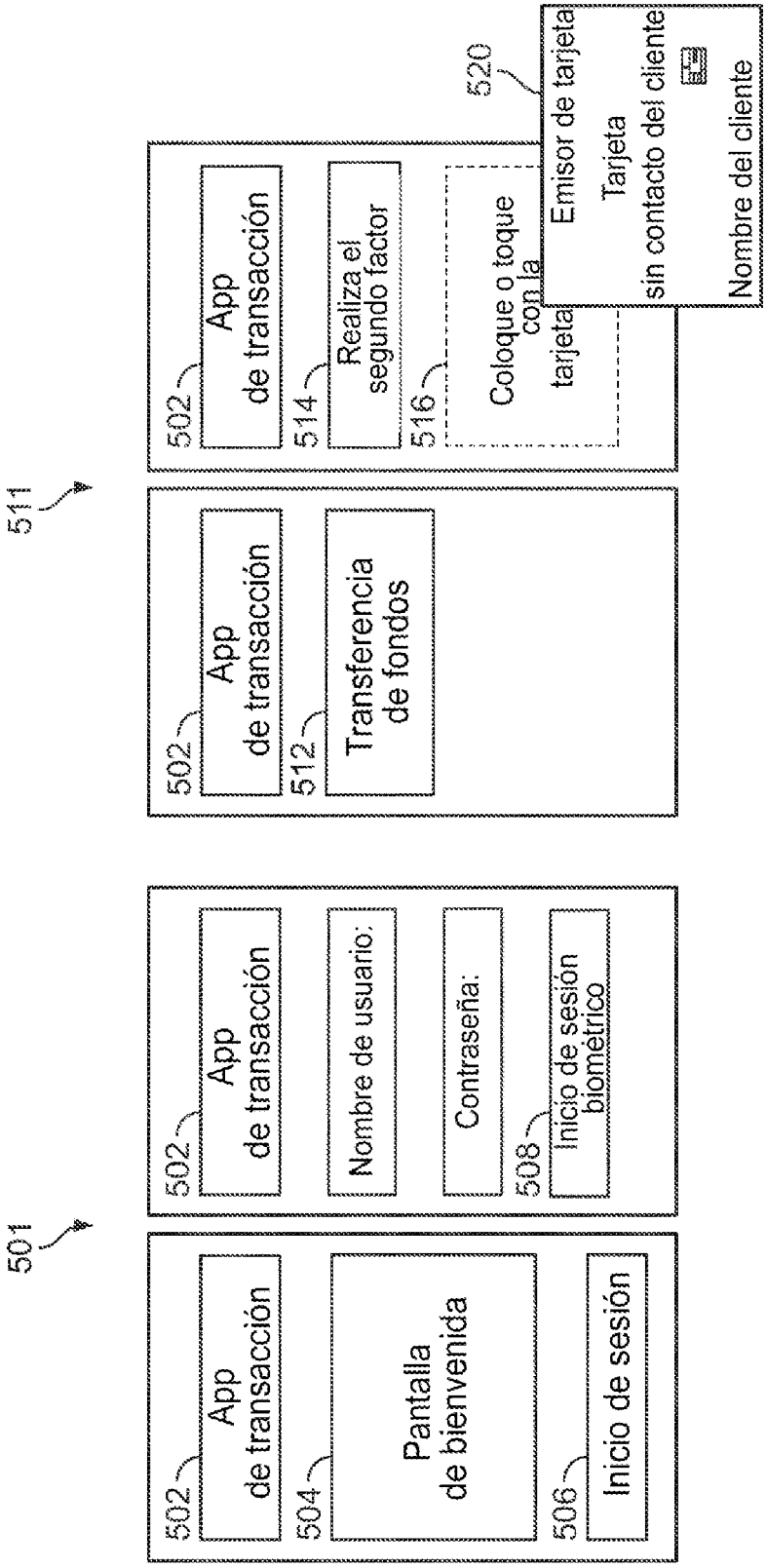
501
502
App de transacción
504
Pantalla de bienvenida
506
Inicio de sesión
Nombre de usuario:
Contraseña:
508
Inicio de sesión biométrico
511
512
Transferencia de fondos
514
Realiza el segundo factor
516
Coloque o toque con la tarjeta
520
Emisor de tarjeta
Tarjeta sin contacto del cliente
Nombre del cliente

FIG. 5

600
Configuraciones de dispositivo 602
Ocho apps instaladas
Tres de ocho apps son apps de redes sociales; tres son apps de entretenimiento; una app es de alimentos; una app es de mapas
Dos dispositivos inalámbricos conectados
Cinco dispositivos inalámbricos guardados a la lista de dispositivos inalámbricos
No conectado a WiFi
Cuatro redes wifi guardadas
La versión del sistema operativo es 2.0
Configuración de visualización: el modo de hibernación se activa después de 3 min.
Configuración de notificación: vibración
Biométricos de comportamiento de usuario 604
Raramente sostiene horizontalmente el aparato de usuario
Siempre barre de izquierda a derecha
Sin atajos gestuales
Escribe 55 palabras aproximadamente por minuto en el aparato de usuario
Presiona el botón de inicio para cambiar entre apps y rara vez utiliza las pestañas de apps para hacerlo
La mayor parte del tiempo selecciona la app 606 primero y luego la app 608

FIG. 6

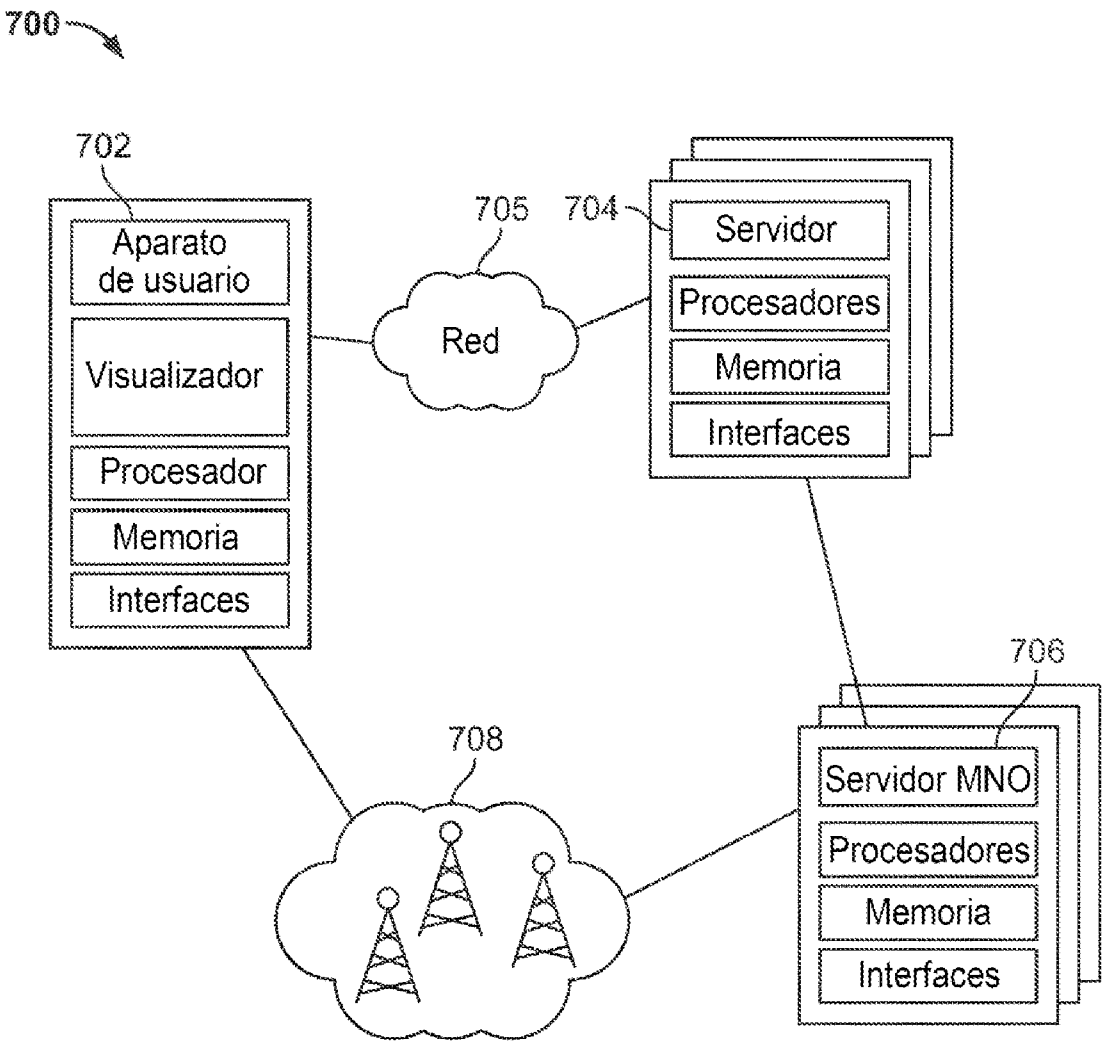
700
702
Aparato de usuario
Visualizador
Procesador
Memoria
Interfaces
705
Red
704
Servidor
Procesadores
Memoria
Interfaces
706
Servidor MNO
Procesadores
Memoria
Interfaces
708

FIG. 7

800

Configuraciones de dispositivo 802	Biométricos de comportamiento de usuario 804
• Diez apps instaladas • Tres de las diez apps son apps de redes sociales; tres son apps de entretenimiento; una es una app de alimentos; una es una app de mapas; otra es una app de TV; una es una app • Un dispositivo inalámbrico conectado • Seis dispositivos inalámbricos guardados en la lista de dispositivos inalámbricos • No conectado al WifFi • Cinco redes WiFi guardadas • La versión del sistema operativo es 2.0. • Configuración de visualización: el modo de hibernación se activa después de 3 min. • Configuración de notificación: Silente	• Raramente sostiene horizontalmente el aparato de usuario • Siempre barre de izquierda a derecha • Sin atajos gestuales • Escribe 50 palabras aproximadamente por minuto en el aparato de usuario • Presiona el botón de inicio para cambiar entre apps y rara vez utiliza las pestañas de apps para hacerlo • La mayor parte del tiempo selecciona la app 606 primero y luego la app 608 • La mayor parte del tiempo selecciona la app 806 primero y luego la app 808

FIG. 8

900

Configuraciones de dispositivo 602	Biométricos de comportamiento de usuario 604
• Ocho apps instaladas • Tres de las ocho apps son apps de redes sociales; tres son apps de entretenimiento; una es una app de alimentos; una es una app de mapas • Dos dispositivos inalámbricos conectados • Cinco dispositivos inalámbricos guardados en la lista de dispositivos inalámbricos • No conectado a WiFi • Cuatro redes WiFi conectadas • Versión del sistema operativo es 2.0. • Configuración de visualización: el modo de hibernación se activa después de 3 min. • Configuración de notificación: vibración	• Raramente sostiene horizontalmente el aparato de usuario • Siempre barre de izquierda a derecha • Sin atajos gestuales • Escribe 55 palabras aproximadamente por minuto en el aparato de usuario • Presiona el botón de inicio para cambiar entre apps y rara vez utiliza las pestañas de apps para hacerlo • La mayor parte del tiempo selecciona la app 606 primero y luego la app 608
Configuraciones de dispositivo 802	**Biométricos de comportamiento de usuario 804**
• **Diez** apps instaladas • Tres de las diez apps son apps de redes sociales; tres son apps de entretenimiento; una es una app de alimentos; una es una app de mapas; una es una app de TV; una es una app de fotos • **Un** dispositivo inalámbrico conectado • **Seis** dispositivos inalámbricos guardados en la lista de dispositivos inalámbricos • No conectado a WiFi • **Cinco** redes WiFi conectadas guardadas • Versión del sistema operativo es 2.0. • Configuración de visualización: el modo de hibernación se activa después de 3 min. • Configuración de notificación: **Silente**	• Raramente sostiene horizontalmente el aparato de usuario • Siempre barre de izquierda a derecha • Sin atajos gestuales • Escribe **50 palabras** aproximadamente **por minuto** en el aparato de usuario • Presiona el botón de inicio para cambiar entre apps y rara vez utiliza las pestañas de apps para hacerlo • La mayor parte del tiempo selecciona la app 606 primero y luego la app 608 • La mayor parte del tiempo selecciona la app **806** primero y luego la app **808**

FIG. 9

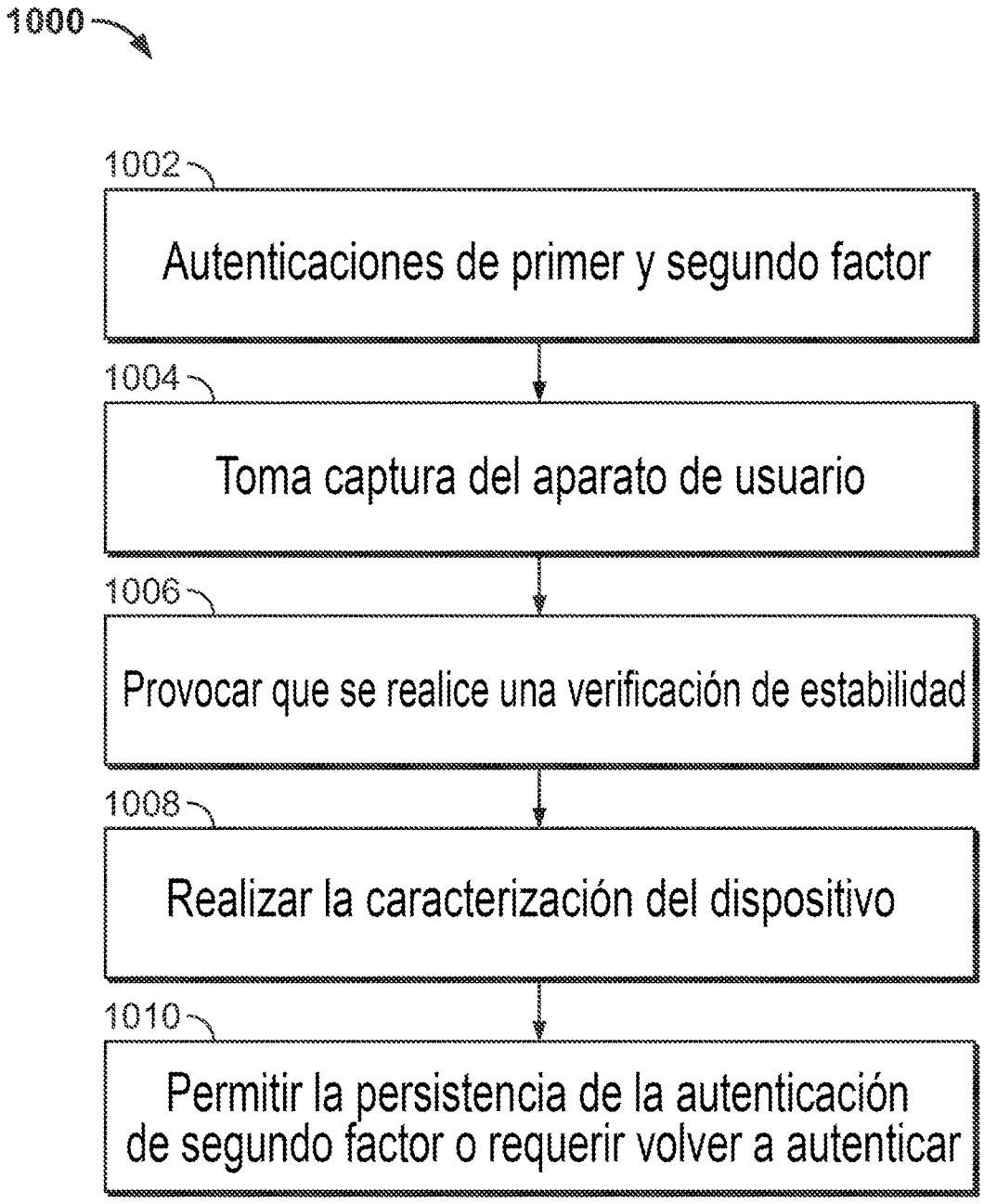
1000
1002
Autenticaciones de primer y segundo factor
1004
Toma captura del aparato de usuario
1006
Provocar que se realice una verificación de estabilidad
1008
Realizar la caracterización del dispositivo
1010
Permitir la persistencia de la autenticación de segundo factor o requerir volver a autenticar

FIG. 10