(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 741 402**

(51) Int. CI.:

G06F 21/00	(2013.01)	***H04W 88/02***	(2009.01)
H04L 9/32	(2006.01)	***G06F 21/74***	(2013.01)
G06Q 20/40	(2012.01)		
H04W 12/06	(2009.01)		
G06F 21/32	(2013.01)		
G06F 21/35	(2013.01)		
G06F 21/42	(2013.01)		
H04L 29/06	(2006.01)		
G06F 21/53	(2013.01)		
G06Q 20/32	(2012.01)		

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **28.08.2015 PCT/US2015/047492**

(87) Fecha y número de publicación internacional: **03.03.2016 WO16033499**

(96) Fecha de presentación y número de la solicitud europea: **28.08.2015 E 15835740 (0)**

(97) Fecha y número de publicación de la concesión europea: **10.07.2019 EP 3186739**

(54) Título: **Autenticación segura de titulares de tarjetas, incorporada en el dispositivo, que hace uso de datos biométricos**

(30) Prioridad:

29.08.2014 US 201462043818 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
10.02.2020

(73) Titular/es:

MASTERCARD INTERNATIONAL INCORPORATED (100.0%)
2000 Purchase Street
Purchase, New York, NY 10577, US

(72) Inventor/es:

KAMAL, ASHFAQ;
REANY, BOB y
WILLIAMSON, GREGORY D.

(74) Agente/Representante:

ELZABURU, S.L.P

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

Autenticación segura de titulares de tarjetas, incorporada en el dispositivo, que hace uso de datos biométricos

Referencia cruzada con solicitud relacionada

Esta solicitud reivindica el beneficio de la solicitud de patente provisional de Estados Unidos n.º 62/043.818 presentada el 29 de agosto de 2015.

Campo de la invención

Las realizaciones se refieren, en general, a procesos de autenticación segura de titulares de tarjetas y que hacen uso de datos biométricos. En particular, las realizaciones se refieren al uso de un dispositivo móvil de consumidor para capturar datos biométricos de un usuario y para comparar los datos capturados con plantillas biométricas almacenadas localmente en el dispositivo móvil de consumidor de acuerdo con técnicas de autenticación multifactorial, segura, para autenticar un titular de una tarjeta.

Antecedentes

Cada vez más transacciones implican operaciones llevadas a cabo por un usuario en un dispositivo móvil. Uno de los ejemplos comunes de transacción es una transacción de pago (o transacción de compra), aunque un número elevado de otros tipos de transacciones se benefician de las técnicas mejoradas de autenticación descritas en la presente. Por comodidad, se describirán transacciones de pago aunque aquellos versados en la materia, tras la lectura de esta exposición, apreciarán que, con las técnicas de autenticación descritas en la presente, pueden usarse otros tipos de transacciones. En muchos tipos de transacción, es cada vez más importante autenticar al usuario involucrado en dichas transacciones. Normalmente, el usuario se autentica usando un número de identificación personal ("PIN") o similar. No obstante, está resultando cada vez más importante proporcionar capas de autenticación adicionales (a lo que se hace referencia, en la presente, como autenticación "multifactorial") para lograr una seguridad y una autenticación mejoradas.

En la actualidad, los emisores de tarjetas y otras entidades financieras ofrecen o usan protocolos de transacción por "internet" normalizados para mejorar el rendimiento y la seguridad de las transacciones en línea y para acelerar el crecimiento del comercio electrónico. Bajo algunos protocolos normalizados, los emisores de tarjetas de pago o entidades financieras (FIs) de emisión, tales como los bancos emisores, pueden autenticar transacciones reduciendo, así, la probabilidad de fraude y las devoluciones asociadas que se atribuyen a transacciones no autorizadas por el titular de la tarjeta. Uno de los ejemplos de un protocolo normalizado del tipo mencionado es el Protocolo 3-D Secure. La presencia de una transacción autenticada puede dar como resultado que un banco emisor asuma la responsabilidad del fraude en caso de que el mismo se produzca, a pesar de los esfuerzos por autenticar al titular de la tarjeta durante una compra en línea. Los comerciantes tienen la garantía, por parte de los emisores de tarjetas o entidades financieras (FIs) de emisión, tales como los bancos emisores, de que cobrarán por todas las transacciones autenticadas por el emisor. El protocolo 3-D Secure es consistente con los programas de autenticación ofrecidos por muchos emisores de tarjetas (por ejemplo, Verified de Visa o MasterCard SecureCode), y es la base de los mismos, para autenticar clientes ante comerciantes durante transacciones remotas, tales como aquellas asociadas a Internet.

El Protocolo 3-D Secure hace uso de la funcionalidad de cifrado de la Capa de Conexión Segura (SSL) existente y proporciona una seguridad mejorada a través de la autenticación del titular de la tarjeta por el emisor durante una sesión de compra en línea. Sería deseable proporcionar procesos de autenticación multifactorial y segura para autenticar a un usuario que utiliza un dispositivo de consumidor, en donde el dispositivo de consumidor se usa para capturar datos biométricos del usuario y comparar de manera segura los datos biométricos capturados con plantillas biométricas almacenadas con el fin de autenticar al usuario.

El documento US 2014/0189808 A1 describía un sistema de autenticación multifactorial e inicio de sesión completo para redes de servidor-cliente.

Compendio de la invención

El alcance de la presente invención queda definido por las reivindicaciones contenidas en la presente.

Breve descripción de los dibujos

Características y ventajas de algunas realizaciones, y la forma según la cual se logran las mismas, se pondrán más fácilmente de manifiesto en referencia a la siguiente descripción detallada considerada en combinación con los dibujos adjuntos, los cuales ilustran realizaciones a modo de ejemplo, y en donde:

la figura 1A es un diagrama de bloques de una parte de un sistema de transacciones para llevar a cabo un proceso de autenticación segura de usuario con un dispositivo móvil de consumidor de acuerdo con algunas realizaciones de la exposición;

la figura 1B es un diagrama de bloques de una realización de un dispositivo móvil de consumidor que ilustra aspectos de *hardware* que se pueden utilizar durante un procesado de autenticación de usuario de acuerdo con algunas realizaciones de la exposición;

la figura 2 es un diagrama de bloques de una parte de un sistema de transacciones para llevar a cabo un proceso de autenticación segura de usuario con un dispositivo móvil de consumidor de acuerdo con otra realización de la exposición;

la figura 3 es un diagrama de bloques de una parte de un sistema de transacciones para llevar a cabo un proceso de autenticación segura de usuario con un dispositivo móvil de consumidor de acuerdo todavía con otra realización de la exposición;

la figura 4 es un diagrama de bloques de una parte de un sistema de transacciones para llevar a cabo un proceso de autenticación segura de usuario con un dispositivo móvil de consumidor de acuerdo con una realización adicional de la exposición; y

la figura 5 es un diagrama de bloques de una parte de un sistema de transacciones para llevar a cabo un proceso de autenticación segura de usuario con un dispositivo móvil de consumidor de acuerdo todavía con otra realización adicional de la exposición.

Descripción detallada

En general, y con la finalidad de introducir conceptos de realizaciones novedosas descritas en la presente, se proporcionan sistemas, aparatos y métodos para llevar a cabo un proceso de autenticación segura de usuarios utilizando un dispositivo móvil de consumidor, tal como un teléfono inteligente, con vistas a autenticar un titular de una tarjeta durante una transacción, tal como una transacción financiera.

En la presente se usarán varios términos. El uso de dichos términos no está destinado a ser limitativo, sino que, por el contrario, los mismos se utilizan por comodidad y facilidad en la exposición. Por ejemplo, según se usa en la presente, el término “titular de tarjeta” se puede usar de forma intercambiable con el término “consumidor” y/o con el término “usuario”, y estos términos se usan en la presente para referirse a un consumidor, persona, individuo, negocio u otra entidad que sea propietaria de (o esté autorizada a usar) una cuenta financiera, tal como una cuenta de una tarjeta de pago (tal como una cuenta de una tarjeta de crédito) o algún otro tipo de cuenta (tal como una cuenta de una tarjeta de fidelización o una cuenta de acceso al transporte público). Además, el término “cuenta de tarjeta de pago” puede incluir una cuenta de tarjeta de crédito, una cuenta de tarjeta de débito y/o una cuenta de un depósito u otro tipo de cuenta financiera a la que pueda acceder el titular de una cuenta o el titular de una tarjeta. El término “número de cuenta de tarjeta de pago” incluye un número que identifica una cuenta de un sistema de tarjetas de pago o un número lleva una tarjeta de pago, y/o un número que se usa para encaminar una transacción en un sistema de pago que gestiona transacciones de tarjetas de débito y/o tarjetas de crédito y similares. Por otra parte, según se usa en la presente, los términos “sistema de tarjetas de pago” y/o “red de pago” se refieren a un sistema y/o red para procesar y/o gestionar transacciones de compra y transacciones relacionadas, que pueden ser llevadas a cabo por el operador de un sistema de tarjetas de pago tal como MasterCard International Incorporated, o un sistema similar. En algunas realizaciones, el término “sistema de tarjetas de pago” se puede limitar a sistemas en los cuales entidades financieras (tales como bancos) que son miembros de los mismos emiten cuentas de tarjetas de pago para individuos, negocios y/u otras entidades u organizaciones. Además, los términos “datos de transacciones del sistema de pago” y/o datos de transacciones de la red de pago, o “datos de transacciones de la tarjeta de pago” o “datos de transacciones de la red de tarjetas de pago” se refieren a datos de transacciones asociados a transacciones de pago o compra que se han procesado a través de una red de pagos o sistema de pagos. Por ejemplo, los datos de transacciones de un sistema de pagos pueden incluir una serie de registro de datos asociados a transacciones de pagos individuales (o transacciones de compra) de titulares de tarjetas, que se han procesado a través de un sistema de tarjetas de pago o red de tarjetas de pago. En algunas realizaciones, los datos de transacciones del sistema de pagos pueden incluir información que identifica a un titular de una tarjeta, a un dispositivo de pago o cuenta de pago del titular de una tarjeta, la fecha y la hora de una transacción, la cantidad de la transacción, mercancías o servicios que se han comprado, e información que identifica a un comerciante y/o una categoría de comerciante. En algunas realizaciones también puede haber disponibles detalles de transacción adicionales.

En algunas realizaciones, se dan a conocer técnicas y métodos mejorados de autenticación de titulares de tarjetas que proporcionan una experiencia de usuario mejorada para comerciantes y para usuarios o consumidores o titulares de tarjetas que usan dispositivos de consumidor. Por ejemplo, un proceso de autenticación segura de titulares de tarjetas incluye recibir, por parte de un dispositivo móvil de consumidor, una solicitud para autenticar un usuario desde una entidad en combinación con una transacción. A continuación, el dispositivo móvil de consumidor puede determinar por lo menos unos criterios de autenticación sobre la base de una política asociada a la entidad. En algunas implementaciones, seguidamente el dispositivo móvil de consumidor captura datos biométricos de usuario o de titular de tarjeta usando uno o más sensores biométricos del dispositivo móvil, compara los datos biométricos capturados con datos biométricos almacenados localmente de acuerdo con los criterios de autenticación y, a continuación, transmite una respuesta positiva de autenticación del titular de la tarjeta a la entidad cuando los

datos biométricos capturados del usuario coinciden con los datos biométricos almacenados localmente de acuerdo con los criterios de autenticación. Los datos biométricos almacenados localmente se pueden almacenar, por ejemplo, en un elemento de almacenamiento de un(os) sensor(es) biométrico(s), en un elemento de almacenamiento biométrico independiente del(de los) sensor(es) biométrico(s) (por ejemplo, el elemento de almacenamiento biométrico seguro puede ser un dispositivo de memoria que resida en un entorno de ejecución enriquecido), o en un elemento de almacenamiento biométrico seguro independiente del(de los) sensor(es) biométrico(s) (por ejemplo, el elemento de almacenamiento biométrico seguro puede ser un dispositivo de memoria que resida en un entorno de ejecución de confianza).

En algunas implementaciones, las técnicas de autenticación descritas en la presente pueden incluir niveles adicionales de autenticación de titulares de tarjetas. Los niveles adicionales de autenticación de titulares de tarjetas se pueden determinar y/o pueden ser requeridos por parte de, por ejemplo, una institución financiera emisora de tarjetas, y se pueden aplicar sobre la base de cada transacción individual. Dicha funcionalidad permite mejorar, en algunas situaciones, el nivel de autenticación de titulares de tarjetas requerido para cualquier transacción dada de una pluralidad de transacciones. Realizaciones descritas en la presente proporcionan una adopción mejorada de dichas técnicas y/o niveles de autenticación de titulares de tarjetas, así como una reducción ventajosa del número de transacciones denegadas que, de hecho, son transacciones legítimas sin presencia física de la tarjeta (dando como resultado una experiencia mejorada en las transacciones para titulares de las tarjetas aunque también beneficiando a comerciantes e instituciones financieras emisoras).

Según algunas realizaciones, para aprovechar los factores adicionales con vistas a una autenticación en transacciones en línea se puede usar el dispositivo móvil o dispositivo móvil de consumidor de un usuario o titular de tarjeta (tal como un teléfono inteligente, un ordenador de tipo tableta, un ordenador portátil, un asistente personal digital (PDA), un reproductor digital de música, o similares). Realizaciones utilizan una tecnología de autenticación segura residente en el dispositivo móvil de consumidor para aportar una experiencia de usuario óptima y proporcionar factores de autentificación por capas. Por ejemplo, con las configuraciones descritas en la presente del dispositivo móvil de consumidor se pueden utilizar tecnologías de autenticación, tales como biometría por huellas dactilares, biometría de reconocimiento facial, biometría de voz, y/u otros tipos de biometría. Realizaciones utilizan las configuraciones del dispositivo móvil de consumidor (que se describirán adicionalmente en la presente) para permitir el uso de una identificación del(de los) proceso(s) de autenticación del titular de tarjeta adecuado(s) para una transacción particular en relación con un usuario o titular de tarjeta dado.

El dispositivo móvil de consumidor se puede usar en combinación con una serie de tipos diferentes de procesos de transacción para proporcionar la autenticación adecuada del usuario o titular de tarjeta. Además, el dispositivo móvil de consumidor puede llevar a cabo localmente diferentes tipos de métodos de verificación de titulares de tarjeta (CVMs) para autenticar un usuario, en donde cualquier CVM particular puede depender de criterios especificados por cualquiera de una pluralidad de entidades. Por ejemplo, el Comerciante 1 puede requerir un CVM que requiera la introducción de un número de identificación personal móvil (mPIN) y la provisión de una huella dactilar para autenticar el usuario en relación con una transacción particular, mientras, para una transacción similar, el Comerciante 2 puede requerir un CVM que requiera al usuario que proporcione un escaneo de iris y datos faciales (de una fotografía del usuario). De acuerdo con procesos descritos en la presente, el dispositivo móvil del consumidor está equipado para gestionar requisitos de CVM diversos o diferentes del tipo mencionado haciendo que el usuario utilice uno o más sensores biométricos del dispositivo móvil de consumidor con el fin de proporcionar los datos biométricos de usuario requeridos. Y hacer que estos últimos se comparen con datos de autenticación de usuario almacenados localmente.

Durante la totalidad de esta exposición, se describirá un ejemplo de una transacción financiera. No obstante, aquellos versados en la materia apreciarán que realizaciones pueden usarse con resultados deseables para otros tipos de transacciones, tales como transacciones que permitan a un titular de una tarjeta acceder a un edificio y/o transacciones que permitan a titulares de tarjetas entrar en una estación de un sistema de transporte público, tal como una estación de metro o una estación de autobuses del transporte público.

A continuación, se hará referencia detalladamente a diversas realizaciones y/o implementaciones novedosas, cuyos ejemplos se ilustran en los dibujos adjuntos. Debe entenderse que los dibujos y sus descripciones no están destinados a limitar la invención a ninguna(s) realización(es) particular(es). Por el contrario, las descripciones proporcionadas en la presente están destinadas a cubrir alternativas, modificaciones, y equivalentes de las mismas. En la siguiente descripción, se exponen numerosos detalles específicos con el fin de proporcionar una comprensión minuciosa de las diversas realizaciones, pero algunas o la totalidad de estas realizaciones se pueden poner en práctica sin algunos o ninguno de los detalles específicos. En otros casos, operaciones bien conocidas de procesos no se han descrito de forma detallada con el fin de no complicar innecesariamente aspectos novedosos.

La figura 1A es un diagrama de bloques de una parte de un sistema 100 de transacciones que se puede utilizar para llevar a cabo un proceso de autenticación segura de usuarios o titulares de tarjeta de acuerdo con algunas realizaciones. Debe entenderse que un sistema de acuerdo con algunas realizaciones implica una serie de dispositivos y/o componentes y/o entidades que interactúan para llevar a cabo un proceso de autenticación de usuarios como parte de una transacción, tal como una transacción de pago. Por ejemplo, un usuario o titular de tarjeta puede actuar sobre un dispositivo móvil 102 de consumidor para interaccionar con un ordenador de una

entidad financiera (FI) emisora, el cual puede ser un ordenador servidor de un sistema de control de acceso de emisor (ACS) de emisor), con el fin de llevar a cabo un proceso de autenticación de usuarios según se da a conocer en la presente. De este modo, aunque, en la figura 1A, se muestra solamente un único dispositivo móvil de consumidor junto con una FI emisora 104A de acceso, un ordenador emisor 104B de *tokens*, y un "Otras" entidades 104N (cada una de las cuales puede ser un ordenador de ACS asociado a una entidad u organización diferente), en la práctica, en un sistema de transacciones del tipo mencionado de acuerdo con esta exposición, puede verse involucrado un número elevado de dichos dispositivos móviles de consumidor y/u otros componentes y/o dispositivos (que pueden incluir una red informática que incluya, por ejemplo, una pluralidad de ordenadores servidores interconectados). Las Otras entidades 104N pueden incluir, aunque sin carácter limitativo, proveedores de servicios financieros, tales como Apple Inc., Google Inc., y Amazon.com, Inc., los cuales pueden proporcionar, por ejemplo, servicios de pago en línea o remotos a consumidores y/o comerciantes.

Tal como se muestra en la figura 1A, el dispositivo móvil 102 de consumidor tiene una serie de componentes lógicos y/o funcionales (además de los componentes normales que se encuentran típicamente en un dispositivo móvil, tales como una antena, un(os) microprocesador(es) de dispositivo móvil, uno o más dispositivos de memoria y similares, que se explicarán posteriormente). Tal como se muestra, algunos de los componentes incluyen una aplicación móvil y/o explorador 106, que pueden ser proporcionados por un proveedor de red de pagos, tal como MasterCard International Incorporated, una interfaz de programación de aplicaciones (API) autenticadora 108, y por lo menos un sensor 110. En la realización mostrada en la figura 1A, cada uno de estos componentes (aplicación móvil/explorador 106, API autenticadora 108, y sensor 110) está configurado para funcionar en un entorno de ejecución enriquecido (REE) 112. El REE 112 es un entorno de procesado "normal" en donde se ejecutan el sistema operativo del dispositivo y otras aplicaciones. El sensor 110 representa uno o más sensores biométricos, tales como un sensor de huellas dactilares y/o un micrófono y/o una cámara, y cada uno de estos sensores está configurado para gestionar y/o administrar de manera segura la captura de datos biométricos, el almacenamiento de datos biométricos, y el cotejo de datos biométricos. En particular, el(los) sensor(es) biométrico(s) 110 funcionan para capturar datos de muestreo biométrico de un usuario con una aplicación 110A de captura biométrica, y, a continuación, utilizan una aplicación 110B de cotejo biométrico para intentar cotejar la muestra biométrica tomada del usuario con una o más plantillas biométricas que se han almacenado localmente en un componente 111 de almacenamiento. En particular, en la realización de la figura 1A, la(s) plantilla(s) biométrica(s) se almacenan de manera segura dentro del propio sensor biométrico 110, en el componente 111 de memoria segura del sensor, tal como se muestra.

La figura 1B es un diagrama de bloques de una realización de un dispositivo móvil 102 del usuario para ilustrar algunos aspectos de *hardware* del dispositivo que se pueden utilizar durante el procesado de autenticación segura del usuario de acuerdo con realizaciones descritas en la presente. En este ejemplo, el dispositivo móvil del usuario es un teléfono móvil 102 que puede tener (aunque no es necesario) capacidades para funcionar como dispositivo de pago sin contacto. En particular, el dispositivo móvil 102 del usuario puede ser un dispositivo móvil habilitado para pagos capaz de iniciar transacciones de pago en un sistema de tarjetas de pago. En sus aspectos de *hardware*, el teléfono móvil 102 puede utilizar componentes convencionales, y algunos de sus componentes o aspectos de *software* también pueden ser convencionales, aunque pueden estar configurados para proporcionar la funcionalidad novedosa que se describe en la presente. No obstante, en algunas otras realizaciones, la funcionalidad novedosa que se describe en la presente puede ser el resultado, al menos parcialmente, de *software* y/o microprogramas novedosos que programan o dan instrucciones a uno o más procesadores de dispositivo móvil correspondientes al teléfono móvil 102.

El teléfono móvil 102 puede incluir una carcasa convencional (indicada con la línea de trazos 120) que contiene y/o sustenta los otros componentes del teléfono móvil. El teléfono móvil 102 incluye un procesador principal 122 para controlar el funcionamiento global, por ejemplo, puede estar programado adecuadamente para permitir que el teléfono móvil 102 se involucre en comunicaciones de datos y/o mensajería de texto con otros dispositivos inalámbricos y/o dispositivos electrónicos, y para permitir una interacción con páginas web a las que se accede mediante *software* explorador a través de Internet, lo cual no se muestra de manera independiente. Otros componentes del teléfono móvil 102, que estén en comunicación con y/o son controlados por la circuitería 122 de control, incluyen uno o más dispositivos 124 de almacenamiento (por ejemplo, dispositivos de memoria de programas y/o memoria de trabajo y/o dispositivos de almacenamiento seguro, y similares), una tarjeta 126 de módulo de identificación de abonado (SIM) convencional, y un módulo 128 de visualización de pantalla táctil para visualizar información y/o para recibir entradas del usuario.

El teléfono móvil 102 incluye, también, circuitería 130 de recepción/transmisión convencional que está en comunicación también con y/o es controlada por el procesador principal 122. La circuitería 130 de recepción/transmisión está acoplada operativamente a una antena 132, y proporciona el(los) canal(es) de comunicación por medio del(de los) cual(es) se comunica el teléfono móvil a través de una red móvil (no mostrada). El teléfono móvil 102 incluye, además, un micrófono convencional 134 acoplado operativamente a la circuitería 130 de recepción/transmisión, pudiéndose hacer funcionar dicho micrófono 134 para recibir entrada de voz del usuario. Además, un altavoz 136 está también acoplado operativamente a la circuitería 130 de recepción/transmisión y proporciona una salida sonora al usuario.

El teléfono móvil 102 también puede incluir un controlador 138 de pago de proximidad que puede ser un circuito integrado (IC) o *chipset* del tipo incorporado comúnmente en tarjetas de pago sin contacto. El controlador 138 de

pago de proximidad está conectado operativamente a una antena 140 y puede funcionar para interaccionar con un lector de proximidad (no mostrado) de Identificación por Radiofrecuencia (RFID) y/o Comunicación de Campo Cercano (NFC), que puede estar asociado, por ejemplo, a un terminal de Punto de Venta (POS) de un comerciante. Por ejemplo, el controlador 138 de pago de proximidad puede proporcionar información, tal como el número de cuenta de la tarjeta de pago de un usuario, cuando el consumidor usa el teléfono móvil 102 para llevar a cabo una transacción de compra con un terminal de POS asociado a un comerciante.

El teléfono móvil 102 puede incluir uno o más sensores y/o circuitería que funciona para proporcionar y/u obtener datos de autenticación referentes al teléfono móvil y/o al usuario. En particular, el teléfono móvil 102 puede ser un teléfono inteligente que incluye una cámara integrada 142 conectada operativamente al procesador principal 122 y que se puede utilizar para diversas funciones. Por ejemplo, la cámara integrada 142 puede obtener imágenes, se puede hacer funcionar para leer un código de barras bidimensional (2D) con el fin de obtener información, y/o se puede hacer funcionar durante un proceso de autenticación para obtener una imagen de la cara del usuario y/o de otros elementos relevantes. El teléfono móvil 102 también puede incluir circuitería 144 del Sistema de Posicionamiento Global (GPS) conectada operativamente al procesador principal 122, y que se puede hacer funcionar para generar información referente a la ubicación del teléfono móvil.

El teléfono móvil 102 también puede incluir uno o más sensor(es) 146 de movimiento, un sensor 148 de huellas dactilares, y/o un sensor bioquímico 150. El(los) sensor(es) 146 de movimiento se pueden hacer funcionar para generar datos de movimiento, por ejemplo, que pueden ser utilizados por el procesador principal 122 para autenticar a un usuario mediante, por ejemplo, la identificación del modo de caminar o marcha del usuario. En otro ejemplo, el(los) sensor(es) 146 de movimiento pueden funcionar para generar datos de fuerza asociados a, por ejemplo, la fuerza generada por el dedo del usuario cuando el mismo toca la pantalla táctil 128. El sensor 148 de huellas dactilares puede incluir un panel táctil u otro componente (no mostrado) para ser usado por el usuario con el fin de que toque o se pase por su dedo índice cuando se requieren datos de huellas dactilares para autenticar al usuario con vistas a efectuar una transacción (tal como proporcionar entrada a un edificio). El sensor bioquímico 150 puede incluir uno o más componentes y/o sensores que se pueden hacer funcionar para obtener datos biológicos del usuario, tales como datos de respiración del usuario, y/u otros tipos de datos biológicos que puedan estar asociados al usuario del dispositivo móvil 120. Los datos obtenidos por el(los) sensor(es) 146 de movimiento, el sensor 148 de huellas dactilares y/o el sensor bioquímico 150, se pueden comparar con datos biométricos y/o información del usuario almacenados, por ejemplo, en uno o más del(de los) dispositivo(s) 124 de almacenamiento local con el fin de autenticar al usuario del teléfono móvil 102. Además, en algunas realizaciones, el procesador principal 122 y la circuitería 130 de receptor/transmisor se pueden hacer funcionar para transmitir los resultados del proceso de autenticación del titular de la tarjeta o usuario (háyase producido o no una coincidencia) a un ACS 104A de emisor (Véase la figura 1A) para un procesado adicional. El procesador principal 122 y la circuitería 130 de receptor/transmisor también se pueden hacer funcionar para transmitir datos GPS generados a un ACS de emisor en relación con la ubicación actual del dispositivo móvil. El dispositivo móvil del usuario también puede contener otro u otros tipos de sensores, tales como un dispositivo de escáner de iris (no mostrado) para generar datos de escaneo de iris del ojo de un usuario, los cuales pueden resultar útiles para identificar datos biométricos u otros datos personales del usuario del dispositivo móvil.

En algunas realizaciones, se puede requerir que un consumidor o usuario o titular de tarjeta participe en un proceso de registro del dispositivo móvil de consumidor y de inscripción para autenticación del usuario antes de que pueda producirse el procesado de autenticación del usuario de acuerdo con métodos descritos en la presente. En algunas implementaciones, un proceso de registro del tipo mencionado puede incluir que un usuario o consumidor o titular de tarjeta actúe sobre su dispositivo móvil de consumidor para interaccionar con uno o más sistemas o redes de procesado de pagos (no mostrados). Por ejemplo, en un ejemplo de red de procesado de pagos, un titular de tarjeta puede registrar información asociada a una entidad financiera asociada a la cuenta de pago del usuario o titular de tarjeta (tal como un banco emisor de tarjetas de crédito que emitió una cuenta de tarjeta de crédito y/o una cuenta de tarjeta de débito para el usuario o consumidor).

En un proceso ilustrativo de registro del dispositivo móvil e inscripción biométrica, una primera etapa de transacción puede incluir que el titular de la tarjeta dé órdenes a su dispositivo móvil para transmitir un mensaje de solicitud de registro o inscripción a un ordenador (no mostrado) del sistema de procesado de pagos para iniciar un proceso de registro. El usuario o titular de la tarjeta puede crear dicho mensaje de solicitud de inscripción para registrar el dispositivo móvil 102 de consumidor interactuando con la aplicación móvil 106 del dispositivo móvil. el mensaje de solicitud de registro se puede transmitir por medio de una red de comunicaciones, tal como Internet, a un servidor FIDO (u otro tipo de ordenador servidor) de una red de procesado de pagos para iniciar el registro del dispositivo móvil de consumidor y/o del usuario. A continuación, el servidor de la red de procesado de pagos puede generar y transmitir un mensaje de desafío para la solicitud de registro de consumidor hacia el dispositivo móvil del consumidor invitando al usuario a que proporcione datos biométricos para su uso en la autenticación de ese usuario. Por ejemplo, si el dispositivo móvil del consumidor incluye un sensor de huellas dactilares, tal como un componente lector de huellas dactilares, entonces puede invitarse al usuario a que coloque su pulgar o dedo índice en el lector de huellas dactilares con el fin de capturar ese tipo de datos biométricos. A continuación, los datos de huellas dactilares capturados se almacenarían localmente, por ejemplo, en un área de almacenamiento seguro del dispositivo móvil del consumidor. De acuerdo con métodos y realizaciones descritos en la presente y que se explicarán de manera adicional posteriormente, en algunas implementaciones dichos datos de huellas dactilares son almacenados

localmente por el propio sensor, y/o son almacenados en un dispositivo de almacenamiento seguro del dispositivo móvil de consumidor, y/o son cifrados y almacenados en un elemento de almacenamiento del dispositivo de consumidor. De este modo, en algunas realizaciones, además de almacenarse en un dispositivo de almacenamiento seguro y/o por parte del propio sensor, los datos biométricos también se pueden cifrar con fines relacionados con la seguridad.

En algunas realizaciones, el proceso de inscripción del usuario puede venir seguido por el registro, por parte de un usuario o titular de tarjeta, de una serie de elementos de datos biométricos, que pueden depender de los componentes y/o capacidades disponibles del dispositivo móvil de consumidor. Al usuario también se le puede permitir que registre una serie o pluralidad de dispositivos móviles de consumidor. Por otra parte, una vez que el usuario ha registrado un dispositivo móvil de consumidor y un conjunto de datos biométricos, esos datos de registro del usuario se pueden usar para autenticar al usuario en asociación con una pluralidad de diferentes tipos de transacciones, en donde cualquier transacción particular puede implicar o requerir un método de autenticación de usuario que sea diferente del correspondiente requerido por otro tipo de transacción. Como parte del proceso de inscripción del usuario, el usuario puede transmitir un identificador (ID) de dispositivo de consumidor y/o un número de directorio móvil ("MDN") desde el dispositivo móvil de consumidor a una entidad, tal como un servidor de una red de procesado de pagos o una entidad financiera emisora. En la configuración de sistema mostrada en la figura 1A, los datos biométricos (que pueden incluir, por ejemplo, uno o más de datos biométricos de huellas dactilares de usuario, una huella vocal, datos faciales, y otros datos tales como datos del pulso o similares), el ID de dispositivo, y el MDN se almacenan en o son almacenados por el propio sensor de manera que estos datos pueden ser recuperados y utilizados por el dispositivo móvil del usuario según se requiera cuando se lleve a cabo un procesado de autenticación del usuario.

En referencia nuevamente a la figura 1A, durante una transacción en donde se requiere la autenticación de un usuario, la entidad financiera (FI) emisora 104A, por ejemplo, puede transmitir una solicitud a la aplicación móvil 106 para realizar un proceso de autenticación biométrico del usuario del tipo en-nombre-de (OBO). (Debe entenderse que otra plataforma, u otra parte llamante de confianza como un ACS de emisor, puede realizar dicha solicitud de autenticación de usuario). El proceso de autenticación biométrica OBO puede estar predeterminado o dispuesto previamente por una entidad, tal como una red de procesado de pagos, y, ventajosamente, mejora y/o acelera el procesado de las transacciones ya que el procesado de autenticación del usuario es gestionado por el dispositivo móvil del consumidor en lugar de requerir la transmisión de datos de autenticación y su verificación por parte de, por ejemplo, un ordenador servidor remoto explotado por una entidad financiera emisora. Después de recibir la solicitud de autenticación OBO, la aplicación/exploración 106 de dispositivo móvil transmite una solicitud a uno o más sensores 110 para la captura de datos biométricos por medio de la API autenticadora expuesta 108. A continuación, la API autenticadora 108 implementa un mecanismo de control de acceso (no mostrado) que comprueba que la aplicación móvil 106 está autorizada a usar la API autenticadora 108. En algunas implementaciones, la API autenticadora 108 es también una Capa de Abstracción que abstrae partes llamantes a partir de las características de *hardware* de bajo nivel del(de los) sensor(es) biométrico(s) consiguiendo que el desarrollo y la interacción sean sin fisuras.

En referencia nuevamente a la figura 1A, si la aplicación móvil/explorador 106 está autorizado, entonces se invita al usuario (por ejemplo, mediante un mensaje visualizado en una pantalla de visualización del teléfono inteligente del consumidor) a que proporcione una o más formas de datos biométricos usando el(los) sensor(es) 110 que se encuentran en el dispositivo móvil 102 del consumidor. Por ejemplo, reglas comerciales predeterminadas en relación con la autenticación de un usuario para una compra que supere los cien dólares ($100) pueden requerir que un consumidor proporcione dos formas de datos biométricos (por ejemplo, una huella dactilar y una huella vocal). En este caso, cada uno de entre un sensor de huellas dactilares y un micrófono captura los propios datos biométricos, lleva a cabo un proceso de cotejo de los mismos, y a continuación los almacena. Si se produce una coincidencia para los datos biométricos de usuario capturados (tanto los datos de huellas dactilares como los datos de huella vocal) y la(s) plantilla(s) biométrica(s) (que se han generado y almacenado en el(los) sensor(es) durante la inscripción para autenticación del usuario y el registro del dispositivo), entonces se transmite de vuelta una respuesta de autenticación a la aplicación móvil/exploración 106 por medio de la API autenticadora 108 para su reenvío a la FI emisora 104A (o a otra parte llamante de confianza que realizó la solicitud de autenticación, tal como el Emisor 104B de *tokens*). De esta manera, puede utilizarse una técnica de autenticación multifactorial y segura en función del contexto y/o los atributos de una transacción particular.

La figura 2 es un diagrama de bloques de una parte de un sistema 200 de transacciones para llevar a cabo un proceso de autenticación segura de usuarios con un dispositivo 202 de consumidor de acuerdo con una segunda realización. Tal como se ha mencionado anteriormente, debe entenderse que un sistema acorde a las realizaciones descritas involucra una serie de dispositivos y/o componentes y/o entidades que interactúan para llevar a cabo un proceso de autenticación de usuarios como parte de una transacción, tal como una transacción de pago. Por ejemplo, un usuario o consumidor puede actuar sobre un dispositivo móvil 202 de consumidor para interaccionar con un ordenador 104A de una entidad financiera (FI) emisora, el cual puede ser un ordenador de un sistema de control de acceso de emisor (ACS de emisor), con el fin de llevar a cabo un proceso de autenticación de usuario según se da a conocer en la presente. De este modo, aunque, en la figura 2, se muestra solamente un único dispositivo móvil de consumidor junto con una única FI emisora 104A, un emisor 104B de *tokens*, y un Otras Entidades 104N (cada una de las cuales puede estar asociada a una entidad u organización diferente), en la práctica en un sistema de

acuerdo con esta exposición, puede verse involucrado un número elevado de dichos dispositivos de consumidor y FIs emisoras y/u ordenadores servidores del sistema de control de acceso y/u otros dispositivos.

En referencia a la figura 2, el dispositivo 202 de consumidor incluye una serie de componentes lógicos y/o funcionales (además de los componentes normales que se encuentran típicamente en un dispositivo móvil, tal como una antena, microprocesador(es), dispositivo(s) de memoria y similares según se ha explicado anteriormente en referencia a la figura 1A). Tal como se muestra, algunos de los componentes incluyen una aplicación móvil/explorador 204, que puede ser proporcionado por una entidad procesadora de cuentas de tarjeta de pago, y una interfaz de programación de aplicaciones (API) autenticadora 206. Tal como se muestra, los componentes de la aplicación móvil/explorador 204 y de la API autenticadora 206 están configurados para funcionar en un entorno de ejecución enriquecido (REE) 207. También se muestran en la figura 2 una aplicación autenticadora 208 de confianza y un sistema biométrico 210 de entorno de ejecución de confianza (TEE), los cuales están configurados para funcionar en un entorno de ejecución de confianza (TEE) 212.

El TEE 212 es un área segura que es independiente y/o está segregada del REE 207, y que puede residir, por ejemplo, en el procesador principal 122 de un dispositivo móvil 102 de consumidor (por ejemplo, véase la figura 1A). El TEE 212 garantiza que los datos sensibles se almacenan, se procesan y se protegen en un entorno de confianza. En algunas realizaciones, el TEE 212 es a prueba de manipulaciones indebidas ya que el TEE incluye una capacidad indicadora de manipulaciones indebidas (para la protección de manipulaciones indebidas), la cual es una función de seguridad deseada para almacenar credenciales de autenticación de titulares de tarjeta y/o credenciales de pago. La capacidad del TEE de ofrecer una ejecución segura de *software* de seguridad autorizado, al que, en ocasiones, se hace referencia como “aplicaciones de confianza”, permite que el TEE proporcione una seguridad de extremo-a-extremo imponiendo protección, confidencialidad, integridad y derechos de acceso a datos.

En referencia nuevamente a la figura 2, el sistema biométrico 210 de TEE representa uno o más sensores biométricos 214 que se ejecutan en el TEE, tales como un sensor de huellas dactilares y/o un micrófono y/o una cámara. Los sensores biométricos 214 pueden incluir *hardware* de sensores y aplicaciones de *software*, y pueden incluir uno o más microprocesadores conectados operativamente al(a los) sensor(es) y configurados para procesar y/o gestionar y/o administrar de manera segura procesos de captura 216 de datos biométricos, de cotejo 218 de datos biométricos, y de almacenamiento 220 de datos biométricos entre una o más muestras biométricas obtenidas a partir del usuario o titular de tarjeta y una o más plantillas biométricas que han sido almacenadas en los mismos.

También como se ha mencionado anteriormente, en algunas realizaciones se requiere que un titular de tarjeta o usuario participe en un proceso de registro del dispositivo de consumidor y de inscripción para autenticación del usuario antes de que pueda producirse un procesado de autenticación del usuario de acuerdo con uno o más de los métodos que se describen en la presente. En algunas implementaciones, un proceso de registro del tipo mencionado puede incluir que un usuario o titular de tarjeta haga funcionar su dispositivo móvil de consumidor para interaccionar con un o más sistemas o redes (no mostrados) de procesado de pagos, y para proporcionar información y/o datos con el fin de registrar su dispositivo de consumidor junto con una o más formas de datos biométricos con fines relacionados con la autenticación. El usuario o consumidor puede utilizar su dispositivo de consumidor para la inscripción o registro, y responder a un mensaje de desafío para solicitud de registro de consumidor de una entidad (tal como un ordenador servidor de procesador de pagos) que invita al usuario a que proporcione datos biométricos para su uso en la autenticación del consumidor a usuario. Con respecto a la configuración 202 del dispositivo móvil de consumidor que se muestra en la figura 2, los datos biométricos capturados durante el proceso de inscripción del usuario se almacenan en la parte 220 de almacenamiento del sistema biométrico 210 de TEE del dispositivo 202 de consumidor, y dichos datos biométricos pueden estar cifrados.

En general, el proceso de inscripción puede venir seguido por el registro, por parte de un usuario o consumidor, de una serie de elementos de datos biométricos, en función de las capacidades del dispositivo de consumidor, y también puede incluir la provisión de un identificador (ID) de dispositivo de consumidor y/o un número de directorio móvil (“MDN”) desde el dispositivo móvil del consumidor a, por ejemplo, un servidor de una red de procesado de pagos. En algunas realizaciones, los datos biométricos (que pueden incluir, por ejemplo, uno o más de datos biométricos de huellas digitales de usuario, datos de huella vocal, datos faciales, y otros tipos de datos biométricos, tales como datos del pulso y similares), el ID del dispositivo y el MDN se almacenan en un área de almacenamiento en el TEE por parte del dispositivo móvil de consumidor, de manera que estos datos sensibles pueden ser recuperados y utilizados según se requiera cuando se lleve a cabo el procesado de autenticación del usuario.

En referencia nuevamente a la figura 2, durante una transacción en donde se requiere una autenticación de un usuario, la FI emisora 104A, por ejemplo, puede transmitir una solicitud de autenticación de usuario a la aplicación móvil/explorador 204 que está funcionando en el entorno de ejecución enriquecido (REE) con el fin de llevar a cabo un proceso de autenticación biométrica del usuario de tipo en-nombre-de (OBO). (Debe entenderse que otra plataforma o parte llamante de confianza, en lugar de la FI emisora 104A, tal como el Emisor 104B de *tokens* puede realizar la solicitud de autenticación de usuario). El proceso particular de autenticación biométrica de usuarios OBO que se va a utilizar puede ser predeterminado o estar dispuesto previamente por una entidad, tal como una red de procesado de pagos. El proceso de autenticación biométrica de usuarios OBO sirve para mejorar y/o acelerar el procesado de las transacciones ya que el procesado de autenticación del usuario es gestionado por el dispositivo móvil del consumidor en lugar de, por ejemplo, por un servidor remoto asociado a una entidad financiera emisora.

Después de recibir la solicitud de autenticación OBO, la aplicación móvil/explorador 204 transmite una solicitud a la API autenticadora expuesta 206 (que funciona también en el REE) para que lleve a cabo un proceso de autenticación de usuario, y, en primer lugar, la API autenticadora implementa un mecanismo de control de acceso para comprobar si a la aplicación móvil se le permite usar la API autenticadora. Tal como se ha mencionado anteriormente, en algunas implementaciones, la API autenticadora 206 es también una capa de abstracción que abstrae partes llamantes a partir de las características de *hardware* de bajo nivel del(de los) sensor(es) biométrico(s) haciendo que el desarrollo y la interacción resulten sin fisuras. Por tanto, si la aplicación móvil está autorizada, entonces la API autenticadora 206 transmite la solicitud al sistema biométrico 210 de TEE (que está funcionando en el entorno de ejecución de confianza o TEE 212) para la captura y el procesado de datos biométricos usando uno o más sensores biométricos y otros componentes con el fin de autenticar el usuario. En algunas implementaciones, al usuario se le invita (por ejemplo, por medio de un mensaje visualizado en una pantalla de visualización del dispositivo móvil del consumidor, tal como un teléfono inteligente) a que proporcione una o más formas de datos biométricos usando el(los) sensor(es) que se encuentran en el dispositivo móvil del consumidor.

Por ejemplo, reglas comerciales predeterminadas y almacenadas en relación con la autenticación de un usuario para una compra inferior a $50 pueden requerir que un consumidor o usuario únicamente proporcione un tipo o una forma de datos biométricos (por ejemplo, datos faciales usando una cámara integrada en el dispositivo móvil del consumidor). En este caso, una cámara integrada del dispositivo del consumidor captura 216 una fotografía de la cara del usuario (conocida convencionalmente como “selfie”), y, a continuación, uno o más componentes del sistema biométrico 210 de TEE (que está funcionando en el entorno de ejecución de confianza) lleva a cabo un proceso 218 de cotejo y almacena los datos biométricos en un área 220 de almacenamiento del TEE 212. El resultado del proceso de autenticación se transmite desde el sistema biométrico 210 de TEE a la aplicación autenticadora 208 de confianza que se ejecuta dentro del TEE. Por ejemplo, si se produce una coincidencia para los datos biométricos de usuario capturados (es decir, los datos fotográficos coinciden con una plantilla almacenada en el componente de almacenamiento biométrico del TEE), entonces, la aplicación autenticadora 208 de confianza valida la confianza autenticando el sensor biométrico, y, a continuación, firma el mensaje de autenticación antes de enviarlo a la aplicación móvil/explorador 204 por medio de la API autenticadora 206. A continuación, la API autenticadora 206 transmite la respuesta de autenticación, por medio de la aplicación móvil/explorador 204, de vuelta a la FI emisora 104A (o a cualquiera otra parte llamante de confianza que realizó la solicitud de autenticación). Debe entenderse que esta técnica de autenticación multifactorial, segura, se puede utilizar de muchas maneras diferentes en función del contexto y/o los atributos de una transacción particular. Por ejemplo, pueden utilizarse diferentes criterios y/o reglas comerciales que dictaminan qué sensores biométricos diferentes y/o cuántos de ellos se usarán para una transacción particular. Dichos criterios y/o reglas comerciales pueden estar predeterminados por un tercero, tal como una entidad financiera emisora y/o una red de pagos.

La figura 3 es un diagrama de bloques de otra realización de una parte de un sistema 300 de transacciones para llevar a cabo un proceso de autenticación segura de usuarios. Tal como se ha mencionado anteriormente, realizaciones descritas pueden involucrar un número de dispositivos y/o componentes y/o entidades que interaccionan para llevar a cabo un proceso de autenticación de usuario como parte de una transacción, tal como una transacción de pago. De este modo, un usuario o consumidor puede actuar sobre un dispositivo móvil 302 de consumidor para interaccionar con un ordenador 104A de una entidad financiera (FI) emisora, que puede ser un ordenador de un sistema de control de acceso de emisor (ACS de emisor), con el fin de llevar a cabo un proceso de autenticación de usuario. De este modo, aunque, en la figura 3, se muestra solamente un único dispositivo móvil 302 de consumidor junto con una FI emisora 104A, un emisor 104B de *tokens*, y un ordenador 104N de Otras Entidades (cada una de las cuales puede estar asociada a una entidad u organización diferente), en la práctica, en el sistema global, puede verse involucrado un número elevado de dichos dispositivos móviles de consumidor y otros componentes y/o dispositivos.

En referencia a la figura 3, el dispositivo 302 de consumidor incluye una serie de componentes lógicos y/o funcionales (que pueden presentarse de manera adicional con respecto a los componentes normales de *software* y *hardware* que se encuentran típicamente en un dispositivo móvil, tales como un sistema operativo, una antena, microprocesador(es), dispositivo(s) de memoria y similares). Tal como se muestra, algunos de los componentes incluyen una aplicación móvil/explorador 304, que puede ser proporcionado por un procesador de cuentas de tarjetas de pago, una interfaz de programación de aplicaciones (API) autenticadora 306, y uno o más sensor(es) biométrico(s) 308. La aplicación móvil 304, el(los) sensor(es) biométrico(s) 308 y los componentes de la API autenticadora 306 funcionan en un entorno de ejecución enriquecido (REE) 310. En la figura 3 se muestran también una aplicación 310 de cotejo, una parte 312 de almacenamiento biométrico, y una aplicación autenticadora 314 de confianza, que funcionan, todas ellas, en un entorno de ejecución de confianza (TEE) 303. El sensor biométrico 308 representa uno o más sensores biométricos, tales como un sensor de huellas dactilares y/o un micrófono y/o una cámara. En la configuración de la figura 3, el(los) sensor(es) biométrico(s) 308 pueden incluir *hardware* y aplicaciones de *software* de sensores, que funcionan para capturar la información biométrica del usuario y almacenar esos datos biométricos durante un proceso de registro o inscripción del usuario, y actúan de manera que capturan datos biométricos de un usuario durante el proceso de autenticación del usuario.

Tal como se ha explicado anteriormente, algunas implementaciones requieren que un consumidor o usuario lleve a cabo un proceso de inscripción de usuario y de registro de dispositivo antes de que pueda producirse el procesado de autenticación de usuario de acuerdo con los métodos descritos en la presente. En algunas implementaciones, el

usuario o consumidor actúa sobre su dispositivo móvil de consumidor para interaccionar con uno o más sistemas o redes (no mostrados) de procesado de pagos con el fin de proporcionar información y/o datos para registrar su dispositivo móvil de consumidor junto con una o más formas de datos biométricos con fines destinados a la autenticación. De este modo, el usuario o consumidor puede utilizar su dispositivo móvil para inscribirse o registrarse, y responder a un mensaje de desafío para solicitud de registro de consumidor proveniente de una entidad (tal como un ordenador servidor de procesador de pagos) que invita al usuario a que proporcione datos biométricos para su uso en la autenticación de usuarios. Con respecto a la configuración del dispositivo móvil de consumidor mostrada en la figura 3, los datos biométricos capturados durante el proceso de inscripción se almacenan en la parte 312 de almacenamiento biométrico del TEE del dispositivo de consumidor, y dichos datos biométricos pueden estar cifrados.

En general, el proceso de inscripción puede venir seguido por el registro, por parte de un usuario o consumidor, de una serie de elementos de datos biométricos, en función de las capacidades del dispositivo de consumidor, y también pueden incluir la provisión de un identificador (ID) de dispositivo de consumidor y/o un número de directorio móvil ("MDN") desde el dispositivo móvil del consumidor a, por ejemplo, un servidor de una red de procesado de pagos. En algunas realizaciones, los datos biométricos (que pueden incluir, por ejemplo, uno o más de datos biométricos de huellas dactilares de usuario, una huella vocal, datos faciales, y otros datos tales como el pulso o similares), el ID de dispositivo y el MDN se almacenan en el área 312 de almacenamiento biométrico del TEE por parte del dispositivo móvil de consumidor, de manera que estos datos pueden ser recuperados y utilizados según se requiera cuando se lleve a cabo un procesado de autenticación.

En referencia nuevamente a la figura 3, durante una transacción en donde se requiere una autenticación de usuario, la FI emisora 104A, por ejemplo, puede transmitir una solicitud a la aplicación móvil 304 que está funcionando en el entorno de ejecución enriquecido (REE) para llevar a cabo un proceso de autenticación biométrica del tipo en-nombre-de (OBO). (Tal como se ha mencionado anteriormente, otra plataforma u otra parte llamante de confianza, en lugar de la FI emisora 104A, puede realizar la solicitud de autenticación). El proceso particular de autenticación biométrica de usuario OBO que se usará puede estar predeterminado o dispuesto previamente por una entidad, tal como una red de procesado de pagos, y mejora y/o acelera el procesado de las transacciones en comparación con métodos convencionales debido a que el proceso de autenticación es gestionado por el dispositivo móvil 302 del consumidor. Después de recibir la solicitud de autenticación OBO, la aplicación móvil/explorador 304 transmite una solicitud a la API autenticadora expuesta 306 (que funciona también en el REE) para llevar a cabo un proceso de autenticación de usuario, y, en primer lugar, la API autenticadora implementa un mecanismo de control de acceso para comprobar si se le permite a la aplicación móvil usar la API autenticadora. En caso afirmativo, entonces la API autenticadora 306 invita a un usuario (por ejemplo, mediante un mensaje visualizado en una pantalla de visualización del dispositivo móvil del consumidor) a que proporcione una o más formas de datos biométricos usando el(los) sensor(es) biométrico(s) asociado(s) al dispositivo móvil del consumidor, y da instrucciones al(a los) sensor(es) biométrico(s) 308 (que funcionan en el REE) para que capturen datos biométricos de usuario. A continuación, los datos biométricos de usuario capturados son transmitidos de manera segura por el(los) sensor(es) biométrico(s) 308 hacia la aplicación 310 de cotejo que está ejecutándose en el entorno de ejecución de confianza (TEE). En algunas realizaciones, la aplicación 310 de cotejo compara los datos de usuario biométricos capturados con una o más plantillas biométricas que están asociadas al usuario, y que están almacenadas en la parte 312 de almacenamiento biométrico situada dentro del TEE. Si el resultado de la comparación es una coincidencia, entonces la aplicación 310 de cotejo valida la confianza confirmando que los datos de usuario biométricos capturados provenían de un(unos) sensor(es) biométrico(s) reconocido(s), firma el resultado, y, a continuación, transmite el resultado del proceso de cotejo a la aplicación autenticadora 314 de confianza que se ejecuta dentro del TEE. A continuación, el(los) resultado(s) de coincidencia biométrica firmado(s) (verificado(s)) se comunican de vuelta a la aplicación móvil/explorador 304 por medio de la API autenticadora 306 para su transmisión de vuelta a la FI emisora 104A (u otra entidad de confianza que solicitase la autenticación del usuario).

Debe entenderse que, en algunas implementaciones, la aplicación móvil/explorador 304 únicamente recibe el resultado de la autenticación biométrica, y no recibe ninguno de los datos biométricos del titular de tarjeta. De este modo, los datos de usuario biométricos de titular de tarjeta almacenados localmente nunca abandonan los confines y/o los límites del TEE 303. Así, esta técnica de autenticación multifactorial, segura, se puede utilizar de muchas maneras diferentes en función del contexto y/o los atributos de una transacción particular (por ejemplo, utilizando criterios y/o reglas comerciales diferentes que gobiernan qué sensores biométricos diferentes y/o cuántos de ellos se utilizarán para un tipo particular de transacción).

La figura 4 es un diagrama de bloques de una parte de un sistema de transacciones para llevar a cabo un proceso de autenticación segura de usuarios de acuerdo todavía con otra realización. Esta realización descrita también puede involucrar una serie de dispositivos y/o componentes y/o entidades que interaccionan para efectuar un proceso de autenticación de usuario como parte de una transacción, tal como una transacción de pago. De este modo, un usuario o consumidor puede actuar sobre un dispositivo móvil 402 de consumidor para interaccionar con un ordenador 104A de una entidad financiera (FI) emisora, el cual puede ser un ordenador de un sistema de control de acceso de emisor (ACS de emisor), u otra entidad o plataforma para llevar a cabo un proceso de autenticación de usuario según se da a conocer en la presente. Así, aunque, en la figura 4, se muestra solamente un único dispositivo móvil 402 de consumidor junto con un ordenador 104A de FI emisora, un ordenador emisor 104B de *tokens*, y una pluralidad de ordenadores 104N de Otras Entidades (cada uno de los cuales puede estar asociado a una entidad u

organización diferente), en la práctica, en el sistema global, puede verse involucrado un número elevado de dichos dispositivos consumidores y/u otros componentes y/o dispositivos.

En referencia a la figura 4, el dispositivo móvil 402 de consumidor incluye una serie de componentes lógicos y/o funcionales (que se pueden presentar, además de los componentes normales de *software* y *hardware* que se encuentran típicamente en un dispositivo móvil del usuario, tales como un sistema operativo, una antena, microprocesador(es), dispositivo(s) de memoria y similares según se ha descrito anteriormente en la presente). Tal como se muestra, algunos de los componentes incluyen una aplicación móvil/explorador 404, que puede ser proporcionado por un procesador de cuentas de tarjeta de pago, una interfaz de programación de aplicaciones (API) autenticadora 406, uno o más sensor(es) biométrico(s) 408, y un área 410 de almacenamiento biométrico. Los componentes de la aplicación móvil 404, del(de los) sensor(es) biométrico(s) 408, del área 410 de almacenamiento biométrico, y de la API autenticador 306 funcionan en un entorno de ejecución enriquecido (REE) 403. En la figura 4 se muestran también una aplicación 412 de cotejo y una aplicación autenticadora 414 de confianza, que funcionan en un entorno de ejecución de confianza (TEE) 405. El sensor biométrico 408 representa uno o más sensores biométricos, tales como un sensor de huellas dactilares y/o un micrófono y/o una cámara. En la configuración mostrada en la figura 4, el(los) sensor(es) biométrico(s) pueden incluir *hardware* y aplicaciones de *software* de sensores, y funcionan para capturar datos biométricos de un usuario durante el proceso de autenticación de usuarios.

Tal como se ha explicado anteriormente, implementaciones del proceso de autenticación de usuarios requieren que un consumidor o usuario inscriba y registre su dispositivo de consumidor antes de que pueda producirse un procesado de autenticación de usuario de acuerdo con los métodos descritos en la presente. En algunas implementaciones, el usuario puede actuar sobre su dispositivo móvil de consumidor para interaccionar con uno o más sistemas de procesado de pago u otras redes (no mostradas) con el fin de proporcionar la información y/o datos para registrar su dispositivo de consumidor junto con una o más formas de datos de usuario biométricos con fines relacionados con la autenticación. De este modo, durante el proceso de registro, el usuario o consumidor puede utilizar su dispositivo móvil de consumidor para responder a un mensaje de desafío para solicitud de registro de consumidor proveniente de una entidad (tal como un ordenador de un servidor de un procesador de pagos) que invita al usuario a que proporcione datos biométricos para un uso posterior en un proceso de autenticación de usuarios. Con respecto a la configuración del dispositivo móvil de consumidor mostrada en la figura 4, los datos biométricos capturados durante el proceso de inscripción se cifran y, a continuación, se almacenan en la parte 410 de almacenamiento biométrico del REE del dispositivo móvil de consumidor.

En general, el proceso de inscripción seguido por un usuario o consumidor se puede usar para proporcionar una serie de elementos de datos biométricos asociados al usuario, que pueden depender de las capacidades del dispositivo móvil de consumidor. Al consumidor también se le puede invitar, por ejemplo, por parte de un servidor de una red de procesado de pagos, a que proporcione un identificador (ID) de dispositivo de consumidor y/o un número de directorio móvil ("MDN") desde el dispositivo móvil del consumidor. En algunas realizaciones, los datos biométricos del usuario (que pueden incluir, por ejemplo, uno o más de datos biométricos de huellas dactilares de usuario, una huella vocal, datos faciales, y otros datos, tales como el pulso o similares), el ID de dispositivo, y el MDN se pueden cifrar y, a continuación, almacenar en el área 410 de almacenamiento biométrico del REE por parte del dispositivo móvil de consumidor, de manera que estos datos pueden ser recuperados y utilizados según se requiera cuando se lleve a cabo el procesado de autenticación.

En referencia nuevamente a la figura 4, durante una transacción en donde se requiere una autenticación de usuario, el ordenador 104A de FI emisora, por ejemplo, puede transmitir una solicitud a la aplicación móvil 404 que funciona en el entorno de ejecución enriquecido (REE) para realizar un proceso de autenticación biométrica de tipo en-nombre-de (OBO). (Tal como se ha mencionado anteriormente, otra plataforma u otra parte llamante de confianza, en lugar del ordenador 104A de FI emisora, puede realizar la solicitud de autenticación). El proceso particular de autenticación biométrica OBO que se utilizará puede estar predeterminado o dispuesto previamente por la entidad que realiza la solicitud de autenticación, tal como una red de procesado de pagos, y sirve para mejorar y/o acelerar el procesado de las transacciones en comparación con procesos convencionales ya que el procesado de la autenticación es gestionado por el dispositivo móvil 402 del consumidor.

Después de recibir la solicitud de autenticación OBO, la aplicación móvil/explorador 404 transmite una solicitud a la API autenticadora expuesta 406 (que funciona también en el REE) para efectuar un proceso de autenticación de usuario, y la API autenticadora 405 en primer lugar implementa un mecanismo de control de acceso para comprobar si se le permite a la aplicación móvil/explorador 404 usar la API autenticadora. Cuando se toma la determinación de que se permite a la aplicación móvil/explorador 404 usar la API autenticadora 406, entonces la API autenticadora 406 invita a un usuario (por ejemplo, mediante un mensaje visualizado en una pantalla de visualización del ordenador tipo tableta del consumidor) a que proporcione una o más formas de datos biométricos usando uno o más sensor(es) 408 del dispositivo móvil del consumidor, y da instrucciones al(a los) sensor(es) biométrico(s) 408 (que funcionan en el REE 403) para capturar los datos de usuario biométricos ya que el usuario proporciona dichos datos utilizando uno o más sensores biométricos. A continuación, los datos de usuario biométricos capturados se pueden cifrar y transmitir sobre un canal autenticador seguro 409 por parte del(de los) sensor(es) biométrico(s) 408 a la aplicación 412 de cotejo que se está ejecutando en el entorno de ejecución de confianza (TEE) 405. En algunas realizaciones, la aplicación 412 de cotejo descifra los datos de usuario biométricos capturados, y los compara con

una o más plantillas biométricas almacenadas en la parte 410 de almacenamiento biométrico situada dentro del REE 402 (en algunas implementaciones, la aplicación 412 de cotejo debe, en primer lugar, descifrar las plantillas biométricas que están almacenadas en el área 410 de almacenamiento biométrico antes de realizar una o más comparaciones). Si el resultado de la comparación es una coincidencia, entonces la aplicación 412 de cotejo valida la confianza confirmando que los datos de usuario biométricos capturados procedieron de un(os) sensor(es) biométrico(s) reconocido(s) 408, firma el resultado, y, a continuación, transmite el resultado del proceso de cotejo a la aplicación autenticadora 414 de confianza que se ejecuta dentro del TEE 405. A continuación, el resultado de coincidencia biométrica firmado (verificado) se comunica de vuelta a la aplicación móvil 404 por medio de la API autenticadora 406 para su transmisión de vuelta al ACS 104A de emisor (u otra entidad de confianza que solicitase la autenticación de usuario). De este modo, esta técnica de autenticación multifactorial, segura, se puede utilizar de muchas maneras diferentes en función del contexto y/o los atributos de una transacción particular (por ejemplo, utilizando diferentes criterios y/o reglas comerciales que dictaminan qué sensores biométricos diferentes y/o cuántos de ellos se van a utilizar para una transacción particular).

La figura 5 es un diagrama de bloques de una parte de un sistema 500 de transacciones para llevar a cabo un proceso de autenticación segura de usuario con un dispositivo móvil 502 de consumidor en el contexto de la utilización de *tokens* de pago para una transacción de acuerdo con una realización. Tal como se ha mencionado anteriormente, debe entenderse que un sistema acorde a las realizaciones descritas involucra una serie de dispositivos y/o componentes y/o entidades que interaccionan para llevar a cabo un proceso de autenticación de usuario como parte de una transacción, tal como una transacción de pago. De este modo, aunque, en la figura 5, se muestra solamente un único dispositivo móvil 502 de consumidor junto con un ordenador 104A de FI emisora, un emisor 104B de *tokens*, y ordenadores 104N de Otras Entidades (cada uno de los cuales puede estar asociado a una entidad u organización diferente), en la práctica, en un sistema de acuerdo con esta exposición, puede verse involucrado un número elevado de dichos dispositivos móviles de consumidor y otros componentes y/o dispositivos.

En referencia a la figura 5, el dispositivo móvil 502 de consumidor incluye una serie de componentes lógicos y/o funcionales (además de los componentes normales que se encuentran típicamente en un dispositivo móvil, tales como una antena, un(os) microprocesador(es), un(os) dispositivo(s) de memoria y similares). Tal como se muestra, algunos de los componentes incluyen una aplicación móvil/explorador 504, que puede ser proporcionado por un procesador de cuentas de tarjetas de pago, y una interfaz de programación de aplicaciones (API) autenticadora 506. Los componentes de la aplicación móvil/explorador 504 y de la API autenticadora 506 están configurados para funcionar en un entorno de ejecución enriquecido (REE) 503. En la figura 5 se muestran también una aplicación autenticadora 508 de confianza, un sistema biométrico 510, y un depósito (*vault*) 512 de *tokens*, cuyos componentes están configurados para funcionar en un entorno de ejecución de confianza (TEE) 505. El sistema biométrico 510 de TEE representa uno o más sensores biométricos que se ejecutan en el TEE 505, tales como un sensor de huellas dactilares y/o un micrófono y/o una cámara. Los sensores biométricos pueden incluir *hardware* 518 de sensores y aplicaciones de *software*, y pueden incluir uno o más microprocesadores conectados operativamente al(a los) sensor(es), y configurados para procesar y/o gestionar y/o administrar de manera segura la captura 520 de datos biométricos, el cotejo 522 de datos biométricos entre una o más muestras biométricas tomadas del usuario o titular de tarjeta y una o más plantillas biométricas almacenadas, y el almacenamiento 524 de datos biométricos. Debe indicarse que el depósito 512 de *tokens* forma parte del dispositivo móvil de consumidor, por contraposición a muchos sistemas de autenticación convencionales que sitúan un depósito de *tokens* en un ordenador servidor de una entidad, tal como un proveedor tercero de servicios de autenticación.

Tal como se ha mencionado anteriormente también en la presente, en algunas realizaciones se requiere que un titular de tarjeta o usuario participe en un proceso de registro del dispositivo de consumidor y de inscripción para autenticación del usuario antes de que pueda producirse un procesado de autenticación de usuario de acuerdo con uno o más de los métodos descritos en la presente. En algunas implementaciones, un proceso de registro del tipo mencionado puede incluir que un usuario o titular de tarjeta haga funcionar su dispositivo móvil de consumidor para interaccionar con uno o más sistemas o redes (no mostrados) de procesado de pagos, y proporcionar información y/o datos con el fin de registrar su dispositivo de consumidor junto con una o más formas de datos biométricos con fines relacionados con la autenticación. El usuario o consumidor puede utilizar su dispositivo móvil de consumidor para inscribirse o registrarse, y responder a un mensaje de desafío para solicitud de registro de consumidor proveniente de una entidad (tal como un ordenador servidor de un procesador de pagos) que invita al usuario a que proporcione datos de usuario biométricos para su uso en la autenticación del usuario. Con respecto a la configuración del dispositivo móvil de consumidor mostrado en la figura 5, los datos biométricos capturados durante el proceso de inscripción se almacenan en el área 524 de almacenamiento del sistema biométrico 510 de TEE en el TEE 505 del dispositivo de consumidor, y dichos datos biométricos se pueden cifrar. Además, el usuario o titular de tarjeta puede interaccionar con un emisor 104B de *tokens* para obtener *tokens* de pago que se almacenan en el depósito 512 de *tokens* del TEE 505, en donde dichos *tokens* de pago se pueden usar durante una transacción de pago en línea (a la que se hace referencia, en ocasiones, como transacción “sin presencia física de tarjeta” o CNP 514) o durante una transacción 516 de pago “presencial” (F2F) que puede producirse, por ejemplo, en un terminal de punto de venta (POS) en una tienda minorista.

Debe entenderse que cada *token* almacenado en el depósito 512 de *tokens* del TEE 505 es exclusivo y confidencial entre comerciantes. Los *tokens* del depósito de *tokens* están también controlados en cuanto al dominio, lo cual significa que un *token* asociado al Comerciante “A” únicamente se puede usar para transacciones con el

Comerciante “A” y no para ninguna transacción con cualquier(cualesquiera) otro(s) comerciante(s). Además, en algunas realizaciones, cada *token* puede estar asociado a un tipo de diferente de proceso de autorización de usuario. Por ejemplo, un *token* asociado al Comerciante “B” puede requerir que el usuario del dispositivo móvil de consumidor proporcione datos de huellas dactilares, un número de identificación personal (PIN) y datos de voz con fines relacionados con la autenticación del usuario. No obstante, un *token* asociado al Comerciante “C” puede requerir que el usuario del dispositivo móvil de consumidor proporcione un número de identificación personal (PIN) y datos de escaneo del iris con fines relacionados con la autenticación del usuario.

El proceso de inscripción puede dar como resultado que el usuario o titular de tarjeta registre una serie de elementos de datos biométricos, en función de las capacidades del dispositivo móvil de consumidor, y también puede incluir la provisión de un identificador (ID) de dispositivo de consumidor y/o un número de directorio móvil (“MDN”) desde el dispositivo móvil del consumidor a, por ejemplo, un servidor de una red de procesado de pagos. En algunas realizaciones, los datos biométricos (que pueden incluir, por ejemplo, uno o más de datos biométricos de huellas dactilares de usuario, una huella vocal, datos faciales, y otros datos tales como el pulso o similares), el ID del dispositivo y el MDN se almacenan en un área de almacenamiento en el TEE 505 por parte del dispositivo móvil de consumidor, de manera que estos datos pueden recuperarse y utilizarse según se requiera cuando se lleva a cabo un procesado de autenticación.

En referencia nuevamente a la figura 5, si el titular de tarjeta desea usar *tokens* de pago durante una transacción de compra, entonces se requiere una autenticación del usuario, y, en algunas realizaciones, el usuario o titular de tarjeta puede utilizar la aplicación móvil/explorador 504 que está funcionando en el entorno de ejecución enriquecido (REE) 503 para llevar a cabo un proceso de autenticación biométrica. El proceso particular de autenticación biométrica que se utilizará puede estar predeterminado o dispuesto previamente por una entidad, tal como el emisor 104B de *tokens*, y sirve para mejorar y/o acelerar el procesado de las transacciones en comparación con procesos convencionales de autenticación ya que el procesado de autenticación es gestionado por el dispositivo móvil 502 del consumidor. Después de recibir la solicitud de autenticación de usuario, la aplicación/explorador 504 transmite una solicitud a la API autenticadora expuesta 506 (que funciona también en el REE) para llevar a cabo un proceso de autenticación de usuario, y la API autenticadora, en primer lugar, implementa un mecanismo de control de acceso para comprobar si se le permite a la aplicación móvil (o la misma dispone de permiso o autorización) usar la API autenticadora. Si la aplicación móvil está autorizada, entonces la API autenticadora 506 transmite la solicitud al sistema biométrico 510 de TEE (que funciona en el TEE 505) para la captura y el procesado de datos biométricos usando uno o más sensores biométricos y otros componentes con el fin de autenticar al usuario. En algunas implementaciones, se invita al usuario (por ejemplo, mediante un mensaje visualizado en una pantalla de visualización del dispositivo móvil del consumidor) a que proporcione una o más formas de datos biométricos usando el(los) sensor(es) que se encuentran en el dispositivo móvil 502 del consumidor. Seguidamente, uno o más componentes del sistema biométrico 510 de TEE (que funcione en el TEE 505) lleva a cabo un proceso de cotejo, y el resultado del proceso de autenticación se transmite desde el sistema biométrico 510 de TEE a la aplicación autenticadora 508 de confianza que se ejecuta dentro del TEE 505. Si se produjese una coincidencia para los datos biométricos de usuario capturados y los datos de usuario biométricos almacenados, entonces la aplicación autenticadora 508 de confianza valida la confianza autenticando el sensor biométrico, y, a continuación, puede firmar el mensaje de autenticación y enviarlo a la aplicación móvil/explorador 504 por medio de la API autenticadora 506. La aplicación autenticadora 508 de confianza también da órdenes al depósito 512 de *tokens* para que libere uno o más *tokens* de pago con el fin de satisfacer el pago correspondiente a una transacción CNP 514 y/o correspondiente a una transacción F2F 514. La API autenticadora 506 también puede transmitir la respuesta de autenticación, por ejemplo, al emisor 104B de *tokens*.

Se contempla que dicho procesado de autenticación de usuario en conjunción con un depósito de *tokens* se podría utilizar con las configuraciones de dispositivo móvil de consumidor mostradas en las figuras 3 y 4, y con otras configuraciones de dispositivo móvil de consumidor que tengan un TEE. También debería entenderse que esta técnica de autenticación multifactorial, segura, se puede utilizar de muchas maneras diferentes en un contexto de pago por *tokens* (por ejemplo, utilizando diferentes criterios y/o reglas comerciales que gobiernan qué sensores biométricos diferentes y/o cuántos de ellos se van a utilizar para una transacción particular).

Por lo tanto, de acuerdo con los procesos de autenticación segura de usuario descritos en la presente, los componentes de *hardware* y/o *software* de un dispositivo móvil de consumidor llevan a cabo una serie de operaciones, funciones o servicios tales como, por ejemplo, un método de registro de datos biométricos para autenticación de usuarios o titulares de tarjetas, un método garantizador de identificación biométrica, un método de autenticación biométrica y un servicio de atestiguación. El dispositivo móvil de consumidor también se puede configurar para proporcionar servicios y/o componentes (*hardware* y/o *software*) que proporcionen soporte para diferentes protocolos o técnicas de autenticación biométrica, tales como una tecnología de huella vocal, una tecnología de huellas dactilares, una tecnología de huella facial, una tecnología biométrica de iris (ojo), y similares. También se pueden proporcionar diferentes infraestructuras de tipo autenticador para proporcionar soporte para diferentes tipos de autenticador. Por ejemplo, se pueden proporcionar infraestructuras para técnicas de autenticación por huellas dactilares, por voz, faciales, por el pulso u otras técnicas biométricas. También se pueden proporcionar infraestructuras para diferentes tipos de dispositivo móvil (por ejemplo, diferentes marcas y modelos de teléfono móvil, que pueden ejecutar diferentes tipos de sistemas operativos, y/o similares) así como para diferentes componentes de *hardware* y *software*. El dispositivo móvil de consumidor también se puede configurar para

proporcionar datos y componentes asociados a diferentes infraestructuras garantizadoras de identificación que pueden incluir un administrador de políticas, analítica, puntuación y almacenamiento de datos de *tokens* para garantizar la identificación. Dichas subestructuras y componentes permiten que una amplia variedad de dispositivos móviles de consumidor proporcione un procesado de autenticación segura de usuario así como proporcionar acceso a una amplia variedad de usuarios de autenticación con el fin de interaccionar con vistas a proporcionar diferentes niveles de seguridad para la autenticación que pueden ser usados para una amplia variedad de diferentes transacciones.

Con respecto a las configuraciones del dispositivo móvil de consumidor de las figuras 1A y 2 a 4, una vez que el usuario ha sido autenticado, se puede devolver una confirmación de autenticación a la entidad financiera (FI) emisora o servicio de control de acceso (ACS) de emisor, la cual permite completar una transacción de pago. Además, las realizaciones descritas en la presente permiten usar la autenticación biométrica de usuarios del tipo mencionado en combinación con una amplia variedad de diferentes transacciones. Además, reglas comerciales y/u otros criterios pueden definir qué tipo de autenticación se va a usar en una transacción dada con un dispositivo móvil de consumidor dado. El resultado es un sistema y un método que proporcionan una autenticación multifactorial para su uso con dispositivos móviles de consumidor con el fin de llevar a cabo transacciones (o con el fin de proporcionar otros servicios, tales como entrar a un edificio y/o entrar en un sistema de transporte público y/o similares) y que incluye una amplia variedad de técnicas de autenticación.

No debe considerarse que las anteriores descripciones e ilustraciones de procesos en la presente implican un orden fijo para llevar a cabo las etapas de los procesos. Por el contrario, las etapas de los procesos se pueden llevar a cabo en cualquier orden que pueda ponerse en práctica, incluyendo una ejecución simultánea de al menos algunas etapas.

Aunque la presente invención se ha descrito en relación con realizaciones a modo de ejemplo específicas, debe entenderse que, en las realizaciones dadas a conocer, se pueden realizar varios cambios, sustituciones y modificaciones, claras para aquellos versados en la técnica, sin desviarse con respecto al alcance de la invención según se expone en las reivindicaciones adjuntas.

REIVINDICACIONES

1. Método de autenticación de usuarios de dispositivos móviles, que comprende:

recibir, por parte de una aplicación móvil (204; 304; 404; 504) que se ejecuta en un procesador (122) de dispositivo móvil de un dispositivo móvil (102) de consumidor, una solicitud de autenticación de usuario desde una entidad;

transmitir, por parte de la aplicación móvil mediante una interfaz de programación de aplicaciones “API” autenticadora (206; 306; 406; 506) que funciona en un entorno de ejecución enriquecido “REE” (207; 301; 403; 503) del dispositivo móvil de consumidor, a por lo menos un sensor biométrico del dispositivo móvil, una solicitud de captura de datos biométricos;

determinar, por parte de la API autenticadora mediante un mecanismo de control de acceso que se ejecuta en el procesador de dispositivo móvil, que la aplicación móvil está autorizada a utilizar la API autenticadora;

cuando se determina que la aplicación móvil está autorizada a utilizar la API autenticadora,

invitar, por parte del procesador de dispositivo móvil, al usuario del dispositivo móvil de consumidor a proporcionar por lo menos una forma de datos biométricos de acuerdo con reglas comerciales predeterminadas de la entidad; llevar a cabo, en un entorno de ejecución de confianza “TEE” del dispositivo móvil de consumidor, un proceso de autenticación, en donde una respuesta de autenticación de usuario como consecuencia del proceso de autenticación se transmite desde el TEE a una aplicación de autenticación de confianza que funciona en el TEE, y en donde el TEE comprende dicho por lo menos un sensor biométrico;

cuando la por lo menos una forma de datos biométricos proporcionada por el usuario coincide con datos biométricos almacenados localmente, validar, por parte de la aplicación autenticadora de confianza que funciona en el entorno de ejecución de confianza “TEE” (212; 303; 405; 505) del dispositivo móvil de consumidor, la respuesta de autenticación de usuario del por lo menos un sensor biométrico autenticando el por lo menos un sensor biométrico;

firmar, por parte de la aplicación autenticadora de confianza, la respuesta de autenticación de usuario validada;

transmitir, por parte de la aplicación autenticadora de confianza, la respuesta de autenticación de usuario firmada a la API autenticadora que funciona en el REE del dispositivo móvil de consumidor;

recibir, por parte de la aplicación móvil mediante la API autenticadora, la respuesta de autenticación de usuario firmada cuando la por lo menos una forma de datos biométricos proporcionada por el usuario coincide con los datos biométricos almacenados localmente;

generar, por parte de la aplicación móvil que se ejecuta en el procesador de dispositivo móvil del dispositivo móvil de consumidor, un mensaje de respuesta de autenticación de usuario positiva basándose en la respuesta de autenticación de usuario firmada; y

transmitir, por parte de la aplicación móvil a la entidad, el mensaje de respuesta de autenticación de usuario positiva.

2. Método de la reivindicación 1, en donde la solicitud de captura de datos biométricos se basa en criterios de autenticación requeridos por la entidad.

3. Método de la reivindicación 2, en donde los criterios de autenticación comprenden obtener por lo menos dos formas diferentes de datos biométricos del usuario utilizando por lo menos dos sensores biométricos diferentes.

4. Método de la reivindicación 2, en donde los criterios de autenticación se basan en un tipo de transacción que es efectuada por el usuario.

5. Método de la reivindicación 1, en donde la entidad comprende uno de un servidor de control de acceso, un ordenador de una entidad financiera emisora, y una red de pagos.

6. Método de la reivindicación 1, en donde la aplicación móvil y el por lo menos un sensor biométrico (308; 408) funcionan en el REE del dispositivo móvil de consumidor.

7. Método de la reivindicación 1, en donde el por lo menos un sensor biométrico (214; 518) funciona en el TEE del dispositivo móvil de consumidor.

8. Método de la reivindicación 1, en donde la API autenticadora y el por lo menos un sensor biométrico (308; 408) funcionan en el REE del dispositivo móvil de consumidor, y que comprende, además, antes de la validación por parte de la aplicación autenticadora de confianza:

transmitir, por parte del por lo menos un sensor biométrico a una aplicación (310; 412) de cotejo que funciona en el TEE del dispositivo móvil de consumidor, datos biométricos capturados del usuario del dispositivo móvil de

consumidor;

comparar, por parte de la aplicación de cotejo, los datos de usuario biométricos capturados con por lo menos una plantilla biométrica asociada al usuario y que está almacenada en una parte de almacenamiento biométrico del TEE; y

transmitir, por parte de la aplicación de cotejo a la aplicación autenticadora de confianza que funciona en el TEE, la respuesta de autenticación de usuario cuando los datos de usuario biométricos capturados coinciden con la por lo menos una plantilla biométrica.

9. Método de la reivindicación 1, en donde la API autenticadora, el por lo menos un sensor biométrico (408), y una parte (410) de almacenamiento biométrico funcionan en el REE del dispositivo móvil de consumidor, y en donde la parte de almacenamiento biométrico almacena plantillas biométricas de usuario cifradas, y que comprende, además, antes de la validación por parte de la aplicación autenticadora de confianza:

capturar y cifrar, por parte del por lo menos un sensor biométrico, datos biométricos proporcionados por el usuario del dispositivo móvil de consumidor;

transmitir, por parte del por lo menos un sensor biométrico a una aplicación (412) de cotejo que funciona en el TEE del dispositivo móvil de consumidor, los datos biométricos capturados y cifrados del usuario;

descifrar, por parte de la aplicación de cotejo, los datos biométricos capturados y cifrados del usuario;

obtener, por parte de la aplicación de cotejo, por lo menos una plantilla biométrica cifrada asociada al usuario y que está almacenada en la parte de almacenamiento biométrico del REE;

descifrar, por parte de la aplicación de cotejo, la por lo menos una plantilla biométrica cifrada;

comparar, por parte de la aplicación de cotejo, los datos de usuario biométricos capturados y descifrados con la por lo menos una plantilla biométrica descifrada; y

transmitir, por parte de la aplicación de cotejo a la aplicación autenticadora de confianza que funciona en el TEE, la respuesta de autenticación de usuario cuando los datos de usuario biométricos capturados y descifrados coinciden con la por lo menos una plantilla biométrica descifrada.

10. Método de la reivindicación 9, en donde la transmisión de los datos de usuario biométricos capturados comprende, además, utilizar un canal autenticado seguro (409) entre el por lo menos un sensor biométrico y la aplicación de cotejo que funciona en el TEE.

11. Método de la reivindicación 1, en donde la entidad es un emisor de *tokens* y la aplicación móvil y la API autenticadora funcionan en el REE, y el por lo menos un sensor biométrico (518) funciona en el TEE del dispositivo móvil de consumidor, y que comprende, además, antes de la transmisión de la respuesta de autenticación de usuario firmada:

dar instrucciones, por parte de la aplicación autenticadora de confianza, a un depósito (512) de *tokens* para que libere por lo menos un *token* de pago con el fin de satisfacer el pago correspondiente a una transacción que utiliza la aplicación móvil.

12. Método de la reivindicación 11, que comprende, además, dar instrucciones, por parte de la aplicación autenticadora de confianza, al depósito (512) de *tokens* que funciona en el TEE, para liberar por lo menos un *token* de pago con el fin de satisfacer el pago correspondiente a una de una transacción sin presencia física de la tarjeta “CNP” o para una transacción presencial “F2F”.

13. Método de la reivindicación 11, que comprende, además, transmitir, por parte de la API autenticadora por medio de la aplicación móvil, la respuesta de autenticación de usuario al emisor de *tokens*.

14. Sistema de transacciones que comprende:

por lo menos un ordenador de una entidad financiera “FI” emisora;

una pluralidad de ordenadores de entidad; y

un dispositivo móvil de consumidor configurado para comunicarse con el por lo menos un ordenador de FI emisora y la pluralidad de ordenadores de entidad, que comprende:

un procesador de dispositivo móvil;

por lo menos un dispositivo de almacenamiento;

circuitería de recepción y transmisión; y

por lo menos un sensor biométrico;

en donde el dispositivo móvil de consumidor comprende, además, una aplicación móvil, una interfaz de programación de aplicaciones “API” autenticadora que funciona en un entorno de ejecución enriquecido “REE” del dispositivo móvil de consumidor, una aplicación autenticadora de confianza que funciona en un entorno de ejecución enriquecido “TEE” del dispositivo móvil de consumidor, y un mecanismo de control de acceso que se ejecuta en el procesador de dispositivo móvil;

y en donde el por lo menos un medio de almacenamiento del dispositivo móvil de consumidor comprende instrucciones configuradas para conseguir que el procesador del dispositivo móvil lleve a cabo el método de cualquier reivindicación anterior.

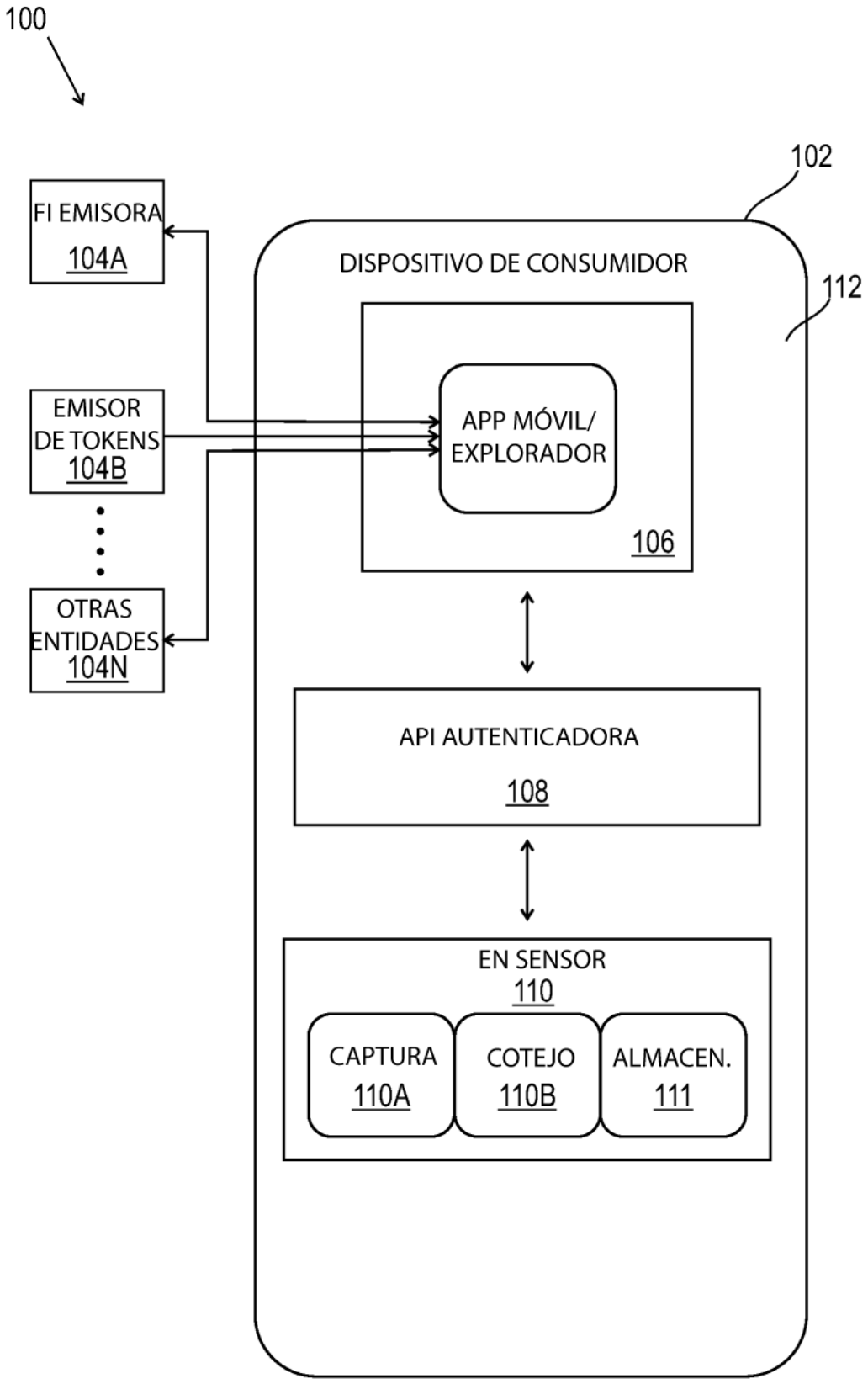
100
102
FI EMISORA
104A
DISPOSITIVO DE CONSUMIDOR
112
EMISOR
DE TOKENS
104B
APP MÓVIL/
EXPLORADOR
106
OTRAS
ENTIDADES
104N
API AUTENTICADORA
108
EN SENSOR
110
CAPTURA
110A
COTEJO
110B
ALMACEN.
111

FIG. 1A

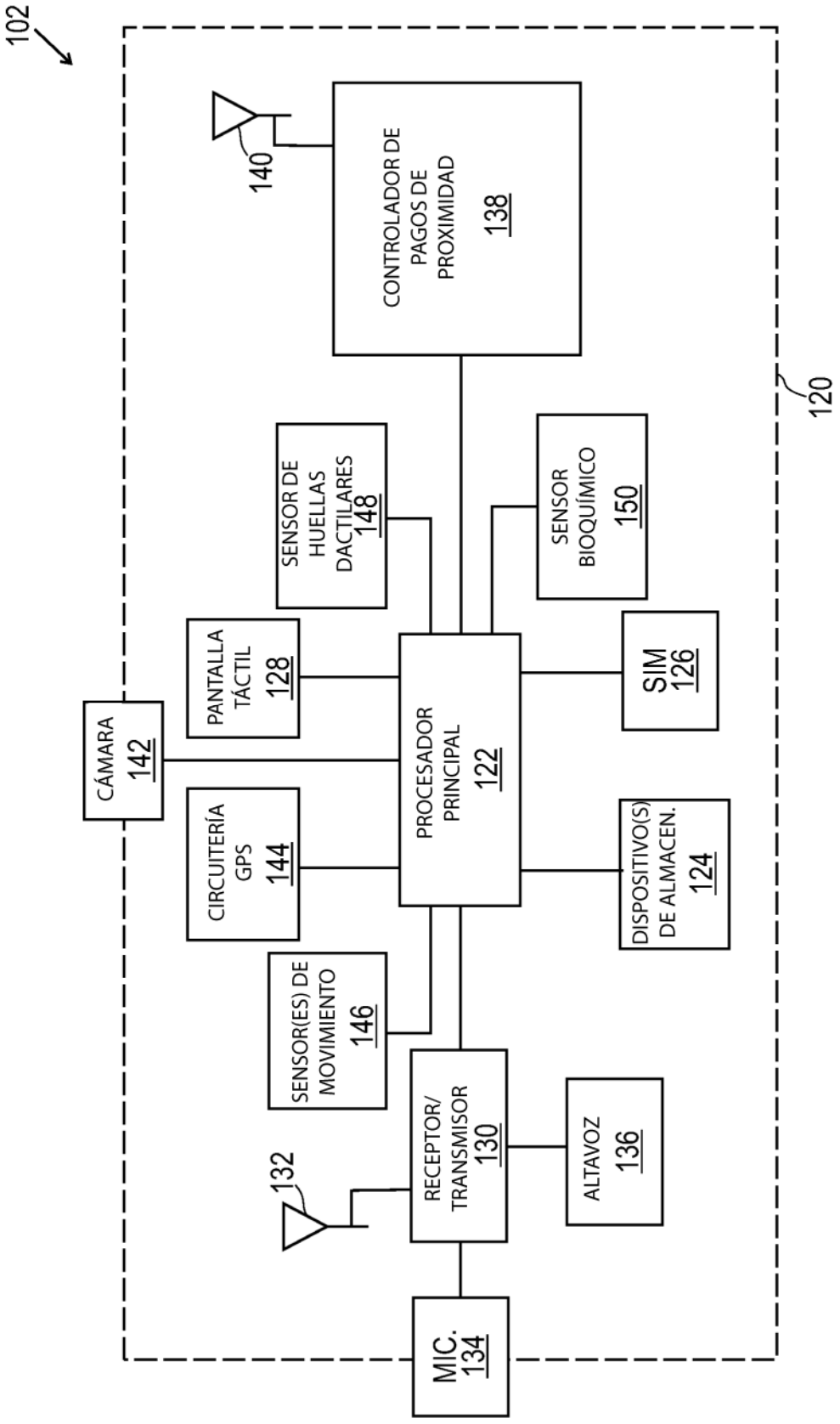
102
120
140
CONTROLADOR DE PAGOS DE PROXIMIDAD 138
SENSOR DE HUELLAS DACTILARES 148
SENSOR BIOQUÍMICO 150
PANTALLA TÁCTIL 128
SIM 126
CÁMARA 142
PROCESADOR PRINCIPAL 122
CIRCUITERÍA GPS 144
DISPOSITIVO(S) DE ALMACEN. 124
SENSOR(ES) DE MOVIMIENTO 146
132
RECEPTOR/ TRANSMISOR 130
ALTAVOZ 136
MIC. 134

FIG. 1B

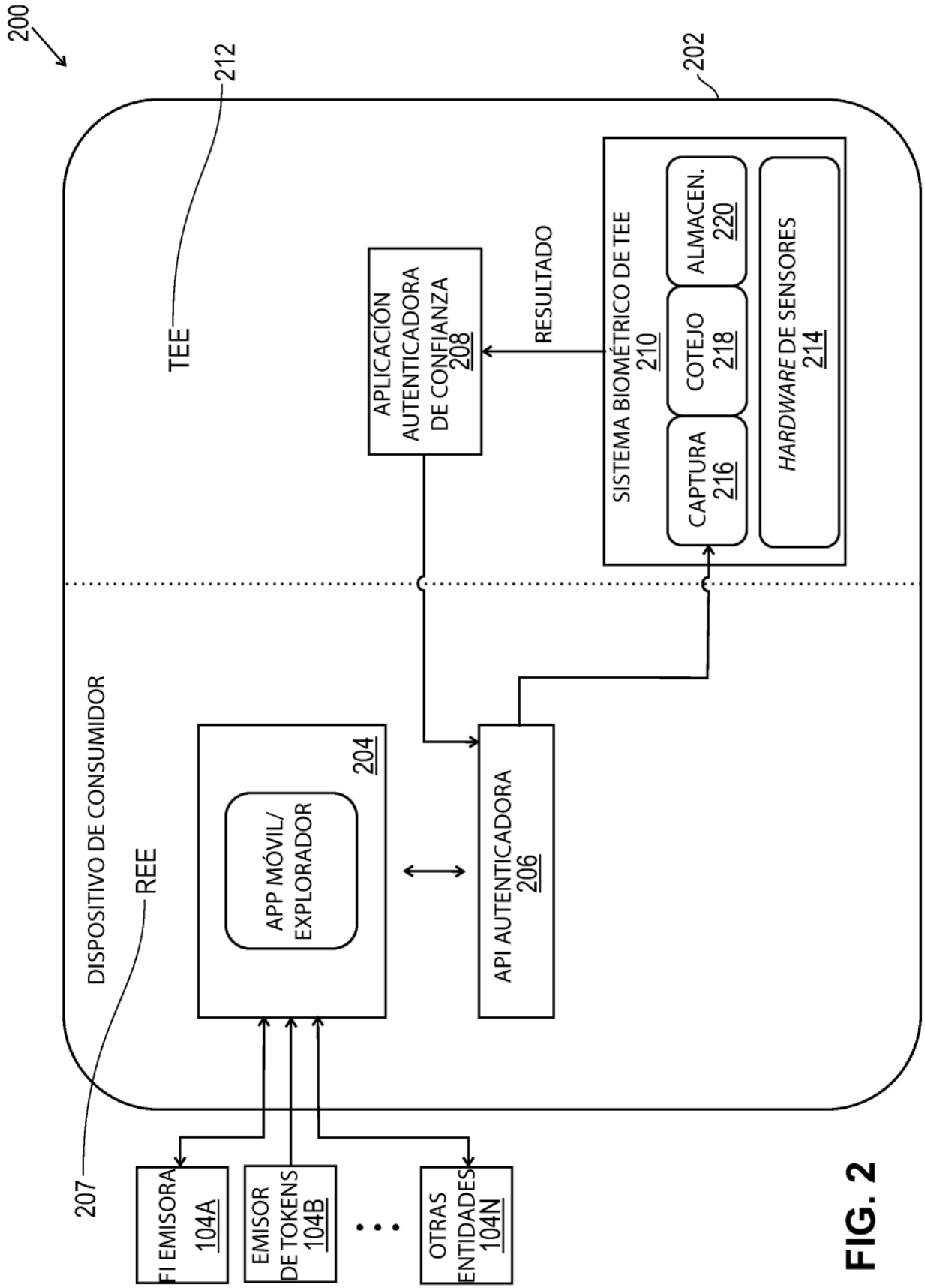
200
212
202
TEE
APLICACIÓN AUTENTICADORA DE CONFIANZA 208
RESULTADO
SISTEMA BIOMÉTRICO DE TEE 210
CAPTURA 216
COTEJO 218
ALMACEN. 220
HARDWARE DE SENSORES 214
DISPOSITIVO DE CONSUMIDOR
REE
APP MÓVIL/ EXPLORADOR
204
API AUTENTICADORA 206
207
FI EMISORA 104A
EMISOR DE TOKENS 104B
OTRAS ENTIDADES 104N

FIG. 2

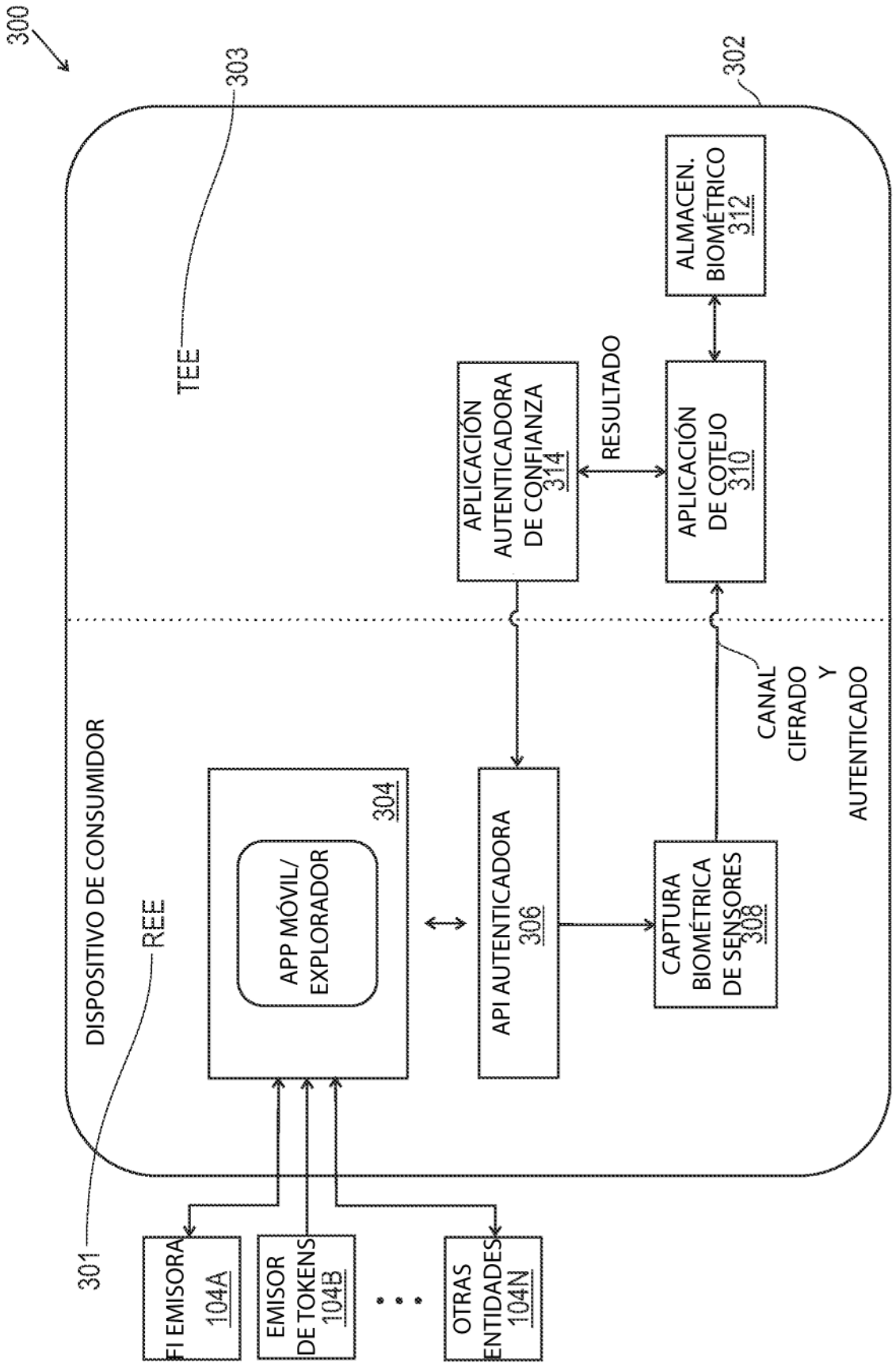
300
303
302
TEE
ALMACEN. BIOMÉTRICO 312
APLICACIÓN AUTENTICADORA DE CONFIANZA 314
RESULTADO
APLICACIÓN DE COTEJO 310
DISPOSITIVO DE CONSUMIDOR
CANAL CIFRADO Y AUTENTICADO
304
APP MÓVIL/ EXPLORADOR
API AUTENTICADORA 306
CAPTURA BIOMÉTRICA DE SENSORES 308
REE
301
FI EMISORA 104A
EMISOR DE TOKENS 104B
OTRAS ENTIDADES 104N

FIG. 3

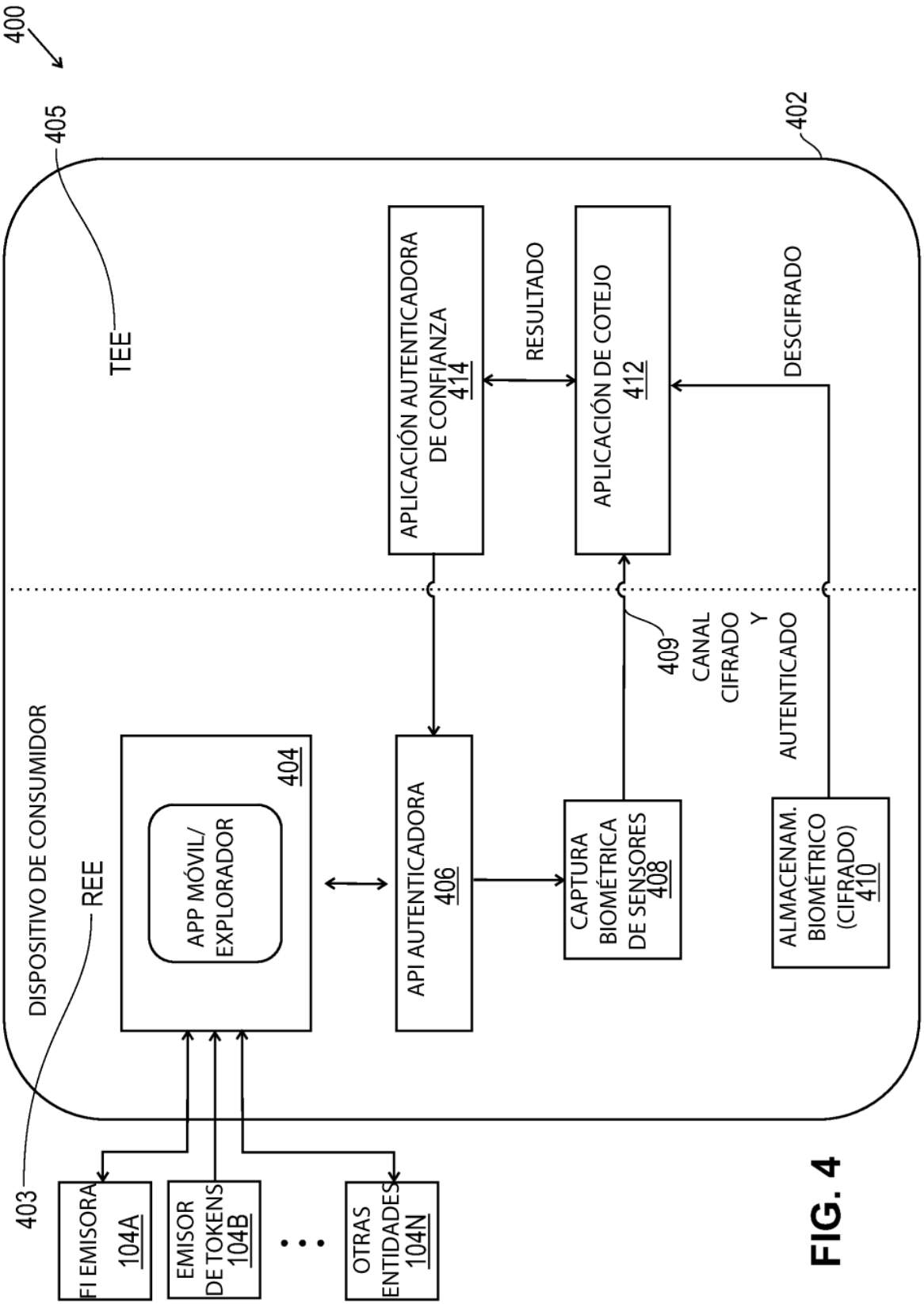
400
405
TEE
402
APLICACIÓN AUTENTICADORA DE CONFIANZA 414
RESULTADO
APLICACIÓN DE COTEJO 412
DESCIFRADO
409
CANAL CIFRADO Y AUTENTICADO
DISPOSITIVO DE CONSUMIDOR
REE
404
APP MÓVIL/ EXPLORADOR
API AUTENTICADORA 406
CAPTURA BIOMÉTRICA DE SENSORES 408
ALMACENAM. BIOMÉTRICO (CIFRADO) 410
403
FI EMISORA 104A
EMISOR DE TOKENS 104B
OTRAS ENTIDADES 104N

FIG. 4

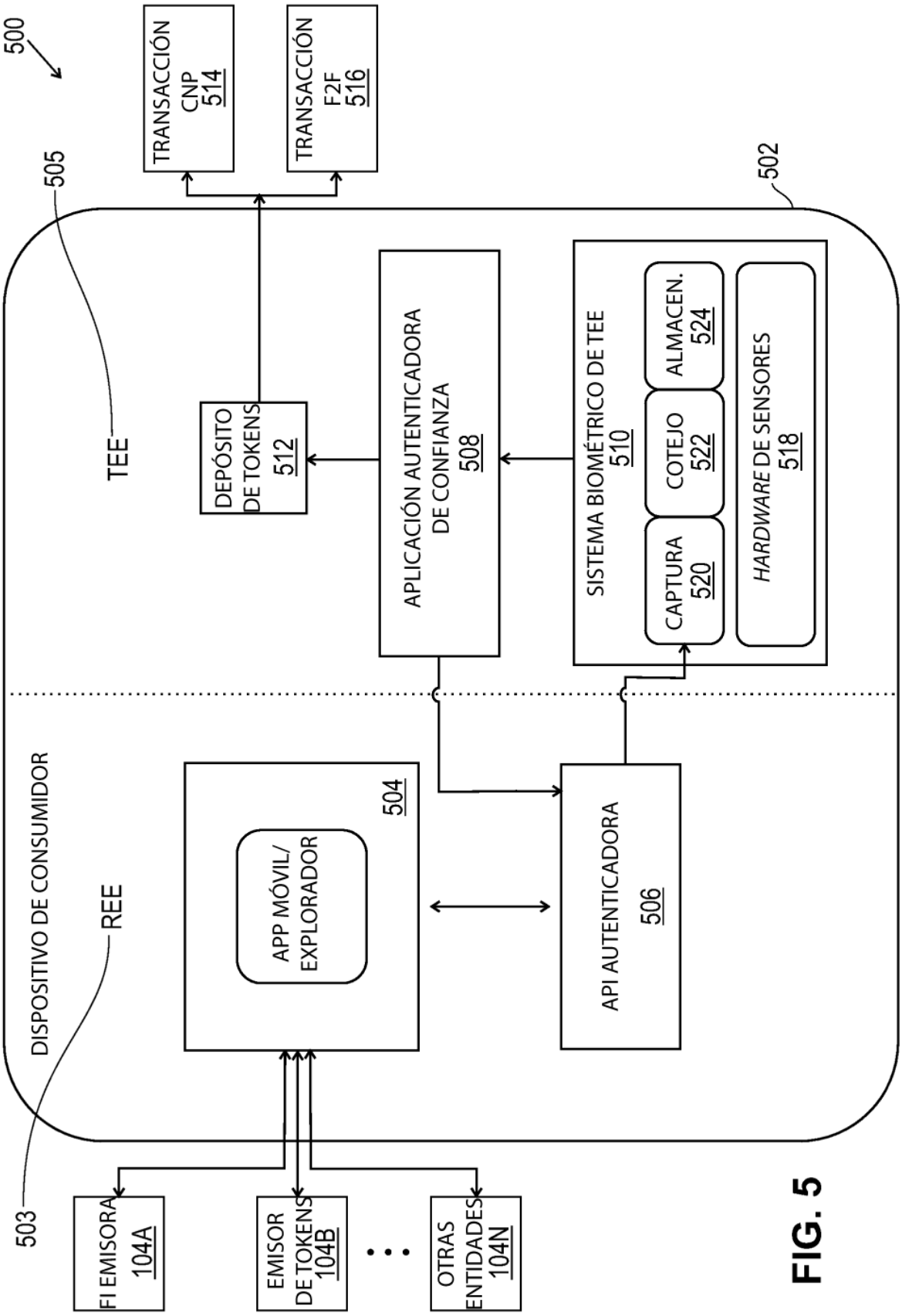
500
TRANSACCIÓN CNP 514
TRANSACCIÓN F2F 516
505
502
TEE
DEPÓSITO DE TOKENS 512
APLICACIÓN AUTENTICADORA DE CONFIANZA 508
SISTEMA BIOMÉTRICO DE TEE 510
CAPTURA 520
COTEJO 522
ALMACEN. 524
HARDWARE DE SENSORES 518
DISPOSITIVO DE CONSUMIDOR
REE
504
APP MÓVIL/ EXPLORADOR
API AUTENTICADORA 506
503
FI EMISORA 104A
EMISOR DE TOKENS 104B
OTRAS ENTIDADES 104N

FIG. 5