(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 970 201**

(51) Int. Cl.:

G06F 21/34 (2013.01)
G06F 21/35 (2013.01)
G06Q 20/32 (2012.01)
G06Q 20/38 (2012.01)
G06Q 20/40 (2012.01)
G06Q 20/34 (2012.01)
H04L 9/40 (2012.01)
G07F 7/10 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **23.11.2020 PCT/US2020/061864**

(87) Fecha y número de publicación internacional: **01.07.2021 WO21133494**

(96) Fecha de presentación y número de la solicitud europea: **23.11.2020 E 20830025 (1)**

(97) Fecha y número de publicación de la concesión europea: **27.12.2023 EP 4081921**

(54) Título: **Sistema de identificación personal con tarjeta sin contacto**

(30) Prioridad:

23.12.2019 US 201916725133

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.05.2024

(73) Titular/es:

CAPITAL ONE SERVICES, LLC (100.0%)
1680 Capital One Drive
McLean, Virginia 22102, US

(72) Inventor/es:

OSBORN, KEVIN;
CHIGURUPATI, SRINIVASA y
RULE, JEFFREY

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Sistema de identificación personal con tarjeta sin contacto

Antecedentes

La clonación de tarjetas de crédito, o "skimming", es una técnica mediante la cual un actor malintencionado copia información de una tarjeta de crédito asociada a una cuenta en una tarjeta falsificada. La clonación normalmente se realiza deslizando la tarjeta de crédito a través de un clonador para extraer ("skim") la información de la tarjeta de crédito de la banda magnética de la tarjeta y almacenar la información en la tarjeta falsificada. La tarjeta falsificada puede usarse para incurrir en cargos en la cuenta.

EMV (originalmente Europay, Mastercard, Visa) define un estándar para el uso de tarjetas de pago inteligentes, así como de terminales y cajeros automáticos que las acepten.

Las tarjetas EMV son tarjetas inteligentes (es decir, tarjetas con chip o tarjetas IC (circuito integrado)) que incluyen circuitos integrados configurados para almacenar información de la tarjeta además de información de la banda magnética (para compatibilidad con versiones anteriores). Las tarjetas EMV incluyen tarjetas físicamente insertadas (o "dipped") en un lector, así como tarjetas sin contacto que pueden leerse a corta distancia usando tecnología de comunicación de campo cercano (NFC).

Algunas tarjetas EMV usan tecnología de Chip y PIN (número de identificación personal) para superar los problemas asociados con la clonación. Por ejemplo, para autorizar una transacción, un usuario puede ingresar un número de identificación personal (PIN) en un terminal de transacciones después de deslizar la tarjeta. Un PIN almacenado, recuperado de la tarjeta por el terminal de transacciones, puede compararse con el PIN ingresado y la transacción puede aprobarse sólo en caso de que coincidan los dos. Esta solución puede reducir la actividad fraudulenta, pero sigue siendo vulnerable al robo de PIN causado por escuchas ilegales, intermediarios u otro tipo de ataque.

"Card Payments Roadmap in the United States: How Will EMV Impact the Future Payments infrastructure?", 1 de septiembre de 2012 (2012-09-01), XP055065063, describe la educación de las partes interesadas en toda la cadena de valor de pagos sobre los aspectos críticos de la implementación de una solución EMV en sus entornos comerciales.

Compendio

Según un aspecto de la invención, un sistema, dispositivo y método de autenticación multifactor combina un procedimiento de validación de Número de Identificación Personal (PIN) con un proceso de autenticación de tarjeta sin contacto para reducir el potencial de pérdida por clonación de tarjetas.

Según un aspecto, un método para la autenticación de doble factor de una solicitud de acceso a una cuenta asociada con un cliente incluye los pasos de: recibir un PIN de entrada desde una interfaz de usuario; activar una tarjeta sin contacto, almacenar la tarjeta sin contacto un pin asociado con el cliente; reenviar el pin de entrada a la tarjeta sin contacto; recibir, en respuesta a una correspondencia del pin de entrada con el pin almacenado, un criptograma desde la tarjeta sin contacto, usando el criptograma formado una clave dinámica de la tarjeta sin contacto, usando la clave dinámica formada un valor de contador mantenido por la tarjeta sin contacto, donde el criptograma incluye datos de tarjetas sin contacto codificados mediante la clave dinámica; reenviar el criptograma a un dispositivo de autenticación; y autorizar la solicitud en respuesta a la autenticación del criptograma por parte del dispositivo de autenticación.

Según otro aspecto, un método para la autenticación de doble factor de una solicitud de acceso a una cuenta asociada con un cliente incluye los pasos de: recibir un PIN de entrada desde una interfaz de usuario. El método también incluye activar una tarjeta sin contacto, almacenar la tarjeta sin contacto un pin asociado con el cliente. El método también incluye recibir un criptograma desde la tarjeta sin contacto, usando el criptograma formado una clave dinámica de la tarjeta sin contacto, usando la clave dinámica formada un contador mantenido por la tarjeta sin contacto, donde el criptograma incluye datos de la tarjeta sin contacto, incluido el PIN, y está codificado. usando la clave dinámica. El método también incluye reenviar el pin de entrada y el criptograma a un dispositivo de autenticación. El método también incluye autorizar la solicitud en respuesta a la autenticación del pin de entrada y el criptograma por parte del dispositivo de autenticación.

También se describe un dispositivo que incluye una interfaz de tarjeta sin contacto configurada para comunicarse con una tarjeta sin contacto asociada con un cliente, incluyendo la tarjeta sin contacto un PIN almacenado, una interfaz de usuario, un procesador y una memoria no volátil que tiene un código de programa almacenado en ella para autenticar una solicitud por parte del cliente. El código de programa operable cuando lo ejecuta el procesador para reenviar un pin de entrada recibido por la interfaz de usuario a la tarjeta sin contacto y recibir, en respuesta a una correspondencia del pin de entrada con el pin almacenado, un criptograma desde la tarjeta sin contacto, usando el criptograma formado una clave dinámica de la tarjeta sin contacto, usando la clave dinámica formada un valor de contador mantenido por la tarjeta sin contacto, donde el criptograma incluye datos de la tarjeta sin contacto que se codifican usando la clave dinámica. El código de programa puede funcionar además para reenviar el criptograma a un dispositivo de autenticación y autorizar la solicitud en respuesta a la autenticación del criptograma por parte del dispositivo de autenticación.

Breve descripción de los dibujos

La FIG. 1A es un diagrama de bloques de un sistema de transmisión de datos configurado para proporcionar autenticación multifactor de solicitudes de clientes usando números de identificación personal (PIN) según una realización de ejemplo;

la FIG. 1B es un diagrama de flujo de datos que ilustra una realización de una secuencia para proporcionar acceso autenticado usando datos almacenados en una tarjeta sin contacto;

las FIG. 2A y 2B ilustran una realización de un sistema y método para autenticación basada en PIN de doble factor como se describe en el presente documento;

las FIG. 3A y 3B ilustran una realización alternativa de un sistema y método para autenticación basada en PIN de doble factor como se describe en el presente documento;

las FIG. 4A y 4B ilustran una realización alternativa de un sistema y método basado en PIN de doble factor

las FIG. 5A y 5B ilustran una realización alternativa de un sistema y método para autenticación basada en PIN de doble factor como se describe en el presente documento;

la FIG. 6 es un ejemplo de una tarjeta sin contacto para almacenar información de autenticación que puede usarse en el sistema de la FIG. 1A;

la FIG. 7 es un diagrama de bloques que ilustra componentes ejemplares que pueden incluirse en la tarjeta sin contacto de la FIG. 3;

la FIG. 8 ilustra campos ejemplares de un criptograma que puede usarse como parte de un intercambio de PIN como se describe en diversas realizaciones en el presente documento;

la FIG. 9 es un diagrama de bloques detallado de los componentes de un sistema de la FIG. 1A que puede utilizarse para soportar aspectos de la invención; y

la FIG. 10 representa indicaciones que pueden ser proporcionadas por una interfaz de usuario de un dispositivo cliente según una realización descrita en el presente documento.

Descripción detallada

La seguridad de los datos y la integridad de las transacciones son de importancia crítica para las empresas y los consumidores. Esta necesidad continúa creciendo a medida que las transacciones electrónicas constituyen una proporción cada vez mayor de la actividad comercial y los actores maliciosos se vuelven cada vez más agresivos en sus esfuerzos por violar la seguridad de las transacciones.

Las realizaciones de la presente descripción proporcionan un sistema, método y dispositivo para la autenticación multifactor de transacciones recibidas en un dispositivo de cliente usando un Número de Identificación Personal (PIN) junto con una tarjeta sin contacto.

La tarjeta sin contacto puede incluir un sustrato que incluye una memoria que almacena uno o más subprogramas, un valor de contador y una o más claves. En algunas realizaciones, la memoria puede almacenar además un PIN que controla el uso de la tarjeta sin contacto como se describe en el presente documento. En una realización, el valor del contador se puede usar para generar un criptograma único que se puede usar para autenticar transacciones con tarjeta sin contacto. El criptograma se puede utilizar junto con el PIN para proporcionar autenticación de doble factor en transacciones con tarjeta sin contacto.

El criptograma puede formarse como se describe en la Solicitud o Solicitudes de Patente de los EE.UU. de Número de Serie 16/205,119 archivada el 29 de noviembre de 2018, por Osbom, et al., titulado "Systems and Methods for Cryptographc Authentication of Contactless Cards" (en adelante, la Solicitud '119). En algunas realizaciones, el criptograma puede formarse a partir de un hash criptográfico de un secreto compartido, una pluralidad de claves y un valor de contador.

Según un aspecto, el criptograma puede usarse junto con el PIN, para proporcionar autenticación multifactor de transacciones con tarjeta sin contacto. La autenticación multifactor puede implicar validar el conocimiento que tiene un usuario del PIN de una tarjeta antes o como parte de la autenticación de una transacción usando el criptograma. En algunas realizaciones, el criptograma puede formarse utilizando el PIN. En algunas realizaciones, el criptograma puede incluir un PIN codificado. En cualquier caso, la seguridad de la transacción se mantiene porque el PIN nunca se transmite en un formato discernible y, por lo tanto, se reduce la posibilidad de robo. Este sistema, que usa el PIN junto con un criptograma para la autenticación de doble factor, protege contra la clonación de la tarjeta sin contacto por parte de terceros no autorizados.

En algunas realizaciones, la validación del PIN puede realizarse mediante la tarjeta como condición previa para la generación de criptogramas. En otras realizaciones, la validación del PIN puede ser realizada por el dispositivo de transacción o por un servidor de autenticación de fondo como parte de la autenticación de criptograma. Cada uno de estos métodos se describe con mayor detalle a continuación.

Se aprecia que en diversos sistemas que incluyen clientes, dispositivos de cliente y servidores de autenticación, las funciones de almacenamiento de PIN, en diversas realizaciones, cifrado y autenticación, pueden ser realizadas por diferentes componentes. En algunas realizaciones, se puede mantener una copia del PIN en una memoria de la tarjeta sin contacto. En tal realización, la copia del PIN puede usarse para validar a un usuario de una tarjeta sin contacto como parte de un proceso de autenticación de criptograma. En algunas realizaciones, el PIN puede usarse para generar una firma digital o criptograma. En algunas realizaciones, la autenticación de criptograma se puede realizar mediante un dispositivo de transacción, un servidor de autenticación o alguna combinación de los mismos.

Por lo tanto, el sistema actual proporciona autenticación de doble factor que establece tanto el conocimiento (es decir, el número PIN) como la posesión (es decir, la tarjeta sin contacto y la clave dinámica), lo que reduce la capacidad de los actores malintencionados de clonar con éxito la tarjeta sin contacto.

Estas y otras características de la invención se describirán ahora con referencia a las figuras, en las que se usan números de referencia similares para referirse a elementos similares en todas partes. Con referencia general a las notaciones y nomenclatura usadas en el presente documento, las descripciones detalladas que siguen pueden presentarse en términos de procesos de programa ejecutados en un ordenador o red de ordenadores. Los expertos en la técnica usan estas descripciones y representaciones de procesos para transmitir de la forma más eficaz la sustancia de su trabajo a otros expertos en la técnica.

Un proceso puede concebirse aquí, y en general, como una secuencia autoconsistente de operaciones que conducen a un resultado deseado. Estas operaciones son aquellas que requieren manipulaciones físicas de cantidades físicas. Generalmente, aunque no necesariamente, estas cantidades toman la forma de señales eléctricas, magnéticas u ópticas capaces de almacenarse, transferirse, combinarse, compararse y manipularse de otro modo. A veces resulta conveniente, principalmente por razones de uso común, referirse a estas señales como bits, valores, elementos, símbolos, caracteres, términos, números o similares. Cabe señalar, sin embargo, que todos estos términos y otros similares deben asociarse con las cantidades físicas apropiadas y son simplemente etiquetas convenientes aplicadas a esas cantidades.

Además, las manipulaciones realizadas a menudo se denominan en términos como sumar o comparar, que se asocian comúnmente con operaciones mentales realizadas por un operador humano. Dicha capacidad de un operador humano no es necesaria, ni deseable en la mayoría de los casos, en cualquiera de las operaciones descritas en el presente documento que forman parte de una o más realizaciones. Más bien, las operaciones son operaciones de máquina. Las máquinas útiles para realizar operaciones de diversas realizaciones incluyen ordenadores digitales de uso general o dispositivos similares.

Varias realizaciones también se refieren a aparatos o sistemas para realizar estas operaciones. Este aparato puede construirse especialmente para el propósito requerido, o puede comprender un ordenador de uso general activado o reconfigurado selectivamente por un programa informático almacenado en el ordenador. Los procesos presentados en este documento no están inherentemente relacionados con un ordenador u otro aparato en particular. Se pueden usar varias máquinas de uso general con programas escritos de acuerdo con las enseñanzas del presente documento, o puede resultar conveniente construir aparatos más especializados para realizar los pasos del método requeridos. La estructura requerida para una variedad de estas máquinas aparecerá en la descripción dada.

Ahora se hace referencia a los dibujos, en los que se usan números de referencia similares para referirse a elementos similares en todas partes. En la siguiente descripción, con fines explicativos, se exponen numerosos detalles específicos para proporcionar una comprensión profunda de los mismos. Puede resultar evidente, sin embargo, que las nuevas realizaciones se pueden poner en práctica sin estos detalles específicos. En otros casos, las estructuras y dispositivos conocidos se muestran en forma de diagrama de bloques para facilitar su descripción. La intención es cubrir todas las modificaciones, equivalentes y alternativas consistentes con el tema reivindicado.

La FIG. 1A ilustra un sistema de transmisión de datos según una realización ejemplar. Como se analiza más adelante, el sistema 100 puede incluir una tarjeta 105 sin contacto, un dispositivo 110 cliente, una red 115 y un servidor 120. Aunque la FIG. 1A ilustra instancias únicas de los componentes, el sistema 100 puede incluir cualquier número de componentes.

El sistema 100 puede incluir una o más tarjetas 105 sin contacto. En una realización, una tarjeta 105 sin contacto comprende una tarjeta del tamaño de una tarjeta de crédito que incluye un circuito integrado, un dispositivo de almacenamiento y una interfaz que permite que la tarjeta se comunique con un dispositivo transmisor usando un protocolo de Comunicación de Campo Cercano (NFC). Una tarjeta sin contacto que puede usarse en el presente documento incluye la descrita en la Solicitud `119, por ejemplo.

El sistema 100 puede incluir el dispositivo 110 cliente, que puede ser un ordenador habilitado para red. Como se menciona en el presente documento, un ordenador habilitado para red puede incluir, entre otros, un dispositivo

informático o un dispositivo de comunicaciones que incluye, por ejemplo, un servidor, un dispositivo de red, un ordenador personal, una estación de trabajo, un teléfono, un PC portátil, un asistente digital personal, un cliente ligero, un cliente pesado, un navegador de Internet u otro dispositivo. El dispositivo 110 cliente también puede ser un dispositivo móvil; por ejemplo, un dispositivo móvil puede incluir un iPhone, iPod, iPad de Applet o cualquier otro dispositivo móvil que ejecute sistema operativo iOS® de Apple , cualquier dispositivo que ejecute el sistema operativo móvil Windows® de Microsoft, cualquier dispositivo que ejecute el sistema operativo Android® de Google y/o cualquier otro teléfono inteligente, tableta o dispositivo móvil portátil similar.

El dispositivo 110 cliente puede incluir un procesador y una memoria, y se entiende que el circuito de procesamiento puede contener componentes adicionales, incluyendo procesadores, memorias, verificadores de errores y paridad/CRC, codificadores de datos, algoritmos anticolisión, controladores, decodificadores de comandos, primitivas de seguridad y hardware a prueba de manipulaciones, según sea necesario para realizar las funciones descritas en este documento. El dispositivo 110 cliente puede incluir además un elemento de visualización y dispositivos de entrada. El elemento de visualización puede ser cualquier tipo de dispositivo para presentar información visual, como un monitor informático, un elemento de visualización plano y una pantalla de dispositivo móvil, incluidos elementos de visualización de cristal líquido, elementos de visualización de diodos emisores de luz, paneles de plasma y elementos de visualización de tubos de rayos catódicos. Los dispositivos de entrada pueden incluir cualquier dispositivo para ingresar información en el dispositivo del usuario que pueda estar disponible y soportado por el dispositivo del usuario, tal como una pantalla táctil, teclado, ratón, dispositivo de control del cursor, pantalla táctil, micrófono, cámara digital, grabadora de vídeo o videocámara. Estos dispositivos pueden usarse para ingresar información e interactuar con el software y otros dispositivos descritos en este documento.

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

El dispositivo 110 cliente puede estar en comunicación con uno o más servidores 120 a través de una o más redes 115 y puede funcionar como un par de interfaces delado de cliente a lado de servidor respectivos con el servidor 120. El dispositivo 110 cliente puede transmitir, por ejemplo, desde una aplicación de dispositivo móvil ejecutando en el dispositivo 110 cliente, una o más solicitudes al servidor 120. La una o más solicitudes pueden estar asociadas con la recuperación de datos del servidor 120. El servidor 120 puede recibir una o más solicitudes del dispositivo 110 cliente. Con base en la una o más solicitudes desde el dispositivo cliente 110, el servidor 120 puede configurarse para recuperar los datos solicitados de una o más bases de datos (no mostradas). Con base en la recepción de los datos solicitados desde una o más bases de datos, el servidor 120 puede configurarse para transmitir los datos recibidos al dispositivo 110 cliente, respondiendo los datos recibidos a una o más solicitudes.

El sistema 100 puede incluir una o más redes 115. En algunos ejemplos, la red 115 puede ser una o más de una red inalámbrica, una red cableada o cualquier combinación de red inalámbrica y red cableada y puede configurarse para conectar el dispositivo cliente 110 al servidor 120. Por ejemplo, la red 115 puede incluir una o más de una red de fibra óptica, una red óptica pasiva, una red de cable, una red de Internet, una red de satélite, una red de área local (LAN) inalámbrica, un Sistema Global para Comunicaciones Móviles, un servicio de comunicación personal, una red de área personal, protocolo de aplicación inalámbrica, servicio de mensajería multimedia, servicio de mensajería mejorado, servicio de mensajes cortos, sistemas basados en multiplexación por división de tiempo, sistemas basados en acceso múltiple por división de código, D-AMPS, Wi-Fi, datos inalámbricos fijos , IEEE 802.11b, 802.15.1, 802.11n y 802.11g, Bluetooth, NFC, identificación por radiofrecuencia (RFID), Wi-Fi y/o similares.

Además, la red 115 puede incluir, sin limitación, líneas telefónicas, fibra óptica, IEEE Ethernet 902.3, una red de área amplia, una red de área personal inalámbrica, una LAN o una red global tal como Internet. Además, la red 115 puede soportar una red de Internet, una red de comunicación inalámbrica, una red móvil o similares, o cualquier combinación de las mismas. La red 115 puede incluir además una red, o cualquier número de los tipos ejemplares de redes mencionadas anteriormente, que funcionan como una red independiente o en cooperación entre sí. La red 115 puede utilizar uno o más protocolos de uno o más elementos de red a los que están acoplados comunicativamente. La red 115 puede traducir hacia o desde otros protocolos a uno o más protocolos de dispositivos de red. Aunque la red 115 se representa como una única red, se debe apreciar que según uno o más ejemplos, la red 115 puede comprender una pluralidad de redes interconectadas, tales como, por ejemplo, Internet, la red de un proveedor de servicios, una red de televisión por cable, redes corporativas, como redes de asociaciones de tarjetas de crédito y redes domésticas.

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

La FIG. 1B es un diagrama de tiempos que ilustra una secuencia ejemplar para autenticar transacciones con tarjeta sin contacto según una o más realizaciones de la presente descripción. En particular, la FIG. 1B describe un proceso

ejemplar para intercambiar datos de autenticación, incluido un criptograma, entre una tarjeta 105 sin contacto y un dispositivo 110 cliente. El sistema 100 puede comprender una tarjeta 105 sin contacto y un dispositivo 110 cliente, que puede incluir una aplicación 122 y un procesador 124. La FIG. 1B puede hacer referencia a componentes similares a los ilustrados en la FIG. 1A.

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

En el paso 104, después de que se haya establecido la comunicación entre el dispositivo 110 cliente y la tarjeta 105 sin contacto, la tarjeta 105 sin contacto genera un criptograma de código de autenticación de mensaje (MAC). En algunos ejemplos, esto puede ocurrir cuando la aplicación 122 lee la tarjeta 105 sin contacto. En particular, esto puede ocurrir tras una lectura, tal como una lectura NFC, de una etiqueta de intercambio de datos de campo cercano (NDEF), que puede crearse de acuerdo con el Formato de Intercambio de Datos NFC. Por ejemplo, un lector, tal como la aplicación 122, puede transmitir un mensaje, tal como un mensaje de selección de subprograma, con el ID de subprograma de un subprograma productor de NDEF. Tras la confirmación de la selección, se puede transmitir una secuencia de mensajes de selección de archivos seguidos de mensajes de lectura de archivos. Por ejemplo, la secuencia puede incluir "Seleccionar archivo de capacidades", "Leer archivo de capacidades" y "Seleccionar archivo NDEF". En este punto, se puede actualizar o incrementar un valor de contador mantenido por la tarjeta sin contacto 105, lo que puede ir seguido de "Leer archivo NDEF". En este punto, se puede generar el mensaje que puede incluir una cabecera y un secreto compartido.

Luego se pueden generar claves de sesión. En una realización, se puede generar una clave diversificada usando un hash criptográfico para combinar una clave simétrica maestra con un valor de contador dinámico mantenido por la tarjeta sin contacto. Ejemplos de algoritmos hash criptográficos que pueden usarse incluyen algoritmos de cifrado simétrico, el algoritmo HMAC y un algoritmo CMAC. Los ejemplos no limitantes de los algoritmos simétricos que pueden usarse para cifrar el nombre de usuario y/o el criptograma pueden incluir un algoritmo de cifrado simétrico tal como 3DES (Algoritmo de Cifrado de Datos Triple) o Estándar de Cifrado Avanzado (AES) 128; un algoritmo simétrico de Autenticación de Mensajes Basado en Hash (HMAC), tal como HMAC-SHA-256; y un algoritmo de código de autenticación de mensajes basado en cifrado simétrico (CMAC) como AES-CMAC. Se entiende que los expertos en la técnica conocen numerosas formas de cifrado, y la presente descripción no se limita a aquellas identificadas específicamente en el presente documento.

El criptograma MAC puede crearse a partir del mensaje, que puede incluir la cabecera y el secreto compartido. En algunas realizaciones, la información compartida, que incluye, entre otros, un secreto compartido y/o un PIN, puede luego concatenarse con uno o más bloques de datos aleatorios y codificarse usando un algoritmo criptográfico y la clave diversificada para generar un criptograma MAC. A partir de entonces, el criptograma MAC y la cabecera pueden concatenarse, codificarse como ASCII hexadecimal y devolverse en formato de mensaje NDEF (en respuesta al mensaje "Leer archivo NDEF").

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

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

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

En el paso 108, la aplicación 122 comunica el criptograma MAC al procesador 124.

En el paso 112, el procesador 124 verifica el criptograma MAC de acuerdo con una instrucción de la aplicación 122. Por ejemplo, el criptograma MAC puede ser verificado por un servidor de autorización, tal como el servidor 120 de la FIG. 1A. El servidor de autorización puede almacenar, para cada dispositivo 110 cliente, una copia del contador, el secreto compartido y las claves del dispositivo cliente. En algunas realizaciones, como se describe con más detalle a continuación, el servidor de autorización también puede almacenar un PIN asociado con el dispositivo cliente. El servidor de autorización puede actualizar el contador para cada transacción con tarjeta sin contacto según un protocolo establecido entre el dispositivo 110 cliente y el servidor de autorización de manera que los contadores permanezcan sincronizados. El servidor de autorización puede usar su copia del contador, claves, secreto compartido y/o PIN para construir un criptograma MAC esperado.

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

El servidor de autorización puede comparar el criptograma MAC recibido de la tarjeta sin contacto con el criptograma MAC esperado generado por el servidor de autorización. Un acuerdo de este tipo mejora la seguridad de las transacciones de diversas maneras. En primer lugar, la naturaleza dinámica del criptograma resultante de su construcción usando valores de contador variables que se actualizan periódicamente según un protocolo establecido entre el cliente y el servidor reduce la capacidad de un tercero malintencionado de reutilizar la información de autenticación. En segundo lugar, el uso de algoritmos criptográficos protege aún más la información confidencial contra el descubrimiento mediante escuchas ilegales. En tercer lugar, incorporar la validación del código PIN junto con la autenticación con criptogramas añade un calificativo de conocimiento para la autenticación de doble factor.

Las Figuras 2A y 2B ilustran un sistema y proceso respectivos de una realización de un sistema de autenticación de doble factor configurado para soportar métodos de autenticación usando un PIN junto con y/o como parte de un criptograma.

En el sistema 200 de la FIG. 2A, se muestra que el dispositivo 222 de transacción (que puede ser un dispositivo móvil de cliente, un dispositivo de transacción comercial o cualquier dispositivo que comprenda capacidad de comunicación NFC) incluye una interfaz 225 de usuario para recibir información, tal como un PIN de entrada, de un usuario 202. También se muestra que el dispositivo 222 de transacción incluye una interfaz 220 NFC configurada para soportar comunicaciones NFC con una tarjeta 205 sin contacto y una Interfaz 227 de Red configurada para soportar comunicaciones de red, incluidas, entre otras, comunicaciones de protocolo de Internet (IP) con un servidor 223 de autenticación.

Según un aspecto, la tarjeta 205 sin contacto comprende una lógica 210 de correspondencia de PIN, que puede incluir hardware, software o una combinación de los mismos configurado para comparar un PIN, almacenado en la memoria de la tarjeta sin contacto, con un PIN recibido desde el dispositivo 222 de transacción, por ejemplo, como parte de un registro NDEF. La tarjeta 205 también incluye lógica 211 de generación de criptograma, configurada para generar un criptograma, por ejemplo, como se describe en la solicitud '119.

La lógica 211 de criptograma puede comprender una combinación de componentes de hardware y software, que incluyen, entre otros, un dispositivo de almacenamiento configurado para almacenar una o más claves y un valor de contador para la tarjeta 205. La tarjeta sin contacto puede incluir además contadores, cifrado y/o hardware y software de hash, etc., para su uso en la generación de una clave dinámica diversificada para su uso en la codificación de mensajes desde la tarjeta sin contacto. En algunas realizaciones, la lógica 211 de criptograma se puede implementar al menos en parte como un subprograma almacenado en una memoria de la tarjeta 205 sin contacto. Aunque la lógica 210 de PIN y la lógica 211 de criptograma se muestran delineadas por separado, se aprecia que la funcionalidad puede ser repartida de manera diferente en varias realizaciones. Por ejemplo, en algunas realizaciones la lógica 210 de PIN y la lógica 211 de criptograma pueden implementarse mediante un único subprograma.

Se muestra que el servidor 223 incluye lógica 228 de validación de criptograma. La lógica 228 de validación de criptograma puede comprender una combinación de componentes de hardware y software, que incluyen, entre otros, dispositivos de almacenamiento que almacenan claves de cliente y valores de contador, contadores, hardware y software de cifrado y/o hash, etc. En una realización, la lógica 228 de validación de criptograma puede configurarse para generar claves dinámicas diversificadas para usar en la generación de un criptograma esperado, y la lógica de validación puede comparar el criptograma esperado con un criptograma recibido desde el dispositivo cliente. Los criptogramas correspondientes indican una coordinación entre los contadores del dispositivo cliente y el servidor de autenticación. Además, los criptogramas correspondientes también pueden indicar conocimiento de información como secretos compartidos, PIN y similares.

La FIG. 2B ilustra un método para la autenticación de doble factor usando el sistema de la FIG. 2A. En el paso 251 el usuario 202 inicia una transacción; por ejemplo, el usuario puede intentar acceder a una cuenta, realizar una compra o realizar de otro modo una acción que se beneficie del método de autenticación de doble factor descrito en el presente documento. En el paso 252, se solicita al usuario 202 que ingrese un PIN y al recibir el PIN ingresado, el dispositivo 222 de transacción puede iniciar un intercambio de criptogramas de autenticación dual con la tarjeta 205 sin contacto, por ejemplo, solicitando al usuario que toque la tarjeta 205 en el dispositivo 222 de transacción o de otro modo poner la tarjeta 205 sin contacto en el rango de comunicación con el dispositivo 222 de transacción.

Cuando la tarjeta sin contacto está dentro del alcance del dispositivo de transacción, en el paso 253 el dispositivo 222 de transacción reenvía el PIN ingresado a la tarjeta 205 sin contacto, por ejemplo, como un registro de PIN, y emite una lectura de una etiqueta NFC asociada con un subprograma generador de criptograma. En el paso 254, la lógica 210 de correspondencia de PIN puede comparar el PIN de entrada con el PIN 215 almacenado. Si se determina una "correspondencia" en el paso 255, se ordena al subprograma generador de criptograma que genere un criptograma en el paso 256 y que transmita el criptograma de nuevo a el dispositivo 222 de transacción.

Si, en el paso 257 no se recibe un criptograma, por ejemplo, debido a una discrepancia de PIN, en el paso 259 se puede cancelar la transacción. Si se recibe un criptograma en el paso 257, entonces en el paso 258 el dispositivo de transacción 222 solicita la autenticación de la transacción, reenviando el criptograma al servidor 223 de autenticación.

En el paso 260, al recibir el criptograma por parte del servidor 223 de autenticación, el servidor de autenticación recupera los datos de cliente, incluidos contadores, claves, secretos compartidos y similares que están asociados con la tarjeta 205 sin contacto. Usando esta información, en el paso 261 el servidor de autenticación genera un criptograma esperado y en el paso 262 determina si el criptograma generado corresponde a la firma digital única proporcionada por el criptograma recibido. En el paso 263, el servidor de autenticación devuelve una respuesta de autorización/rechazo al dispositivo 222 de transacción. Si el dispositivo 222 de transacción determina en el paso 264 que la transacción está autorizada, entonces la transacción puede ejecutarse en el paso 265. Si la transacción se rechaza, el dispositivo de transacción cancela la transacción en el paso 250.

El sistema de autenticación basado en PIN de doble factor descrito mejora la seguridad de las transacciones protegiendo el PIN 215 almacenado contra el descubrimiento; Como se mencionó, el PIN almacenado no se transmite públicamente y, por lo tanto, no se puede obtener mediante una monitorización maliciosa durante un intercambio de PIN. En el caso de que se pueda obtener un PIN, un secreto compartido y/o un valor de contador mediante clonación, una tarjeta clonada sin conocimiento del protocolo de contador dinámico implementado entre la tarjeta y el servidor de autenticación sería inoperable.

Las FIG. 3A y 3B revelan otra realización de un sistema y método de autorización basado en PIN de doble factor, donde el servidor 323 de autenticación puede proporcionar la funcionalidad de Correspondencia de PIN como parte de la lógica 328 de validación de criptograma. En el sistema 300 de la FIG. 3A, la tarjeta 305 almacena el PIN 315 único para la tarjeta sin contacto y comprende una lógica 311 de criptograma que, como se describió anteriormente, puede comprender un subprograma generador de criptograma. Según una realización y descrita con más detalle a continuación, el criptograma proporcionado por la tarjeta 305 sin contacto puede incluir y/o formarse usando el PIN 315.

El dispositivo 322 de transacción incluye una interfaz 325 de usuario, una interfaz 320 NFC y una interfaz 327 de red. Además, el dispositivo de transacción puede incluir lógica 324 de encapsulación que en una realización puede comprender código para cifrar el PIN de entrada y/o criptograma antes de reenviar la pareja PIN/criptograma de entrada en el servidor 323 de autenticación.

El servidor 323 de autenticación incluye una lógica 328 de validación de criptograma, que puede funcionar para extraer el PIN de entrada del par de PIN de entrada/criptograma cifrado. La lógica 328 de validación de criptograma puede configurarse además para generar un criptograma esperado usando el PIN de entrada y los datos del cliente almacenados, tales como datos de contador y clave. La lógica 328 de validación de criptograma puede luego comparar el criptograma esperado con el criptograma extraído para determinar una correspondencia, indicando la correlación entre el PIN ingresado y el PIN almacenado, así como la información de contador y de clave.

La FIG. 3B es un diagrama de flujo de un proceso de autenticación de doble factor que puede ser realizado por el sistema 300. Después de que se inicia una transacción en el paso 351, en el paso 352 se solicita al usuario 302 que ingrese un PIN. En el paso 353, se inicia un proceso de autenticación de criptograma como se describió anteriormente, por ejemplo, el dispositivo 322 de transacción puede emitir una operación de lectura NFC a un subprograma productor de etiquetas NDEF de la tarjeta 305, en particular un subprograma productor de etiquetas NDEF configurado para recuperar el PIN 315. desde la tarjeta 305 sin contacto para su inclusión en la carga útil del criptograma. En el paso 356, el subprograma de la tarjeta sin contacto puede ensamblar datos de criptograma en la forma de <ID de usuario><Contador><MAC de ID de usuario+Contador+PIN). En algunas realizaciones, se puede usar una clave diversificada, formada usando el contador, para codificar el <MAC de ID de usuario+Contador+PIN> usando un algoritmo de hash criptográfico o similar. Alternativamente, se pueden usar algoritmos asimétricos de clave pública, por ejemplo, el Algoritmo de Firma Digital y el algoritmo RSA, o protocolos de conocimiento cero, para realizar esta verificación.

La tarjeta 305 sin contacto devuelve el criptograma al dispositivo 322 de transacción, y en el paso 354 el dispositivo 322 de transacción combina el PIN ingresado con el criptograma recibido. En algunas realizaciones, el PIN de entrada y/o el criptograma recibido se pueden cifrar para ofuscar la información del PIN de entrada, por ejemplo, usando algoritmos de cifrado simétrico. La combinación se envía al servidor de autenticación 323.

En el paso 360, el servidor 323 de autenticación recupera información de autenticación (incluido un valor de contador, claves, secreto compartido o similar) relacionada con la tarjeta sin contacto del almacenamiento. Usando esta información, en el paso 361 el servidor de autenticación puede ensamblar un criptograma esperado, por ejemplo, en forma de <MAC de ID de usuario+Contador almacenado+PIN de entrada>. En el paso 362, el servidor de autenticación determina si existe una correspondencia entre el criptograma esperado y el criptograma recuperado de la tarjeta sin contacto y devuelve el estado de autorización al dispositivo 322 de transacción en el paso 363. En respuesta a la recepción del estado de autorización en el paso 364, si la transacción continúa en el paso 364 o se cancela en el paso 359.

Por consiguiente, en la realización de las FIG. 3A y 3B, aunque el criptograma generado por la tarjeta sin contacto se forma usando el PIN, el PIN en sí no se transmite de una forma discernible o derivable a través de la red.

Las FIG. 4A y 4B describen otra realización de un sistema y método de autorización basado en PIN de doble factor, en el que el dispositivo de transacción puede realizar la correspondencia de PIN usando criptografía de clave pública. En una realización, la tarjeta 405 sin contacto mantiene una clave 417 privada. La clave 417 privada es conocida sólo por la tarjeta 405 sin contacto y puede usarse para descifrar comunicaciones cifradas a través de la clave pública. La tarjeta sin contacto puede incluir además una lógica de firma 411 digital configurada para generar una firma digital única, un hash criptográfico para proporcionar el criptograma para la comunicación con el dispositivo 422 de transacción.

El dispositivo 422 de transacción incluye una interfaz 425 de usuario y una interfaz 420 NFC. Se muestra que el dispositivo de transacción incluye además un generador 454 de números aleatorios, lógica 424 de cifrado y una memoria 455 de almacenamiento que almacena una clave 457 pública asociada con la tarjeta sin contacto, donde el dispositivo de transacción puede recuperar la clave pública de una autoridad certificada y confiable. El dispositivo de transacción incluye además una lógica 456 de firma digital para generar una firma digital como se describe a continuación. En algunas realizaciones, la clave pública de la tarjeta 405 puede ser almacenada por la tarjeta 405 y leída por el dispositivo de transacción como parte del proceso de autenticación.

Un método para la autenticación de doble factor usando el sistema 400 de la FIG. 4A se muestra en la FIG. 4B. Cuando se determina en el paso 461 que se ha iniciado una transacción, en el paso 462 se solicita al usuario 404 que introduzca un PIN de entrada. En el paso 463, el dispositivo de transacción obtiene la clave pública asociada con la tarjeta sin contacto, ya sea de la propia tarjeta o de una autoridad de certificación confiable. En el paso 465, el dispositivo de transacción genera un número aleatorio que cifra con la clave pública y lo reenvía a la tarjeta 405 sin contacto. En el paso 466, la tarjeta sin contacto descifra el número aleatorio usando su clave privada y genera una firma digital usando una combinación del número aleatorio y el PIN 415 almacenado. La firma digital resultante se reenvía al dispositivo 422 de transacción.

En el paso 467, el dispositivo 422 de transacción también genera una firma digital, usando el número aleatorio junto con el PIN ingresado recibido del usuario 402. En el paso 468, las firmas digitales se comparan para identificar una correspondencia. Dependiendo del estado de correspondencia, la transacción se ejecuta en el paso 470 (correspondencia) o se cancela en el paso 469 (no correspondencia).

Las FIG. 5A y 5B revelan otra realización de un sistema y método de autorización basado en PIN de doble factor, donde los PIN de tarjetas sin contacto se almacenan en el servidor de autenticación y se usan junto con los criptogramas para autenticar transacciones. En el sistema 500 de la FIG. 5A, la tarjeta 505 sin contacto incluye lógica de criptograma 511 para generar un criptograma usando una combinación de contadores, claves dinámicas, secretos compartidos y similares como se describió anteriormente. El dispositivo 522 de transacción incluye una interfaz 520 de usuario, una interfaz 525 NFC y una interfaz 527 de red. Además, el dispositivo de transacción puede incluir lógica 524 de encapsulación que puede, en una realización, comprender código para cifrar el PIN y/o criptograma de entrada antes del reenvío de la pareja de PIN/criptograma de entrada al servidor 523 de autenticación. El servidor 523 de autenticación incluye una tabla 595 de PIN, una lógica 594 de correspondencia de PIN y una lógica 596 de validación de criptograma.

Un método para la autenticación de doble factor usando el sistema 500 de la FIG. 5A se muestra en la FIG. 5B. Después de la imitación de una transacción en el paso 551, en el paso 552 se solicita al usuario 502 que ingrese un PIN, y en el paso 553 el dispositivo 522 de transacción solicita un criptograma de la tarjeta 505 sin contacto. En el paso 555 la tarjeta sin contacto genera un criptograma y lo devuelve al dispositivo 5422 de transacción. En el paso 554, el dispositivo de transacción combina el PIN ingresado, recibido del usuario, con el criptograma de la tarjeta sin contacto, lo cifra y lo reenvía al servidor 523 de autenticación. En el paso 560, el servidor de autorización recupera un PIN, contador y claves asociadas con la tarjeta 505 sin contacto. En el paso 561, el servidor de autorización descifra el mensaje del dispositivo 522 de transacción, extrae el PIN de entrada y en el paso 562 compara el PIN de entrada extraído con el PIN de entrada esperado recuperado de la Tabla de PIN. En el paso 563, el servidor 523 de autenticación también puede extraer el criptograma, recuperado de la tarjeta 505 sin contacto. El servidor 523 de autenticación puede construir un criptograma esperado usando clave almacenada, contador e información secreta compartida almacenada por la lógica de validación del criptograma. En el paso 564, el dispositivo de transacción puede comparar el criptograma esperado con el criptograma extraído para determinar una correspondencia. En respuesta a las comparaciones, el servidor 523 de autenticación devuelve el estado de autorización al dispositivo de transacción en el paso 565. En respuesta a la recepción del estado de autorización en el paso 566, la transacción se ejecuta en el paso 568 (correspondencia) o se cancela en el paso 567 (no correspondencia).

En consecuencia, se han mostrado y descrito diversos sistemas y métodos para proporcionar autenticación basada en PIN de doble factor. A continuación, se describirán componentes ejemplares que pueden incluirse en una tarjeta sin contacto, un dispositivo de transacción y/o un servidor de autorización, junto con y/o en lugar de los componentes ya descritos, para soportar los métodos descritos con respecto a las FIG. 6-10.

La FIG. 6 ilustra una tarjeta 600 sin contacto, que puede comprender una tarjeta de pago, tal como una tarjeta de crédito, tarjeta de débito o tarjeta de regalo, emitida por un proveedor 605 de servicios cuya identidad puede mostrarse en el anverso o reverso de la tarjeta 600. En algunos, Por ejemplo, la tarjeta 600 sin contacto no está relacionada con una tarjeta de pago y puede comprender, sin limitación, una tarjeta de identificación. En algunos ejemplos, la tarjeta

de pago puede comprender una tarjeta de pago sin contacto de interfaz dual. La tarjeta 600 sin contacto puede comprender un sustrato 610, que puede incluir una única capa, o una o más capas laminadas compuestas de plásticos, metales y otros materiales. Los materiales de sustrato ejemplares incluyen cloruro de polivinilo, acetato de cloruro de polivinilo, acrilonitrilo butadieno estireno, policarbonato, poliésteres, titanio anodizado, paladio, oro, carbono, papel y materiales biodegradables. En algunos ejemplos, la tarjeta 600 sin contacto puede tener características físicas que cumplan con el formato ID-1 del estándar ISO/IEC 7810 y, de lo contrario, la tarjeta sin contacto puede cumplir con el estándar ISO/IEC 14443. Sin embargo, se entiende que la tarjeta 600 sin contacto según la presente descripción puede tener diferentes características, y la presente descripción no requiere que se implemente una tarjeta sin contacto en una tarjeta de pago.

La tarjeta 600 sin contacto también puede incluir información 615 de identificación mostrada en el frente y/o reverso de la tarjeta, y un panel 620 de contacto. El panel 620 de contacto puede configurarse para establecer contacto con otro dispositivo de comunicación, tal como un dispositivo de usuario, inteligente. teléfono, ordenador portátil, ordenador de escritorio o tableta. La tarjeta 600 sin contacto también puede incluir circuitos de procesamiento, antena y otros componentes no mostrados en la FIG. 6. Estos componentes pueden estar ubicados detrás panel 620 de contacto o en otro lugar del sustrato 610. La tarjeta 600 sin contacto también puede incluir una tira o cinta magnética, que puede estar ubicada en la parte posterior de la tarjeta (no se muestra en la FIG. 6).

Como se ilustra en la FIG. 7, el panel 720 de contacto puede incluir circuitos de procesamiento para almacenar y procesar información, incluido un microprocesador 730 y una memoria 735. Se entiende que el circuito de procesamiento puede contener componentes adicionales, incluidos procesadores, memorias, verificadores de errores y paridad/CRC, datos codificadores, algoritmos anticolisión, controladores, decodificadores de comandos, primitivas de seguridad y hardware a prueba de manipulaciones, según sea necesario para realizar las funciones descritas en este documento.

La memoria 735 puede ser una memoria de sólo lectura, una memoria de lectura múltiple de una sola escritura o una memoria de lectura/escritura, por ejemplo, RAM, ROM y EEPROM, y la tarjeta 700 sin contacto puede incluir una o más de estas memorias. Una memoria de sólo lectura puede ser programable de fábrica como de sólo lectura o programable una sola vez. La programabilidad única brinda la oportunidad de escribir una vez y luego leer muchas veces. Se puede programar una memoria de escritura única/lectura múltiple en un momento dado después de que el chip de memoria haya salido de fábrica. Una vez programada la memoria, es posible que no se reescriba, pero sí se puede leer muchas veces.

La memoria 735 puede configurarse para almacenar uno o más subprogramas 740, uno o más contadores 745 e información 750 de cliente. Según un aspecto, la memoria 735 también puede almacenar el PIN 777.

El uno o más subprogramas 740 pueden comprender una o más aplicaciones de software asociadas con una o más aplicaciones de proveedor de servicios respectivas y configuradas para ejecutarse en una o más tarjetas sin contacto, tales como un subprograma de tarjeta Java. Por ejemplo, el subprograma puede incluir lógica configurada para generar un criptograma MAC como se describió anteriormente, incluyendo, en algunas realizaciones, un criptograma MAC que se forma al menos en parte usando información de PIN.

El uno o más contadores 745 pueden comprender un contador numérico suficiente para almacenar un número entero. La información 750 de cliente puede comprender un identificador alfanumérico único asignado a un usuario de la tarjeta sin contacto 700 y/o una o más claves que juntas pueden usarse para distinguir al usuario de la tarjeta sin contacto de otros usuarios de tarjetas sin contacto. En algunos ejemplos, la información 750 de cliente puede incluir información que identifica tanto a un cliente como a una cuenta asignada a ese cliente y puede identificar además la tarjeta sin contacto asociada con la cuenta de cliente.

Los elementos de procesador y memoria de las realizaciones ejemplares anteriores se describen con referencia al panel de contacto, pero la presente descripción no se limita a ello. Se entiende que estos elementos pueden implementarse fuera del panel 720 o completamente separados de ella, o como elementos adicionales además del microprocesador 730 y los elementos 735 de memoria ubicados dentro del panel 720 de contacto.

En algunos ejemplos, la tarjeta 700 sin contacto puede comprender una o más antenas 725 colocadas dentro de la tarjeta sin contacto 700 y alrededor del circuito 755 de procesamiento del panel 720 de contacto. Por ejemplo, la una o más antenas pueden ser integrales con el circuito de procesamiento, y la una o más antenas pueden usarse con una bobina de refuerzo externa. Como otro ejemplo, la una o más antenas pueden ser externas al panel 720 de contacto y al circuito de procesamiento.

Como se explicó anteriormente, las tarjetas 700 sin contacto pueden construirse en una plataforma de software operable en tarjetas inteligentes u otros dispositivos que comprendan código de programa, capacidad de procesamiento y memoria, tal como JavaCard. Los subprogramas se pueden configurar para responder a una o más solicitudes, como solicitudes de intercambio de datos de campo cercano (NDEF), desde un lector, como un lector móvil de comunicación de campo cercano (NFC) y producir un mensaje NDEF que comprende una OTP criptográficamente segura codificada como una etiqueta de texto NDEF.

La FIG. 8 ilustra un diseño 800 de registro corto NDEF (SR=1) ejemplar según una realización ejemplar. Un mensaje NDEF proporciona un método estandarizado para que un dispositivo de transacción se comunique con una tarjeta sin contacto. En algunos ejemplos, los mensajes NDEF pueden comprender uno o más registros. El registro 800 NDEF incluye una cabecera 802 que incluye una pluralidad de indicadores que definen cómo interpretar el resto del registro, incluido un indicador 803a de Inicio de Mensaje (MB), un indicador 803b de Fin de Mensaje (ME), un indicador 803c de Fragmento (CF), un indicador 803d de Registro Corto (SR), un indicador 803e de Longitud de ID (IL) y un campo 803f de Formato de Nombre de Tipo (TNF). El MB 803a y el indicador 803b ME pueden configurarse para indicar el primer y último registro respectivos del mensaje. El CF 803c y el indicador 803e IL proporcionan información sobre el registro, incluyendo respectivamente si los datos pueden ser "fragmentados" (datos distribuidos entre múltiples registros dentro de un mensaje) o si el campo 808 de longitud del tipo de ID puede ser relevante. El indicador 803d SR se puede configurar cuando el mensaje incluye solo un registro.

El campo 803f TNF identifica el tipo de contenido que contiene el campo, según lo definido por el protocolo NFC. Estos tipos incluyen vacíos, bien conocidos (datos definidos por la Definición de Tipo de Registro (RTD) del foro NFC), Extensiones de Correo de Internet Multipropósito (MIME) [según lo definido por RFC 2046], Identificador de Recursos Uniforme Absoluto (URI) [según lo definido por RFC 3986], externo (definido por el usuario), desconocido, sin cambios [para fragmentos] y reservado.

Otros campos de un registro NFC incluyen longitud 804 de tipo, longitud 806 de carga útil, longitud 808 de ID, tipo 810, ID 812 y Carga Útil 814. El campo 804 de longitud de tipo especifica el tipo preciso de datos que se encuentran en la carga útil. La longitud 806 de la carga útil contiene la longitud de la carga útil en bytes. Un registro puede contener hasta 4.294.967.295 bytes (o 2^32 - 1 bytes) de datos. La longitud 808 de ID contiene la longitud del campo ID en bytes. El tipo 810 identifica el tipo de datos que contiene la carga útil. Por ejemplo, para fines de autenticación, el Tipo 810 puede indicar que la carga útil 814 es un criptograma formado al menos en parte usando un Número de Identificación Personal (PIN) recuperado de una memoria de la tarjeta sin contacto. El campo 812 ID proporciona los medios para que aplicaciones externas identifiquen toda la carga útil transportada dentro de un registro NDEF. La carga útil 814 comprende el mensaje.

En algunos ejemplos, los datos pueden almacenarse inicialmente en la tarjeta sin contacto implementando ALMACENAR DATOS (E2) bajo un protocolo de canal seguro. Estos datos pueden incluir un ID de usuario personal (pUID) y un PIN que pueden ser exclusivos de la tarjeta, así como una o más claves iniciales, datos de procesamiento criptográfico que incluyen claves de sesión, claves de cifrado de datos, números aleatorios y otros valores que se describirá con más detalle a continuación. En otras realizaciones, el pUID y el PIN pueden cargarse previamente en la tarjeta sin contacto, antes de la entrega de la tarjeta sin contacto al cliente. En algunas realizaciones, el PIN puede ser seleccionado por un cliente asociado con la tarjeta sin contacto y escrito nuevamente en la tarjeta sin contacto luego de la validación del cliente usando varios métodos de autenticación estrictos.

La FIG. 9 ilustra un sistema 900 de comunicación en el que una tarjeta 910 sin contacto y/o un servidor 950 de autenticación pueden almacenar información que puede usarse durante la autenticación de primer factor. Como se describe con respecto a la FIG. 3, cada tarjeta sin contacto puede incluir un microprocesador 912 y una memoria 916 para información 919 de cliente que incluye uno o más atributos de identificación únicos, tales como identificadores, claves, números aleatorios y similares. En un aspecto, la memoria incluye además un subprograma 917 operable cuando lo ejecuta el microprocesador 912 para controlar los procesos de autenticación descritos en el presente documento. Como se describió anteriormente, un PIN 918 puede almacenarse en una memoria 916 de la tarjeta 910 y acceder a él mediante el subprograma y/o como parte de la información 919 de cliente. Además, cada tarjeta 910 puede incluir uno o más contadores 914, y una interfaz 915. En una realización, la interfaz opera NFC u otros protocolos de comunicación.

El dispositivo 920 cliente incluye una interfaz 925 de tarjeta sin contacto para comunicarse con la tarjeta sin contacto y una o más interfaces de red (no mostradas) que permiten que el dispositivo 920 se comunique con un proveedor de servicios usando una variedad de protocolos de comunicación como se describió anteriormente. El dispositivo cliente puede incluir además una interfaz 929 de usuario, que puede incluir uno o más de un teclado o elemento de visualización de pantalla táctil, permitiendo la comunicación entre una aplicación de proveedor de servicios y un usuario del dispositivo 920 cliente. El dispositivo 920 cliente incluye además un procesador 924 y una memoria 922 que almacena información y código de programa que controla la operación del dispositivo 920 cliente cuando el procesador lo ejecuta, incluyendo, por ejemplo, una aplicación 923 del lado del cliente que puede ser proporcionada al cliente por un proveedor de servicios para facilitar el acceso y el uso del servicio. aplicaciones de proveedores. En una realización, la aplicación 923 del lado del cliente incluye un código de programa configurado para comunicar información de autenticación, incluido el código PIN de la tarjeta 910 sin contacto, a uno o más servicios proporcionados por el proveedor de servicios como se describió anteriormente. La aplicación 923 del lado del cliente puede controlarse a través de una interfaz de aplicación mostrada en la interfaz de usuario 926. Por ejemplo, un usuario puede seleccionar un icono, enlace u otro mecanismo proporcionado como parte de la interfaz de la aplicación para iniciar la aplicación del lado del cliente para acceder a los servicios de aplicación, donde parte del lanzamiento incluye validar al cliente mediante un intercambio de criptogramas.

En una realización ejemplar, un intercambio de criptogramas incluye un dispositivo de transmisión que tiene un procesador y una memoria, conteniendo la memoria del dispositivo de transmisión una clave maestra, datos de

transmisión y un valor de contador. El dispositivo de transmisión se comunica con un dispositivo de recepción que tiene un procesador y una memoria, conteniendo la memoria del dispositivo de recepción la clave maestra. El dispositivo de transmisión puede configurarse para: generar una clave diversificada usando la clave maestra y uno o más algoritmos criptográficos y almacenar la clave diversificada en la memoria del dispositivo de transmisión, cifrar el valor del contador usando uno o más algoritmos criptográficos y la clave diversificada para producir un valor de contador cifrado, cifrar los datos de transmisión usando uno o más algoritmos criptográficos y la clave diversificada para producir datos de transmisión cifrados, y transmitir el valor de contador cifrado y los datos de transmisión cifrados al dispositivo receptor como un criptograma. El dispositivo receptor puede configurarse para: generar la clave diversificada con base en la clave maestra almacenada y el valor del contador almacenado y almacenar la clave diversificada en la memoria del dispositivo de recepción; y descifrar el criptograma cifrado (que comprende el contador cifrado y los datos de transmisión cifrados) usando uno o más algoritmos de descifrado y la clave diversificada. El dispositivo de recepción puede autenticar el dispositivo transmisor en respuesta a una correspondencia entre el contador descifrado y el contador almacenado. Luego se pueden incrementar los contadores en cada uno de los dispositivos transmisores y receptores para autenticaciones posteriores, proporcionando así un mecanismo de autenticación dinámica basado en criptogramas para transacciones entre dispositivos transmisores/dispositivos receptores.

Como se mencionó con respecto a la FIG. 1A, el dispositivo 920 cliente puede estar conectado a varios servicios de un proveedor 905 de servicios y administrado por el servidor 906 de aplicaciones. En la realización ilustrada, el servidor 950 de autenticación y el servidor 906 de aplicaciones se muestran como componentes separados, aunque se debe apreciar que una aplicación El servidor puede incluir todas las funciones descritas como incluidas en el servidor de autenticación.

Se muestra que el servidor 950 de autenticación incluye una interfaz 953 de red para comunicarse con miembros de la red a través de la red 930 y una unidad 959 central de procesamiento (CPU). En algunas realizaciones, el servidor de autenticación puede incluir medios de almacenamiento no transitorios para almacenar una tabla 952 de PIN que incluye Información de PIN relacionada con clientes de un proveedor de servicios. Dicha información puede incluir, entre otros, el nombre de usuario del cliente, identificadores personales de cliente y claves y contadores de cliente. En una realización, el servidor de autenticación incluye además una unidad 954 de autenticación para controlar la decodificación del criptograma y la extracción del contador, y una tabla 956 de valores de contador de cliente que puede usarse como se describe a continuación para realizar la autenticación junto con la tarjeta 910 sin contacto. En diversas realizaciones, el servidor de autenticación puede comprender además una tabla 952 de PIN configurada con una entrada para cada par de cliente/tarjeta sin contacto.

La FIG. 10 ilustra un ejemplo de un dispositivo 1000 cliente que comprende un elemento de visualización 1010 que incluye una ventana 1020 de aviso y una parte 1030 de entrada. La ventana de aviso puede mostrar varios avisos para guiar a un cliente a través del proceso de autenticación, por ejemplo, incluyendo un aviso "acercar tarjeta " para fomentar el movimiento de la tarjeta 805 hacia el dispositivo 1000. El mensaje también puede incluir una instrucción tal como "ingresar PIN" como se muestra en la FIG. 10 y proporcionar un teclado u otro mecanismo de entrada para permitir al usuario introducir el PIN. En algunas realizaciones, después de introducir con éxito el PIN y la introducción de la tarjeta, se le puede permitir a un usuario completar la transacción, por ejemplo, completar un cargo, obtener acceso a datos confidenciales, obtener acceso a personas concretas, etc.

En consecuencia, se ha mostrado y descrito un sistema y un método para la autenticación basada en PIN de doble factor que usa un criptograma y un intercambio de PIN con fines de autenticación de múltiples factores para reducir y/o eliminar el potencial de clonación de tarjetas.

Tal como se usan en esta solicitud, los términos "sistema", "componente" y "unidad" pretenden referirse a una entidad relacionada con el ordenador, ya sea hardware, una combinación de hardware y software, software o software en ejecución, ejemplos de los cuales se describen en el presente documento. Por ejemplo, un componente puede ser, entre otros, un proceso que se ejecuta en un procesador, un procesador, una unidad de disco duro, múltiples unidades de almacenamiento, un medio no transitorio legible por ordenador (ya sea de medio de almacenamiento óptico y/o magnético), un objeto, un ejecutable, un hilo de ejecución, un programa y/o un ordenador. A modo de ilustración, tanto una aplicación que se ejecuta en un servidor como el servidor pueden ser un componente. Uno o más componentes pueden residir dentro de un proceso y/o subproceso de ejecución, y un componente puede localizarse en un ordenador y/o distribuirse entre dos o más ordenadores.

Además, los componentes pueden acoplarse comunicativamente entre sí mediante diversos tipos de medios de comunicación para coordinar operaciones. La coordinación puede implicar el intercambio de información unidireccional o bidireccional. Por ejemplo, los componentes pueden comunicar información en forma de señales comunicadas a través de los medios de comunicación. La información puede implementarse como señales asignadas a varias líneas de señal. En tales asignaciones, cada mensaje puede ser una señal. Sin embargo, otras realizaciones pueden emplear alternativamente mensajes de datos. Estos mensajes de datos pueden enviarse a través de varias conexiones. Las conexiones ejemplares incluyen interfaces paralelas, interfaces en serie e interfaces de bus.

Algunas realizaciones pueden describirse usando la expresión "una realización" o "la realización" junto con sus derivados. Estos términos significan que una funcionalidad, estructura o característica particular descrita en relación

con la realización está incluida en al menos una realización. Las apariciones de la frase "en una realización" en varios lugares de la especificación no se refieren necesariamente todas a la misma realización. Además, a menos que se indique lo contrario, se reconoce que las características descritas anteriormente se pueden utilizar juntas en cualquier combinación. Por lo tanto, cualquier característica analizada por separado puede emplearse en combinación entre sí a menos que se observe que las características son incompatibles entre sí.

Con referencia general a las notaciones y nomenclatura utilizadas en el presente documento, las descripciones detalladas del presente documento pueden presentarse en términos de bloques o unidades funcionales que podrían implementarse como procedimientos de programa ejecutados en una computadora o red de computadoras. Los expertos en la técnica usan estas descripciones y representaciones de procedimientos para transmitir de la manera más eficaz la esencia de su trabajo a otros expertos en la técnica.

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

Además, las manipulaciones realizadas a menudo se denominan en términos como sumar o comparar, que se asocian comúnmente con operaciones mentales realizadas por un operador humano. Dicha capacidad de un operador humano no es necesaria, ni deseable en la mayoría de los casos, en cualquiera de las operaciones descritas en el presente documento, que forman parte de una o más realizaciones. Más bien, las operaciones son operaciones de máquina. Las máquinas útiles para realizar operaciones de diversas realizaciones incluyen ordenadores digitales de uso general o dispositivos similares.

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

Se enfatiza que el Resumen de la Descripción se proporciona para permitir al lector determinar rápidamente la naturaleza de la descripción técnica. Se presenta en el entendido de que no se utilizará para interpretar ni limitar el alcance o significado de las reclamaciones. Además, en la descripción detallada anterior, se agrupan diversas características en una única realización para simplificar la descripción. Este método de descripción no debe interpretarse como que refleja la intención de que las realizaciones reivindicadas requieran más características de las que se enumeran expresamente en cada reivindicación. Más bien, como reflejan las siguientes reivindicaciones, el objeto inventivo reside en menos de todas las características de una única realización descrita. Por lo tanto, las siguientes reivindicaciones se incorporan a la Descripción Detallada, siendo cada reivindicación por sí sola una realización separada. En las reivindicaciones adjuntas, los términos "que incluye" y "en el que" se usan como equivalentes en inglés simple de los términos respectivos "que comprende" y "en donde", respectivamente. Además, los términos "primero", "segundo", "tercero", etc., se usan simplemente como etiquetas y no pretenden imponer requisitos numéricos a sus objetos.

Lo que se ha descrito anteriormente incluye ejemplos de la arquitectura descrita. Por supuesto, no es posible describir todas las combinaciones concebibles de componentes y/o metodología, pero un experto en la técnica puede reconocer que son posibles muchas combinaciones y permutaciones adicionales. En consecuencia, se pretende que la nueva arquitectura abarque todas las alteraciones, modificaciones y variaciones que caen dentro del alcance de las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un método para la autenticación de doble factor de una solicitud de acceso a una cuenta asociada con un cliente incluye los pasos de:

recibir (252) un PIN ingresado desde una interfaz de usuario;

acoplar una tarjeta (205) sin contacto, almacenando la tarjeta (205) sin contacto un PIN asociado con el cliente;

reenviar (253) el PIN ingresado a la tarjeta (205) sin contacto;

recibir (256), en respuesta a una correspondencia del PIN ingresado con el PIN almacenado (255), un criptograma de la tarjeta sin contacto, formado el criptograma usando una clave dinámica de la tarjeta sin contacto, la clave dinámica formada usando un valor de contador mantenido por la tarjeta sin contacto, en la que el criptograma comprende datos de tarjeta sin contacto que se codifican usando la clave dinámica;

reenviar (258) el criptograma a un dispositivo de autenticación; y

autorizar (265) la solicitud en respuesta a la autenticación del criptograma por parte del dispositivo de autenticación.

2. El método de la reivindicación 1, en el que el dispositivo de autenticación mantiene una copia de los datos de la tarjeta sin contacto y una copia del valor del contador, y autentica el criptograma mediante:

codificar la copia de los datos de la tarjeta sin contacto usando una clave dinámica esperada formada a partir de la copia del contador para generar un criptograma esperado; y comparar el criptograma esperado con el criptograma reenviado.

3. El método de la reivindicación 2, en donde el valor del contador y la copia del valor del contador se actualizan cada uno según un protocolo predeterminado seguido por el dispositivo de autenticación y la tarjeta sin contacto.

4. El método de la reivindicación 3, en donde la clave dinámica se forma además usando una clave maestra que se almacena en la tarjeta sin contacto, y en donde el dispositivo de autenticación almacena una copia de la clave maestra y usa la copia de la clave maestra junto con el contador para proporcionarla clave dinámica esperada.

5. El método de la reivindicación 4, en donde la tarjeta sin contacto y el dispositivo de autenticación usan cada uno el mismo algoritmo hash criptográfico para generar la clave dinámica y la clave dinámica esperada.

6. El método de la reivindicación 5, en donde los datos de la tarjeta sin contacto que se codifican usando la clave dinámica para formar el criptograma incluyen el PIN almacenado en la tarjeta sin contacto, un secreto compartido, el valor del contador o una combinación de los mismos.

7. El método de la reivindicación 1, que incluye la etapa de codificar los datos de la tarjeta sin contacto, incluye aplicar una función hash criptográfica a los datos de la tarjeta sin contacto.

8. El método de la reivindicación 7, en donde la función hash criptográfica se selecciona de un grupo de funciones que incluyen un 3DES (Algoritmo de Cifrado de Datos Triple), un Estándar de Cifrado Avanzado (AES) 128, un algoritmo de Autenticación de Mensajes Basado en Hash (HMAC) simétrico, y un algoritmo de código de autenticación de mensajes basado en cifrado (CMAC) simétrico, como AES-CMAC.

9. El método de la reivindicación 1, en donde el dispositivo de autenticación comprende un dispositivo cliente, un dispositivo comercial, un servidor de autenticación o una combinación de los mismos.

10. Un método para la autenticación de doble factor de una solicitud de acceso a una cuenta asociada con un cliente incluye los pasos de:

recibir (552) un PIN de entrada desde una interfaz (520) de usuario;

acercar una tarjeta (505) sin contacto, almacenando la tarjeta (505) sin contacto un PIN asociado con el cliente;

recibir un criptograma de la tarjeta sin contacto, formado el criptograma usando una clave dinámica de la tarjeta sin contacto, formada la clave dinámica usando un contador mantenido por la tarjeta sin contacto, en donde el criptograma comprende datos de la tarjeta sin contacto, incluido el PIN, y está codificado usando la clave dinámica;

reenviar (523) el PIN ingresado y el criptograma a un dispositivo de autenticación; y

autorizar (566) la solicitud en respuesta a la autenticación del PIN de entrada y el criptograma por parte del dispositivo de autenticación.

11. El método de la reivindicación 10, en donde el dispositivo de autenticación mantiene una copia de los datos de la tarjeta sin contacto y una copia del contador, y autentica el criptograma mediante:

codificar la copia de los datos de la tarjeta sin contacto y el PIN de entrada usando una clave dinámica esperada formada a partir de la copia del contador para generar un criptograma esperado; y

comparar el criptograma esperado con el criptograma reenviado.

12. El método de la reivindicación 11, en donde el valor del contador y la copia del valor del contador se actualizan cada uno según un protocolo predeterminado seguido por el dispositivo de autenticación y la tarjeta sin contacto.

13. El método de la reivindicación 12, en donde la clave dinámica se forma además usando una clave maestra que se almacena en la tarjeta sin contacto, y en donde el dispositivo de autenticación almacena una copia de la clave maestra y usa la copia de la clave maestra junto con el contador para proporcionar la clave dinámica esperada.

14. El método de la reivindicación 13, en donde la tarjeta sin contacto y el dispositivo de autenticación usan cada uno el mismo algoritmo hash criptográfico para generar la clave dinámica y la clave dinámica esperada.

15. El método de la reivindicación 14, en donde los datos de la tarjeta sin contacto que se codifican usando la clave dinámica para formar el criptograma incluyen el PIN almacenado en la tarjeta sin contacto, un secreto compartido, el valor del contador o una combinación de los mismos.

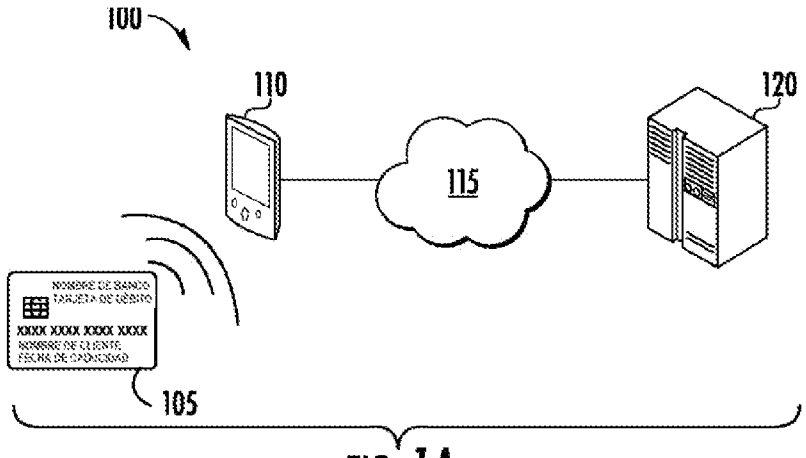
100
110
120
115
105

FIG. 1A

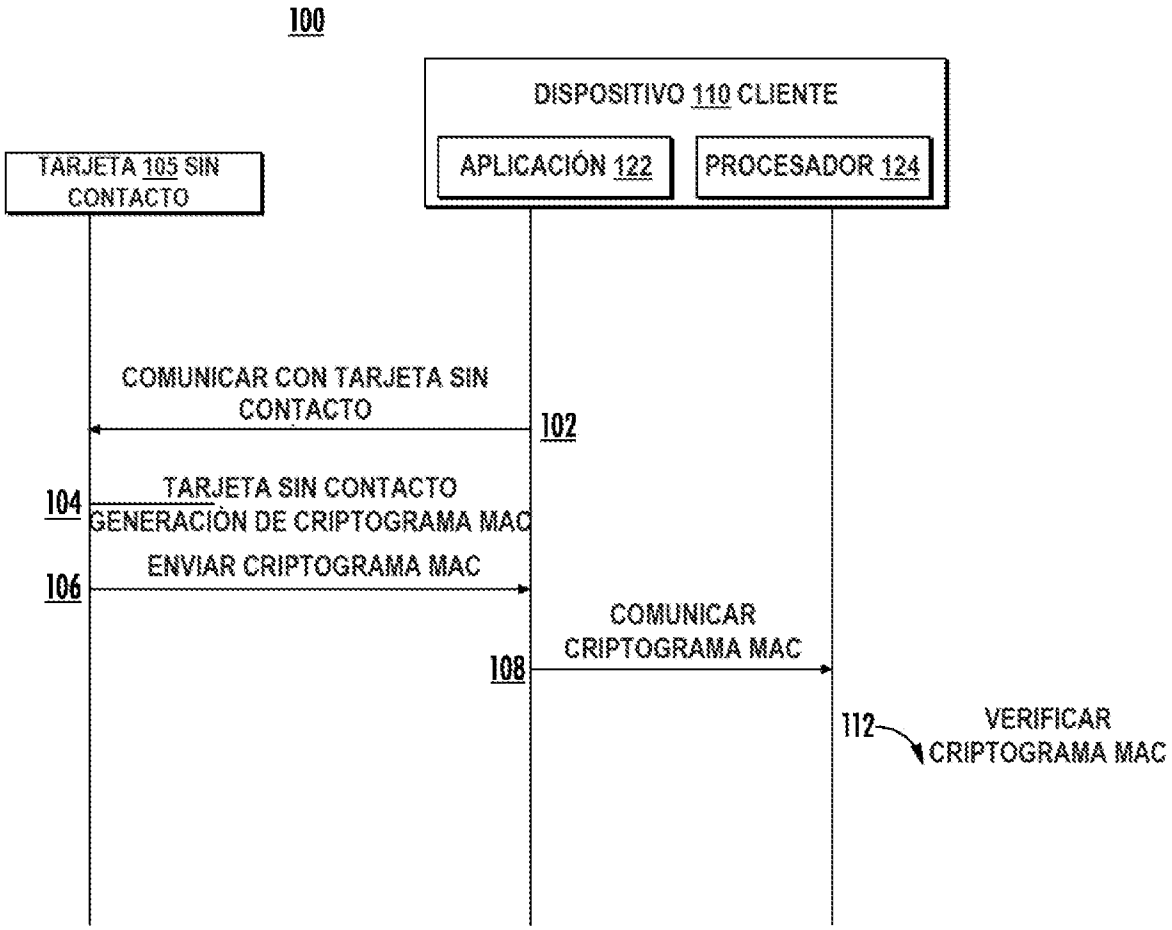
100
DISPOSITIVO 110 CLIENTE
APLICACIÓN 122
PROCESADOR 124
TARJETA 105 SIN CONTACTO
COMUNICAR CON TARJETA SIN CONTACTO
102
104
TARJETA SIN CONTACTO GENERACIÓN DE CRIPTOGRAMA MAC
106
ENVIAR CRIPTOGRAMA MAC
COMUNICAR CRIPTOGRAMA MAC
108
112
VERIFICAR CRIPTOGRAMA MAC

FIG. 1B

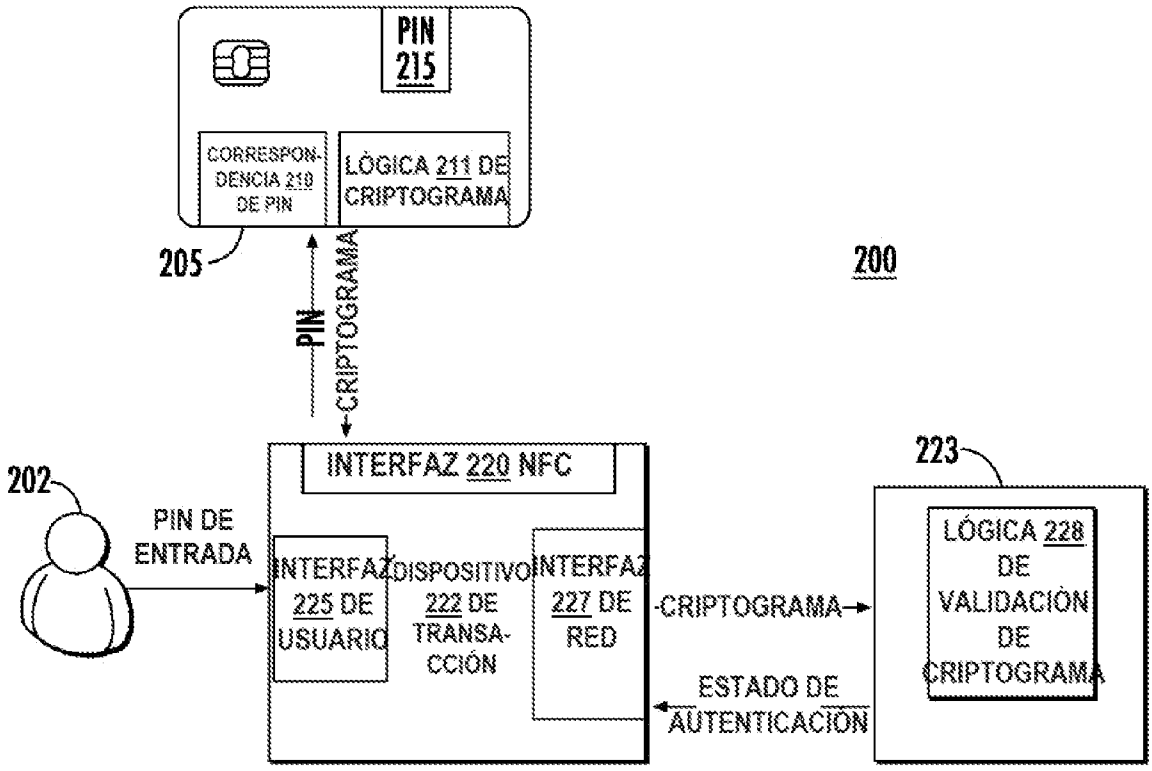
PIN
215
CORRESPON-
DENCIA 219
DE PIN
LÓGICA 211 DE
CRIPTOGRAMA
205
200
PIN
CRIPTOGRAMA
INTERFAZ 220 NFC
223
202
PIN DE
ENTRADA
INTERFAZ
225 DE
USUARIO
DISPOSITIVO
222 DE
TRANSA-
CCIÓN
INTERFAZ
227 DE
RED
CRIPTOGRAMA
LÓGICA 228
DE
VALIDACIÓN
DE
CRIPTOGRAMA
ESTADO DE
AUTENTICACIÓN

FIG. 2A

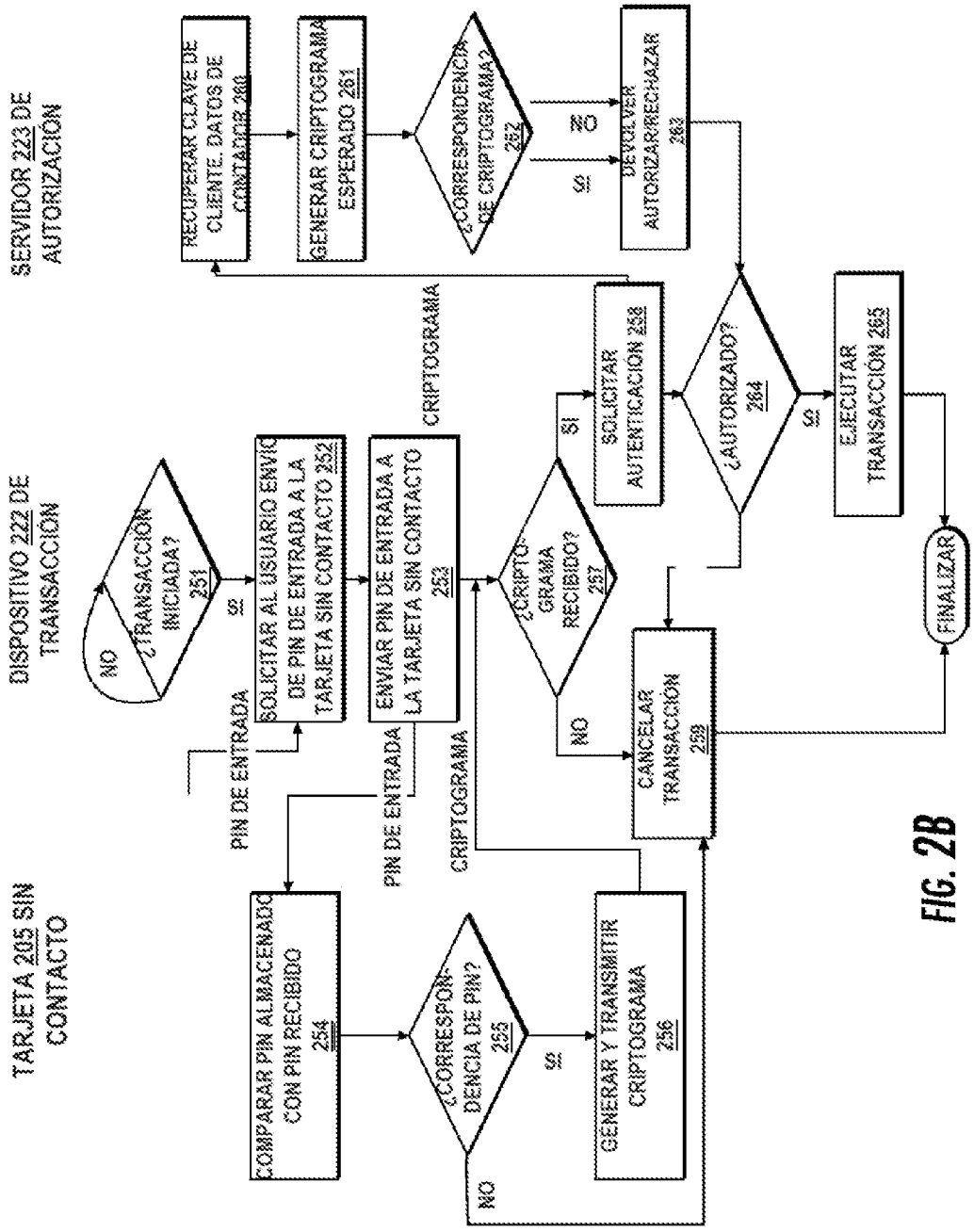
SERVIDOR 223 DE AUTORIZACIÓN
DISPOSITIVO 222 DE TRANSACCIÓN
TARJETA 205 SIN CONTACTO
¿TRANSACCIÓN INICIADA? 251
NO
SÍ
SOLICITAR AL USUARIO ENVÍO DE PIN DE ENTRADA A LA TARJETA SIN CONTACTO 252
PIN DE ENTRADA
ENVIAR PIN DE ENTRADA A LA TARJETA SIN CONTACTO 253
PIN DE ENTRADA
CRIPTOGRAMA
COMPARAR PIN ALMACENADO CON PIN RECIBIDO 254
¿CORRESPONDENCIA DE PIN? 255
NO
SÍ
GENERAR Y TRANSMITIR CRIPTOGRAMA 256
CRIPTOGRAMA
¿CRIPTOGRAMA RECIBIDO? 257
NO
SÍ
CANCELAR TRANSACCIÓN 259
SOLICITAR AUTENTICACIÓN 258
RECUPERAR CLAVE DE CLIENTE, DATOS DE CONTADOR 260
GENERAR CRIPTOGRAMA ESPERADO 261
¿CORRESPONDENCIA DE CRIPTOGRAMA? 262
NO
SÍ
DEVOLVER AUTORIZAR/RECHAZAR 263
¿AUTORIZADO? 264
SÍ
EJECUTAR TRANSACCIÓN 265
FINALIZAR

FIG. 2B

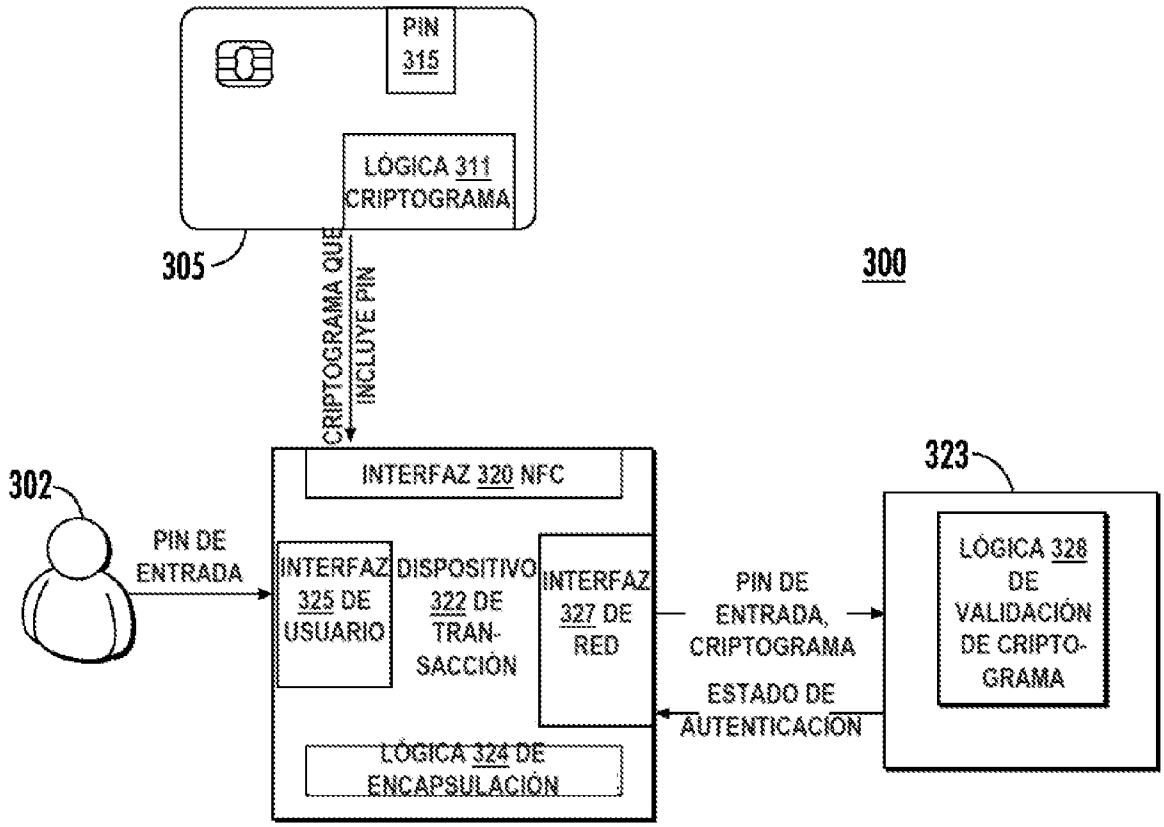
PIN
315
LÓGICA 311
CRIPTOGRAMA
305
300
CRIPTOGRAMA QUE INCLUYE PIN
302
323
INTERFAZ 320 NFC
PIN DE ENTRADA
INTERFAZ 325 DE USUARIO
DISPOSITIVO 322 DE TRANSACCIÓN
INTERFAZ 327 DE RED
PIN DE ENTRADA, CRIPTOGRAMA
ESTADO DE AUTENTICACIÓN
LÓGICA 328 DE VALIDACIÓN DE CRIPTOGRAMA
LÓGICA 324 DE ENCAPSULACIÓN

FIG. 3A

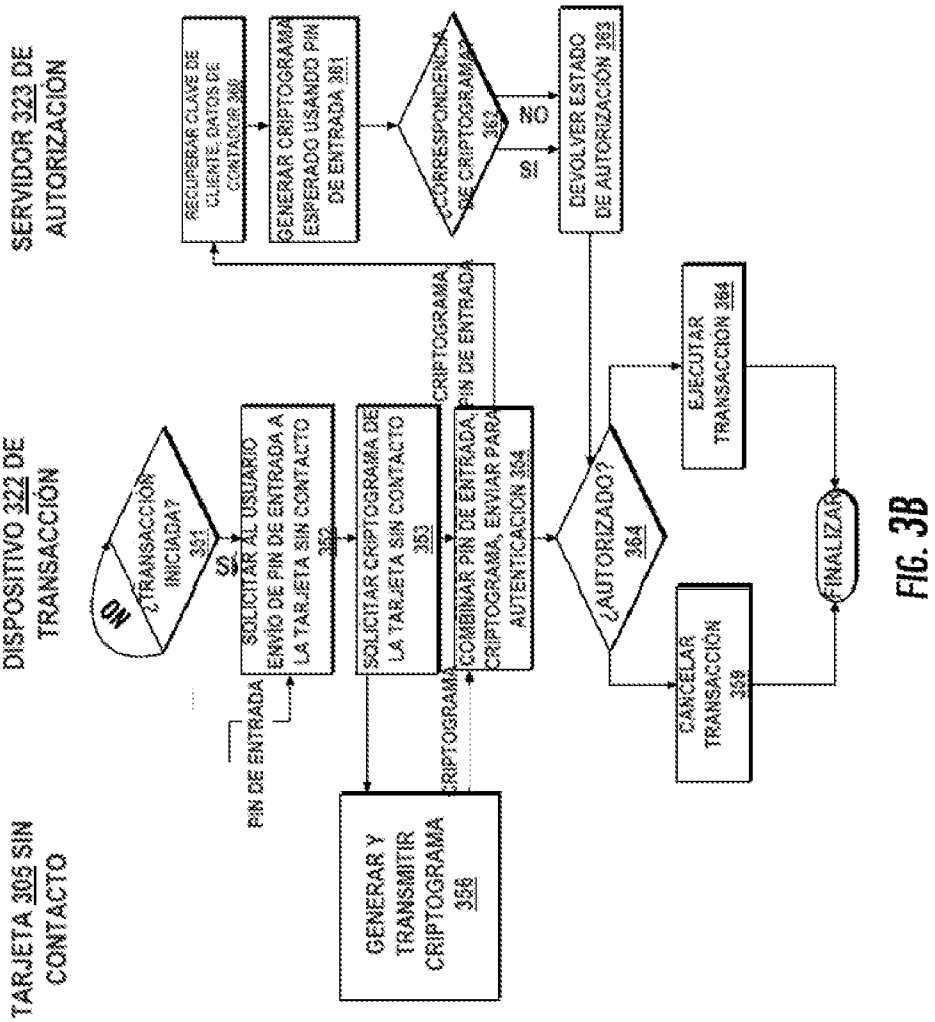
SERVIDOR 323 DE AUTORIZACIÓN
DISPOSITIVO 322 DE TRANSACCIÓN
TARJETA 305 SIN CONTACTO
¿TRANSACCIÓN INICIADA? 361
NO
SÍ
SOLICITAR AL USUARIO ENVÍO DE PIN DE ENTRADA A LA TARJETA SIN CONTACTO 362
SOLICITAR CRIPTOGRAMA DE LA TARJETA SIN CONTACTO 363
COMBINAR PIN DE ENTRADA, CRIPTOGRAMA, ENVIAR PARA AUTENTICACIÓN 364
¿AUTORIZADO? 364
EJECUTAR TRANSACCIÓN 364
CANCELAR TRANSACCIÓN 365
FINALIZAR
RECUPERAR CLAVE DE CLIENTE, DATOS DE CONTACTO 380
GENERAR CRIPTOGRAMA ESPERADO USANDO PIN DE ENTRADA 381
¿CORRESPONDENCIA DE CRIPTOGRAMAS? 382
SÍ
NO
DEVOLVER ESTADO DE AUTORIZACIÓN 383
CRIPTOGRAMA, PIN DE ENTRADA
PIN DE ENTRADA
CRIPTOGRAMA
GENERAR Y TRANSMITIR CRIPTOGRAMA 366

FIG. 3B

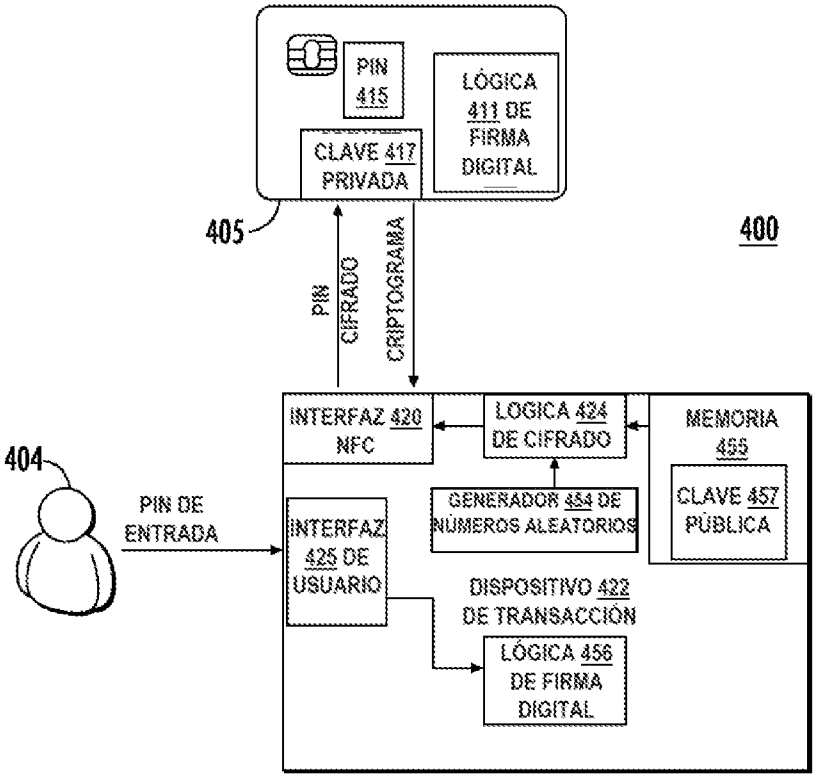
PIN 415
LÓGICA 411 DE FIRMA DIGITAL
CLAVE 417 PRIVADA
405
400
PIN CIFRADO
CRIPTOGRAMA
INTERFAZ 420 NFC
LOGICA 424 DE CIFRADO
MEMORIA 455
CLAVE 457 PÚBLICA
404
PIN DE ENTRADA
INTERFAZ 425 DE USUARIO
GENERADOR 454 DE NÚMEROS ALEATORIOS
DISPOSITIVO 422 DE TRANSACCIÓN
LÓGICA 456 DE FIRMA DIGITAL

FIG. 4A

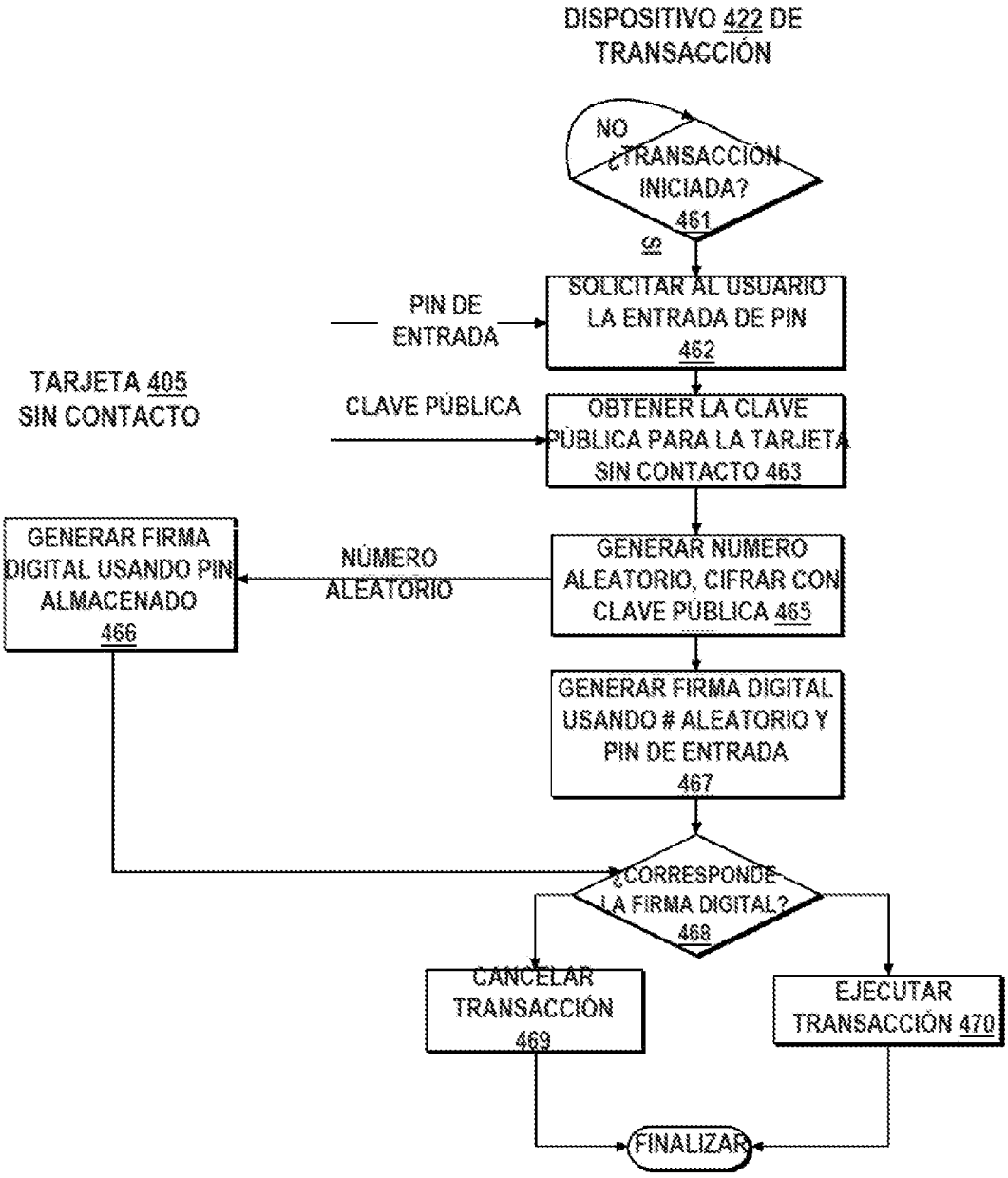
DISPOSITIVO 422 DE TRANSACCIÓN
NO
¿TRANSACCIÓN INICIADA?
461
SÍ
PIN DE ENTRADA
SOLICITAR AL USUARIO LA ENTRADA DE PIN
462
TARJETA 405 SIN CONTACTO
CLAVE PÚBLICA
OBTENER LA CLAVE PÚBLICA PARA LA TARJETA SIN CONTACTO 463
GENERAR FIRMA DIGITAL USANDO PIN ALMACENADO
466
NÚMERO ALEATORIO
GENERAR NÚMERO ALEATORIO, CIFRAR CON CLAVE PÚBLICA 465
GENERAR FIRMA DIGITAL USANDO # ALEATORIO Y PIN DE ENTRADA
467
¿CORRESPONDE LA FIRMA DIGITAL?
468
CANCELAR TRANSACCIÓN
469
EJECUTAR TRANSACCIÓN 470
FINALIZAR

FIG. 4B

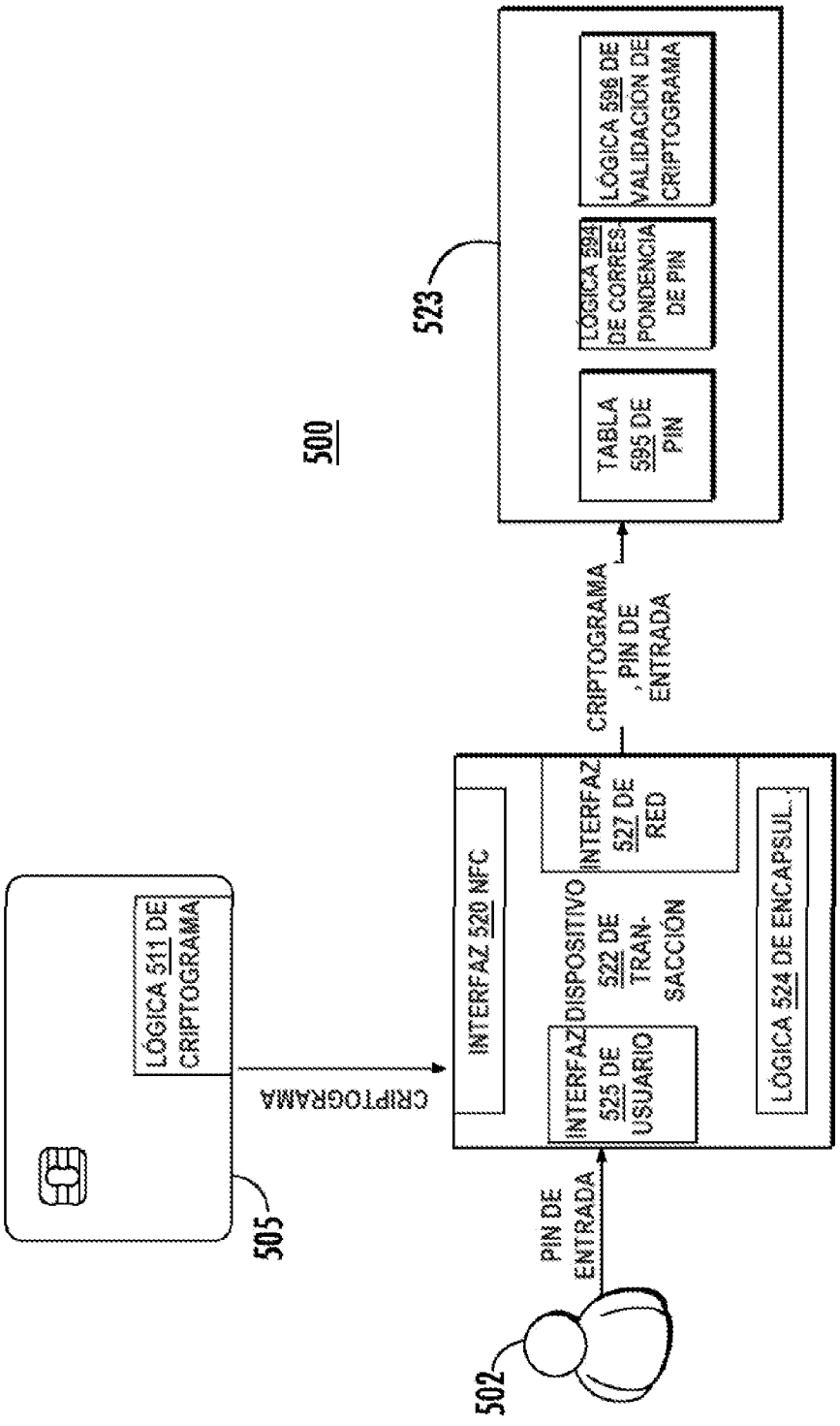
500
523
TABLA 595 DE PIN
LÓGICA 594 DE CORRESPONDENCIA DE PIN
LÓGICA 596 DE VALIDACIÓN DE CRIPTOGRAMA
CRIPTOGRAMA , PIN DE ENTRADA
INTERFAZ 520 NFC
INTERFAZ 527 DE RED
DISPOSITIVO 522 DE TRANSACCIÓN
INTERFAZ 525 DE USUARIO
LÓGICA 524 DE ENCAPSUL.
LÓGICA 511 DE CRIPTOGRAMA
CRIPTOGRAMA
PIN DE ENTRADA
505
502

FIG. 5A

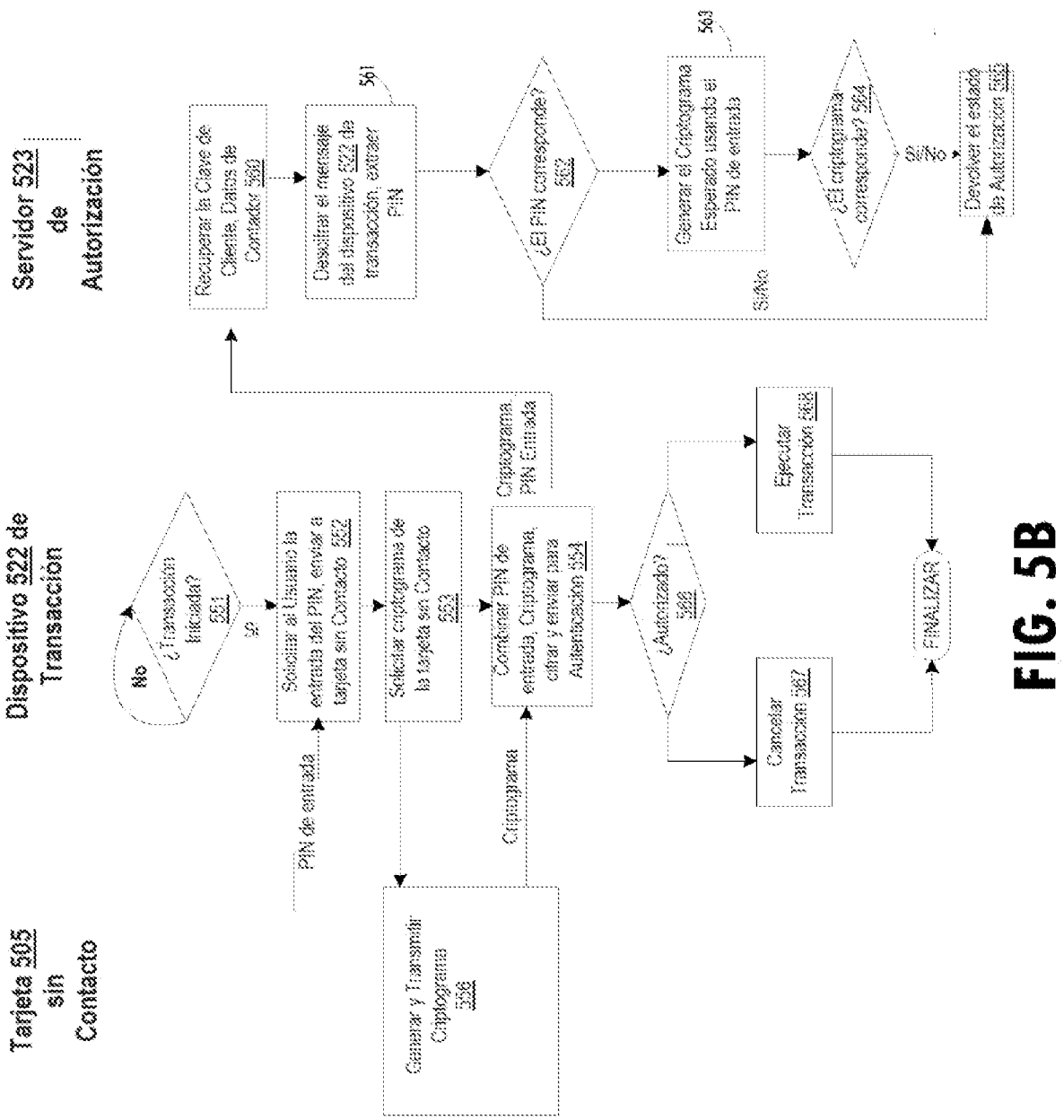
Tarjeta 505 sin Contacto
Dispositivo 522 de Transacción
Servidor 523 de Autorización
¿Transacción Iniciada? 551
No
Sí
Solicitar al Usuario la entrada del PIN, enviar a tarjeta sin Contacto 552
Solicitar criptograma de la tarjeta sin Contacto 553
Cifrar PIN de entrada, Criptograma, cifrar y enviar para Autenticación 554
¿Autorizado? 566
Ejecutar Transacción 568
Cancelar Transacción 567
FINALIZAR
Generar y Transmitir Criptograma 556
PIN de entrada
Criptograma
Criptograma, PIN Entrada
Recuperar la Clave de Cliente, Datos de Contador 560
Descifrar el mensaje del dispositivo 522 de transacción, extraer PIN 561
¿El PIN corresponde? 562
Generar el Criptograma Esperado usando el PIN de entrada 563
¿El criptograma corresponde? 564
Sí/No
Sí/No
Devolver el estado de Autorización 569

FIG. 5B

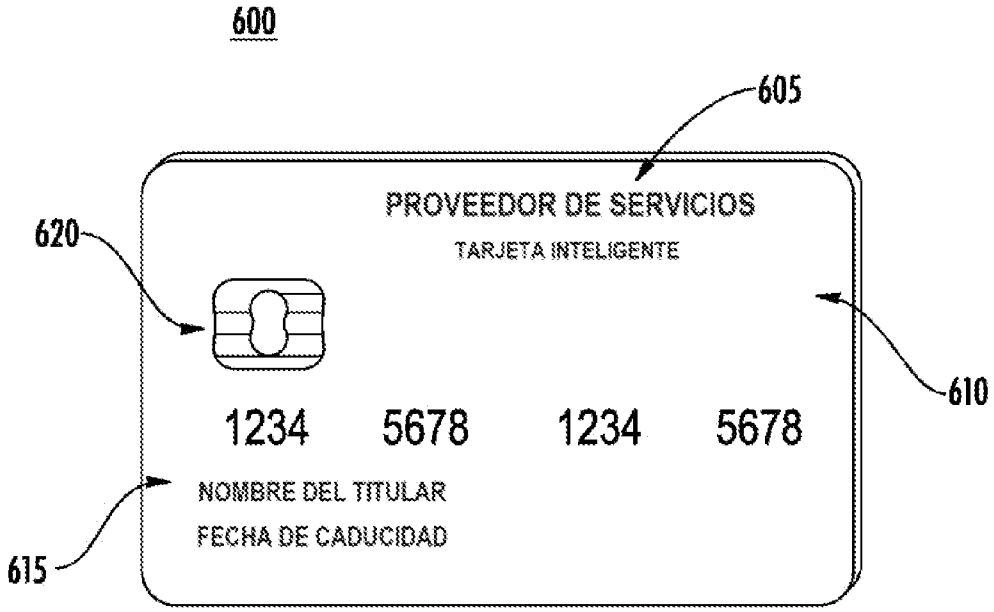
600
605
PROVEEDOR DE SERVICIOS
TARJETA INTELIGENTE
620
610
1234 5678 1234 5678
NOMBRE DEL TITULAR
FECHA DE CADUCIDAD
615

FIG. 6

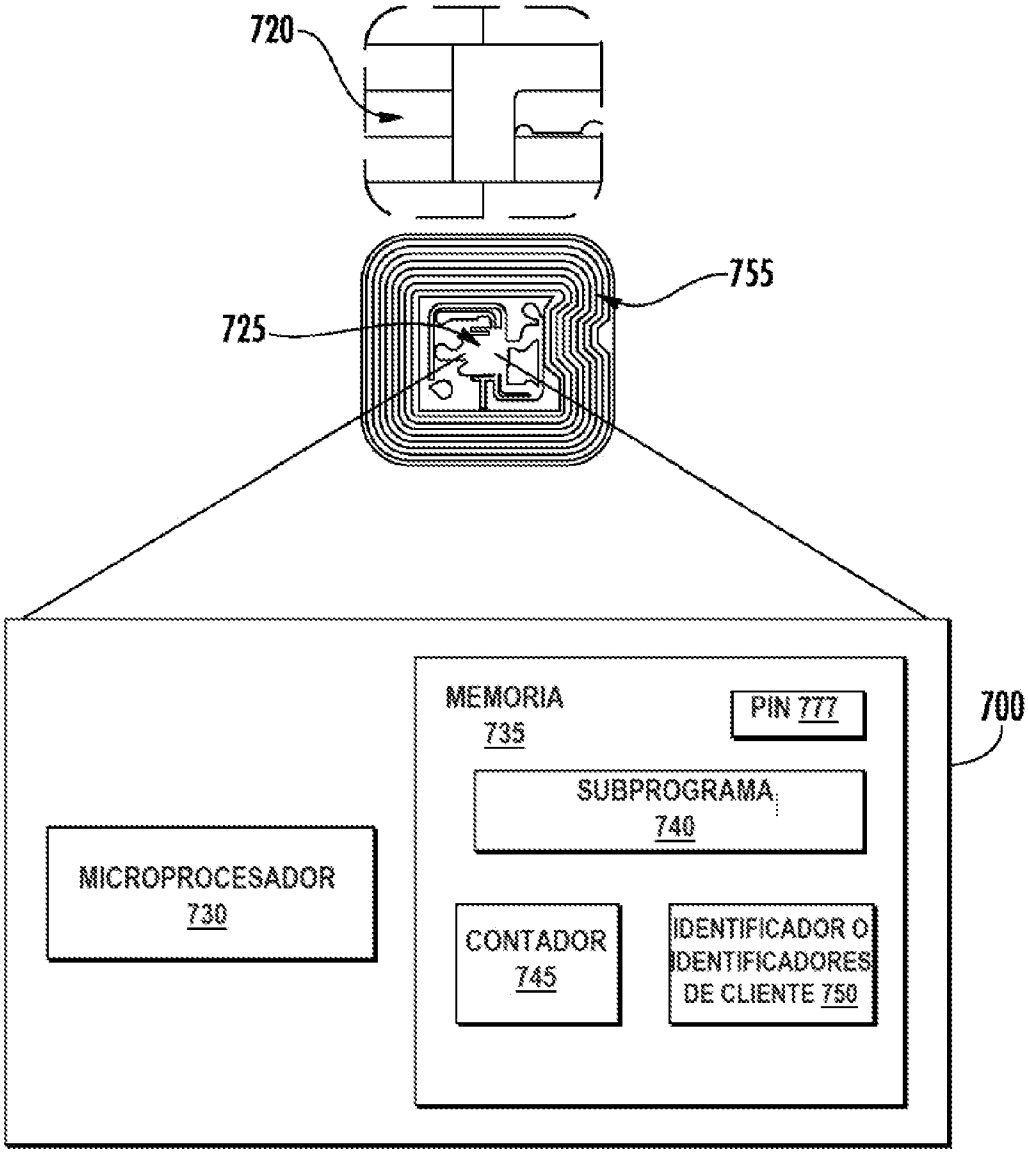
720
755
725
MEMORIA
735
PIN 777
700
SUBPROGRAMA
740
MICROPROCESADOR
730
CONTADOR
745
IDENTIFICADOR O
IDENTIFICADORES
DE CLIENTE 750

FIG. 7

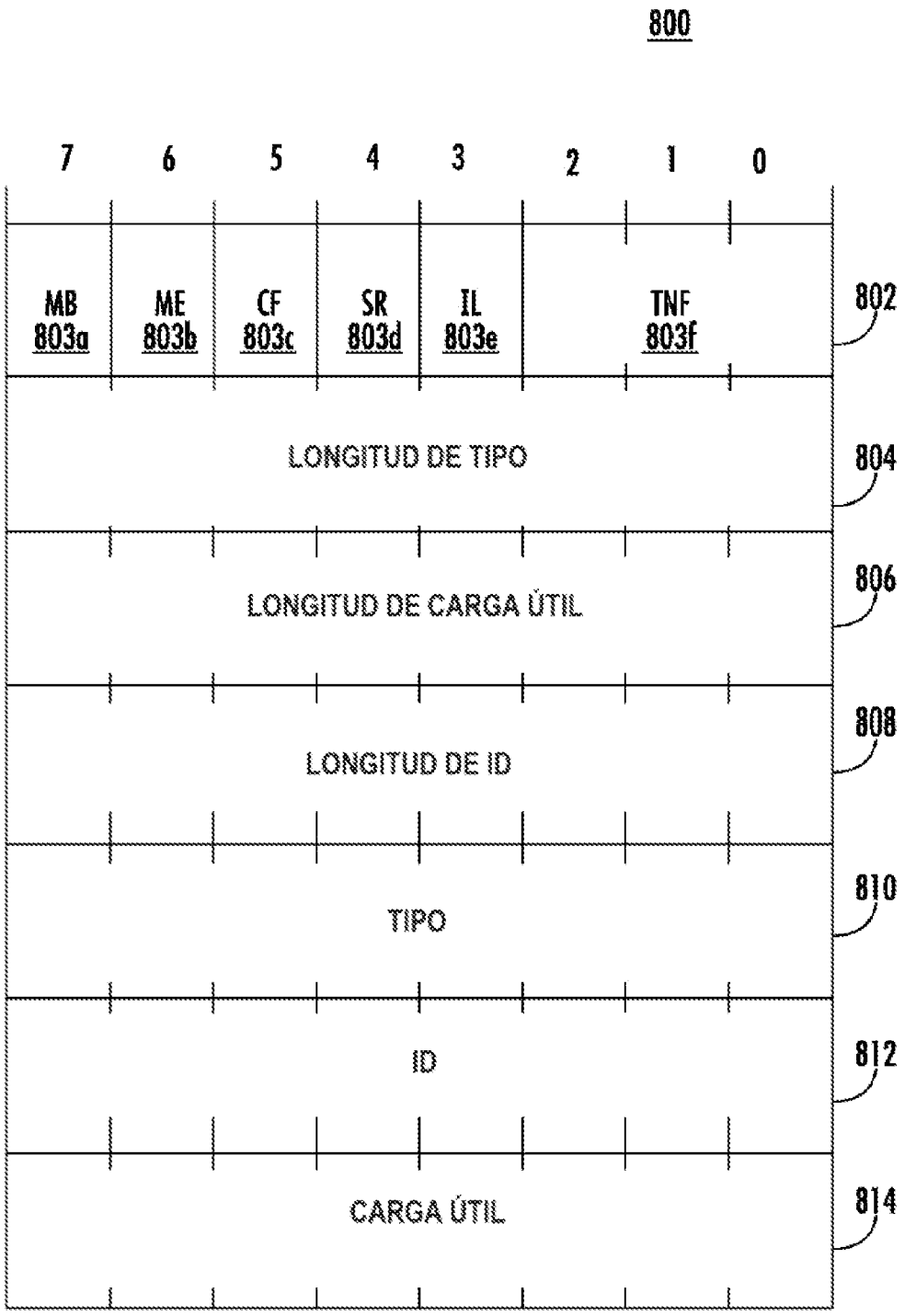
800
7
6
5
4
3
2
1
0
MB
803a
ME
803b
CF
803c
SR
803d
IL
803e
TNF
803f
802
LONGITUD DE TIPO
804
LONGITUD DE CARGA ÚTIL
806
LONGITUD DE ID
808
TIPO
810
ID
812
CARGA ÚTIL
814

FIG. 8

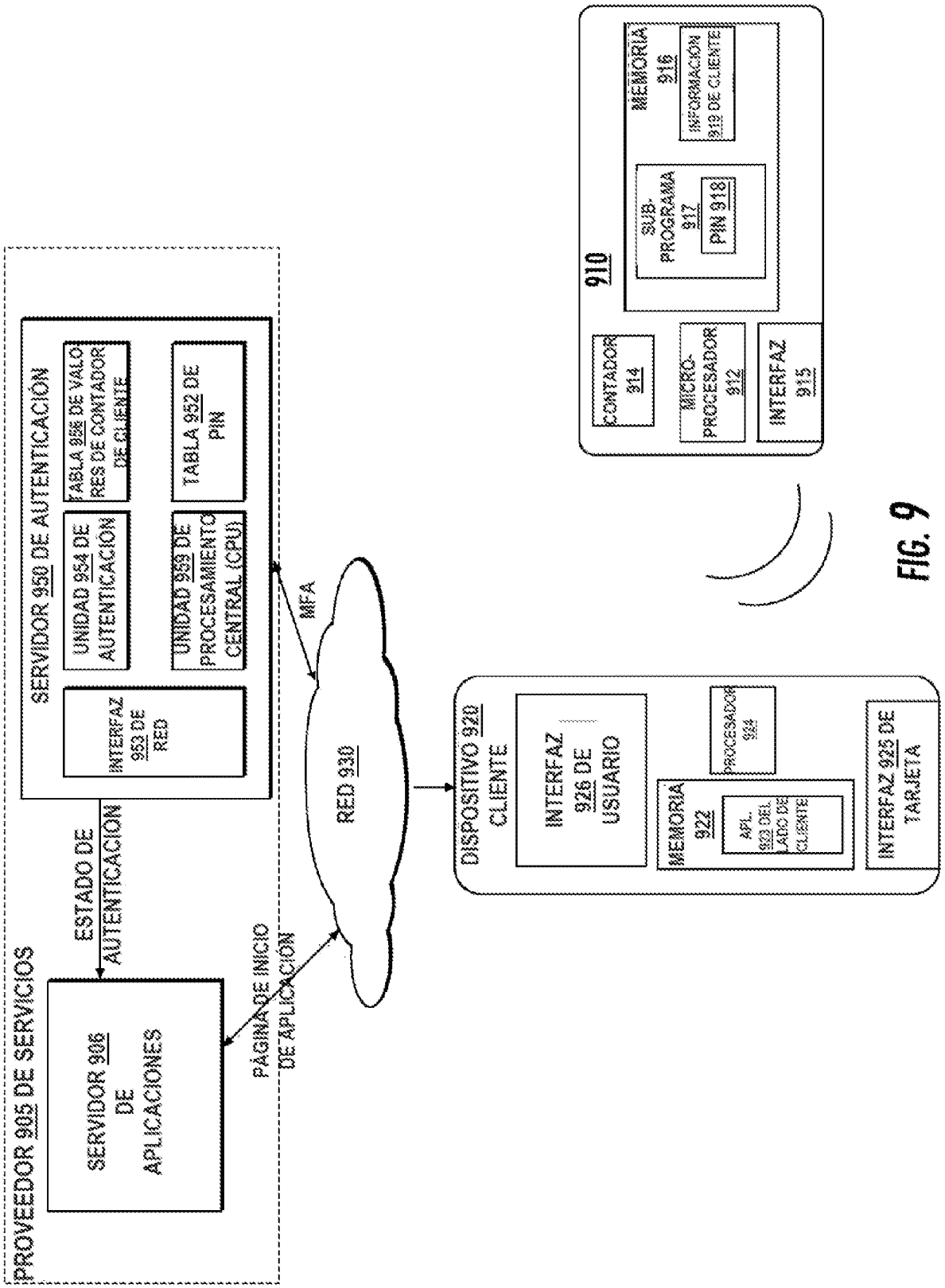
PROVEEDOR 905 DE SERVICIOS
SERVIDOR 906 DE APLICACIONES
ESTADO DE AUTENTICACIÓN
PÁGINA DE INICIO DE APLICACIÓN
SERVIDOR 950 DE AUTENTICACIÓN
INTERFAZ 953 DE RED
UNIDAD 954 DE AUTENTICACIÓN
UNIDAD 959 DE PROCESAMIENTO CENTRAL (CPU)
TABLA 956 DE VALORES DE CONTADOR DE CLIENTE
TABLA 952 DE PIN
RED 930
MFA
DISPOSITIVO 920 CLIENTE
INTERFAZ 926 DE USUARIO
MEMORIA 922
APL. 923 DEL LADO DE CLIENTE
PROCESADOR 924
INTERFAZ 925 DE TARJETA
910
CONTADOR 914
MICRO-PROCESADOR 912
INTERFAZ 915
MEMORIA 916
SUB-PROGRAMA 917
PIN 918
INFORMACIÓN 919 DE CLIENTE

FIG. 9

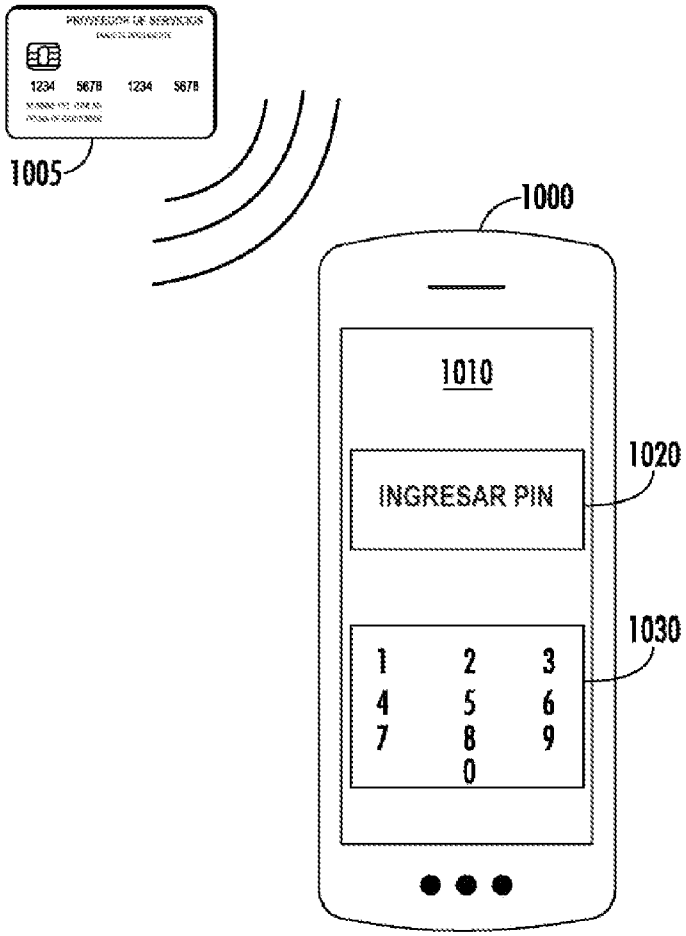
1234 5678 1234 5678
1005
1000
1010
1020
INGRESAR PIN
1030
1 2 3
4 5 6
7 8 9
0

FIG. 10