

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **3 001 510**

51 Int. Cl.:

G06F 21/62 (2013.01)

G06Q 20/34 (2012.01)

G06F 21/35 (2013.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **11.02.2021** **E 21156457 (0)**

97 Fecha y número de publicación de la concesión europea: **27.11.2024** **EP 3905089**

54 Título: **Sistemas y métodos para el control de acceso a datos utilizando una tarjeta sin contacto**

30 Prioridad:

30.04.2020 US 202016863952

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

05.03.2025

73 Titular/es:

CAPITAL ONE SERVICES, LLC (100.00%)

1680 Capital One Drive

McLean, Virginia 22102, US

72 Inventor/es:

ILINCIC, RAJKO

74 Agente/Representante:

SÁEZ MAESO, Ana

ES 3 001 510 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Sistemas y métodos para el control de acceso a datos utilizando una tarjeta sin contacto

5 Campo de la descripción

La presente descripción se refiere, en general, al control de datos del usuario y, más específicamente, a un sistema y método ejemplar para el control activo del acceso del usuario a los datos a través de la interacción de un transceptor de corto alcance con un dispositivo cliente.

10

Antecedentes

Un usuario típico tiene múltiples cuentas diferentes con una o más entidades. Cuando un usuario crea una cuenta, generalmente proporcionará una cierta cantidad de información personal e identificativa sobre el usuario, así como información para el acceso a la cuenta, como un nombre de usuario y una contraseña. Cada entidad puede tener, por ejemplo, diferentes políticas de retención de datos de usuario, diferentes políticas de uso y diferentes políticas para compartir de datos de usuario. Las políticas de uso de la información del usuario pueden cambiar además sin ninguna notificación al usuario. Además, el poseedor de la información del usuario también puede cambiar a través de una fusión o adquisición de una entidad por otra, muchas veces sin ningún aviso al usuario.

20

El acceso a la cuenta a menudo dependerá de las credenciales de inicio de sesión (por ejemplo, nombre de usuario y contraseña) para confirmar la identidad del titular de la tarjeta. Sin embargo, si las credenciales de inicio de sesión son comprometidas, otra persona podría tener acceso a la cuenta del usuario. Además, cuantas más entidades o individuos con los que un usuario comparta su información personal, mayor será el riesgo de que la información del usuario sea robada debido a una violación en una de las entidades. Además, un usuario puede desear compartir solo ciertas piezas de información personal con una entidad o individuo para propósitos limitados o por un tiempo limitado.

25

Por lo tanto, puede ser beneficioso proporcionar sistemas y métodos ejemplares que permitan a los usuarios controlar el uso de la información del usuario para superar al menos algunas de las deficiencias descritas aquí.

30

El documento US2012331529 A1 describe un método que incluye: recibir una primera solicitud de un primer dispositivo de usuario para acceder a un primer recurso que comprende datos de una segunda cuenta de usuario para la cual el acceso a los datos está restringido a usuarios autorizados, la primera solicitud incluyendo un token de autorización y asociado con un primer identificador de usuario que identifica a un primer usuario; determinar que el primer identificador de usuario no identifica a un usuario autorizado y en respuesta: determinar que el primer identificador de usuario identifica a un usuario autorizado basado en el token de autorización, y proporcionar el primer recurso al primer dispositivo de usuario; recibir una segunda solicitud para acceder a los datos de la segunda cuenta de usuario, la segunda solicitud asociada con el primer identificador de usuario; y basado en que se determina que el primer identificador de usuario identifica a un usuario autorizado, proporcionar acceso a los datos de la segunda cuenta de usuario en respuesta a la segunda solicitud.

35

40

El documento US2020104833 A1 describe sistemas y métodos para la autenticación criptográfica de tarjetas sin contacto.

45

El documento US2015271200 A1 describe técnicas para contener el movimiento lateral de atacantes a través de cuentas provisionadas justo a tiempo (JIT) que comprenden un componente de gestión de cuentas para recibir una solicitud de una primera cuenta a través de un dispositivo cliente para una segunda cuenta para acceder a un dispositivo servidor en un conjunto de dispositivos servidor, un componente de autorización de cuentas para autorizar la solicitud para la segunda cuenta basada al menos parcialmente en la información de cuenta asociada con la primera cuenta, un componente de aprovisionamiento de cuentas para aprovisionar la segunda cuenta para permitir que un cliente acceda al dispositivo servidor, y un componente de notificación de cuentas para proporcionar información de cuenta asociada con la segunda cuenta a un cliente a través del dispositivo cliente.

50

55

Resumen

La invención está definida por las reivindicaciones anexas.

Los aspectos de la tecnología descrita incluyen sistemas y métodos para controlar el acceso a los datos a través de la interacción de una tarjeta sin contacto con un dispositivo cliente. El control de acceso a datos se proporciona en el contexto de la información de la cuenta, incluyendo el manejo de solicitudes para vincular una primera cuenta con una segunda cuenta, a través de la interacción de una tarjeta sin contacto, con un dispositivo cliente de tal manera que la divulgación de cierta información de identificador de cuenta, o información de inicio de sesión de la cuenta, no sea necesario ser divulgada a individuos o entidades que solicitan acceso a los datos de cuenta de otro individuo o entidad.

60

65

Las modalidades de la presente descripción proporcionan un sistema de control de acceso a datos, que comprende: una base de datos que almacena información para una pluralidad de cuentas que comprende, para una primera cuenta asociada con un titular de la primera cuenta, un identificador de la primera cuenta y datos de la primera cuenta, y, para una segunda cuenta asociada con un titular de la segunda cuenta, un identificador de la segunda cuenta; un servidor configurado para comunicarse a través de una red con una pluralidad de dispositivos cliente, incluyendo un primer dispositivo cliente asociado con el titular de la primera cuenta y un segundo dispositivo cliente asociado con el titular de la segunda cuenta; una tarjeta sin contacto que comprende una interfaz de comunicación, un procesador y una memoria, la memoria almacena un applet y un token, en donde la tarjeta sin contacto está asociada con el titular de la primera cuenta; una aplicación cliente que comprende instrucciones para ser ejecutadas en el primer dispositivo cliente y el segundo dispositivo cliente, la aplicación cliente configurada para: cuando se ejecute en el segundo dispositivo cliente: en respuesta a una acción de toque entre la tarjeta sin contacto y el segundo dispositivo cliente: recibir el token de la tarjeta sin contacto, y transmitir al servidor el token y una solicitud de vinculación de cuenta para vincular la primera cuenta con la segunda cuenta; y recibir del servidor un mensaje de confirmación de vinculación de cuenta que incluye instrucciones para el acceso a los datos de la primera cuenta; y, cuando se ejecute en el primer dispositivo cliente: en respuesta a una solicitud de aprobación de vinculación del servidor para aprobar la solicitud de vinculación de cuenta, transmitir al servidor un mensaje de aprobación de vinculación que aprueba la solicitud de vinculación de cuenta; y, un procesador en comunicación de datos con el servidor y la base de datos, el procesador configurado para: recibir del segundo dispositivo cliente el token y la solicitud de vinculación de cuenta; identificar la primera cuenta en base al token; transmitir al primer dispositivo cliente la solicitud de aprobación de vinculación para aprobar la solicitud de vinculación de cuenta; recibir del primer dispositivo cliente el mensaje de aprobación de vinculación que aprueba la solicitud de vinculación de cuenta; y transmitir al segundo dispositivo cliente el mensaje de confirmación de vinculación de cuenta que incluye instrucciones para el acceso a los datos de la primera cuenta.

Las modalidades de la presente descripción proporcionan un método para controlar el acceso a los datos, que comprende: establecer una base de datos que almacene información para una pluralidad de cuentas que comprende, para una primera cuenta asociada con un titular de la primera cuenta, un identificador de la primera cuenta, datos de la primera cuenta y parámetros de control de datos, y, para una segunda cuenta asociada con un titular de la segunda cuenta, un identificador de la segunda cuenta; recibir, por un procesador, de un dispositivo cliente del titular de la segunda cuenta, a través de una red, una solicitud de vinculación de cuenta para vincular la primera cuenta con la segunda cuenta, la solicitud de vinculación de cuenta generada en respuesta a una acción de toque entre una tarjeta sin contacto y el dispositivo cliente del titular de la segunda cuenta, la solicitud de vinculación de cuenta acompañada por un token almacenado en la tarjeta sin contacto, en donde la tarjeta sin contacto está asociada con el titular de la primera cuenta; identificar, por el procesador, la primera cuenta basada en el token; transmitir, por el procesador, a un dispositivo cliente del titular de la primera cuenta, a través de la red, una solicitud de aprobación de vinculación para aprobar la solicitud de vinculación de cuenta; recibir, por el procesador, del dispositivo cliente del titular de la primera cuenta, a través de la red, un mensaje de aprobación de vinculación, el mensaje de aprobación de vinculación generado en respuesta a una indicación del titular de la primera cuenta aprobando la solicitud de vinculación de cuenta; y transmitir, por el procesador, al dispositivo cliente del titular de la segunda cuenta, a través de la red, un mensaje de confirmación de vinculación de cuenta, el mensaje de confirmación de vinculación de cuenta confirmando la aprobación de la solicitud de vinculación de cuenta y proporcionando instrucciones para el acceso a los datos de la primera cuenta.

Se explican a continuación características adicionales del diseño descrito, así como las ventajas que ofrece, en mayor detalle con referencia a modalidades de ejemplo específicas que se describen a continuación e ilustradas en los dibujos acompañantes.

Descripción breve de las figuras

La Figura 1A es un diagrama de un sistema de control de acceso a datos de acuerdo con una o más modalidades de ejemplo.

La Figura 1B es un diagrama que ilustra una secuencia para proporcionar control de acceso a datos de acuerdo con una o más modalidades de ejemplo.

La Figura 2 ilustra componentes de un dispositivo cliente utilizado en un sistema de control de acceso a datos de acuerdo con una o más modalidades de ejemplo.

La Figura 3 ilustra los componentes de un transceptor de corto alcance utilizado en un sistema de control de acceso a datos de acuerdo con una o más modalidades de ejemplo.

La Figura 4 es un diagrama que ilustra la interacción entre un dispositivo cliente y un transceptor de corto alcance utilizado en un sistema de control de acceso a datos de acuerdo con una o más modalidades de ejemplo.

La Figura 5 es un diagrama que ilustra la interacción entre un dispositivo cliente y un transceptor de corto alcance utilizado en un sistema de control de acceso a datos de acuerdo con una o más modalidades de ejemplo.

5 La Figura 6 es un diagrama de flujo que describe un método de control de acceso a datos de acuerdo con una o más modalidades de ejemplo.

La Figura 7 es un diagrama de flujo que describe un método de control de acceso a datos de acuerdo con una o más modalidades de ejemplo.

10 La Figura 8 es un diagrama de flujo que describe un método de control de acceso a datos de acuerdo con una o más modalidades de ejemplo.

Descripción detallada

15 La siguiente descripción de modalidades proporciona ejemplos representativos no limitativos que hacen referencia a números para describir particularmente características y enseñanzas de diferentes aspectos de la invención. Las modalidades descritas deben ser reconocidas como capaces de implementarse por separado, o en combinación, con otras modalidades de la descripción de las modalidades. Una persona con habilidades ordinarias en la técnica que revise la descripción de las modalidades debería ser capaz de aprender y entender los diferentes aspectos descritos de la invención. La descripción de modalidades debería facilitar la comprensión de la invención a tal punto que otras implementaciones, no específicamente cubiertas, pero dentro del conocimiento de una persona experta en la materia que haya leído la descripción de modalidades, se entenderían como consistentes con una aplicación de la invención.

25 Las modalidades ejemplares de los sistemas y métodos que se describen proporcionan el control del acceso a los datos a través de la interacción de un transceptor de corto alcance, como una tarjeta sin contacto, con un dispositivo cliente. El control de acceso a datos puede ser proporcionado en el contexto de controlar el acceso a la información de la cuenta. Las solicitudes para vincular una primera cuenta con una segunda cuenta pueden ser gestionadas mediante la interacción de un transceptor de corto alcance, como una tarjeta sin contacto, con un dispositivo cliente de tal manera que la divulgación de cierta información identificadora de la cuenta, o información de inicio de sesión de la cuenta, no necesite ser revelada a individuos o entidades que solicitan acceso a los datos de la cuenta de otro individuo o entidad. Los beneficios de la tecnología descrita pueden incluir una mejor seguridad de datos para la información de la cuenta, una mejor prevención del fraude y una mejor experiencia del usuario.

La Figura 1A muestra un diagrama que ilustra un sistema de control de acceso a datos 100 de acuerdo con una o más modalidades de ejemplo. Como se discute más adelante, el sistema 100 puede incluir el dispositivo cliente 101, el dispositivo cliente 103, el transceptor de corto alcance 105, el servidor 110, el procesador 120 y la base de datos 130. El dispositivo cliente 101 y el dispositivo cliente 103 pueden comunicarse con el servidor 110 a través de la red 115. Aunque la Figura 1 ilustra ciertos componentes conectados de ciertas maneras, el sistema 100 puede incluir componentes adicionales o múltiples conectados de diversas maneras.

45 El sistema 100 puede incluir uno o más dispositivos cliente, como el dispositivo cliente 101 y/o el dispositivo cliente 103, que pueden ser cada uno un ordenador habilitado para la red. Como se menciona en el presente documento, un ordenador habilitado para red puede incluir, pero no se limita a, un dispositivo informático o un dispositivo de comunicación que incluye, por ejemplo, un servidor, un equipo de red, un ordenador personal, una estación de trabajo, un teléfono, un ordenador portátil, un asistente digital personal, un cliente ligero, un cliente pesado, un navegador de Internet, u otro dispositivo. Cada uno de los dispositivos cliente 101 y 103 también puede 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, tableta o dispositivo móvil portátil similar. Las características adicionales que pueden incluirse en un dispositivo cliente, como el dispositivo cliente 101 y/o el dispositivo cliente 103, se describen a continuación con referencia a la Figura 2.

El sistema 100 puede incluir uno o más transceptores de corto alcance, como el transceptor de corto alcance 105. El transceptor de corto alcance 105 puede estar en comunicación inalámbrica con un dispositivo cliente, como el dispositivo cliente 101 y/o el dispositivo cliente 103, dentro de un campo de comunicaciones de corto alcance, como, por ejemplo, la comunicación de campo cercano (NFC). El transceptor de corto alcance 105 puede incluir, por ejemplo, una tarjeta sin contacto, una tarjeta inteligente, o puede incluir un dispositivo con un factor de forma variable, como un llavero, un colgante u otro dispositivo configurado para comunicarse dentro de un campo de comunicaciones de corto alcance. En otras modalidades, el transceptor de corto alcance 105 puede ser el mismo o similar a los dispositivos del cliente 101, 103. Las características

adicionales que pueden incluirse en un transceptor de corto alcance, como el transceptor de corto alcance 105, se describen a continuación con referencia a la Figura 3.

5 El sistema 100 puede incluir uno o más servidores 110. En algunas modalidades de ejemplo, el servidor 110 puede incluir uno o más procesadores (como, por ejemplo, un microprocesador) que están acoplados a la memoria. El servidor 110 puede estar configurado como un sistema central, servidor o plataforma para controlar y llamar a varios datos en diferentes momentos para ejecutar una pluralidad de acciones de flujo de trabajo. El servidor 110 puede ser un ordenador servidor dedicado, como servidores en cuchilla, o puede ser ordenadores personales, ordenadores portátiles, ordenadores de notebook, ordenadores de mano, 10 ordenadores de red, dispositivos móviles, o cualquier dispositivo controlado por un procesador capaz de soportar el sistema 100.

15 El servidor 110 puede estar configurado para la comunicación de datos (como, por ejemplo, a través de una conexión) con uno o más procesadores, como el procesador 120. En algunas modalidades de ejemplo, el servidor 110 puede incorporar el procesador 120. En algunas modalidades de ejemplo, el servidor 110 puede estar físicamente separado y/o remoto del procesador 120. El procesador 120 puede estar configurado para funcionar como un procesador del lado del servidor. El procesador 120 puede estar configurado para la comunicación de datos (como, por ejemplo, a través de una conexión) con la base de datos 130 y/o el servidor 110. El procesador 120 puede incluir uno o más dispositivos de procesamiento, como un 20 microprocesador, un procesador RISC, un ASIC, etc., junto con la circuitería de procesamiento asociada. El procesador 120 puede incluir, o estar conectado a, una memoria que almacena instrucciones ejecutables y/o datos. El procesador 120 puede comunicarse, enviar o recibir mensajes, solicitudes, notificaciones, datos, etc. a/de otros dispositivos, como los dispositivos clientes 101 y/o 103, a través del servidor 110.

25 El servidor 110 puede estar configurado para la comunicación de datos (como, por ejemplo, a través de una conexión) con una o más bases de datos, como la base de datos 130. La base de datos 130 puede ser una base de datos relacional o no relacional, o una combinación de más de una base de datos. En algunas modalidades de ejemplo, el servidor 110 puede incorporar la base de datos 130. En algunas modalidades de ejemplo, la base de datos 130 puede estar físicamente separada y/o remota del servidor 110, ubicada en otro 30 servidor, en una plataforma basada en la nube, o en cualquier dispositivo de almacenamiento que esté en comunicación de datos con el servidor 110.

35 Las conexiones entre el servidor 110, el procesador 120 y la base de datos 130 pueden realizarse a través de cualquier línea de comunicación, enlace o red, o combinación de los mismos, ya sea por cable y/o inalámbrica, adecuada para comunicarse entre estos componentes. Dicha red puede incluir la red 115 y/o una o más redes del mismo tipo o similar a las descritas aquí en referencia a la red 115. En algunas modalidades de ejemplo, las conexiones entre el servidor 110, el procesador 120 y la base de datos 130 pueden incluir una LAN corporativa.

40 El servidor 110 y/o la base de datos 130 pueden incluir credenciales de inicio de sesión de usuario utilizadas para controlar el acceso a las cuentas de usuario. Las credenciales de inicio de sesión pueden incluir, sin limitación, nombres de usuario, contraseñas, códigos de acceso, preguntas de seguridad, patrones de deslizamiento, reconocimiento de imágenes, escaneos de identificación (por ejemplo, escaneo de licencia de conducir y escaneo de pasaporte), registros de dispositivos, números de teléfono, direcciones de correo 45 electrónico, información de acceso a cuentas de redes sociales e identificación biométrica (por ejemplo, reconocimiento de voz, escaneos de huellas dactilares, escaneos de retina y escaneos faciales).

50 La base de datos 130 puede contener datos relacionados con una o más cuentas. Las cuentas pueden ser mantenidas por (o en nombre de) y/o relacionarse con una o más de una variedad de entidades, tales como, por ejemplo (y sin limitación) un banco, comerciante, minorista en línea, proveedor de servicios, comerciante, fabricante, proveedor de redes sociales, proveedor o promotor de eventos deportivos o de entretenimiento, o cadena hotelera. Por ejemplo, la base de datos 130 puede incluir, sin limitación, información de identificación de la cuenta (por ejemplo, número de cuenta, número de identificación del propietario de la cuenta, nombre del propietario de la cuenta e información de contacto - cualquiera de los cuales puede comprender un 55 identificador de cuenta), características de la cuenta (por ejemplo, tipo de cuenta, limitaciones de financiamiento y negociación, y restricciones sobre el acceso y otras actividades), y puede incluir datos pertinentes a la cuenta, incluyendo información financiera (como información de saldo, historial de pagos e historial de transacciones), información social y/o personal. Los datos almacenados en la base de datos 130 pueden ser almacenados en cualquier formato adecuado, y pueden ser cifrados y almacenados en un 60 formato seguro para prevenir el acceso no autorizado. Cualquier algoritmo/procedimiento adecuado puede ser utilizado para la encriptación de datos y para la desencriptación autorizada.

65 El servidor 110 puede estar configurado para comunicarse con uno o más dispositivos cliente, como el dispositivo cliente 101 y/o el dispositivo cliente 103, a través de una o más redes, como la red 115. La red 115 puede incluir 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 dispositivos cliente 101 y/o 103 al

servidor 110. 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 de Comunicaciones Móviles, un Servicio de Comunicación Personal, una Red de Área Personal, Protocolo de Aplicación Inalámbrica, Servicio de Mensajería Multimedia, Servicio de Mensajería Mejorado, Servicio de Mensajes Cortos, sistemas basados en Multiplexión 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 902.3, 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, operando 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 cuales están acoplados comunicativamente. La red 115 puede traducir de o a otros protocolos a uno o más protocolos de dispositivos de red. Aunque la red 115 se representa como una única red, se debe apreciar que de acuerdo con una o más modalidades de ejemplo, la red 115 puede comprender 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, como las redes de asociaciones de tarjetas de crédito, una LAN y/o redes domésticas.

En algunas modalidades de ejemplo, el servidor 110 puede acceder a registros, incluidos los registros en la base de datos 130, para determinar un método o métodos para comunicarse con el dispositivo cliente 101 y/o el dispositivo cliente 103. El método de comunicación puede incluir una notificación push accionable con una aplicación almacenada en el dispositivo cliente 101 y/o el dispositivo cliente 103. Otros métodos de comunicación pueden incluir un mensaje de texto o un correo electrónico, u otras técnicas de mensajería apropiadas en una configuración de cliente/servidor basado en red. Los mensajes o solicitudes de los dispositivos cliente 101 y/o 103 pueden ser comunicados al servidor 110 a través de una aplicación en el dispositivo cliente, o pueden ser enviados por un mensaje de texto o un correo electrónico, o por otras técnicas de mensajería apropiadas en una configuración de cliente/servidor basado en red. Las comunicaciones que se originan con el dispositivo cliente 101 o el dispositivo cliente 103 pueden enviarse al servidor 110 utilizando el mismo método de comunicación que las comunicaciones que se originan con el servidor 110, o a través de un método de comunicación diferente.

La Figura 1B muestra un diagrama que ilustra una secuencia para proporcionar control de acceso a datos de acuerdo con una o más modalidades de ejemplo, que pueden incluir una solicitud para vincular dos cuentas, cada una de las cuales es mantenida por titulares de cuentas separados. La Figura 1B hace referencia a componentes similares del sistema de modalidad de ejemplo 100, como se ilustra en la Figura 1A. El dispositivo cliente 101 puede estar asociado con un titular de la primera cuenta. El titular de la primera cuenta puede tener una primera cuenta asociada, que puede incluir un identificador de la primera cuenta y datos de la primera cuenta. El dispositivo cliente 101 puede incluir la aplicación 102, que puede incluir instrucciones para la ejecución por el dispositivo cliente 101. El dispositivo cliente 101 puede incluir características que se describen a continuación con referencia a la Figura 2. La solicitud 102 puede estar configurada para proporcionar una interfaz de usuario para el titular de la primera cuenta al usar el dispositivo cliente 101. La aplicación 102 puede estar configurada para comunicarse, a través del dispositivo cliente 101, con otros dispositivos cliente, con el transceptor de corto alcance 105 y con el servidor 110. La aplicación 102 puede estar configurada para recibir solicitudes y enviar mensajes como se describe aquí en referencia al dispositivo cliente 101. La información de la cuenta, incluyendo identificadores de cuenta y datos de cuenta, puede ser almacenada en la base de datos 130.

El dispositivo cliente 103 puede estar asociado con un titular de la segunda cuenta. El titular de la segunda cuenta puede tener una segunda cuenta asociada, que puede incluir un identificador de la segunda cuenta. El dispositivo cliente 103 puede incluir la aplicación 104, que puede incluir instrucciones para la ejecución por el dispositivo cliente 103. El dispositivo cliente 103 puede incluir características que se describen a continuación con referencia a la Figura 2. La aplicación 104 puede estar configurada para proporcionar una interfaz de usuario para el titular de la segunda cuenta al utilizar el dispositivo cliente 103. La aplicación 104 puede estar configurada para comunicarse, a través del dispositivo cliente 103, con otros dispositivos cliente, con el transceptor de corto alcance 105 y con el servidor 110. La aplicación 104 puede estar configurada para enviar solicitudes y recibir mensajes como se describe aquí en relación con el dispositivo cliente 103.

El transceptor de corto alcance 105 puede estar asociado con el titular de la primera cuenta. El transceptor de corto alcance 105 puede incluir, por ejemplo, una tarjeta sin contacto, y puede incluir características que se describen a continuación con referencia a la Figura 3. El transceptor de corto alcance 105 puede tener memoria que almacena un applet 106 y/o un token 107, siendo el token 107 asociado con el titular de la primera cuenta.

Un token puede ser utilizado para aumentar la seguridad a través de la autorización del token. El servidor 110 puede enviar una solicitud de validación al dispositivo cliente 101 y/o 103, recibir información de respuesta del dispositivo cliente 101 y/o 103, y si es validado, enviar un token de validación de vuelta al dispositivo cliente 101 y/o 103. El token de validación puede basarse en un token preestablecido, o puede ser un token dinámico basado en un algoritmo que puede ser secreto y conocido solo por el servidor 110 y el dispositivo cliente 101 y/o 103; el algoritmo puede incluir parámetros en vivo verificables de forma independiente por los participantes, como la temperatura en una ubicación particular o el tiempo. El token puede ser utilizado para verificar la identidad del titular de la primera cuenta o del titular de la segunda cuenta. La solicitud de validación y/o el token de validación pueden basarse en el token 107 almacenado en el transceptor de corto alcance 105.

En algunas modalidades de ejemplo, la aplicación 104 puede mostrar una instrucción en el dispositivo cliente 103 que solicite al titular de la segunda cuenta que inicie una acción de toque entre el transceptor de corto alcance 105 y el dispositivo cliente 103. Como se utiliza en este documento, una acción de toque puede incluir tocar el transceptor de corto alcance 105 contra el dispositivo cliente 103 (o viceversa). Por ejemplo, si el transceptor de corto alcance 105 es una tarjeta sin contacto y el dispositivo cliente 103 es un dispositivo móvil, la acción de toque puede incluir tocar la tarjeta sin contacto en una pantalla u otra parte del dispositivo cliente 103. Sin embargo, una acción de toque no se limita a un toque físico por parte del transceptor de corto alcance 105 contra el dispositivo cliente 103, y puede incluir otros gestos, como, por ejemplo, un movimiento de mano u otro movimiento del transceptor de corto alcance 105 en las cercanías del dispositivo cliente 103 (o viceversa).

En la etiqueta 150, puede haber una acción de toque entre el transceptor de corto alcance 105 y el dispositivo cliente 103. La acción de toque puede ser en respuesta a un aviso mostrado en el dispositivo cliente 103.

En la etiqueta 152, la aplicación 104 puede comunicarse (a través del dispositivo cliente 103) con el transceptor de corto alcance 105 (por ejemplo, después de que el transceptor de corto alcance 105 se acerque al dispositivo cliente 103). La comunicación entre la aplicación 104 y el transceptor de corto alcance 105 puede implicar que el transceptor de corto alcance 105 (como, por ejemplo, una tarjeta sin contacto) esté lo suficientemente cerca de un lector de tarjetas (no mostrado) del dispositivo cliente 103 para permitir la transferencia de datos NFC entre la aplicación 104 y el transceptor de corto alcance 105, y puede ocurrir en conjunto con (o en respuesta a) una acción de toque entre el transceptor de corto alcance 105 y el dispositivo cliente 103 (como, por ejemplo, la acción de toque en la etiqueta 150). La comunicación puede incluir el intercambio de datos o comandos para establecer una sesión de comunicación entre la aplicación 104 y el transceptor de corto alcance 105. El intercambio de datos puede incluir la transferencia o el intercambio de una o más claves, que pueden ser claves preexistentes o generadas como claves de sesión. En algunas modalidades de ejemplo, la comunicación puede ocurrir al entrar el transceptor de corto alcance 105 en un campo de comunicación de corto alcance del dispositivo cliente 103 antes de una acción de toque entre el transceptor de corto alcance 105 y el dispositivo cliente 103.

En la etiqueta 154, el transceptor de corto alcance 105 puede enviar el token 107 asociado con el titular de la primera cuenta a la aplicación 104. El Token 107 puede incluir el identificador de la primera cuenta, que puede ser único para una cuenta de usuario específica. En una modalidad de ejemplo, el token 107 puede incluir un identificador único para el titular de la primera cuenta, pero no para una cuenta específica; en cuyo caso, si el titular de la primera cuenta tiene más de una cuenta, el titular de la segunda cuenta necesitaría seleccionar la cuenta que se va a vincular. En algunas modalidades de ejemplo, el token 107 puede incluir una clave asociada con el titular de la primera cuenta. En algunas modalidades de ejemplo, el envío del token 107 a la aplicación 104 puede ser en conjunto con (o en respuesta a) una acción de toque entre el transceptor de corto alcance 105 y el dispositivo cliente 103 (como, por ejemplo, la acción de toque en la etiqueta 150). En algunas modalidades de ejemplo, el envío del token 107 a la aplicación 104 puede ocurrir al entrar el transceptor de corto alcance 105 en un campo de comunicación de corto alcance del dispositivo cliente 103 antes de una acción de toque entre el transceptor de corto alcance 105 y el dispositivo cliente 103.

En la etiqueta 156, la aplicación 104 puede enviar el token 107 al servidor 110, junto con una solicitud de vinculación de cuenta para vincular la primera cuenta (asociada con el titular de la primera cuenta) con la segunda cuenta (asociada con el titular de la segunda cuenta). Esto puede llevarse a cabo en respuesta a una acción de toque entre el transceptor de corto alcance 105 y el dispositivo cliente 103 (como, por ejemplo, la acción de toque en la etiqueta 150).

En la etiqueta 158, el procesador 120 puede recibir (por ejemplo, a través del servidor 110) el token y la solicitud de vinculación de cuenta. El procesador 120 puede utilizar el token para identificar la primera cuenta asociada con el titular de la primera cuenta. En algunas modalidades de ejemplo, la identificación de la primera cuenta puede llevarse a cabo utilizando el identificador de la primera cuenta en el token para buscar información de la cuenta en la base de datos 130. En algunas modalidades de ejemplo, en la etiqueta 159, si el token incluye la clave asociada con el titular de la primera cuenta, el procesador 120 puede utilizar la clave

en el token para autenticar al titular de la primera cuenta como el titular de la primera cuenta asociado con el transceptor de corto alcance 105.

En la etiqueta 160, el procesador 120 puede enviar (por ejemplo, a través del servidor 110) una solicitud de aprobación de vinculación al dispositivo cliente 101, solicitando que el titular de la primera cuenta apruebe la solicitud de vinculación de cuenta, realizada por el titular de la segunda cuenta, para vincular la primera cuenta con la segunda cuenta. La solicitud de aprobación de vinculación puede incluir, por ejemplo, el nombre del titular de la segunda cuenta y cualquier información o instrucciones requeridas por el titular de la primera cuenta para considerar la solicitud. La solicitud de aprobación de vinculación puede incluir un aviso de que el titular de la primera cuenta puede aprobar o denegar la solicitud. La solicitud de aprobación de vinculación puede ser enviada como una notificación push a la aplicación 102 (a través del dispositivo cliente 101). En algunas modalidades de ejemplo, la aplicación 102 puede mostrar una instrucción en el dispositivo cliente 101 que solicita al titular de la primera cuenta iniciar una acción de toque entre el transceptor de corto alcance 105 y el dispositivo cliente 101.

En la etiqueta 162, puede haber una acción de toque entre el transceptor de corto alcance 105 y el dispositivo cliente 101. La acción de toque puede ser sensible a la solicitud de aprobación de vinculación (y/o a un mensaje mostrado en el dispositivo cliente 101), y puede indicar la aprobación por parte del titular de la primera cuenta de la solicitud de vinculación de cuenta.

En la etiqueta 164, la aplicación 102 puede enviar un mensaje de aprobación de vinculación al servidor, indicando la aprobación por parte del titular de la primera cuenta de la solicitud de vinculación de cuenta. Esto puede llevarse a cabo en respuesta a una acción de toque entre el transceptor de corto alcance 105 y el dispositivo cliente 101 (como, por ejemplo, la acción de toque en la etiqueta 162). En una modalidad de ejemplo, la aplicación 102 puede en su lugar enviar un mensaje de denegación (no mostrado) al servidor, indicando la denegación por parte del titular de la primera cuenta de la solicitud de vinculación de cuenta.

En la etiqueta 166, el procesador 120 puede enviar (por ejemplo, a través del servidor 110) un mensaje de confirmación de vinculación al dispositivo cliente 103, confirmando la aprobación de la solicitud para vincular la primera cuenta con la segunda cuenta. El mensaje de confirmación de vinculación puede enviarse como una notificación push a la aplicación 104 (a través del dispositivo cliente 103). En algunas modalidades de ejemplo, la información de la primera cuenta y/o la segunda cuenta en la base de datos 130 puede ser actualizada con el permiso otorgado por el titular de la primera cuenta para vincular la primera y la segunda cuentas.

En una modalidad de ejemplo, el procesador 120 puede en su lugar enviar una notificación de denegación (no mostrada) al dispositivo cliente 103, indicando la denegación por parte del titular de la primera cuenta de la solicitud de vinculación de cuenta.

En la etiqueta 168, el procesador 120 puede enviar (por ejemplo, a través del servidor 110) al dispositivo cliente 103 instrucciones para obtener acceso a los datos de la primera cuenta en la primera cuenta. Las instrucciones para acceder a los datos de la primera cuenta pueden incluirse con el mensaje de confirmación de vinculación (en la etiqueta 166), o pueden enviarse como parte de una comunicación separada, incluyendo una notificación push a la aplicación 104.

El procesador 120 puede recuperar los datos de la primera cuenta solicitada de la base de datos 130 y transmitir los datos al dispositivo cliente 103. El procesador 120 puede cifrar los datos de la primera cuenta solicitados, antes de la transmisión al dispositivo cliente 103, utilizando cualquier método de cifrado adecuado, como Triple DES, cifrado de clave pública-privada RSA, cifrado asimétrico, cifrado Blowfish, cifrado Twofish, Estándar de Cifrado Avanzado (AES), distribución de claves cuánticas, Cifrado Honey, etc. En algunas modalidades, los datos de la primera cuenta solicitada pueden estar ya cifrados tal como se almacenan en la base de datos 130 antes de ser recuperados por el procesador 120.

Al recibir los datos de la primera cuenta solicitados, el dispositivo cliente 103 puede descifrar la información, si la información fue cifrada antes de la transmisión por el procesador 120. El dispositivo cliente 103 puede recibir una clave de descifrado separada de la primera comunicación de datos de la primera cuenta cifrados. La encriptación puede permitir el control de acceso a datos de la primera cuenta de acuerdo con los parámetros de control de datos. Por ejemplo, los datos de la primera cuenta pueden estar cifrados de tal manera que se requiera que el dispositivo cliente 103 solicite una nueva clave al procesador 120 cada vez que el dispositivo cliente 103 desee acceder a los datos de la primera cuenta, de modo que los datos tendrían que ser descifrados para cada acceso por parte del dispositivo cliente 103; este procedimiento permitiría que el procesador 120 mantenga un registro y garantice que los datos de la primera cuenta no sean accedidos de manera inconsistente con los parámetros de control de datos.

En una modalidad de ejemplo, el titular de la segunda cuenta puede iniciar sesión en la segunda cuenta y, a través de la compartición de datos en el lado del servidor, obtener acceso a los datos de la primera cuenta, de acuerdo con los parámetros de control de datos.

La aplicación 104 que se ejecuta en el dispositivo cliente 103 puede, mediante el uso de interfaces de programación de aplicaciones (API), realizar los pasos de enviar y recibir mensajes y solicitudes con el servidor 110/procesador 120. La aplicación 104 puede estar configurada para recibir, descifrar y acceder a los datos de la primera cuenta solicitada. A través de la interacción con la aplicación 104, el procesador 120 puede monitorear el acceso a los datos de la primera cuenta solicitados por el dispositivo cliente 103, incluyendo de acuerdo con los parámetros de control de datos. Por ejemplo, el procesador 120 puede, a través de la interacción con la aplicación 104, determinar el número de veces que el dispositivo cliente 103 ha obtenido acceso a los datos de la primera cuenta solicitada, o el(los) período(s) de tiempo en que ocurrió dicho acceso. En algunas modalidades, la aplicación 104 puede tener permitido almacenar los datos de la primera cuenta solicitados en una base de tiempo limitado, o en un número limitado de usos.

En una modalidad de ejemplo, el procesador 120 puede estar configurado para determinar si la primera cuenta es elegible para ser vinculada con la segunda cuenta. La elegibilidad para la vinculación de cuentas puede basarse, por ejemplo, en el tipo de cuentas involucradas (por ejemplo, cuentas de negocios), o en la identidad de los titulares de las cuentas (por ejemplo, miembros de la familia o miembros de la misma entidad empresarial). La elegibilidad también puede basarse en si el titular de la primera cuenta ha aprobado o revocado previamente la aprobación de la vinculación de cuentas, o si el acceso solicitado violaría los parámetros de control de datos (discutido más adelante). La elegibilidad para la vinculación de cuentas puede, por ejemplo, indicarse en una bandera almacenada en la base de datos 130 o en la memoria del transceptor de corto alcance 105.

En una o más modalidades de ejemplo, el acceso del titular de la segunda cuenta a los datos de la primera cuenta puede estar limitado de acuerdo con los parámetros de control de datos. En una modalidad de ejemplo, los parámetros de control de datos pueden ser almacenados en la base de datos 130 junto con la información de la primera cuenta. La aplicación 102 puede proporcionar una interfaz para que el titular de la primera cuenta seleccione los parámetros de control de datos almacenados en la base de datos 130. Los parámetros de control de datos seleccionados pueden ser almacenados en la base de datos 130 y pueden ser aplicados para limitar el acceso del titular de la segunda cuenta a los datos de la primera cuenta. La aplicación 102 también puede transmitir los parámetros de control de datos seleccionados al transceptor de corto alcance 105. En una modalidad de ejemplo, los parámetros de control de datos pueden ser almacenados en la memoria del transceptor de corto alcance 105. Los parámetros de control de datos almacenados en la memoria del transceptor de corto alcance 105 pueden ser enviados a la aplicación 104 y utilizados por la aplicación 104 para limitar el acceso del titular de la segunda cuenta a los datos de la primera cuenta. El applet 106 puede estar configurada para recibir los parámetros de control de datos y almacenar los parámetros de control de datos en la memoria del transceptor de corto alcance 105. El applet 106 puede estar configurado además para transmitir los parámetros de control de datos al dispositivo cliente 103. En algunas modalidades de ejemplo, el titular de la primera cuenta puede seleccionar parámetros de control de datos en el momento de aprobar la solicitud para vincular cuentas, y la aplicación 102 puede transmitir los parámetros de control de datos seleccionados al servidor 110 junto con el mensaje de aprobación de vinculación. Los parámetros de control de datos seleccionados pueden ser almacenados en la base de datos 130 y pueden ser aplicados para limitar el acceso del titular de la segunda cuenta a los datos de la primera cuenta.

En una o más modalidades de ejemplo, los parámetros de control de datos pueden ser utilizados para limitar el acceso del titular de la segunda cuenta a los datos de la primera cuenta de una o más maneras. Por ejemplo, los parámetros de control de datos pueden permitir el acceso solo por un período de tiempo específico o limitado. Como otro ejemplo, los parámetros de control de datos pueden permitir el acceso a un único uso por parte del titular de la segunda cuenta. Como otro ejemplo, los parámetros de control de datos pueden permitir el acceso por un período de tiempo ilimitado, a menos que el titular de la primera cuenta revoque la aprobación de la solicitud para vincular la primera cuenta con la segunda cuenta. Como otro ejemplo, los parámetros de control de datos pueden permitir el acceso solo a porciones de los datos de la primera cuenta que correspondan a una categoría predefinida. Como otro ejemplo, los parámetros de control de datos pueden proporcionar diferentes permisos de acceso basados en la identidad del titular de la segunda cuenta. Como otro ejemplo, los parámetros de control de datos pueden permitir el acceso solo cuando se detecta el transceptor de corto alcance 105 dentro del rango de un campo de comunicación de corto alcance del dispositivo cliente 103. En algunas modalidades de ejemplo, cada vez que el titular de la segunda cuenta intenta acceder a los datos de la primera cuenta después de obtener la aprobación para la vinculación de cuentas, el procesador 120 puede verificar si dicho acceso está permitido en función de los parámetros de control de datos y cualquier revocación por parte del titular de la primera cuenta.

En una modalidad de ejemplo, la aplicación 104 puede ser lanzada en respuesta a una acción de toque entre el transceptor de corto alcance 105 y el dispositivo cliente 103. En una modalidad de ejemplo, la aplicación

102 puede ser lanzada en respuesta a una acción de toque entre el transceptor de corto alcance 105 y el dispositivo cliente 101.

La Figura 2 ilustra los componentes de un dispositivo cliente 200 utilizado en un sistema de control de acceso a datos de acuerdo con una o más modalidades de ejemplo. En una o más modalidades de ejemplo, el dispositivo cliente 200 puede ser uno o más de los dispositivos clientes 101 y/o 103, descritos anteriormente con referencia a la Figura 1A y la Figura 1B. El dispositivo cliente 200 puede incluir una o más aplicaciones 201, uno o más procesadores 202, una interfaz de comunicaciones de corto alcance 203 y una interfaz de red 204. La aplicación 201 puede incluir una aplicación de software o código de programa ejecutable que se ejecute en el procesador 202 y configurado para llevar a cabo las características descritas aquí para cualquiera de los dispositivos cliente, como los dispositivos cliente 101 y/o 103, y/o cualquiera de las características descritas aquí en relación con la aplicación 102. La aplicación 201 puede estar configurada, por ejemplo, para transmitir y/o recibir datos con otros dispositivos a través del dispositivo cliente 200, como a través de la interfaz de comunicaciones de corto alcance 203 y/o la interfaz de red 204. Por ejemplo, la aplicación 201 puede estar configurada para iniciar una o más solicitudes, como solicitudes de intercambio de datos de campo cercano a un transceptor de corto alcance (como una tarjeta sin contacto). La aplicación 201 también puede estar configurada para proporcionar una interfaz de usuario a través de una pantalla (no mostrada) para un usuario del dispositivo cliente. La aplicación 201 puede ser almacenada en la memoria del dispositivo cliente 200; la memoria puede incluir una memoria de solo lectura, memoria de escritura única y lectura múltiple y/o memoria de lectura/escritura, por ejemplo, RAM, ROM y EEPROM.

El procesador 202 puede incluir uno o más dispositivos de procesamiento, como un microprocesador, un procesador RISC, un ASIC, etc., y puede incluir circuitería de procesamiento asociada. El procesador 202 puede incluir, o estar conectado a, memoria que almacena instrucciones ejecutables y/o datos, según sea necesario o apropiado para controlar, operar o relacionarse con las otras características del dispositivo cliente 200, incluyendo la aplicación 201. El procesador 202 (incluyendo cualquier circuito de procesamiento asociado) puede contener componentes adicionales incluyendo procesadores, memorias, verificadores de error y paridad/CRC, codificadores de datos, algoritmos de anticorrupción, controladores, decodificadores de comandos, primitivas de seguridad y hardware a prueba de manipulaciones, según sea necesario para realizar las funciones descritas aquí.

La interfaz de comunicaciones de corto alcance 203 puede soportar la comunicación a través de un campo de comunicación inalámbrica de corto alcance, como NFC, RFID o Bluetooth. La interfaz de comunicaciones de corto alcance 203 puede incluir un lector, como un lector NFC de dispositivo móvil. La interfaz de comunicaciones de corto alcance 203 puede estar incorporada en la interfaz de red 204, o puede ser proporcionada como una interfaz separada.

La interfaz de red 204 puede incluir capacidad de comunicación de datos por cable o inalámbrica. Estas capacidades pueden apoyar la comunicación de datos con una red de comunicación cableada o inalámbrica, incluyendo Internet, una red celular, una red de área amplia, una red de área local, una red personal inalámbrica, una red de área corporal amplia, cualquier otra red cableada o inalámbrica para transmitir y recibir una señal de datos, o cualquier combinación de las mismas. Dicha red puede incluir, sin limitación, líneas telefónicas, fibra óptica, IEEE Ethernet 902.3, una red de área amplia, una red de área local, una red personal inalámbrica, una red de área corporal amplia o una red global como Internet.

El dispositivo cliente 200 también puede incluir una pantalla (no mostrada). Dicha pantalla puede ser cualquier tipo de dispositivo para presentar información visual, como un monitor de computadora, una pantalla de panel plano o una pantalla de dispositivo móvil, incluyendo pantallas de cristal líquido, pantallas de diodos emisores de luz, paneles de plasma y pantallas de tubo de rayos catódicos.

El dispositivo cliente 200 también puede incluir una o más entradas del dispositivo (no mostradas). Tales entradas pueden incluir cualquier dispositivo para ingresar información en el dispositivo cliente que esté disponible y sea compatible con el dispositivo cliente 300, como una pantalla táctil, teclado, ratón, dispositivo de control de cursor, pantalla táctil, micrófono, cámara digital, grabadora de video o videocámara. Las entradas del dispositivo pueden ser utilizadas para ingresar información e interactuar con el dispositivo cliente 200 y, por extensión, con los sistemas descritos aquí.

La Figura 3 ilustra los componentes de un transceptor de corto alcance 300 utilizado en un sistema de control de acceso a datos de acuerdo con una o más modalidades de ejemplo. En una o más modalidades de ejemplo, el transceptor de corto alcance 300 puede ser uno o más de los transceptores de corto alcance 105, que se describen arriba con referencia a la Figura 1A y la Figura 1B. El transceptor de corto alcance 300 puede incluir, por ejemplo, una tarjeta sin contacto, o puede incluir un dispositivo con un factor de forma variable, como un llavero, un colgante u otro dispositivo configurado para comunicarse dentro de un campo de comunicaciones de corto alcance. El transceptor de corto alcance 300 puede incluir un procesador 301, memoria 302 y una interfaz de comunicaciones de corto alcance 305.

El procesador 301 puede incluir uno o más dispositivos de procesamiento, como un microprocesador, un procesador RISC, un ASIC, etc., y puede incluir circuitería de procesamiento asociada. El procesador 301 puede incluir, o estar conectado a, memoria que almacena instrucciones ejecutables y/o datos, según sea necesario o apropiado para controlar, operar o interactuar con las otras características del transceptor de corto alcance 300, incluyendo el applet 303. El procesador 301 (incluyendo cualquier circuito de procesamiento asociado) puede contener componentes adicionales incluyendo procesadores, memorias, verificadores de error y paridad/CRC, codificadores de datos, algoritmos de anticorrupción, controladores, decodificadores de comandos, primitivas de seguridad y hardware a prueba de manipulaciones, según sea necesario para realizar las funciones descritas aquí.

La memoria 302 puede ser una memoria de solo lectura, una memoria de escritura única y lectura múltiple o una memoria de lectura/escritura, por ejemplo, RAM, ROM y EEPROM. La memoria 302 puede estar configurada para almacenar uno o más applets 303 y uno o más tokens 304. El applet 303 puede comprender una o más aplicaciones de software configuradas para ejecutarse en el procesador 301, como un applet de Java Card que puede ser ejecutable en una tarjeta sin contacto. Sin embargo, se entiende que el applet 303 no está limitado a applets de Java Card, y en su lugar puede ser cualquier aplicación de software operable en tarjetas sin contacto u otros dispositivos que tengan memoria limitada. El applet 303 puede estar configurado para responder a una o más solicitudes, como solicitudes de intercambio de datos de campo cercano de un dispositivo cliente, incluyendo solicitudes de un dispositivo que tenga un lector, como un lector NFC de un dispositivo móvil. El applet 303 puede estar configurado para leer (o escribir) datos, incluyendo el token 304, de (o en) la memoria 302 y proporcionar los datos, incluyendo el token 304, en respuesta a una solicitud.

El token 304 puede incluir un identificador alfanumérico único asignado a un usuario del transceptor de corto alcance 300, y el identificador puede distinguir al usuario del transceptor de corto alcance 300 de otros usuarios de otros transceptores de corto alcance (como otros usuarios de tarjetas sin contacto). En algunas modalidades de ejemplo, el token 304 puede identificar tanto a un cliente como a una cuenta asignada a ese cliente y puede además identificar el transceptor de corto alcance (como una tarjeta sin contacto) asociado con la cuenta del cliente. En algunas modalidades de ejemplo, el token 304 puede incluir una clave única para el usuario o cliente con el que se asocia el transceptor de corto alcance.

La interfaz de comunicaciones de corto alcance 305 puede soportar la comunicación a través de un campo de comunicación inalámbrica de corto alcance, como NFC, RFID o Bluetooth. El transceptor de corto alcance 300 también puede incluir una o más antenas (no mostradas) conectadas a la interfaz de comunicaciones de corto alcance 305 para proporcionar conectividad con un campo de comunicaciones inalámbricas de corto alcance.

La Figura 4 es un diagrama que ilustra la interacción 400 entre un dispositivo cliente 401 y un transceptor de corto alcance 420 utilizado en un sistema de control de acceso a datos de acuerdo con una o más modalidades de ejemplo, incluyendo modalidades descritas anteriormente con referencia a las Figuras 1A-1B. El dispositivo cliente 401 puede ser el dispositivo cliente 103 descrito anteriormente con referencia a la Figura 1A y Figura 1B. El dispositivo cliente 401 puede estar asociado con el titular de la segunda cuenta. La interfaz de usuario 402 puede ser generada por la aplicación 104 descrita anteriormente con referencia a la Figura 1B. El transceptor de corto alcance 420 puede ser el transceptor de corto alcance 105 descrito anteriormente con referencia a la Figura 1A y Figura 1B. Al entrar el transceptor de corto alcance 420 en un campo de comunicación de corto alcance del dispositivo cliente 401 (como, por ejemplo, a través de una acción de toque), el dispositivo cliente 401 puede comunicarse con el transceptor de corto alcance 420. El dispositivo cliente 401 puede enviar datos o comandos al transceptor de corto alcance 420 a través de la señal de transmisión 431, y puede recibir datos del transceptor de corto alcance 420, incluyendo el token 422, a través de la señal de recepción 432. La comunicación entre el dispositivo cliente 401 y el transceptor de corto alcance 420 puede proceder como se describe anteriormente con referencia a la Figura 1B (por ejemplo, el dispositivo cliente 101 o 103 y el transceptor de corto alcance 105).

La interfaz de usuario 402 puede presentar en el dispositivo cliente 401 una pantalla de visualización para una solicitud de vinculación de cuenta 410, que puede incluir el campo 411 y el campo 412. Si es necesario, el titular de la segunda cuenta puede ingresar un nombre de usuario en el campo 411 y una contraseña en el campo 412. La pantalla puede incluir una instrucción 414 que solicita al titular de la segunda cuenta que toque el transceptor de corto alcance 420 (en el ejemplo mostrado, el transceptor de corto alcance 420 puede ser una tarjeta sin contacto) para iniciar una solicitud de vinculación de cuenta que vincule la primera cuenta con la segunda cuenta. La Instrucción 414 puede ser una notificación push del servidor 110 (mostrado en las Figuras 1A y 1B). El dispositivo cliente 401 puede transmitir una solicitud de vinculación de cuenta al servidor 110 (mostrado en la Figura 1A y la Figura 1B) en respuesta a una acción de toque.

La Figura 5 es un diagrama que ilustra la interacción 500 entre un dispositivo cliente 501 y un transceptor de corto alcance 520 utilizado en un sistema de control de acceso a datos de acuerdo con una o más modalidades de ejemplo, incluyendo modalidades descritas anteriormente con referencia a las Figuras 1A-1B. El dispositivo cliente 501 puede ser el dispositivo cliente 101 descrito anteriormente con referencia a la Figura

1A y Figura 1B. El dispositivo cliente 501 puede estar asociado con el titular de la primera cuenta. La interfaz de usuario 502 puede ser generada por la aplicación 102 descrita anteriormente con referencia a la Figura 1B. El transceptor de corto alcance 520 puede ser el transceptor de corto alcance 105 descrito anteriormente con referencia a la Figura 1A y Figura 1B. Al entrar el transceptor de corto alcance 520 en un campo de comunicación de corto alcance del dispositivo cliente 501 (como, por ejemplo, a través de una acción de toque), el dispositivo cliente 501 puede comunicarse con el transceptor de corto alcance 520. El dispositivo cliente 501 puede enviar datos o comandos al transceptor de corto alcance 520 a través de la señal de transmisión 531, y puede recibir datos del transceptor de corto alcance 520, incluyendo el token 522, a través de la señal de recepción 532. La comunicación entre el dispositivo cliente 501 y el transceptor de corto alcance 520 puede proceder como se describe anteriormente con referencia a la Figura 1B (por ejemplo, el dispositivo cliente 101 o 103 y el transceptor de corto alcance 105).

La interfaz de usuario 502 puede presentar en el dispositivo cliente 501 una pantalla de visualización para una solicitud de vinculación de cuenta 510, que puede incluir el campo 511 y el campo 512. Si es necesario, el titular de la primera cuenta puede ingresar un nombre de usuario en el campo 511 y una contraseña en el campo 512. La pantalla puede incluir una instrucción 514 notificando al titular de la primera cuenta que el titular de la segunda cuenta (nombrado 2_Acc_Hldr como se muestra en el ejemplo) ha solicitado vincular la primera cuenta con la segunda cuenta, y solicitando al titular de la primera cuenta que toque el transceptor de corto alcance 520 (en el ejemplo mostrado, el transceptor de corto alcance 520 puede ser una tarjeta sin contacto) para aprobar la solicitud de vinculación de cuentas para vincular la primera cuenta con la segunda cuenta. La Instrucción 514 puede resultar de una notificación push del servidor 110 (mostrado en la Figura 1A y la Figura 1B). El dispositivo cliente 501 puede transmitir un mensaje de aprobación de vinculación de cuenta al servidor 110 en respuesta a una acción de toque. En algunas modalidades de ejemplo, la interfaz de usuario 502 puede proporcionar al titular de la primera cuenta la opción de seleccionar parámetros de control de datos en el momento de aprobar la solicitud para vincular cuentas. El dispositivo cliente 501 puede transmitir los parámetros de control de datos seleccionados al servidor 110 junto con el mensaje de aprobación de vinculación; los parámetros de control de datos seleccionados pueden ser almacenados y pueden ser aplicados para limitar el acceso del titular de la segunda cuenta a los datos de la primera cuenta, como se discutió anteriormente.

La Figura 6 es un diagrama de flujo que ilustra un método de control de acceso a datos 600 de acuerdo con una o más modalidades de ejemplo, con referencia a los componentes y características descritos anteriormente, incluyendo, pero no limitado a las figuras y la descripción asociada. El método de control de acceso a datos 600 puede ser llevado a cabo por la aplicación 104 que se ejecuta en el dispositivo cliente 103 asociado con el titular de la segunda cuenta. El transceptor de corto alcance 105 está asociado con el titular de la primera cuenta.

En el bloque 610, la aplicación 104 puede hacer que el dispositivo cliente 103 muestre una pantalla de solicitud de vinculación de cuenta (como se muestra y se describe arriba con referencia a la Figura 4). La pantalla de solicitud de vinculación de cuenta puede incluir una instrucción para tocar el transceptor de corto alcance 105 con/contra el dispositivo cliente 103 para iniciar la solicitud de vinculación de cuenta. Como se describe anteriormente con referencia a la Figura 4, el transceptor de corto alcance 420 (y, por lo tanto, el transceptor de corto alcance 105) puede ser una tarjeta sin contacto.

En el bloque 620, se puede detectar una acción de toque entre el transceptor de corto alcance 105 y el dispositivo cliente 103.

En el bloque 630, se puede recibir el token 107 del transceptor de corto alcance 105. La recepción del token 107 puede ser en respuesta a la acción de toque del bloque 620. El token 107 puede incluir el identificador de la primera cuenta. En algunas modalidades de ejemplo, el token 107 puede incluir una clave asociada con el titular de la primera cuenta.

En el bloque 640, el token 107 puede ser transmitido al servidor 110 junto con una solicitud de vinculación de cuenta para vincular la primera cuenta con la segunda cuenta. La transmisión del token 107 y la solicitud de vinculación de cuenta al servidor 110 puede ser en respuesta a la acción de toque del bloque 620.

En el bloque 650, se puede recibir un mensaje de confirmación de vinculación de cuenta del servidor 110 junto con instrucciones para acceder a los datos de la primera cuenta. Como se discutió anteriormente, las instrucciones pueden ser parte del mensaje de confirmación de vinculación de cuenta, o parte de un mensaje separado.

En el bloque 660, el titular de la segunda cuenta puede acceder a los datos de la primera cuenta de acuerdo con las instrucciones recibidas. Como se discutió anteriormente, en algunas modalidades de ejemplo, el acceso a los datos de la primera cuenta puede ser proporcionado únicamente de acuerdo con los parámetros de control de datos. En algunas modalidades de ejemplo, los parámetros de control de datos se almacenan en la base de datos 130 junto con la información de la primera cuenta, y el acceso a los datos está limitado

por el procesador 120. En algunas modalidades de ejemplo, los parámetros de control de datos se almacenan en la memoria del transceptor de corto alcance 105 y son recibidos por la aplicación 104 desde el transceptor de corto alcance 105. En algunas modalidades de ejemplo, los datos de la primera cuenta pueden ser cifrados antes de recibir instrucciones para el acceso a los datos de la primera cuenta. La descifrado de los datos de la primera cuenta encriptados puede ser realizado utilizando la clave asociada con el titular de la primera cuenta.

La Figura 7 es un diagrama de flujo que ilustra un método de control de acceso a datos 700 de acuerdo con una o más modalidades de ejemplo, con referencia a los componentes y características descritos anteriormente, incluyendo, pero no limitado a las figuras y la descripción asociada. El método de control de acceso a datos 700 puede ser llevado a cabo por la aplicación 102 ejecutándose en el dispositivo cliente 101 asociado con el titular de la primera cuenta. El transceptor de corto alcance 105 está asociado con el titular de la primera cuenta.

En el bloque 710, se puede recibir una solicitud de aprobación de vinculación del servidor 110 que busca la aprobación para vincular la primera cuenta con la segunda cuenta.

En el bloque 720, la aplicación 102 puede hacer que el dispositivo cliente 101 muestre una pantalla de solicitud de vinculación de cuenta (como se muestra y se describe arriba con referencia a la Figura 5). La pantalla de solicitud de vinculación de cuenta puede incluir una instrucción para tocar el transceptor de corto alcance 105 con/contra el dispositivo cliente 101 para aprobar la solicitud de vinculación de cuenta. Como se describe anteriormente con referencia a la Figura 5, el transceptor de corto alcance 520 (y, por lo tanto, el transceptor de corto alcance 105) puede ser una tarjeta sin contacto.

En el bloque 730, se puede detectar una acción de toque entre el transceptor de corto alcance 105 y el dispositivo cliente 101 que indica la aprobación de la solicitud de aprobación de vinculación. La acción de toque puede ser receptiva a la solicitud de aprobación de vinculación. En una modalidad de ejemplo, la aprobación puede ser indicada por otros métodos (como, por ejemplo, seleccionar un botón).

En el bloque 740, se puede recibir el token 107 del transceptor de corto alcance 105. El token 107 puede incluir el identificador de la primera cuenta. En algunas modalidades de ejemplo, el token 107 puede incluir una clave asociada con el titular de la primera cuenta.

En el bloque 750, se puede enviar un mensaje de aprobación de vinculación al servidor 110 indicando la aprobación de la solicitud para vincular la primera cuenta con la segunda cuenta.

La Figura 8 es un diagrama de flujo que ilustra un método de control de acceso a datos 800 de acuerdo con una o más modalidades de ejemplo, con referencia a los componentes y características descritos anteriormente, incluyendo, pero no limitado a las figuras y la descripción asociada. El método de control de acceso a datos 800 puede ser realizado por el procesador 120 en comunicación con, a través del servidor 110, el dispositivo cliente 101 asociado con el titular de la primera cuenta y/o el dispositivo cliente 103 asociado con el titular de la segunda cuenta.

En el bloque 810, se puede recibir una solicitud de vinculación de cuenta, junto con el token 107, del dispositivo cliente 103 asociado con el titular de la segunda cuenta, solicitando vincular la primera cuenta con la segunda cuenta. El token 107 puede incluir el identificador de la primera cuenta. En algunas modalidades de ejemplo, el token 107 puede incluir una clave asociada con el titular de la primera cuenta.

En el bloque 820, el remitente de la solicitud de vinculación de cuenta puede ser identificado como el titular de la segunda cuenta.

En el bloque 830, la primera cuenta puede ser identificada en función del token recibido 107. En algunas modalidades de ejemplo, cuando el token 107 incluye la clave asociada con el titular de la primera cuenta, la clave asociada con el titular de la primera cuenta puede ser utilizada para autenticar al titular de la primera cuenta.

En el bloque 840, el procesador puede confirmar que la primera cuenta es elegible para ser vinculada con la segunda cuenta. Como se discutió anteriormente con referencia a la Figura 1B, la elegibilidad para la vinculación de cuentas puede basarse, por ejemplo, en el tipo de cuentas involucradas (por ejemplo, cuentas comerciales), o en la identidad de los titulares de las cuentas (por ejemplo, miembros de la familia o miembros de la misma entidad comercial).

En el bloque 850, se puede enviar una solicitud de aprobación de vinculación al dispositivo cliente 101 asociado con el titular de la primera cuenta, solicitando aprobación para vincular la primera cuenta con la segunda cuenta.

En el bloque 860, se puede recibir un mensaje de aprobación de vinculación del dispositivo cliente 101, que indica la aprobación de la solicitud para vincular la primera cuenta con la segunda cuenta.

En el bloque 870, se puede enviar un mensaje de confirmación de vinculación de cuenta al dispositivo cliente 103 asociado con el titular de la segunda cuenta, junto con instrucciones para acceder a los datos de la primera cuenta. Como se discutió anteriormente, las instrucciones pueden ser parte del mensaje de confirmación de vinculación de cuenta, o parte de un mensaje separado. En algunas modalidades de ejemplo, el acceso a los datos de la primera cuenta puede ser limitado de acuerdo con los parámetros de control de datos. En algunas modalidades de ejemplo, el procesador 120 puede cifrar los datos de la primera cuenta antes de proporcionar al dispositivo cliente 103 instrucciones para acceder a los datos de la primera cuenta. La encriptación de los datos de la primera cuenta puede realizarse utilizando la clave asociada con el titular de la primera cuenta.

La descripción de las modalidades en esta descripción describe ejemplos representativos no limitativos que hacen referencia a figuras y números para describir particularmente características y enseñanzas de diferentes aspectos de la divulgación. Las modalidades descritas deben ser reconocidas como capaces de implementarse por separado, o en combinación, con otras modalidades de la descripción de las modalidades. Una persona con habilidad ordinaria en la técnica que revise la descripción de las modalidades debería ser capaz de aprender y comprender los diferentes aspectos descritos de la divulgación. La descripción de modalidades debería facilitar la comprensión de la divulgación hasta tal punto que otras implementaciones, no específicamente cubiertas, pero dentro del conocimiento de una persona con habilidades en la técnica que haya leído la descripción de modalidades, se entenderían como consistentes con una aplicación de la divulgación.

A lo largo de la especificación y las reivindicaciones, los siguientes términos tienen al menos los significados explícitamente asociados en este documento, a menos que el contexto indique claramente lo contrario. El término "o" se entiende como un "o" inclusivo. Además, los términos "un," "una" y "el" están destinados a significar uno o más, a menos que se especifique lo contrario o se entienda claramente por el contexto que se dirigen a una forma singular.

En esta descripción, se han expuesto numerosos detalles específicos. Sin embargo, se debe entender que las implementaciones de la tecnología descrita pueden practicarse sin estos detalles específicos. En otras instancias, métodos, estructuras y técnicas bien conocidos no se han mostrado en detalle para no oscurecer la comprensión de esta descripción. Las referencias a "algunos ejemplos", "otros ejemplos", "un ejemplo", "unos ejemplos", "varios ejemplos", "una modalidad", "algunas modalidades", "modalidad de ejemplo", "varias modalidades", "una implementación", "una implementación de ejemplo", "varias implementaciones", "algunas implementaciones", etc., indican que las implementaciones de la tecnología descrita pueden incluir una característica, estructura o particularidad específica, pero no todas las implementaciones necesariamente incluyen la característica, estructura o particularidad específica. Además, el uso repetido de las frases "en un ejemplo", "en una modalidad" o "en una implementación" no se refiere necesariamente al mismo ejemplo, modalidad o implementación, aunque puede hacerlo.

Como se utiliza en el presente documento, a menos que se especifique lo contrario, el uso de los adjetivos ordinales "primero", "segundo", "tercero", etc., para describir un objeto común, indica meramente que se están haciendo referencia a diferentes instancias de objetos similares, y no se pretende implicar que los objetos así descritos deben estar en una secuencia determinada, ya sea temporal, espacial, en clasificación, o de cualquier otra manera.

Si bien se han descrito ciertas implementaciones de la tecnología descrita en conexión con lo que actualmente se considera más práctico y diversas implementaciones, se debe entender que la tecnología descrita no se limita a las implementaciones descritas, sino que, por el contrario, se pretende cubrir diversas modificaciones y disposiciones equivalentes incluidas dentro del alcance de las reivindicaciones adjuntas. Aunque se emplean términos específicos en el presente documento, se utilizan de manera genérica y descriptiva únicamente y no con fines de limitación.

Esta descripción escrita utiliza ejemplos para describir ciertas implementaciones de la tecnología descrita, incluyendo la mejor modalidad, y también para permitir que cualquier persona con habilidades en la materia practique ciertas implementaciones de la tecnología descrita, incluyendo la fabricación y el uso de cualquier dispositivo o sistema y la realización de cualquier método incorporado. El alcance patentable de ciertas implementaciones de la tecnología descrita se define en las reivindicaciones, y puede incluir otros ejemplos que se le ocurran a los expertos en la materia. Dichos otros ejemplos están destinados a estar dentro del alcance de las reivindicaciones si tienen elementos estructurales que no difieren del lenguaje literal de las reivindicaciones.

REIVINDICACIONES

1. Un sistema de control de acceso a datos, que comprende:
una base de datos que almacena información para una pluralidad de cuentas que comprende, para
5 una primera cuenta asociada con un titular de la primera cuenta, un identificador de la primera cuenta y datos de la primera cuenta, y, para una segunda cuenta asociada con un titular de la segunda cuenta, un identificador de la segunda cuenta;
un servidor configurado para comunicarse a través de una red con una pluralidad de dispositivos
cliente, incluyendo un primer dispositivo cliente asociado con el titular de la primera cuenta y un segundo
10 dispositivo cliente asociado con el titular de la segunda cuenta;
una tarjeta sin contacto que comprende una interfaz de comunicación, un procesador y una memoria, la memoria que almacena un applet y un token, en donde la tarjeta sin contacto está asociada con el titular de la primera cuenta;
una aplicación cliente que comprende instrucciones para su ejecución en el primer dispositivo cliente y
15 en el segundo dispositivo cliente, la aplicación cliente configurada para:
cuando se ejecuta en el segundo dispositivo cliente:
en respuesta a una acción de toque entre la tarjeta sin contacto y el segundo
dispositivo cliente: recibir el token de la tarjeta sin contacto y transmitir al servidor el
token y una solicitud de vinculación de cuenta para vincular la primera cuenta con la
20 segunda cuenta;
y
recibir del servidor un mensaje de confirmación de vinculación de cuenta que
incluye instrucciones para acceder a los datos de la primera cuenta;
y, cuando se ejecute en el primer dispositivo cliente:
25 en respuesta a una solicitud de aprobación de vinculación del servidor para
aprobar la solicitud de vinculación de cuenta, transmitir al servidor un mensaje de
aprobación de vinculación que apruebe la solicitud de vinculación de cuenta;
y,
un procesador en comunicación de datos con el servidor y la base de datos, el procesador configurado
30 para:
recibir del segundo dispositivo cliente el token y la solicitud de vinculación de cuenta;
identificar la primera cuenta basada en el token;
transmitir al primer dispositivo cliente la solicitud de aprobación de vinculación para aprobar la
solicitud de vinculación de cuenta;
35 recibir del primer dispositivo cliente el mensaje de aprobación de vinculación que aprueba la
solicitud de vinculación de cuenta; y
transmitir al segundo dispositivo cliente el mensaje de confirmación de vinculación de cuenta
que incluye instrucciones para acceder a los datos de la primera cuenta.
40
2. El sistema de control de acceso a datos de la reivindicación 1, en donde el procesador está además
configurado para determinar si la primera cuenta es elegible para vincularse a la segunda cuenta.
3. El sistema de control de acceso a datos de la reivindicación 1, en donde la información de la primera
45 cuenta incluye parámetros de control de datos, y el procesador está configurado además para limitar el
acceso por parte del segundo dispositivo cliente a los datos de la primera cuenta de acuerdo con los
parámetros de control de datos.
4. El sistema de control de acceso a datos de la reivindicación 1, en donde:
la memoria de la tarjeta sin contacto además almacena parámetros de control de datos para la primera
50 cuenta; y
la aplicación cliente está además configurada para, cuando se ejecuta por el segundo dispositivo
cliente:
recibir de la tarjeta sin contacto parámetros de control de datos para la primera cuenta; y
55 limitar el acceso del segundo dispositivo cliente a los datos de la primera cuenta de acuerdo
con los parámetros de control de datos recibidos.
5. El sistema de control de acceso a datos de la reivindicación 4, en donde la aplicación cliente está
además configurada para, al ser ejecutada por el primer dispositivo cliente:
proporcionar una interfaz para seleccionar parámetros de control de datos para controlar el acceso a
60 los datos de la primera cuenta; y
transmitir a la tarjeta sin contacto los parámetros de control de datos seleccionados.
6. El sistema de control de acceso a datos de la reivindicación 5, en donde el applet está configurado
para:
65 recibir los parámetros de control de datos seleccionados y almacenar los parámetros de control de
datos seleccionados en la memoria de la tarjeta sin contacto; y

transmitir los parámetros de control de datos seleccionados al segundo dispositivo cliente.

7. El sistema de control de acceso a datos de la reivindicación 1, en donde la aplicación cliente está además configurada para, cuando se ejecuta por el primer dispositivo cliente, determinar una acción de toque entre la tarjeta sin contacto y el primer dispositivo cliente, la acción de toque en respuesta a la solicitud de aprobación de vinculación para aprobar la solicitud de vinculación de cuenta, la acción de toque indicando la aprobación de la solicitud de vinculación de cuenta.
8. El sistema de control de acceso a datos de la reivindicación 1, en donde:
el token que comprende una clave asociada con el titular de la primera cuenta; y
el procesador está además configurado para utilizar la clave para autenticar al titular de la primera cuenta.
9. El sistema de control de acceso a datos de la reivindicación 1, en donde el procesador está además configurado para encriptar los datos de la primera cuenta antes de proporcionar al segundo dispositivo cliente acceso a los datos de la primera cuenta.
10. El sistema de control de acceso a datos de la reivindicación 9, en donde la aplicación cliente está además configurada para, cuando se ejecute en el segundo dispositivo cliente, descifrar los datos de la primera cuenta después de recibir acceso a los datos de la primera cuenta.
11. Un método para controlar el acceso a los datos, que comprende:
establecer una base de datos que almacena información para una pluralidad de cuentas que comprende, para una primera cuenta asociada con un titular de la primera cuenta, un identificador de la primera cuenta, datos de la primera cuenta y parámetros de control de datos, y, para una segunda cuenta asociada con un titular de la segunda cuenta, un identificador de la segunda cuenta;
recibir, por un procesador, de un dispositivo cliente del titular de la segunda cuenta, a través de una red, una solicitud de vinculación de cuenta para vincular la primera cuenta con la segunda cuenta, la solicitud de vinculación de cuenta generada en respuesta a una acción de toque entre una tarjeta sin contacto y el dispositivo cliente del titular de la segunda cuenta, la solicitud de vinculación de cuenta acompañada por un token almacenado en la tarjeta sin contacto, en donde la tarjeta sin contacto está asociada con el titular de la primera cuenta;
identificar, por el procesador, la primera cuenta en función del token;
transmitir, por el procesador, a un dispositivo cliente del titular de la primera cuenta, a través de la red, una solicitud de aprobación de vinculación para aprobar la solicitud de vinculación de cuenta;
recibir, por parte del procesador, del dispositivo cliente del titular de la primera cuenta, a través de la red, un mensaje de aprobación de vinculación, el mensaje de aprobación de vinculación generado en respuesta a una indicación por parte del titular de la primera cuenta aprobando la solicitud de vinculación de cuenta; y
transmitir, por el procesador, al dispositivo cliente del titular de la segunda cuenta, a través de la red, un mensaje de confirmación de vinculación de cuenta, el mensaje de confirmación de vinculación de cuenta confirmando la aprobación de la solicitud de vinculación de cuenta y proporcionando instrucciones para acceder a los datos de la primera cuenta.
12. El método de la reivindicación 11, en donde el token comprende una clave, el método además comprende usar la clave para autenticar al titular de la primera cuenta.
13. El método de la reivindicación 11, en donde los parámetros de control de datos permiten al titular de la segunda cuenta acceder a los datos de la primera cuenta solo por un período de tiempo limitado.
14. El método de la reivindicación 11, en donde los parámetros de control de datos permiten al titular de la segunda cuenta acceder a los datos de la primera cuenta solo para un único uso.
15. El método de la reivindicación 11, en donde los parámetros de control de datos permiten al titular de la segunda cuenta acceder a los datos de la primera cuenta por un período de tiempo ilimitado a menos que el titular de la primera cuenta revoque la aprobación de la solicitud para vincular la primera cuenta con la segunda cuenta.
16. El método de la reivindicación 11, en donde los parámetros de control de datos permiten al titular de la segunda cuenta acceder solo a porciones de los datos de la primera cuenta que corresponden a una categoría predefinida.
17. El método de la reivindicación 11, en donde los parámetros de control de datos comprenden diferentes permisos de acceso a los datos basados en la identidad del titular de la segunda cuenta.

18. El método de la reivindicación 11, en donde los parámetros de control de datos permiten al titular de la segunda cuenta acceder a los datos de la primera cuenta solo cuando la tarjeta sin contacto es detectada dentro del alcance de un campo de comunicación de corto alcance del dispositivo cliente del titular de la segunda cuenta.

5

19. El método de la reivindicación 11, en donde la indicación del titular de la primera cuenta que aprueba la solicitud de vinculación de cuenta comprende una acción de toque entre la tarjeta sin contacto y el dispositivo cliente del titular de la primera cuenta.

10

20. El método de la reivindicación 11, en donde el acceso a los datos se proporciona de acuerdo con los parámetros de control de datos.

15

20

25

30

35

40

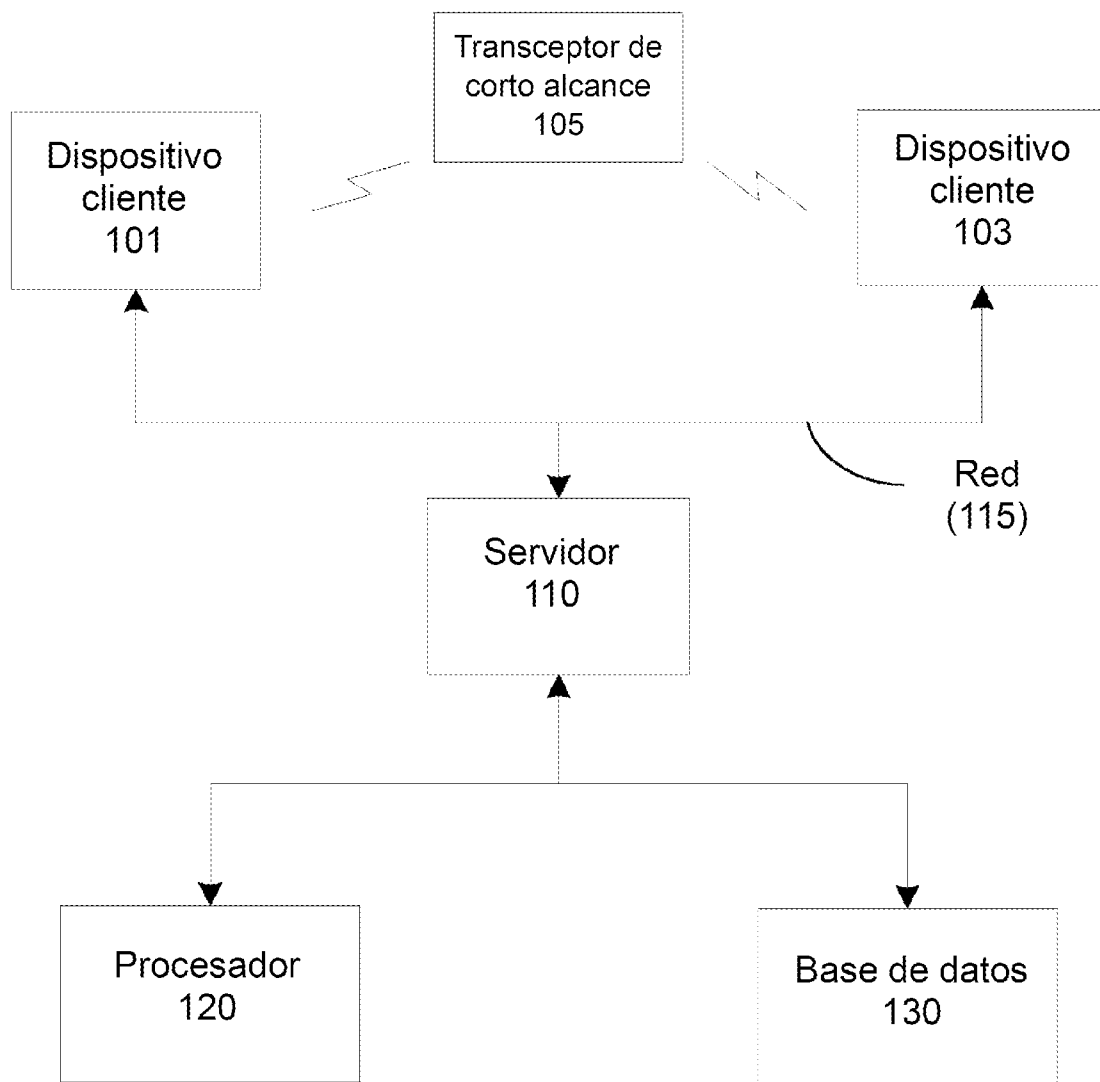
45

50

55

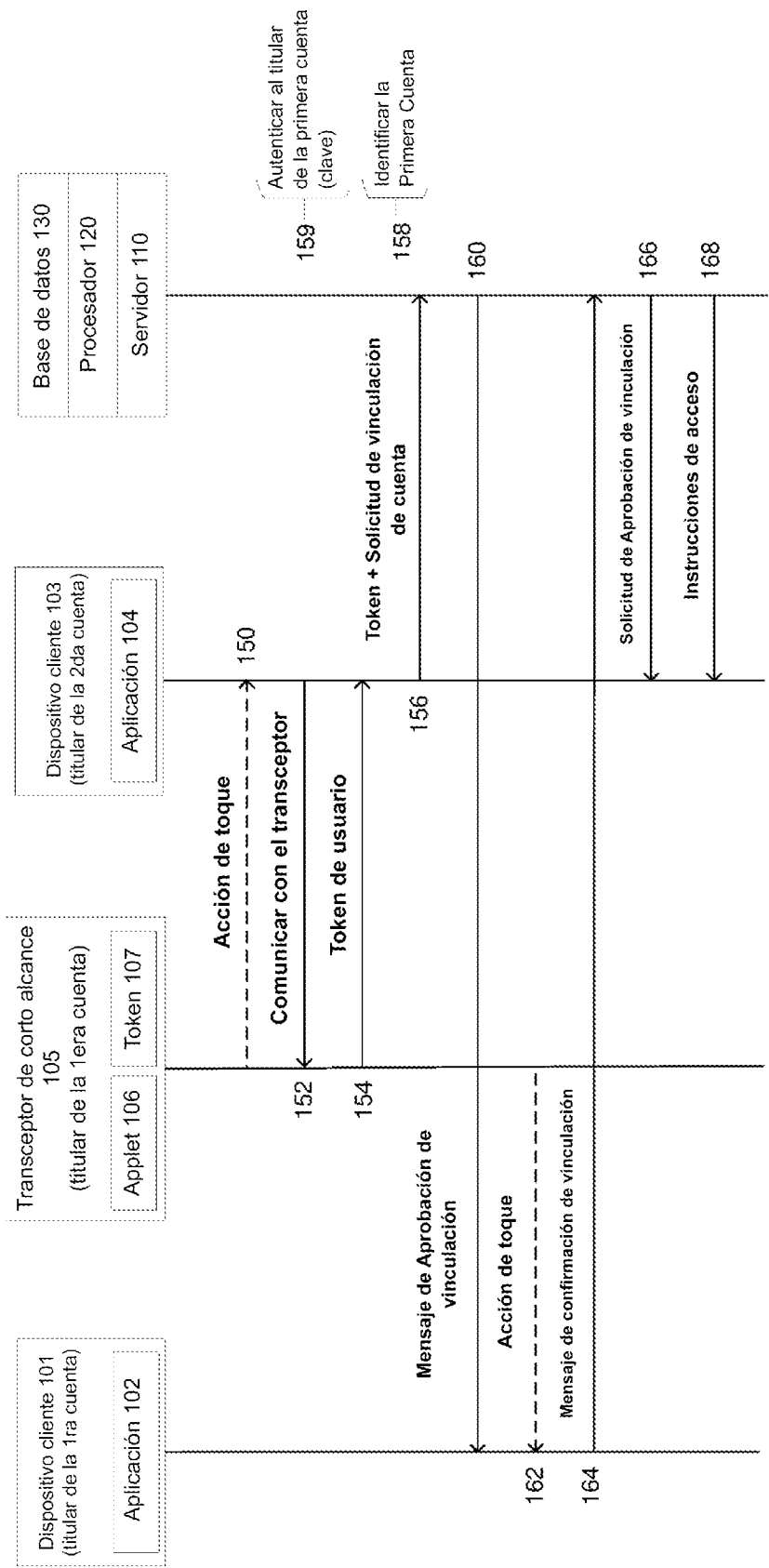
60

65



Sistema 100

FIGURA 1A



Sistema 100

FIGURA 1B



FIGURA 2

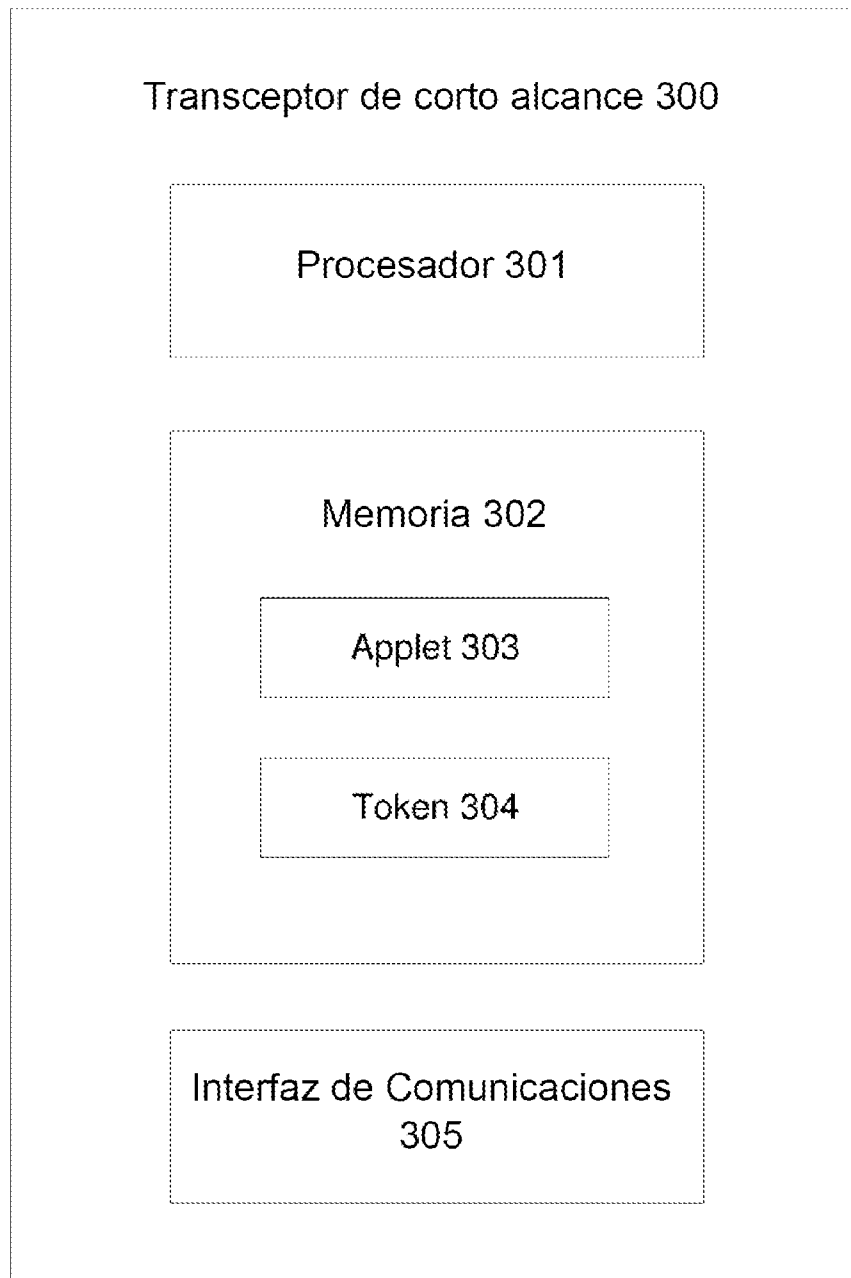


FIGURA 3

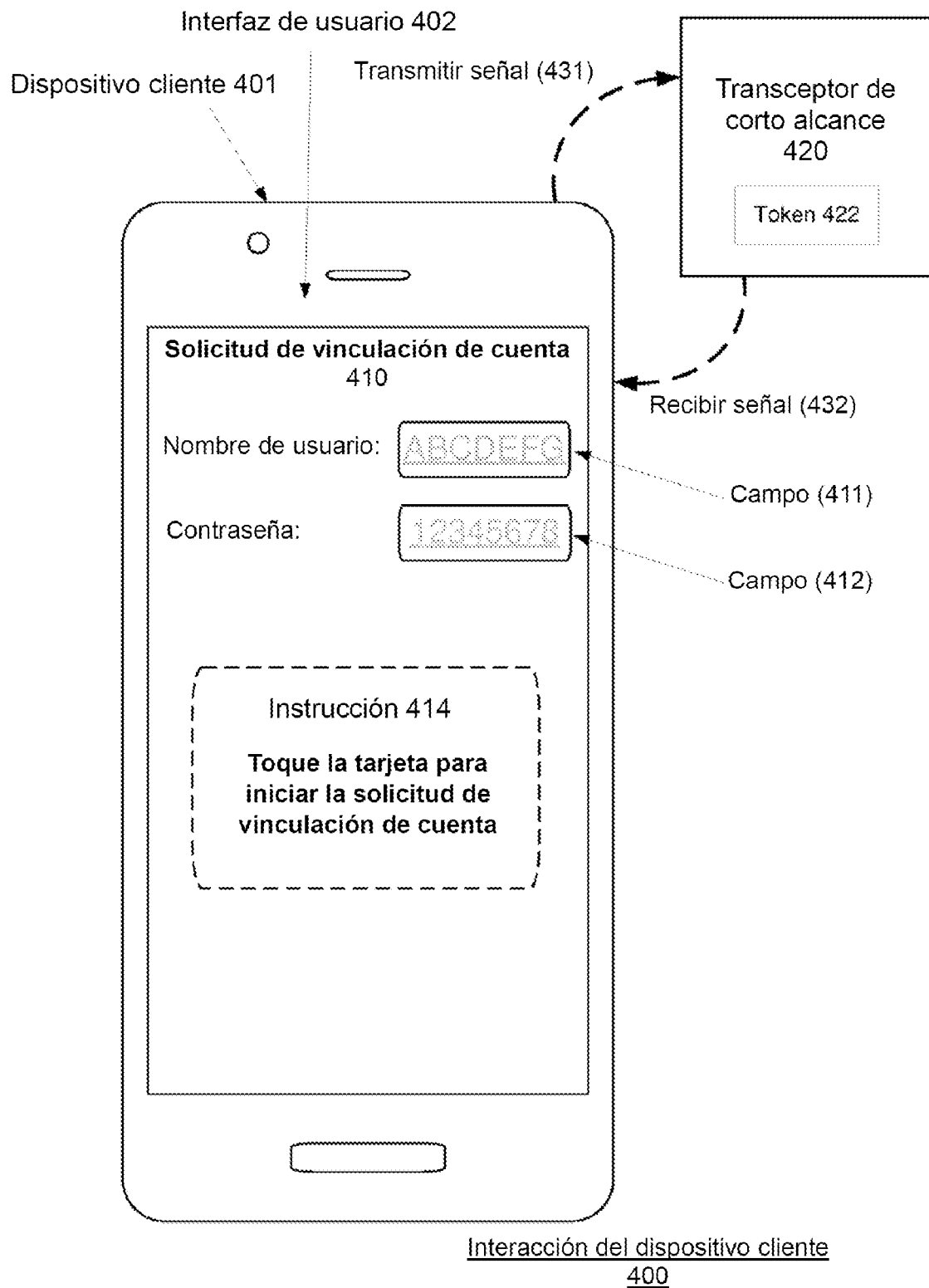


FIGURA 4

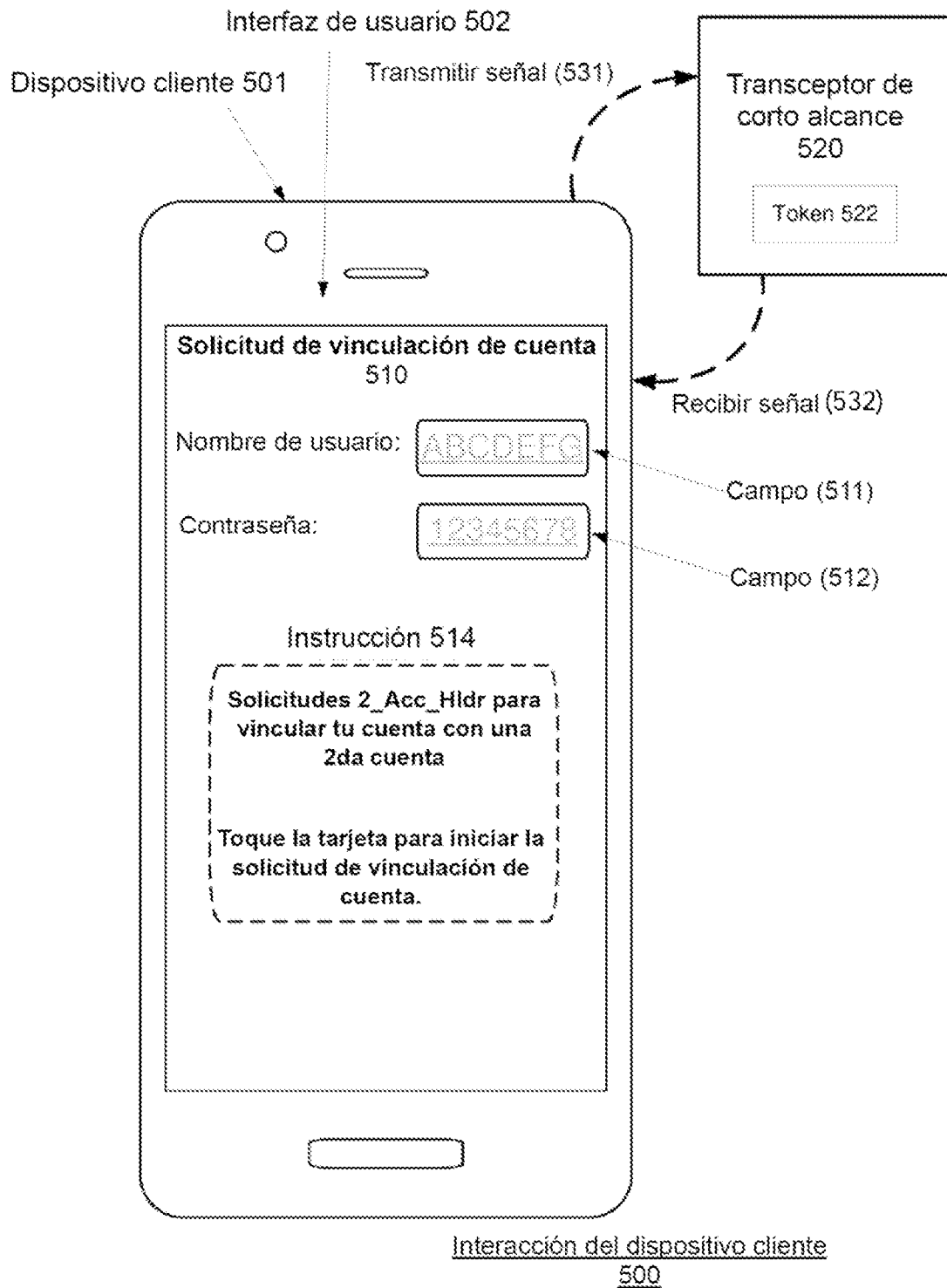
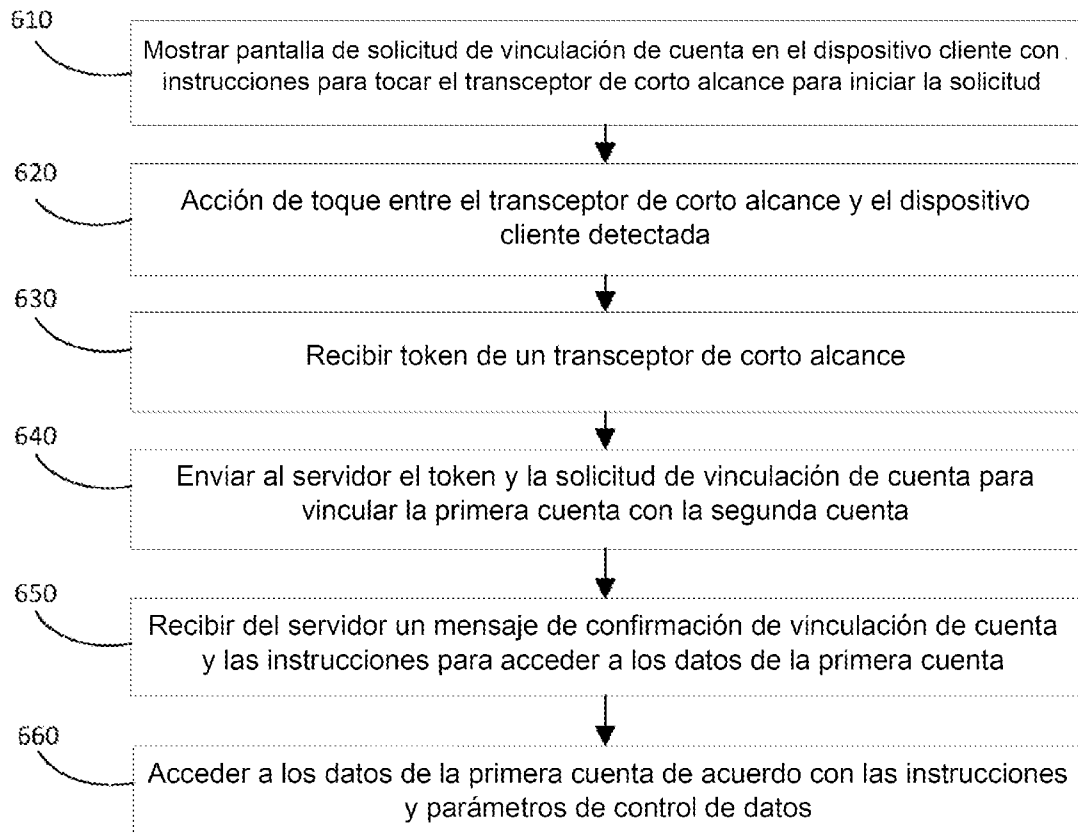
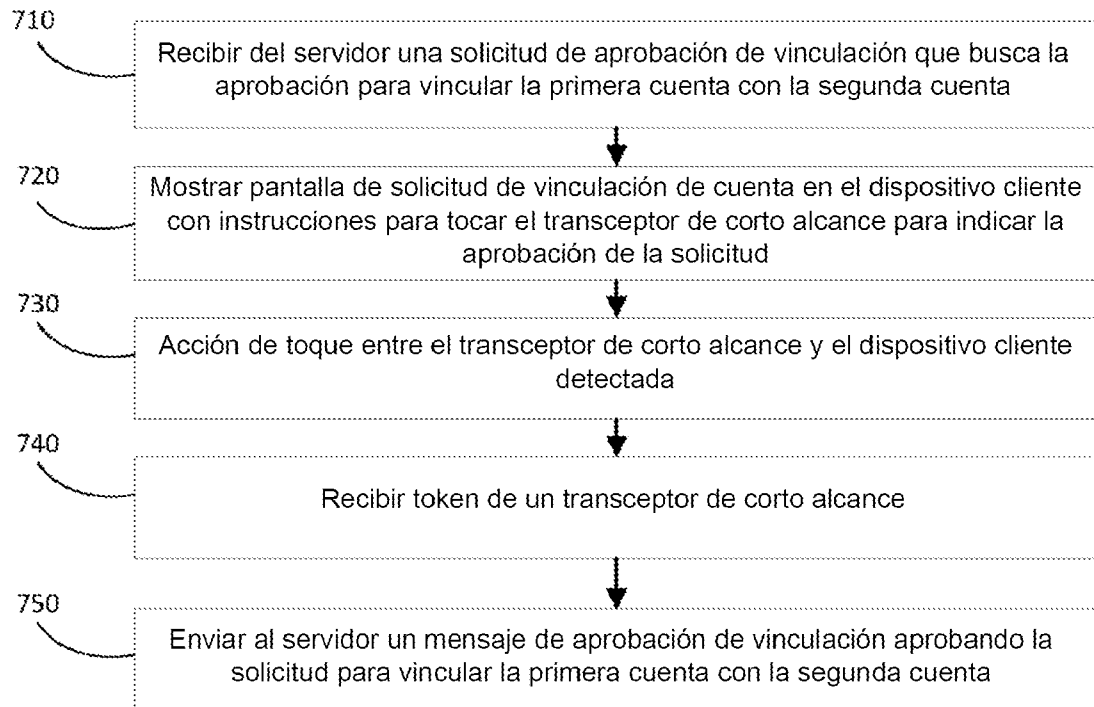


FIGURA 5



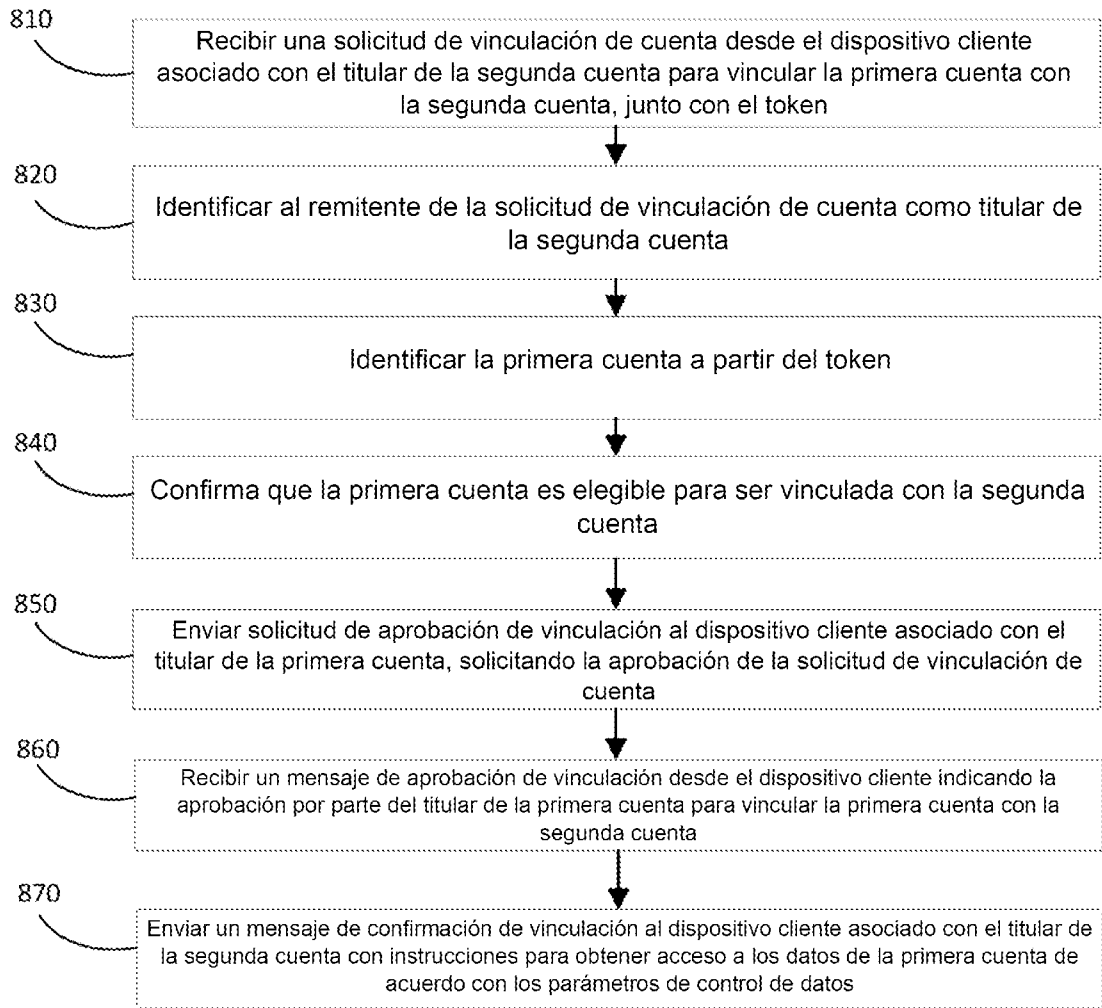
600

FIGURA 6



700

FIGURA 7



800

FIGURA 8