(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 662 826**

(51) Int. CI.:

***G06F 21/53*** (2013.01)
***H04L 29/06*** (2006.01)
***H04W 12/06*** (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **16.09.2015 E 15185560 (8)**

(97) Fecha y número de publicación de la concesión europea: **03.01.2018 EP 2998900**

(54) Título: **Sistema y procedimiento para autenticación segura**

(30) Prioridad:

**16.09.2014 US 201414488160**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**09.04.2018**

(73) Titular/es:

**ENTERSEKT INTERNATIONAL LIMITED (100.0%)**
**Level 3, Alexander House 35 Cybercity**
**Ebene, MU**

(72) Inventor/es:

**BRAND, CHRISTIAAN JOHANNES PETRUS**

(74) Agente/Representante:

**CONTRERAS PÉREZ, Yahel**

**DESCRIPCIÓN**

Sistema y procedimiento para autenticación segura

CAMPO DE LA INVENCIÓN

La presente invención se refiere a la autenticación segura en aplicaciones móviles, particularmente, pero no exclusivamente, para uso en aplicaciones bancarias.

TÉCNICA ANTERIOR

Las aplicaciones bancarias se ejecutan en dispositivos de comunicación móvil de los consumidores para la comunicación con un servidor de aplicaciones bancarias proporcionado por una institución bancaria. Las aplicaciones bancarias proporcionan funcionalidades en los dispositivos de comunicación móvil para realizar acciones e instrucciones bancarias mediante comunicación con el servidor de aplicaciones bancarias.

Las aplicaciones bancarias usualmente se ejecutan dentro de un entorno protegido (*sandbox*) en el sistema operativo del dispositivo de comunicación móvil para hacer que la aplicación bancaria sea segura como una aplicación que se ejecuta por separado con recursos estrechamente controlados que incluyen su propio espacio de memoria protegido con sus propios almacenes de datos.

Se sabe que la autenticación de seguridad adicional es proporcionada por kits de desarrollo de software de autenticación (SDK) para integrar la tecnología de autenticación en las aplicaciones bancarias.

Dichos SDK de autenticación pueden usar una clave privada asociada con el SDK y habilitar la autenticación de múltiples factores. La clave privada del SDK proporciona el factor "algo que tengo" mientras que un inicio de sesión requerido por la aplicación bancaria constituye el factor "algo que conozco".

Los SDK de autenticación también proporcionan autenticación fuera de banda como una comunicación entre una puerta de enlace segura, un dispositivo de hardware del Estándar Federal de Procesamiento de Información (FIPS) 140-2 que tiene un módulo de criptografía, y el SDK de autenticación en el dispositivo de comunicación móvil no utiliza la criptografía del dispositivo de comunicación móvil. El canal está completamente separado de la capa de sockets seguros (SSL) del dispositivo de comunicación móvil, o de cualquier SSL que pueda estar implementada de forma nativa por la aplicación bancaria, negando así cualesquiera ataques en la propia capa de transporte.

Sin embargo, un SDK de autenticación se ejecuta típicamente dentro del mismo entorno protegido que la aplicación bancaria. Esto plantea el problema potencial de seguridad de que si un atacante descubriera una vulnerabilidad en el SDK de autenticación o en la aplicación bancaria, podrían potencialmente comprometer la solución.

En consecuencia, sería beneficioso abordar este problema potencial.

La Solicitud de Patente de Estados Unidos Nº US 2013/0262857 divulga la autenticación segura en un sistema de múltiples partes. Un usuario de red se autentica en otra entidad de red utilizando un primer programa para recibir información de validación de entrada de usuario y almacenar una credencial de usuario. Un segundo programa recibe información, tal como un número aleatorio, de la otra entidad. El primer programa recibe una entrada que le transfiere la información, transmite la información al servidor de autenticación y recibe un identificador de la otra entidad, otra información y requisitos de política de autenticación procedente del servidor de autenticación. A continuación, transmite la información de validación de entrada correspondiente a los requisitos de política de autenticación recibida al servidor de autenticación, y en respuesta recibe una solicitud de credencial de usuario. Firma un mensaje, que incluye la información transferida y la otra información recibida, con la credencial de usuario almacenada, y transmite el mensaje firmado al servidor de autenticación para autenticar al usuario.

RESUMEN DE LA INVENCIÓN

De acuerdo con la invención, se proporciona un procedimiento para autenticación segura realizado en un dispositivo de comunicación móvil que comprende: una aplicación de autenticación que realiza las etapas de: recibir, a través de un controlador de protocolo de aplicación de autenticación, un identificador único para una transacción procedente de una primera aplicación proporcionada en el mismo dispositivo de comunicación móvil que la aplicación de autenticación, en el que el identificador único es enviado localmente entre la primera aplicación y la aplicación de autenticación a través de un primer controlador de protocolo de autenticación proporcionado en la

primera aplicación para invocar a la aplicación de autenticación; recibir una transacción cifrada procedente de un servidor seguro remoto; descifrar u obtener el descifrado de la transacción con una clave privada de la aplicación de autenticación; firmar u obtener la firma de la transacción con la clave privada; firmar la transacción con el identificador único; y transmitir la transacción firmada de vuelta al servidor seguro remoto, en el que la aplicación de autenticación comunica con el servidor seguro remoto a través de un protocolo seguro para autenticación de la transacción.

El primer controlador de protocolo de aplicación y el controlador de protocolo de aplicación de autenticación pueden habilitar la comunicación y el intercambio de datos entre la primera aplicación y la aplicación de autenticación usando identificadores de recursos uniformes y pueden ser controladores de identificadores de recursos uniformes de aplicación personalizada que sólo pueden enviar datos localmente en el dispositivo de comunicación móvil.

En algunas realizaciones, la clave privada de la aplicación de autenticación puede ser almacenada por la aplicación de autenticación y en la que las etapas de descifrar la transacción y firmar la transacción con la clave privada son realizadas por la aplicación de autenticación en el dispositivo de comunicación móvil. Alternativamente, en otras realizaciones, la clave privada de la aplicación de autenticación se puede almacenar en un dispositivo separado y el procedimiento puede incluir: enviar la transacción recibida al dispositivo separado a través de una comunicación de proximidad; y recibir la transacción firmada con la clave privada en la aplicación de autenticación a través de la comunicación de proximidad.

Una característica adicional proporciona que el procedimiento incluya la realización, por parte de la primera aplicación, de la invocación local a la aplicación de autenticación y el envío del identificador único a la aplicación de autenticación. La primera aplicación puede ser una aplicación bancaria, una aplicación bancaria móvil u otra aplicación que requiera una autenticación adicional para una transacción.

Otras características proporcionan que el procedimiento incluya la realización, por parte de la primera aplicación, de las etapas de: enviar una solicitud de transacción a un servidor de transacciones remoto, habiéndose autenticado la solicitud de transacción usando un primer factor; y recibir el identificador único que identifica la transacción.

El identificador único identifica una transacción e identifica a un usuario mediante una clave pública correspondiente a la clave privada de la aplicación de autenticación. En una realización, el identificador único es un Identificador Globalmente Único (GUID) de 128 bytes que es único para una transacción y un usuario.

Otras características proporcionan que el procedimiento incluya la realización, por parte de la aplicación de autenticación, del registro en el servidor seguro remoto. El procedimiento también puede incluir la visualización, por parte de la aplicación de autenticación, de la transacción descifrada antes de firmar la transacción. El procedimiento puede incluir además la realización, por parte de la aplicación de autenticación, de una etapa de autorización que incluye recibir una entrada de un usuario y verificar la entrada antes de firmar la transacción.

El procedimiento puede incluir la cesión, por parte de la aplicación de autenticación, del control localmente de vuelta a la primera aplicación después de transmitir la transacción firmada de vuelta al servidor seguro.

La invención proporciona un sistema para autenticación segura, comprendiendo el sistema un dispositivo de comunicación móvil que incluye: una primera aplicación para comunicarse con un servidor de aplicaciones remoto para realizar una transacción; una aplicación de autenticación para comunicarse con un servidor seguro a través de un protocolo seguro para la autenticación de una transacción, en el que la aplicación de autenticación se proporciona en el mismo dispositivo de comunicación móvil que la aplicación de autenticación; en el que se envía localmente un identificador único para una transacción entre la primera aplicación y la aplicación de autenticación a través de un primer controlador de protocolo de aplicación proporcionado en la primera aplicación para invocar a la aplicación de autenticación; y en el que la aplicación de autenticación incluye: un controlador de protocolo de aplicación de autenticación para recibir un identificador único para una transacción procedente de la primera aplicación; un componente de recepción para recibir una transacción cifrada procedente de un servidor seguro remoto; un componente de descifrado para descifrar u obtener el descifrado de la transacción con una clave privada de la aplicación de autenticación; un primer componente de firma para firmar u obtener la firma de la transacción con la clave privada; un segundo componente de firma para firmar la transacción con el identificador único; y un componente de transmisión para transmitir la transacción firmada de vuelta al servidor seguro remoto.

Otras características proporcionan que la primera aplicación se proporcione en un primer entorno protegido (*sandbox*) en el dispositivo de comunicación móvil y que la aplicación de autenticación se proporcione en un segundo entorno protegido en el dispositivo de comunicación móvil.

La clave privada de la aplicación de autenticación se puede almacenar en la aplicación de autenticación, en cuyo caso el primer y segundo componentes de firma pueden ser un único componente. Alternativamente, la clave

privada de la aplicación de autenticación se puede almacenar en un dispositivo Token separado, en el que el dispositivo Token separado incluye: un componente criptográfico para firmar la transacción con la clave privada; y un componente de comunicación de proximidad capaz de comunicarse con la aplicación de autenticación.

La primera aplicación puede incluir: un componente de solicitud de transacción para enviar una solicitud de transacción a un servidor de transacciones remoto, habiéndose autenticado la solicitud de transacción usando un primer factor; y un componente de recepción para recibir un identificador único para la transacción.

La aplicación de autenticación también puede incluir un componente de registro para registrar la aplicación de autenticación en el servidor seguro remoto.

La aplicación de autenticación puede incluir además un componente de visualización para mostrar la transacción descifrada antes de firmar la transacción.

La aplicación de autenticación puede incluir además un componente de autorización para realizar una etapa de autorización que incluye recibir una entrada de un usuario y verificar la entrada antes de firmar la transacción.

La aplicación de autenticación puede incluir un componente de control para ceder el control localmente de vuelta a la primera aplicación después de transmitir la transacción firmada al servidor seguro.

La invención también proporciona un producto de programa informático para autenticación segura, comprendiendo el producto de programa informático un medio de almacenamiento legible por ordenador que tiene un código de programa legible por ordenador configurado para realizar las etapas: recibir, a través de un controlador de protocolo de aplicación de autenticación, un identificador único para una transacción procedente de una primera aplicación proporcionada en el mismo dispositivo de comunicación móvil que la aplicación de autenticación, en el que el identificador único se envía localmente entre la primera aplicación y la aplicación de autenticación a través de un primer controlador de protocolo de aplicación proporcionado en la primera aplicación para invocar a la aplicación de autenticación; recibir una transacción cifrada procedente de un servidor seguro remoto; descifrar u obtener el descifrado de la transacción con una clave privada de la aplicación de autenticación; firmar u obtener la firma de la transacción con la clave privada; firmar la transacción con el identificador único recibido de la primera aplicación; y transmitir la transacción firmada de vuelta al servidor seguro remoto, en el que la aplicación de autenticación se comunica con el servidor seguro remoto a través de un protocolo seguro para la autenticación de la transacción.

El producto de programa informático puede ser un kit de desarrollo de software proporcionado para integrar procedimientos de autenticación en una aplicación de software.

Otras características proporcionan que el producto de programa informático comprenda un medio de almacenamiento legible por ordenador no transitorio.

Para que la invención se comprenda más completamente, a continuación se describirán implementaciones con referencia a los dibujos adjuntos.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

En los dibujos:

La figura 1A es una ilustración esquemática de una primera realización de un sistema para autenticación segura de acuerdo con la invención;
La figura 1B es una ilustración esquemática de una segunda realización de un sistema para autenticación segura de acuerdo con la invención;
La figura 2 es una ilustración esquemática de un dispositivo de comunicación móvil para autenticación segura de acuerdo con una realización de la invención;
La figura 3A es un diagrama de flujo *swim-lane* de una primera realización de un procedimiento para autenticación segura de acuerdo con una realización de la invención;
La figura 3B es un diagrama de flujo *swim-lane* de una segunda realización de un procedimiento para autenticación segura de acuerdo con una realización de la invención;
La figura 4 es una ilustración esquemática del sistema de la Figura 1A que incluye un flujo de proceso entre los componentes de acuerdo con una realización de la invención;
La figura 5 es un diagrama de bloques de un dispositivo informático que se puede usar en diversas realizaciones de la presente invención; y
La figura 6 es un diagrama de bloques de un dispositivo de comunicación móvil que se puede usar en diversas realizaciones de la presente invención.

ESCRIPCIÓN DETALLADA CON REFERENCIA A LOS DIBUJOS

Se describen sistemas y procedimientos en los que se integra una autenticación en una aplicación separada, denominada aplicación de autenticación, que está separada de una aplicación bancaria en el mismo dispositivo de comunicación móvil. Esto tiene el efecto de aislar las funciones de autenticación de la aplicación bancaria. La aplicación bancaria y la aplicación de autenticación se ejecutan en su propio espacio de memoria protegido, tienen sus propios almacenes de datos protegidos y el sistema operativo las trata como una aplicación separada en un entorno protegido (*sandboxed*). Esto asegura que una vulnerabilidad en una de las aplicaciones no produce una violación del sistema completo.

La figura 1A muestra una primera realización de un sistema de ejemplo (100) para autenticación segura cuando se usa una aplicación bancaria en un dispositivo de comunicación móvil. La descripción se refiere a una aplicación bancaria, en particular una aplicación bancaria móvil, proporcionada en un dispositivo de comunicación móvil. Sin embargo, se puede usar cualquier forma de aplicación que requiera autenticación en el sistema y procedimiento descritos.

El sistema incluye un dispositivo de comunicación móvil (110) que tiene una aplicación bancaria (120) y una aplicación de autenticación (130) en forma de dos aplicaciones separadas, cada una en su propio entorno protegido o *sandbox* (121), (131). La aplicación bancaria (120) y la aplicación de autenticación (130) pueden usar controladores de protocolo (122), (132) para permitir la comunicación y el intercambio de datos entre las aplicaciones usando identificadores de recursos uniformes (URI).

En la presente realización, el dispositivo de comunicación móvil (110) es un teléfono móvil; sin embargo, otras formas de dispositivo de comunicación móvil pueden incluir una tableta informática, un ordenador portátil, un asistente digital personal, o similares que generalmente tienen capacidades de procesamiento limitadas.

El sistema (100) puede incluir un servidor de aplicaciones móviles (140) de una institución bancaria que se comunica con la aplicación bancaria (120) del dispositivo de comunicación móvil (110) a través del corta-fuegos (150) de la institución bancaria que aplica seguridad en la red a la comunicación entre un dispositivo de comunicación móvil (110) y el servidor de aplicaciones móviles (140).

Se puede proporcionar una puerta de enlace segura o *secure gateway* (160) proporcionada por un servidor seguro para procedimientos de autenticación. La puerta de enlace segura (160) puede estar en comunicación con el servidor de aplicaciones móviles (140) y también puede estar protegida por el corta-fuegos de la institución bancaria (150). La puerta de enlace segura (160) puede comunicarse con la aplicación de autenticación (130) del dispositivo de comunicación móvil (110) en un canal mutuamente seguro (190). Se puede proporcionar un enrutador (*router*) de mensajes (170) para encaminar (*routing*) mensajes entre la puerta de enlace segura (160) y la aplicación de autenticación (130) en el canal mutuamente seguro (190).

La aplicación de autenticación (130) es instalada en el dispositivo de comunicación móvil (110), por ejemplo, construyendo un SDK de autenticación en una aplicación separada de una aplicación bancaria (120). El dispositivo de comunicación móvil (110) incluye un módulo de cifrado que proporciona funcionalidad de cifrado a la aplicación de autenticación (130). Debería ser evidente que el módulo de cifrado puede ser compilado como parte de la aplicación de autenticación (130). La aplicación de autenticación (130) incluye una clave privada (133) para usarla con el módulo de cifrado. La clave privada (133) se puede almacenar dentro del entorno protegido o *sandbox* (131) de la aplicación de autenticación (130).

La figura 1B muestra una segunda realización de un sistema de ejemplo (180) para autenticación segura cuando se usa una aplicación bancaria en un dispositivo de comunicación móvil. La segunda realización corresponde a la primera realización mostrada en la Figura 1A, con la excepción de que no se almacena una clave privada en la aplicación de autenticación (130).

En la segunda realización, se proporciona un dispositivo Token separado (181) al usuario. El dispositivo Token (181) puede ser un pequeño dispositivo autónomo o auto-contenido que incluye un componente de comunicación de proximidad (182) para la comunicación con la aplicación de autenticación (130) a través de una capacidad de comunicación de proximidad del dispositivo de comunicación móvil (110). El componente de comunicación de proximidad (182) y la correspondiente capacidad de comunicación del dispositivo de comunicación móvil (110) pueden ser una comunicación Bluetooth, Bluetooth de baja energía (LE) u otra forma de protocolo de comunicaciones de baja energía.

El dispositivo Token (181) puede incluir un componente criptográfico (185) y puede almacenar una clave privada (183) para uso por parte del componente criptográfico (185) en representación de la aplicación de autenticación (130).

La aplicación de autenticación (130) puede comunicar una transacción recibida a través del componente de comunicación de proximidad (182) para su firma con la clave privada (183) en el dispositivo Token (181). El dispositivo Token (181) puede entonces enviar la transacción firmada de vuelta a la aplicación de autenticación (130) usando el componente de comunicación de proximidad (182). De esta manera, la clave privada (183) no se almacena en el dispositivo de comunicación móvil (110) aumentando la seguridad en el caso de que el dispositivo de comunicación móvil (110) se vea comprometido. Opcionalmente, el dispositivo Token (181) también puede almacenar un certificado (184) asociado con la clave privada.

Con referencia a la figura 2, un diagrama de bloques muestra detalles adicionales de una realización de ejemplo de un dispositivo de comunicación móvil (110), la aplicación bancaria (120) y la aplicación de autenticación (130) de la realización de la figura 1A.

La aplicación bancaria (120) puede incluir un componente de solicitud de transacción (221) para solicitar una transacción desde un servidor de aplicaciones móviles (140). La aplicación bancaria (120) puede incluir un componente de autenticación de un primer factor (222), por ejemplo, que requiera la introducción de un número de identificación personal (PIN) por parte de un usuario.

La aplicación bancaria (120) puede incluir un componente de recepción de identificadores (223) para recibir un identificador para una transacción, por ejemplo, en forma de un identificador global único (GUID), y almacenar el identificador en un almacén de datos (224) dentro del entorno protegido o *sandbox* (121) de la aplicación bancaria (120).

El controlador de protocolo (122) de la aplicación bancaria (120) puede invocar a la aplicación de autenticación (130) cuando se lo solicita un componente de solicitud de autenticación (225) de la aplicación bancaria (120).

En la realización ilustrada, la aplicación de autenticación (130) puede incluir una clave privada (133) almacenada en un almacén de datos (234) dentro del entorno protegido (131) de la aplicación de autenticación (130). Como se discutió con relación a la Figura 1B, en una realización alternativa, se puede proporcionar un dispositivo Token separado en el que se almacena y utiliza la clave privada y se pueden comunicar transacciones firmadas con la clave privada a la aplicación de autenticación (130) a través de un protocolo de comunicación de proximidad.

La aplicación de autenticación (130) puede incluir un controlador de protocolo (132) que puede ser invocado por el controlador de protocolo (122) de la aplicación bancaria (120).

La aplicación de autenticación (130) puede incluir un componente de registro (232) para registrarse en la puerta de enlace segura (160) y un componente de recepción (233) para recibir una solicitud de transacción procedente de la puerta de enlace segura (160). El componente de recepción (233) y un componente de transmisión (239) pueden usar un canal mutuamente seguro a través de un enrutador (*router*) de mensajes (170) a la puerta de enlace segura (160). La aplicación de autenticación (130) puede incluir un componente de descifrado (235) para descifrar la solicitud de transacción usando la clave privada almacenada (133).

Opcionalmente, la aplicación de autenticación (130) puede incluir un componente de visualización (236) para mostrar la solicitud de transacción al usuario. La aplicación de autenticación (130) también puede incluir opcionalmente un componente de autorización (237) para recibir una autenticación de usuario tal como un PIN, desafío (*challenge*), escaneo de huella dactilar, etc.

La aplicación de autenticación (130) también puede incluir un componente de recepción de identificador (238) para recibir un identificador procedente de la aplicación bancaria (120). La aplicación de autenticación (130) puede incluir un componente de firma (240) para firmar una solicitud de transacción con la clave privada (133) y con el identificador recibido de la aplicación bancaria (120).

El componente de transmisión (239) puede transmitir la solicitud de transacción firmada de vuelta a la puerta de enlace segura (160). Un componente de control (241) puede ceder el control de vuelta a la aplicación bancaria (120) usando el controlador de protocolo (132).

La realización ilustrada por la Figura 1B puede tener componentes similares a los mostrados en la Figura 2; sin embargo, se puede proporcionar un dispositivo Token separado (181) en comunicación de proximidad con el dispositivo de comunicación móvil (110) y por lo tanto la aplicación de autenticación (130) de modo que al menos algunas de las funciones del componente de descifrado (235) y del componente de firma (240) de la Figura 2 son realizadas por el dispositivo Token (181).

Con referencia a las Figuras 3A y 3B, el diagrama de flujo *swim-lane* (300, 350) muestra realizaciones de ejemplo de procedimientos realizados en un dispositivo de comunicación móvil (110) en una aplicación bancaria (120) y en una aplicación de autenticación (130) ambas residentes en el dispositivo de comunicación móvil (110). El diagrama de flujo *swim-lane* (300) también muestra las etapas realizadas en un servidor de aplicaciones móviles (140) y una puerta de enlace segura (160). La figura 3B muestra adicionalmente las etapas realizadas en un dispositivo Token (181).

El siguiente procedimiento describe la autenticación de una acción. Se describe una acción en forma de una transacción, sin embargo, se puede realizar un procedimiento similar para la autorización de otras acciones, como un inicio de sesión, o cualquier otra operación que requiera un incremento del nivel de autenticación (*step-up authentication*).

La aplicación bancaria (120) envía (301) una solicitud de transacción, que ha sido autenticada usando un primer factor, al servidor de aplicaciones móviles (140).

El servidor de aplicaciones móviles (140) envía (302) una solicitud de autenticación a la puerta de enlace segura (160). La solicitud de autenticación puede contener una referencia al usuario y a la transacción específica a autenticar.

La puerta de enlace segura (160) puede generar (303) un Identificador Globalmente Único (GUID) de 128 bytes único para la transacción y el usuario específicos. El GUID puede incluir una referencia a una clave pública del usuario. La puerta de enlace segura (160) puede responder (304) al servidor de aplicaciones móviles (140) con el GUID. El servidor de aplicaciones móviles (140) puede retransmitir (305) el GUID de vuelta a la aplicación bancaria (120). La aplicación bancaria (120) puede recibir y almacenar (306) el GUID.

La puerta de enlace segura (160) envía (307) la transacción cifrada, sin incluir el GUID, a la aplicación de autenticación (130) a través del canal seguro. La transacción cifrada puede cifrarse de extremo a extremo (*end-to-end*) con la clave pública correspondiente a la clave privada almacenada en la aplicación de autenticación (130).

Se invoca a una solicitud de controlador de identificador de recurso uniforme (URI) (308) en la aplicación bancaria (120) para activar la aplicación de autenticación (120), conteniendo la solicitud el GUID como carga útil.

Una vez que se invoca (309) a la aplicación de autenticación (130), ésta se registra (310) en la puerta de enlace segura (160) y recibe (311) la solicitud de transacción pendiente.

En este punto, las realizaciones de las Figuras 3A y 3B difieren. En la realización de la Figura 3A, la aplicación de autenticación (130) descifra (312) la solicitud de transacción usando su clave privada. La clave privada (133) se puede almacenar en la aplicación de autenticación (130) o alternativamente puede obtenerse de un dispositivo Token separado (181).

Opcionalmente, la aplicación de autenticación (130) puede mostrar (313) la solicitud de transacción descifrada al usuario; esto se puede realizar si se requiere "lo-que-se-ve-es-lo-que-se-firma".

La aplicación de autenticación (130) puede opcionalmente solicitar y recibir una entrada de usuario (314) en forma de un PIN, desafío o escaneo de huella dactilar.

La aplicación de autenticación (130) puede firmar (315) la transacción usando la clave privada de la aplicación de autenticación (130) y firmada con el GUID.

En la realización de la Figura 3B, la solicitud de transacción recibida puede enviarse (351) al dispositivo Token (181) usando una comunicación de proximidad. La aplicación de autenticación (130) puede descifrar la transacción y enviar (351) la transacción descifrada al dispositivo Token (181). Alternativamente, el dispositivo Token (181) puede descifrar (353) la solicitud de transacción utilizando la clave privada almacenada en el dispositivo Token (181). Opcionalmente, el dispositivo Token (181) puede solicitar y recibir una entrada de usuario (352) antes de firmar (354) la solicitud de transacción.

El dispositivo Token (181) puede firmar (354) la solicitud de transacción usando la clave privada y puede enviar (355) la solicitud de transacción firmada de vuelta a la aplicación de autenticación (130). La aplicación de autenticación (130) puede recibir (356) la solicitud de transacción firmada por clave privada y adicionalmente firmarla (357) con el GUID.

Los dos procedimientos continúan entonces de la misma manera devolviendo los datos firmados (316) a la puerta de enlace segura (160) que los reenvía (317) al servidor de aplicaciones móviles (140) en el cual son recibidos (318) para validación.

El control se transfiere automáticamente (319, 320) desde la aplicación de autenticación (130) a la aplicación bancaria (120) usando un controlador de URI registrado. A continuación, se puede realizar un procesamiento adicional entre la aplicación bancaria (120) y el servidor de aplicaciones móviles (140).

Con referencia a la Figura 4, el diagrama del sistema de la Figura 1A se muestra con la secuencia de las etapas del procedimiento mostradas.

Se envía una transacción (401) al servidor de aplicaciones móviles (140) desde la aplicación bancaria (120). Se obtiene un GUID de autorización (402) de la puerta de enlace segura (160) válido para la transacción y el usuario a través de la clave pública. El GUID de autenticación es enviado (403) a la aplicación bancaria (120).

Una transacción cifrada es enviada (404) por la puerta de enlace de seguridad (160) a la aplicación de autenticación (130) para ser firmada y se espera una respuesta firmada con la clave privada y el GUID.

El GUID de autorización es cedido (405) a la aplicación de autenticación (130) desde la aplicación bancaria (120) a través de un controlador de URI.

La transacción firmada se envía (406) de vuelta a la puerta de enlace segura (160) firmada con la clave privada y el GUID. La transacción firmada se retorna (407) al servidor de aplicaciones móviles (140). Mientras tanto, se envía (408) el control a través del controlador de URI desde la aplicación de autenticación (130) de vuelta a la aplicación bancaria (120).

La implementación de la solución de aplicaciones múltiples proporciona las siguientes ventajas.

Se proporcionan múltiples factores de autenticación. El nombre de usuario/contraseña de la aplicación bancaria proporciona un primer factor de autenticación. La clave privada almacenada en el dispositivo de comunicación móvil por la aplicación de autenticación proporciona un segundo factor de autenticación.

Se proporciona comunicación fuera de banda. La aplicación bancaria utiliza un esquema de comunicación diferente al protocolo seguro de la aplicación de autenticación.

Se proporciona la separación física de las aplicaciones bancarias y de autenticación. Esto se proporciona teniendo la aplicación bancaria y la aplicación de autenticación en entornos protegidos (*sandboxes*) separados en el sistema operativo del dispositivo de comunicación móvil.

Los controladores de URI de aplicaciones personalizadas solo pueden enviar datos localmente, lo que proporciona la seguridad de que ambas aplicaciones se ejecutan en el mismo dispositivo de comunicación móvil cuando se recibe la firma correcta.

La figura 5 ilustra un ejemplo de un dispositivo informático (500) en el que se pueden implementar diversos aspectos de la divulgación, por ejemplo, el servidor de aplicaciones móviles y la puerta de enlace segura. El dispositivo informático (500) puede ser adecuado para almacenar y ejecutar código de programa informático. Los diversos participantes y elementos en los diagramas de sistema descritos anteriormente pueden usar cualquier cantidad adecuada de subsistemas o componentes del dispositivo informático (500) para facilitar las funciones descritas en este documento.

El dispositivo informático (500) puede incluir subsistemas o componentes interconectados a través de una infraestructura de comunicación (505), por ejemplo: un bus de comunicaciones, un dispositivo de barra cruzada (*cross-over bar device*) o una red. El dispositivo informático (500) puede incluir al menos un procesador central (510) y al menos un componente de memoria en forma de medios legibles por ordenador.

Los componentes de memoria pueden incluir la memoria del sistema (515), que puede incluir memoria de solo lectura (ROM) y memoria de acceso aleatorio (RAM). Un sistema básico de entrada/salida (BIOS) se puede almacenar en la ROM. El software del sistema se puede almacenar en la memoria del sistema (515), incluido el software del sistema operativo.

Los componentes de memoria también pueden incluir memoria secundaria (520). La memoria secundaria (520) puede incluir un disco fijo (521), tal como un disco duro y, opcionalmente, una o más interfaces de almacenamiento extraíbles (522) para componentes de almacenamiento extraíbles (523).

Las interfaces de almacenamiento extraíble (522) pueden ser en forma de unidades de almacenamiento extraíbles (por ejemplo, unidades de cinta magnética, unidades de disco óptico, unidades de disquetes, etc.) para los correspondientes componentes de almacenamiento extraíbles (por ejemplo, una cinta magnética, un disco óptico, un disquete, etc.), en los que la unidad de almacenamiento extraíble puede escribir y leer.

Las interfaces de almacenamiento extraíble (522) también pueden tener la forma de puertos o conectores (*sockets*) para interconectarse con otras formas de componentes de almacenamiento extraíbles (523) tales como una unidad de memoria flash, un disco duro externo o un chip de memoria extraíble. etc.

El dispositivo informático (500) puede incluir una interfaz de comunicaciones externas (530) para el funcionamiento del dispositivo informático (500) en un entorno de red que permite la transferencia de datos entre múltiples dispositivos informáticos (500). Los datos transferidos a través de la interfaz de comunicaciones externas (530) pueden ser en forma de señales, que pueden ser señales electrónicas, electromagnéticas, ópticas, de radio u otros tipos de señal.

La interfaz de comunicaciones externas (530) puede permitir la comunicación de datos entre el dispositivo informático (500) y otros dispositivos informáticos que incluyen servidores e instalaciones de almacenamiento externo. Los servicios web pueden ser accesibles por el dispositivo informático (500) a través de la interfaz de comunicaciones (530).

La interfaz de comunicaciones externa (530) también puede habilitar otras formas de comunicación hacia y desde el dispositivo informático (500) incluyendo la conexión a canales de comunicación que usan: una red de telefonía móvil, red de transmisión de datos, red Wi-Fi, red de telefonía satelital, red de Internet, red de Internet satelital, etc. La interfaz de comunicaciones externas (530) también puede habilitar otras formas de comunicación de proximidad tales como comunicación de campo cercano, comunicación por Bluetooth, etc.

Los medios legibles por ordenador en forma de los diversos componentes de memoria pueden proporcionar almacenamiento de instrucciones ejecutables por ordenador, estructuras de datos, módulos de programa y otros datos. Se puede proporcionar un producto de programa informático mediante un medio legible por ordenador que tiene un código de programa legible por ordenador almacenado y que es ejecutable por el procesador central (510).

Se puede proporcionar un producto de programa informático a través de un medio no transitorio legible por ordenador, o se puede proporcionar a través de una señal u otro medio transitorio a través de la interfaz de comunicaciones (530).

La interconexión a través de la infraestructura de comunicación (505) permite a un procesador central (510) comunicarse con cada subsistema o componente y controlar la ejecución de instrucciones procedentes de los componentes de memoria, así como el intercambio de información entre subsistemas o componentes.

Los periféricos (como impresoras, escáneres, cámaras o similares) y los dispositivos de entrada/salida (E/S) (como el mouse, panel táctil, teclado, micrófono, joystick o similares) pueden acoplarse al dispositivo informático (500) ya sea directamente o por medio de un controlador de E/S (535). Estos componentes pueden ser conectados al dispositivo informático (500) por cualquier número de medios conocidos en la técnica, tal como un puerto en serie.

Se pueden acoplar uno o más monitores (545) a través de un adaptador de visualización o video (540) al dispositivo informático (500).

La figura 6 muestra un diagrama de bloques de un dispositivo de comunicación móvil (600) que se puede usar en realizaciones de la divulgación. El dispositivo de comunicación móvil (600) puede ser un teléfono móvil, un teléfono con funciones especiales, un teléfono inteligente, un teléfono satelital o un dispositivo informático que tenga capacidad de teléfono.

El dispositivo de comunicación móvil (600) puede incluir un procesador (605) (por ejemplo, un microprocesador) para procesar las funciones del dispositivo de comunicación móvil (600) y una pantalla (620) para permitir que un usuario vea los números de teléfono y otra información y mensajes. El dispositivo de comunicación móvil (600) puede incluir además un elemento de entrada (625) para permitir que un usuario introduzca información en el dispositivo (por ejemplo, botones de entrada, pantalla táctil, etc.), un altavoz (630) para permitir que el usuario escuche la comunicación de voz, música, etc., y un micrófono (635) para permitir que el usuario transmita su voz a través del dispositivo de comunicación móvil (600).

El procesador (605) del dispositivo de comunicación móvil (600) puede conectarse a una memoria (615). La memoria (615) puede ser en forma de un medio legible por ordenador que almacena datos y, opcionalmente, instrucciones ejecutables por ordenador.

El dispositivo de comunicación móvil (600) también puede incluir un elemento de comunicación (640) para la conexión a canales de comunicación (por ejemplo, una red de telefonía móvil, red de transmisión de datos, red Wi-Fi, red de telefonía satelital, red de Internet, Red de Internet satelital, etc.). El elemento de comunicación (640) puede incluir un elemento de transferencia inalámbrica asociado, tal como una antena.

El elemento de comunicación (640) puede incluir un módulo de identidad de suscriptor (SIM) en forma de un circuito integrado que almacena una identidad de suscriptor móvil internacional y la clave relacionada utilizada para identificar y autenticar a un suscriptor que usa el dispositivo de comunicación móvil (600). Uno o más módulos de identidad de suscriptor pueden ser extraíbles del dispositivo de comunicación móvil (600) o estar integrados en el dispositivo de comunicación móvil (600).

El dispositivo de comunicación móvil (600) puede incluir además un elemento sin contacto (650), que se implementa típicamente en forma de un chip semiconductor (u otro elemento de almacenamiento de datos) con un elemento de transferencia inalámbrica asociado, tal como una antena. El elemento sin contacto (650) puede estar asociado (por ejemplo, integrado) al dispositivo de comunicación móvil (600) e instrucciones de datos o control transmitidas a través de una red móvil pueden ser aplicadas al elemento sin contacto (650) por medio de una interfaz de elemento sin contacto (no mostrada). La interfaz del elemento sin contacto puede funcionar para permitir el intercambio de datos y/o instrucciones de control entre la circuitería del dispositivo de comunicación móvil (y por lo tanto la red móvil) y el elemento sin contacto (650).

El elemento sin contacto (650) puede ser capaz de transferir y recibir datos usando una capacidad de comunicaciones de campo cercano (NFC) (o un medio de comunicaciones de campo cercano) típicamente de acuerdo con un protocolo estandarizado o mecanismo de transferencia de datos (por ejemplo, ISO 14443/NFC). La capacidad de comunicaciones de campo cercano es una capacidad de comunicaciones de corto alcance, como la identificación por radiofrecuencia (RFID), Bluetooth, infrarrojos u otra capacidad de transferencia de datos que se puede usar para intercambiar datos entre el dispositivo de comunicación móvil (600) y un dispositivo de interrogación. Por lo tanto, el dispositivo de comunicación móvil (600) puede ser capaz de comunicar y transferir datos y/o instrucciones de control a través de una red móvil y una capacidad de comunicaciones de campo cercano.

Los datos almacenados en la memoria (615) pueden incluir: datos de operación relacionados con el funcionamiento del dispositivo de comunicación móvil (600), datos personales (por ejemplo, nombre, fecha de nacimiento, número de identificación, etc.), datos financieros (por ejemplo, información de cuenta bancaria, número de identificación bancaria, información de número de tarjeta de crédito o débito, información de saldo de cuenta, fecha de vencimiento, números de cuenta de proveedor de confianza, etc.), información de tránsito (por ejemplo, como en un tren o metro), información de acceso (por ejemplo, como en distintivos de acceso), etc. Un usuario puede transmitir estos datos desde el dispositivo de comunicación móvil (600) a receptores seleccionados.

El dispositivo de comunicación móvil (600) puede ser, entre otras cosas, un dispositivo de notificación que puede recibir mensajes de alerta e informes de acceso, un dispositivo comercial portátil que se puede usar para transmitir datos de control que identifican un descuento para su aplicación, así como también como un dispositivo de consumidor portátil que se puede usar para realizar pagos.

La descripción anterior de las realizaciones de la invención se ha expuesto con un propósito ilustrativo; no pretende ser exhaustiva o limitar la invención a las formas concretas divulgadas. Los expertos en la técnica relevante pueden apreciar que son posibles muchas modificaciones y variaciones a la luz de la descripción anterior.

Algunas partes de esta descripción describen las realizaciones de la invención en términos de algoritmos y representaciones simbólicas de operaciones sobre información. Estas descripciones y representaciones algorítmicas son usadas comúnmente por los expertos en las técnicas de procesamiento de datos para transmitir la esencia de su trabajo de manera efectiva a otros expertos en la materia. Se entiende que estas operaciones, aunque se han descrito funcionalmente, computacionalmente o lógicamente, se implementan por medio de programas informáticos o circuitos eléctricos equivalentes, micro código o similar. Las operaciones descritas pueden integrarse en software, firmware, hardware o cualquier combinación de los mismos.

Los componentes o funciones de software descritos en esta aplicación pueden implementarse como código de software para su ejecución por parte de uno o más procesadores usando cualquier lenguaje informático adecuado tal como, por ejemplo, Java, C ++ o Perl que usan, por ejemplo, técnicas convencionales u orientadas a objetos. El código de software se puede almacenar como una serie de instrucciones o comandos en un medio no transitorio legible por ordenador, como una memoria de acceso aleatorio (RAM), una memoria de solo lectura (ROM), un medio

magnético como un disco duro o un disquete, o un medio óptico como un CD-ROM. Cualquiera de dichos medios legibles por ordenador también puede residir en o dentro de un solo aparato informático, y puede estar presente en o dentro de diferentes aparatos informáticos dentro de un sistema o red.

Cualquiera de las etapas, operaciones o procesos descritos en este documento puede realizarse o implementarse con uno o más módulos de hardware o software, solos o en combinación con otros dispositivos. En una realización, se implementa un módulo de software con un producto de programa informático que comprende un medio no transitorio legible por ordenador que contiene código de programa informático, que puede ser ejecutado por un procesador informático para realizar cualquiera o todas las etapas, operaciones o procesos descritos.

La descripción anterior de las realizaciones de la invención se ha presentado con el propósito de ilustrar, y no pretende ser exhaustiva o limitar la invención a las formas concretas que se han descrito. Los expertos en la técnica relevante pueden apreciar que son posibles muchas modificaciones y variaciones a la luz de la descripción anterior, que caen dentro del alcance de la invención.

**REIVINDICACIONES**

1. Un procedimiento para autenticación segura realizada en un dispositivo de comunicación móvil (110) que comprende:
una aplicación de autenticación (130) que realiza las etapas de:
recibir, a través de un controlador de protocolo de aplicación de autenticación (132), un identificador único para una transacción procedente de una primera aplicación (120) proporcionada en el mismo dispositivo de comunicación móvil (110) que la aplicación de autenticación (130), en el que el identificador único se envía localmente entre la primera aplicación (120) y la aplicación de autenticación (130) a través de un primer controlador de protocolo de aplicación (122) proporcionado en la primera aplicación (120) para invocar a la aplicación de autenticación (130);
recibir (311) una transacción cifrada procedente de un servidor seguro remoto (160);
descifrar (312) u obtener el descifrado de la transacción con una clave privada de la aplicación de autenticación (130);
firmar (315) u obtener la firma de la transacción con la clave privada;
firmar (315) la transacción con el identificador único recibido de la primera aplicación (120); y
transmitir (316) la transacción firmada de vuelta al servidor seguro remoto (160),
en el que la aplicación de autenticación (130) se comunica con el servidor seguro remoto (160) a través de un protocolo seguro para la autenticación de la transacción.

2. El procedimiento según la reivindicación 1, en el que el primer controlador de protocolo de aplicación (122) y el controlador de protocolo de aplicación de autenticación (132) permiten la comunicación y el intercambio de datos entre la primera aplicación (120) y la aplicación de autenticación (130) utilizando identificadores de recursos uniformes.

3. El procedimiento según la reivindicación 2, en el que el primer controlador de protocolo de aplicación (122) y el controlador de protocolo de aplicación de autenticación (132) son controladores de identificadores de recursos uniformes de aplicación personalizada que solo pueden enviar datos localmente en el dispositivo de comunicación móvil (110).

4. El procedimiento según una cualquiera de las reivindicaciones anteriores, en el que la clave privada de la aplicación de autenticación (130) es almacenada por la aplicación de autenticación (130) y en el que las etapas de descifrar (312) la transacción y firmar (315) la transacción con la clave privada son realizadas por la aplicación de autenticación (130) en el dispositivo de comunicación móvil (110).

5. El procedimiento según una cualquiera de las reivindicaciones 1 a 3, en el que la clave privada de la aplicación de autenticación (130) es almacenada por un dispositivo separado (181) e incluye:
enviar (351) la transacción recibida al dispositivo separado (181) a través de una comunicación de proximidad; y
recibir (356) la transacción firmada con la clave privada en la aplicación de autenticación (130) a través de la comunicación de proximidad.

6. El procedimiento según una cualquiera de las reivindicaciones anteriores, en el que el procedimiento incluye uno o más de:
invocar, por parte de la primera aplicación (120), a la aplicación de autenticación (130) localmente y enviar el identificador único a la aplicación de autenticación (130);
la realización, por parte de la primera aplicación (120), de las etapas de:
enviar (301) una solicitud de transacción a un servidor de transacciones remoto (140), habiéndose autenticado la solicitud de transacción usando un primer factor; y
recibir el identificador único que identifica la transacción;
mostrar, por parte de la aplicación de autenticación (130), la transacción descifrada antes de firmar la transacción;
realizar, por parte de la aplicación de autenticación (130), una etapa de autorización que incluye recibir una entrada de un usuario y verificar la entrada antes de firmar la transacción; y
ceder, por parte de la aplicación de autenticación (130), el control localmente de vuelta a la primera aplicación (120) después de transmitir la transacción firmada de vuelta al servidor seguro (160).

7. El procedimiento según una cualquiera de las reivindicaciones anteriores, en el que el identificador único identifica una transacción e identifica a un usuario por medio de una clave pública correspondiente a la clave privada de la aplicación de autenticación (130).

8. Un sistema para autenticación segura, comprendiendo el sistema un dispositivo de comunicación móvil (110) que incluye:
una primera aplicación (120) para comunicarse con un servidor de aplicaciones remoto (140) para realizar una transacción; y

una aplicación de autenticación (130) para comunicarse con un servidor seguro (160) a través de un protocolo seguro para autenticación de una transacción, en el que la aplicación de autenticación (130) se proporciona en el mismo dispositivo de comunicación móvil (110) que la primera aplicación (120);
en el que se envía localmente un identificador único para una transacción entre la primera aplicación (120) y la aplicación de autenticación (130) a través de un primer controlador de protocolo de aplicación (122) proporcionado en la primera aplicación (120) para invocar a la aplicación de autenticación (130); y en el que la aplicación de autenticación (130) incluye:
un controlador de protocolo de aplicación de autenticación (132) para recibir un identificador único para una transacción procedente de la primera aplicación (120);
un componente de recepción (233) para recibir una transacción cifrada procedente de un servidor seguro remoto (160);
un componente de descifrado (235) para descifrar u obtener el descifrado de la transacción con una clave privada de la aplicación de autenticación (130);
un primer componente de firma (240) para firmar u obtener la firma de la transacción con la clave privada;
un segundo componente de firma (240) para firmar la transacción con el identificador único; y
un componente de transmisión (239) para transmitir la transacción firmada de vuelta al servidor seguro remoto (160).

9. El sistema según la reivindicación 8, en el que la primera aplicación (120) se proporciona en un primer entorno protegido o *sandbox* (121) en el dispositivo de comunicación móvil (110) y la aplicación de autenticación (130) se proporciona en un segundo entorno protegido o *sandbox* (131) en el dispositivo de comunicación móvil (110).

10. El sistema según la reivindicación 8 o la reivindicación 9, en el que la clave privada de la aplicación de autenticación (130) se almacena en la aplicación de autenticación (130) y el primer y segundo componentes de firma (240) son proporcionados por un único componente.

11. El sistema según la reivindicación 8 o la reivindicación 9, en el que la clave privada de la aplicación de autenticación (130) se almacena en un dispositivo Token separado, en el que el dispositivo Token separado (181) incluye:
un componente criptográfico (185) para firmar la transacción con la clave privada; y
un componente de comunicación de proximidad (182) capaz de comunicarse con la aplicación de autenticación (130).

12. El sistema según una cualquiera de las reivindicaciones 8 a 11, en el que la primera aplicación (120) incluye:
un componente de solicitud de transacción (221) para enviar una solicitud de transacción a un servidor de transacciones remoto (140), habiéndose autenticado la solicitud de transacción usando un primer factor; y
un componente de recepción (223) para recibir un identificador único para la transacción.

13. El sistema según una cualquiera de las reivindicaciones 8 a 12, en el que la aplicación de autenticación (130) incluye uno o más de:
un componente de visualización (236) para mostrar la transacción descifrada antes de firmar la transacción;
un componente de autorización (237) para realizar una etapa de autorización que incluye recibir una entrada de un usuario y verificar la entrada antes de firmar la transacción; y
un componente de control (241) para ceder el control localmente de vuelta a la primera aplicación después de transmitir la transacción firmada de vuelta al servidor seguro.

14. Un producto de programa informático para autenticación segura, comprendiendo el producto de programa informático un medio de almacenamiento legible por ordenador que tiene un código de programa legible por ordenador configurado para realizar las etapas:
recibir (309), a través de un controlador de protocolo de aplicación de autenticación (132), un identificador único para una transacción procedente de una primera aplicación (120) proporcionada en el mismo dispositivo de comunicación móvil (110) que la aplicación de autenticación (130), en el que el identificador único se envía localmente entre la primera aplicación (120) y la aplicación de autenticación (130) a través de un primer controlador de protocolo de aplicación (122) proporcionado en la primera aplicación (120) para invocar a la aplicación de autenticación (130);
recibir (311) una transacción cifrada procedente de un servidor seguro remoto (160);
descifrar (312) u obtener el descifrado de la transacción con una clave privada de la aplicación de autenticación (130);
firmar (315) u obtener la firma de la transacción con la clave privada;
firmar (315) la transacción con el identificador único recibido de la primera aplicación (120); y
transmitir (316) la transacción firmada de vuelta al servidor seguro remoto (160), en el que la aplicación de autenticación (130) se comunica con el servidor seguro remoto (160) a través de un protocolo seguro para la autenticación de la transacción.

15. El producto de programa informático según la reivindicación 14, en el que el producto de programa informático es un kit de desarrollo de software proporcionado para integrar procedimientos de autenticación en una aplicación de software.

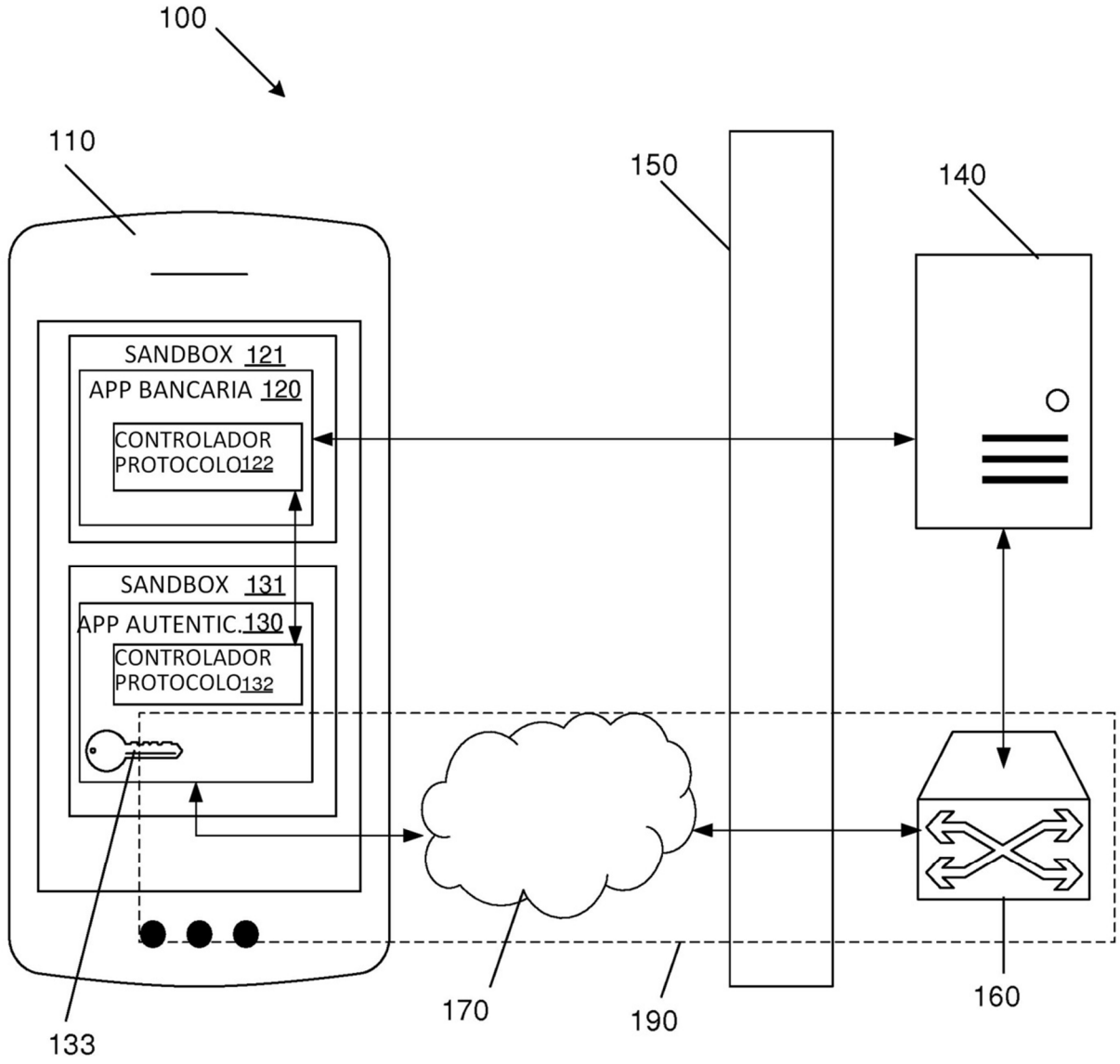
100
110
150
140
SANDBOX 121
APP BANCARIA 120
CONTROLADOR PROTOCOLO122
SANDBOX 131
APP AUTENTIC.130
CONTROLADOR PROTOCOLO132
133
170
190
160

FIG. 1A

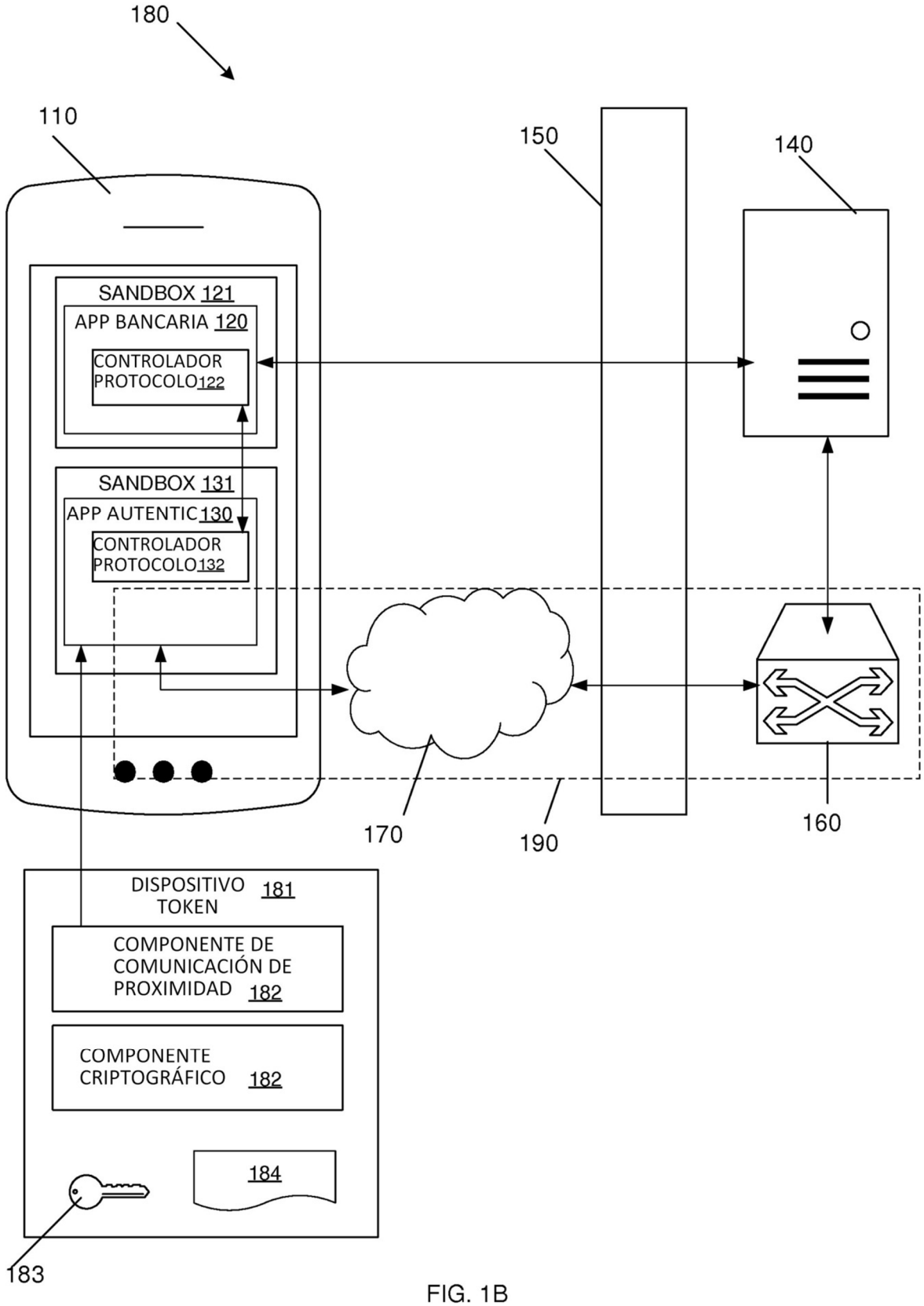
180
110
150
140
SANDBOX 121
APP BANCARIA 120
CONTROLADOR PROTOCOLO122
SANDBOX 131
APP AUTENTIC130
CONTROLADOR PROTOCOLO132
170
190
160
DISPOSITIVO TOKEN 181
COMPONENTE DE COMUNICACIÓN DE PROXIMIDAD 182
COMPONENTE CRIPTOGRÁFICO 182
184
183

FIG. 1B

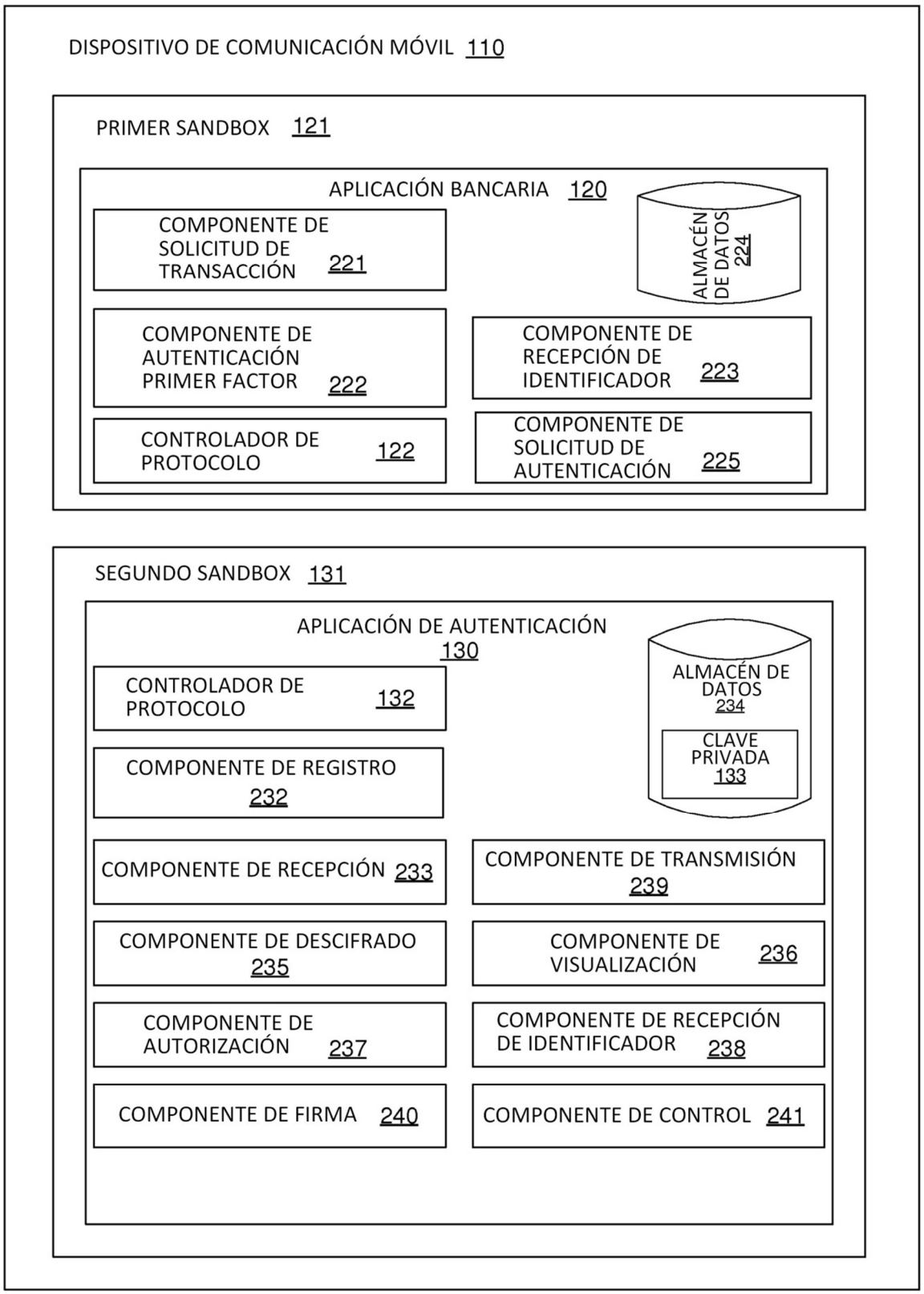
DISPOSITIVO DE COMUNICACIÓN MÓVIL 110
PRIMER SANDBOX 121
APLICACIÓN BANCARIA 120
COMPONENTE DE SOLICITUD DE TRANSACCIÓN 221
ALMACÉN DE DATOS 224
COMPONENTE DE AUTENTICACIÓN PRIMER FACTOR 222
COMPONENTE DE RECEPCIÓN DE IDENTIFICADOR 223
CONTROLADOR DE PROTOCOLO 122
COMPONENTE DE SOLICITUD DE AUTENTICACIÓN 225
SEGUNDO SANDBOX 131
APLICACIÓN DE AUTENTICACIÓN 130
CONTROLADOR DE PROTOCOLO 132
ALMACÉN DE DATOS 234
CLAVE PRIVADA 133
COMPONENTE DE REGISTRO 232
COMPONENTE DE RECEPCIÓN 233
COMPONENTE DE TRANSMISIÓN 239
COMPONENTE DE DESCIFRADO 235
COMPONENTE DE VISUALIZACIÓN 236
COMPONENTE DE AUTORIZACIÓN 237
COMPONENTE DE RECEPCIÓN DE IDENTIFICADOR 238
COMPONENTE DE FIRMA 240
COMPONENTE DE CONTROL 241

FIG. 2

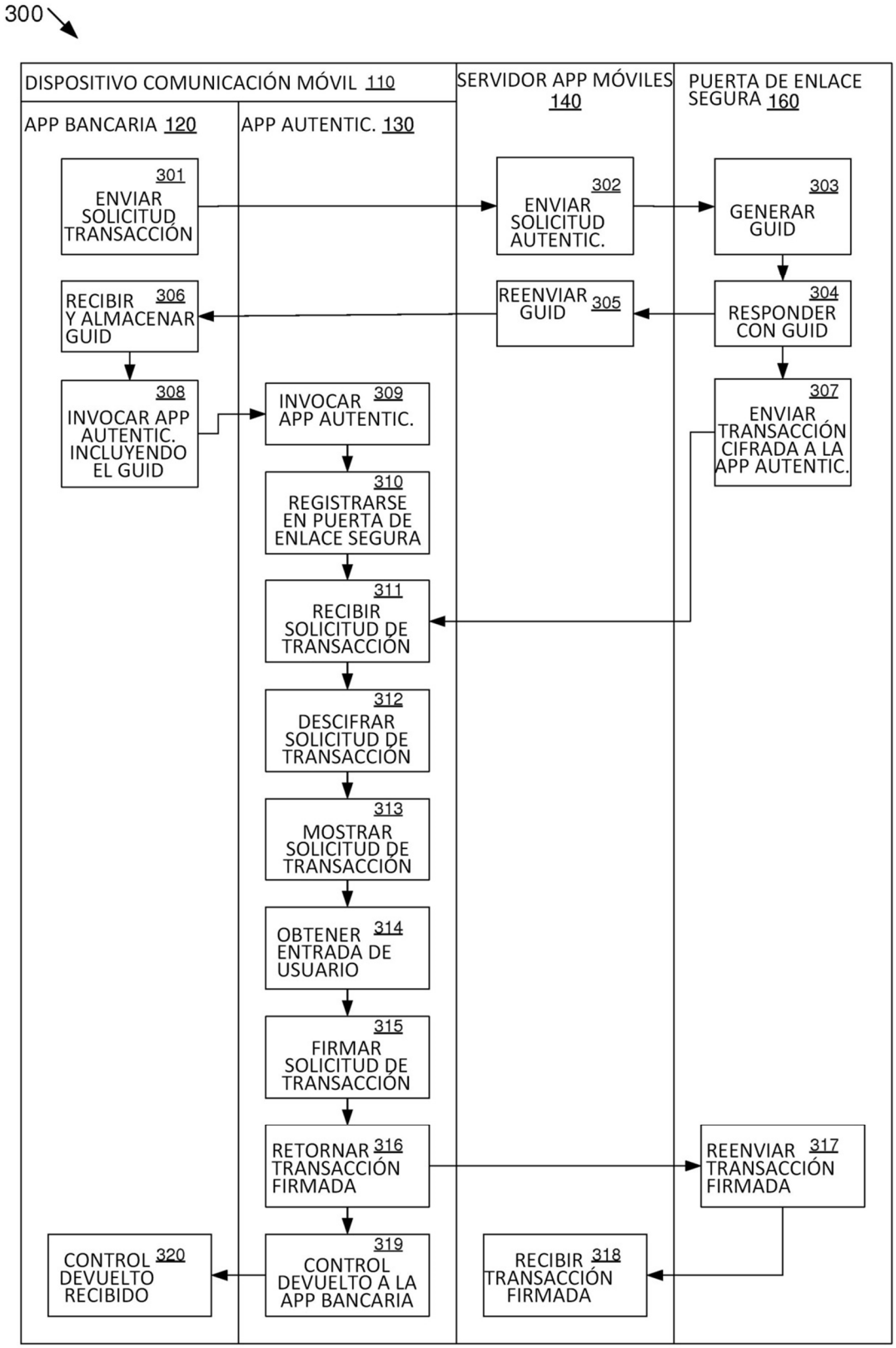
300
DISPOSITIVO COMUNICACIÓN MÓVIL 110
APP BANCARIA 120
APP AUTENTIC. 130
SERVIDOR APP MÓVILES 140
PUERTA DE ENLACE SEGURA 160
301 ENVIAR SOLICITUD TRANSACCIÓN
302 ENVIAR SOLICITUD AUTENTIC.
303 GENERAR GUID
304 RESPONDER CON GUID
305 REENVIAR GUID
306 RECIBIR Y ALMACENAR GUID
307 ENVIAR TRANSACCIÓN CIFRADA A LA APP AUTENTIC.
308 INVOCAR APP AUTENTIC. INCLUYENDO EL GUID
309 INVOCAR APP AUTENTIC.
310 REGISTRARSE EN PUERTA DE ENLACE SEGURA
311 RECIBIR SOLICITUD DE TRANSACCIÓN
312 DESCIFRAR SOLICITUD DE TRANSACCIÓN
313 MOSTRAR SOLICITUD DE TRANSACCIÓN
314 OBTENER ENTRADA DE USUARIO
315 FIRMAR SOLICITUD DE TRANSACCIÓN
316 RETORNAR TRANSACCIÓN FIRMADA
317 REENVIAR TRANSACCIÓN FIRMADA
318 RECIBIR TRANSACCIÓN FIRMADA
319 CONTROL DEVUELTO A LA APP BANCARIA
320 CONTROL DEVUELTO RECIBIDO

FIG. 3A

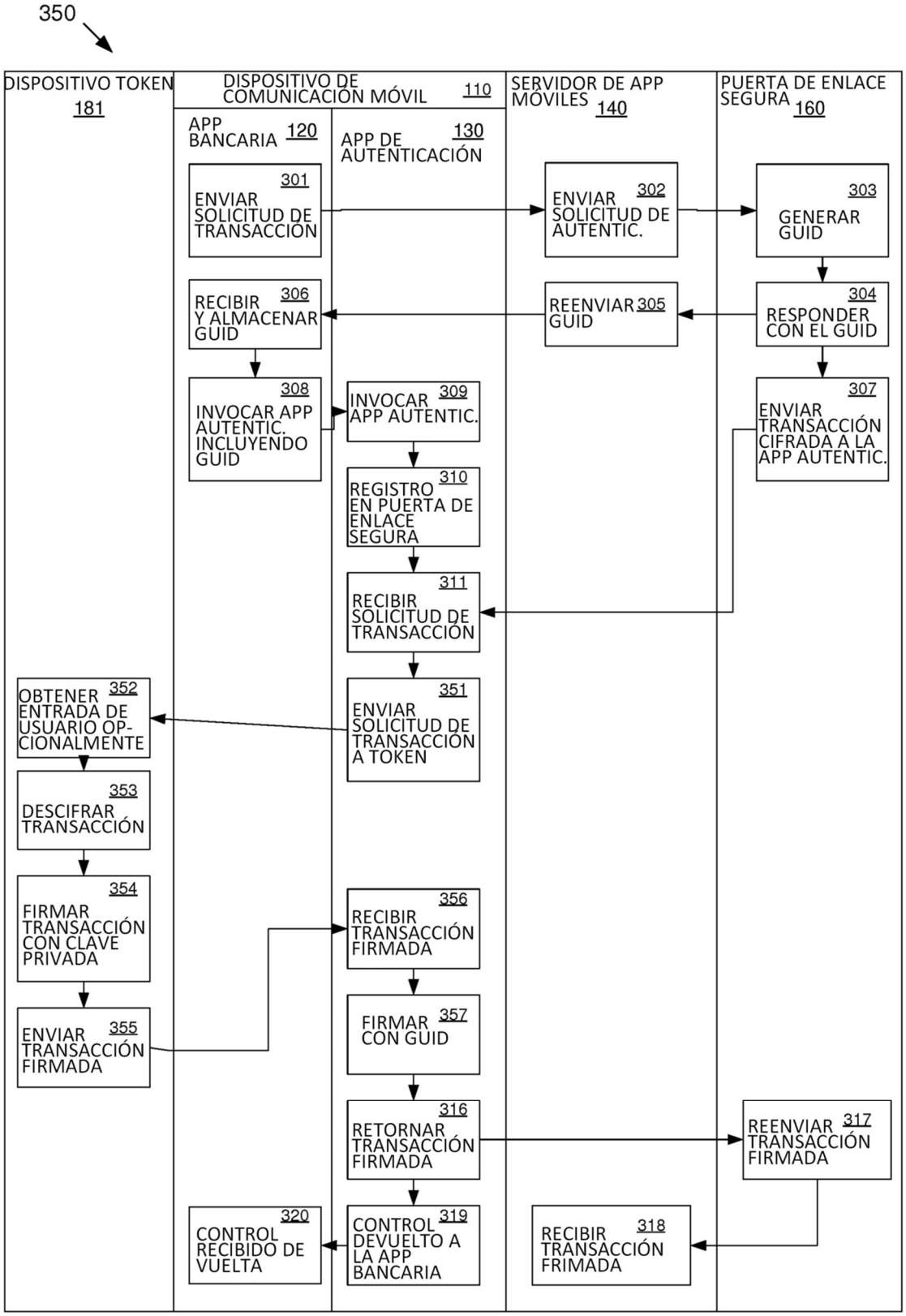
350
DISPOSITIVO TOKEN 181
DISPOSITIVO DE COMUNICACIÓN MÓVIL 110
APP BANCARIA 120
APP DE AUTENTICACIÓN 130
SERVIDOR DE APP MÓVILES 140
PUERTA DE ENLACE SEGURA 160
301 ENVIAR SOLICITUD DE TRANSACCIÓN
302 ENVIAR SOLICITUD DE AUTENTIC.
303 GENERAR GUID
304 RESPONDER CON EL GUID
305 REENVIAR GUID
306 RECIBIR Y ALMACENAR GUID
307 ENVIAR TRANSACCIÓN CIFRADA A LA APP AUTENTIC.
308 INVOCAR APP AUTENTIC. INCLUYENDO GUID
309 INVOCAR APP AUTENTIC.
310 REGISTRO EN PUERTA DE ENLACE SEGURA
311 RECIBIR SOLICITUD DE TRANSACCIÓN
351 ENVIAR SOLICITUD DE TRANSACCIÓN A TOKEN
352 OBTENER ENTRADA DE USUARIO OP-CIONALMENTE
353 DESCIFRAR TRANSACCIÓN
354 FIRMAR TRANSACCIÓN CON CLAVE PRIVADA
355 ENVIAR TRANSACCIÓN FIRMADA
356 RECIBIR TRANSACCIÓN FIRMADA
357 FIRMAR CON GUID
316 RETORNAR TRANSACCIÓN FIRMADA
317 REENVIAR TRANSACCIÓN FIRMADA
318 RECIBIR TRANSACCIÓN FRIMADA
319 CONTROL DEVUELTO A LA APP BANCARIA
320 CONTROL RECIBIDO DE VUELTA

FIG. 3B

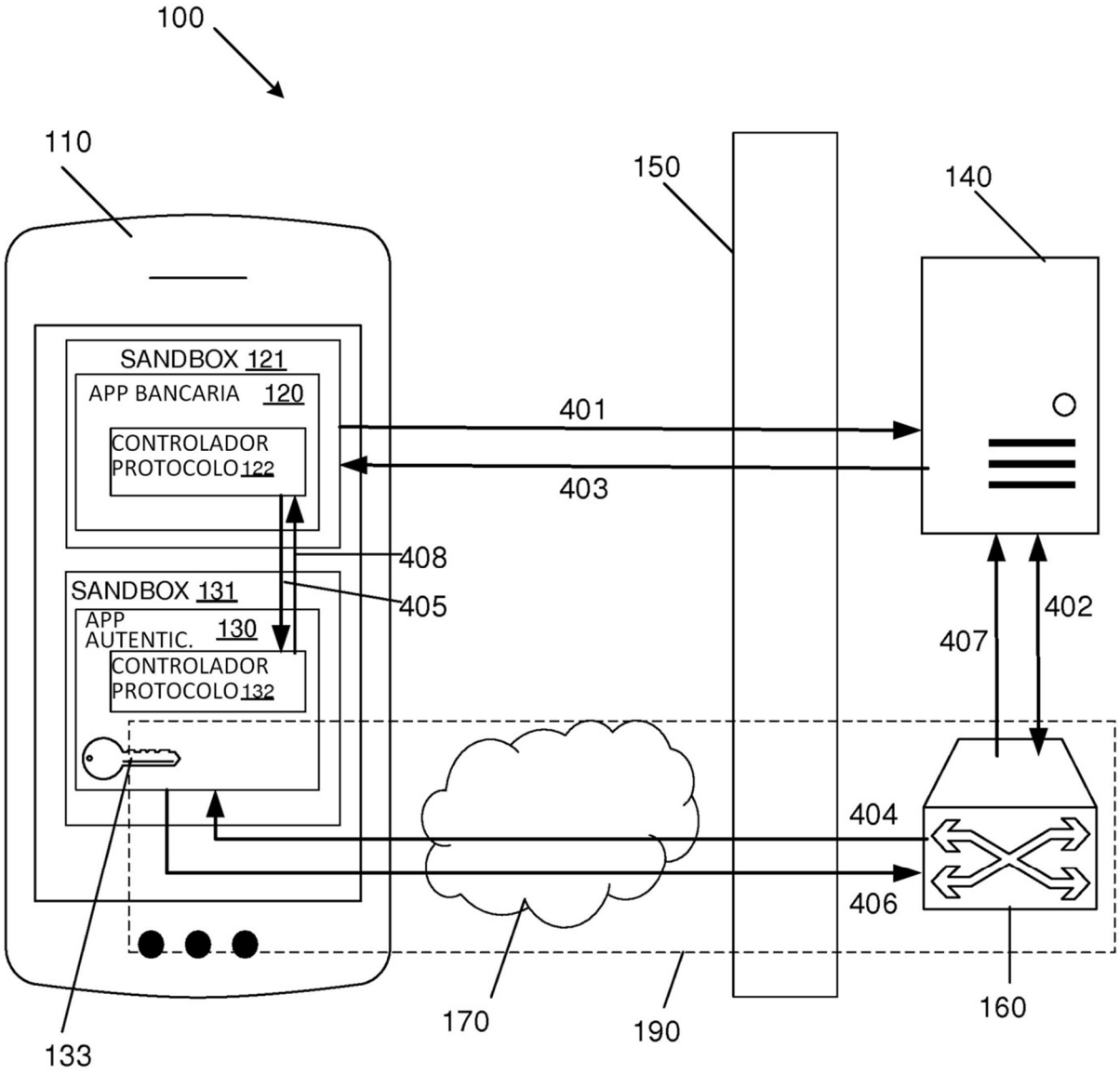
100
110
150
140
SANDBOX 121
APP BANCARIA 120
CONTROLADOR PROTOCOLO 122
401
403
408
405
SANDBOX 131
APP AUTENTIC. 130
CONTROLADOR PROTOCOLO 132
407
402
404
406
133
170
190
160

FIG. 4

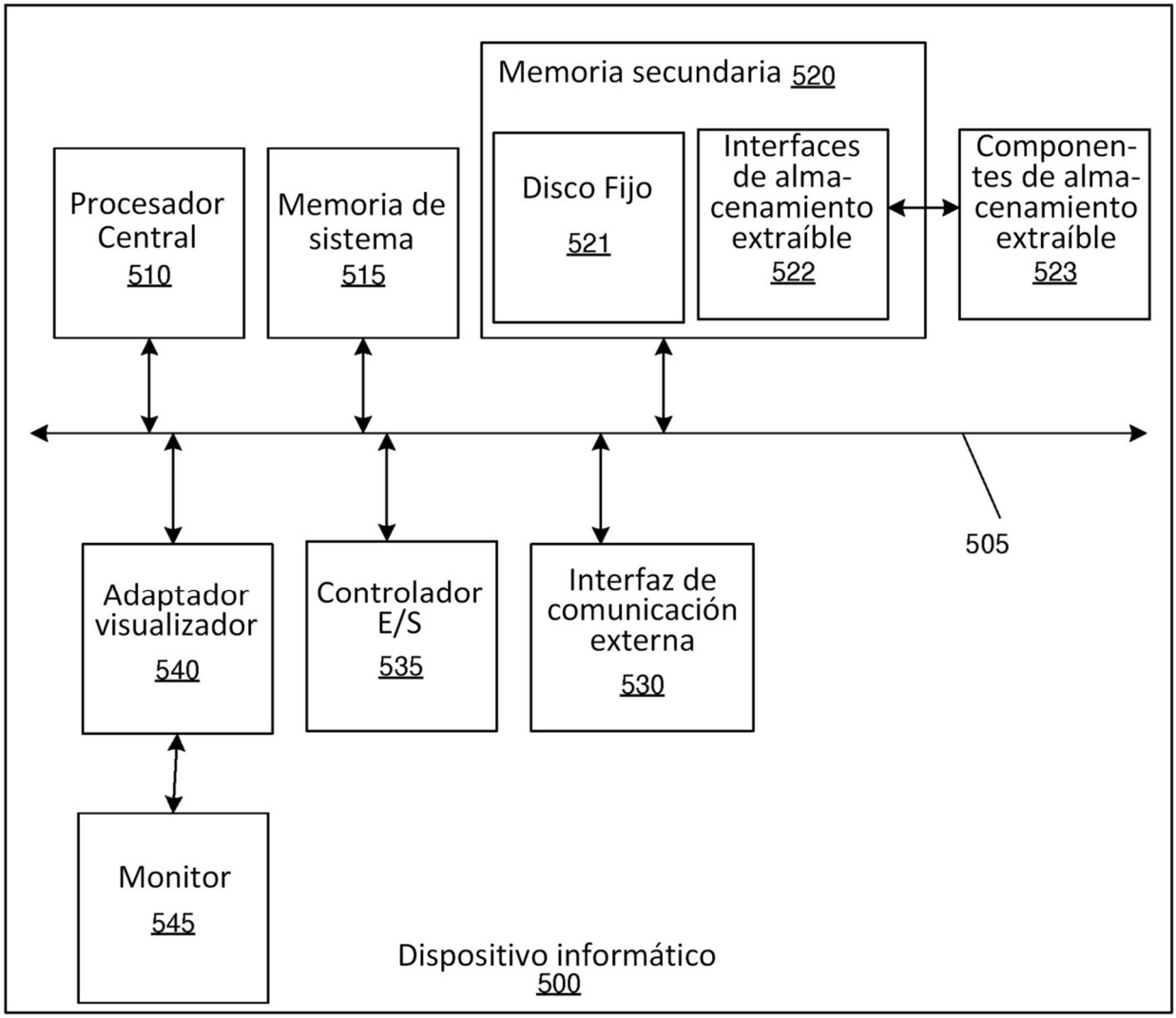
Memoria secundaria 520
Procesador Central 510
Memoria de sistema 515
Disco Fijo 521
Interfaces de alma-cenamiento extraíble 522
Componen-tes de alma-cenamiento extraíble 523
505
Adaptador visualizador 540
Controlador E/S 535
Interfaz de comunicación externa 530
Monitor 545
Dispositivo informático 500

FIG. 5

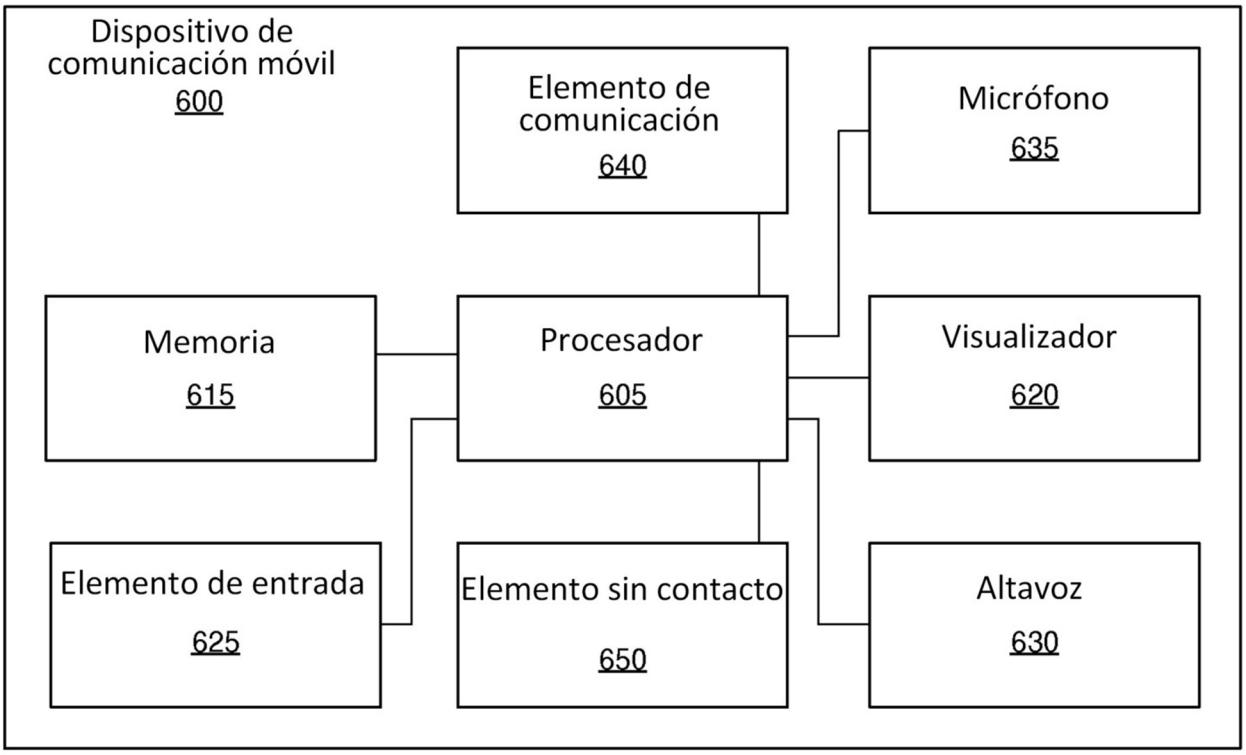
Dispositivo de comunicación móvil
600
Elemento de comunicación
640
Micrófono
635
Memoria
615
Procesador
605
Visualizador
620
Elemento de entrada
625
Elemento sin contacto
650
Altavoz
630

FIG. 6