(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 968 820**

(51) Int. Cl.:

H04L 9/40	(2012.01)	***H04Q 3/00***	(2006.01)
H04M 15/00	(2006.01)	***H04Q 3/72***	(2006.01)
H04W 12/03	(2011.01)	***H04W 12/06***	(2011.01)
H04W 12/069	(2011.01)		
H04W 12/108	(2011.01)		
H04W 12/50	(2011.01)		
H04M 3/493	(2006.01)		
H04W 12/04	(2011.01)		
H04M 15/06	(2006.01)		
H04M 3/42	(2006.01)		

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **15.07.2020 PCT/US2020/042062**

(87) Fecha y número de publicación internacional: **28.01.2021 WO21016009**

(96) Fecha de presentación y número de la solicitud europea: **15.07.2020 E 20750990 (2)**

(97) Fecha y número de publicación de la concesión europea: **22.11.2023 EP 4000238**

(54) Título: **Técnicas de autenticación de llamadas**

(30) Prioridad:

19.07.2019 US 201916517074

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
14.05.2024

(73) Titular/es:

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

(72) Inventor/es:

RULE, JEFFREY;
BHATT, GAURANG;
GUO, ROCKY y
CUAN, LUKIIH

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Técnicas de autenticación de llamadas

Referencia cruzada a solicitudes relacionadas

Antecedentes

Las llamadas telefónicas no solicitadas presentan una molestia y un riesgo de seguridad para los destinatarios de la llamada. Los destinatarios pueden estar sujetos a llamadas molestas, como llamadas de tele-marketing, llamadas de broma, y/o llamadas silenciosas. Las llamadas no solicitadas también pueden utilizarse para iniciar fraudes telefónicos, en donde los impostores se hacen pasar por entidades legítimas en un intento de robar información o fondos.

La autenticación de llamadas telefónicas implica intentar identificar a la persona que llama. Sin embargo, los métodos actuales carecen de la capacidad de autenticar, de forma fiable, los dispositivos desde los que se llama y las partes que llaman desde ellos. Además, estos métodos, en el mejor de los casos, se implementan escasamente y están sujetos a prácticas como la suplantación de identidad, en la que una persona que llama puede utilizar una identidad y/o un número falsos para engañar al destinatario de la llamada para que responda. Como resultado, los usuarios suelen desconfiar, en el mejor de los casos, de los sistemas de comunicación. En el peor de los casos, pueden estar sujetos a molestias y/o riesgos de seguridad.

Los documentos US 2015/0940269 y US 2015/236857 describen sistemas y métodos para autenticar, automáticamente, la identidad de una persona que llama en una llamada telefónica.

Compendio

La invención se define en las reivindicaciones independientes. Realizaciones particulares se establecen en las reivindicaciones dependientes.

Según un aspecto de la invención, un método para realizar autenticación de llamadas entre pares incluye los pasos de recibir un flujo de datos de una llamada entrante de un primer dispositivo de telefonía móvil, comprendiendo el flujo de datos de la llamada entrante un número de la llamada entrante de un segundo dispositivo de telefonía móvil y una carga útil cifrada que comprende datos de carga útil cifrados utilizando una clave privada asociada al primer dispositivo de telefonía móvil. En algunas realizaciones, la clave privada comprende una clave dinámica del primer dispositivo de telefonía móvil y la carga útil cifrada comprende un criptograma. El método puede incluir autenticar el flujo de datos de la llamada entrante en respuesta a una coincidencia entre la carga útil cifrada y la información almacenada relacionada con el primer dispositivo de telefonía móvil. En diversos aspectos, la autenticación incluye reenviar el criptograma a un servidor de autenticación, en donde el servidor de autenticación mantiene y modifica una copia de la clave dinámica, simultáneamente, con el primer dispositivo de telefonía móvil, como la información almacenada relacionada con el primer dispositivo de telefonía móvil. En algunas realizaciones, la autenticación incluye además, recibir una validación del primer dispositivo de telefonía móvil desde el servidor de autenticación en respuesta a una coincidencia de contador entre un contador extraído del criptograma utilizando la copia de la clave dinámica y un contador esperado asociado al primer dispositivo de telefonía móvil. El método puede incluir además, establecer, de forma selectiva, una conexión de llamada entre el primer dispositivo de telefonía móvil y el segundo dispositivo de telefonía móvil en respuesta al paso de autenticación.

Según otro aspecto de la invención, un sistema para autenticar llamadas entre dispositivos comprende una interfaz configurada para recibir un flujo de datos de una llamada entrante de un primer dispositivo de telefonía móvil. En algunas realizaciones, el flujo de datos de la llamada entrante comprende un número de la llamada entrante asociado a un segundo dispositivo de telefonía móvil y una carga útil cifrada que comprende datos de carga útil cifrados utilizando una clave privada asociada al primer dispositivo de telefonía móvil. En algunas realizaciones, el sistema incluye un procesador acoplado a la interfaz y una memoria no volátil con código de programa almacenado en ella, siendo el código de programa operable cuando lo ejecuta el procesador para autenticar el flujo de datos de la llamada entrante en respuesta a una coincidencia entre la información de la carga útil cifrada y la información almacenada relacionada con el primer dispositivo de telefonía móvil. El sistema incluye además, una interfaz de comunicación acoplada al procesador y configurada para establecer, de forma selectiva, una conexión de llamada entre el primer dispositivo de telefonía móvil y el segundo dispositivo de telefonía móvil en respuesta al paso de autenticación.

Según otro aspecto más de la invención, un método para autenticar llamadas entre dispositivos móviles incluye los pasos de recibir un flujo de datos de una llamada entrante de un primer dispositivo de telefonía móvil. En algunas realizaciones, el flujo de datos de la llamada entrante comprende un número de la llamada entrante asociado a un segundo dispositivo de telefonía móvil, y una carga útil cifrada comprende datos de carga útil cifrados utilizando una clave privada asociada al primer dispositivo de telefonía móvil y a un atributo de un mensaje de voz. El método incluye recuperar una clave pública del número de la llamada entrante de un dispositivo de almacenamiento de datos y descifrar la carga útil cifrada utilizando la clave pública del número de la llamada entrante para producir una carga útil descifrada que comprende un identificador. El método incluye comparar el identificador de la carga útil descifrada con un identificador esperado asociado al número de la llamada entrante para determinar una coincidencia de autenticación de primer factor y comparar el atributo del mensaje de voz con un atributo del mensaje de voz esperado

para identificar una coincidencia de autenticación de segundo factor. El método incluye además, establecer, de forma selectiva, una conexión entre el primer dispositivo de telefonía móvil y el segundo dispositivo de telefonía móvil en respuesta a la coincidencia de autenticación de primer factor y a la coincidencia de autenticación de segundo factor.

Con tal disposición, se proporcionan un sistema y un método para autenticar, de forma fiable, llamadas entrantes.

Breve descripción de los dibujos

La **FIG. 1** es un primer diagrama de bloques de un sistema de transmisión de datos configurado para autenticar llamadas de usuarios según una realización de ejemplo;

La **FIG. 2** es un diagrama de bloques detallado que ilustra componentes ejemplares que pueden utilizarse en el sistema de la FIG. 1;

La **FIG. 3** es un diagrama de bloques detallado de los componentes del sistema de la FIG. 1 que pueden utilizarse para apoyar aspectos de la invención;

La **FIG. 4** es un diagrama que ilustra una secuencia para proporcionar acceso autenticado según una realización de ejemplo;

La **FIG. 5** es un diagrama de bloques, es un segundo diagrama de bloques, de un sistema de transmisión de datos configurado para autenticar llamadas de usuarios según una realización de ejemplo;

La **FIG. 6** es un primer flujo lógico proporcionado para describir pasos ejemplares que pueden realizarse durante una realización de un proceso de autenticación de llamada; y

La **FIG. 7** es un segundo flujo lógico proporcionado para describir pasos ejemplares que pueden realizarse durante una realización de un proceso de autenticación de llamada.

Descripción detallada

Un objetivo de algunas realizaciones de la presente descripción es el uso de una o más claves que se han incorporado en una o más tarjetas sin contacto como se describe en la(s) Solicitud(es) de Patente de EE. UU. Número de Serie 16/205,119 presentada el 29 de noviembre de 2018 por Osborn, titulada et al., "Systems and Methods for Cryptographic Authentication of Contactless Cards" e incorporada aquí como referencia (en adelante, la Solicitud '119). La tarjeta sin contacto puede utilizarse para realizar autenticación y otras muchas funciones que, de otro modo, requerirían que el usuario llevara consigo un token físico separado además de la tarjeta sin contacto. Al emplear una interfaz sin contacto, las tarjetas sin contacto pueden proporcionarse con un método para interactuar y comunicarse entre un dispositivo del usuario (como un teléfono móvil) y la propia tarjeta. Por ejemplo, el protocolo de comunicación de campo cercano (NFC), que subyace a muchas transacciones de tarjetas de crédito, incluye un proceso de autenticación que es suficiente para los sistemas operativos para Android® pero presenta desafíos para iOS,®, que es más restrictivo con respecto al uso de NFC, ya que solo puede utilizarse en modo de solo lectura. Las realizaciones ejemplares de las tarjetas sin contacto descritas en la Solicitud '119 pueden utilizar tecnología NFC. La autenticación de usuarios a través de la interfaz de la tarjeta sin contacto puede superar los problemas de robo de identidad de la técnica anterior validando los puntos finales de un enlace de llamada.

Varias realizaciones descritas en la presente memoria están dirigidas a autenticar llamadas utilizando una o más claves asociadas a un usuario específico. En los ejemplos, el usuario es el remitente de una llamada. En diversas realizaciones, cuando se realiza una llamada, se cifra una carga útil de identificación utilizando una clave privada asociada al usuario. La carga útil de identificación cifrada se adjunta al flujo de datos de la llamada. La carga útil de identificación puede descifrarse con una clave pública. En realizaciones, la carga útil de identificación puede verificarse. En diversas realizaciones, pueden realizarse métodos de autenticación adicionales utilizando un objeto como una tarjeta sin contacto para proporcionar uno o más componentes de la carga útil y/o claves de identificación. En realizaciones, puede realizarse una conexión entre el remitente y el destinatario previsto de una llamada en función de la verificación de la carga útil de identificación.

En algunas realizaciones descritas en la presente memoria, la clave privada utilizada para cifrar la carga útil de identificación puede almacenarse o emitirse con respecto a un dispositivo de usuario en particular. Un dispositivo de usuario de este tipo puede ser un ordenador conectado a la red. Como se menciona en la presente memoria, un ordenador conectado a la red puede incluir, pero no se limita a: p. ej., un dispositivo informático, o dispositivo de comunicaciones que incluye, p. ej., un servidor, un dispositivo de red, un ordenador personal (PC), una estación de trabajo, un dispositivo móvil, un teléfono, un PC de mano, un asistente digital personal (PDA), un dispositivo cliente ligero, un dispositivo cliente pesado, u otro dispositivo.

En algunas realizaciones descritas en la presente memoria, la clave privada utilizada para cifrar la carga útil de identificación puede almacenarse o emitirse con respecto a un objeto separado asociado al usuario. Por ejemplo, el objeto separado puede ser una tarjeta sin contacto, como se hace referencia en la solicitud '119 incorporada y con mayor detalle en la presente memoria. Las realizaciones no están limitadas en este contexto.

En diversas realizaciones descritas en la presente memoria, la carga útil de identificación puede comprender datos de texto, datos de audio, datos numéricos, o una combinación de los mismos. Por ejemplo, una carga útil de identificación puede comprender información sobre una asociación del usuario con un proveedor de servicios de comunicación, un mensaje de voz, o un contador asociado a una tarjeta sin contacto. Las realizaciones no están limitadas en este contexto.

Si bien las llamadas no solicitadas pueden provenir de una variedad de interlocutores con diversos propósitos, a menudo son difíciles de identificar para el destinatario, lo que conduce a una mala experiencia de usuario para los clientes del sistema de comunicación y la desconfianza del usuario en el sistema de comunicación.

Por ejemplo, el identificador de llamadas puede indicar al destinatario de la llamada que la persona que llama es un contacto conocido o mostrar el número de teléfono de la persona que llama para que el destinatario pueda reconocer un código de área en él. Sin embargo, la persona que llama puede desactivar el identificador de llamadas. Además, en este ejemplo, el destinatario aún recibe una notificación de la llamada entrante y aun así debe rechazarla deliberadamente. Además, los acosadores pueden evitar una identificación adecuada, por ejemplo, falsificando o bloqueando el identificador de llamadas. En otros ejemplos, los usuarios de voz sobre IP pueden enviar identificadores de llamadas falsos o enrutar llamadas a través de servidores en varios países.

Para el campo de las comunicaciones telefónicas, la FCC ha pedido la implementación del Tratamiento de la Información Declarada Basado en Firmas Utilizando toKENs (SHAKEN) y de los estándares de Identidad Telefónica Segura Revisitada (STIR), pero estos procedimientos tampoco logran autenticar, completamente, la identidad de una persona que llama. En SHAKEN/STIR, el proveedor de servicios de una persona que llama puede crear una firma digital en función de lo que sabe sobre el origen de la llamada, como el cliente y su derecho a usar el número desde el que llama, el cliente (pero no el número), o el punto desde el cual la llamada ingresa a su red. Puede asignarse un identificador de origen para identificar, de forma única, el origen de la llamada. Sin embargo, en estos procedimientos, la verificación final es que quien llama tiene derecho a aparecer como un determinado interlocutor ante el destinatario. Es posible que la llamada en realidad no provenga del número que aparece como la persona que llama. Por ejemplo, la suplantación de identidad aprobada por el proveedor de servicios puede seguir produciéndose. Incluso después de la implementación de dichos métodos, los destinatarios no tendrán certeza de la identidad al otro lado de una comunicación entrante. Existe la necesidad de un sistema mejorado para autenticar las identidades de las partes que originan la comunicación.

Varias realizaciones descritas en la presente memoria incluyen componentes que pueden permitir una o más de las siguientes: (1) autenticación de un iniciador de la comunicación en asociación con el dispositivo utilizado para iniciar la comunicación, (2) autenticación de un iniciador de la comunicación en asociación con el dispositivo utilizado para iniciar la comunicación y separar la información de identificación proporcionada por y/o relacionada con el iniciador de la comunicación, y (3) autenticación de un iniciador de la comunicación en asociación con el dispositivo utilizado para iniciar la comunicación y un objeto separado que posee, exclusivamente, el iniciador de la comunicación, por ejemplo, una tarjeta sin contacto.

La autenticación de las comunicaciones en función del dispositivo desde el que se enviaron reduce la posibilidad de que comunicaciones molestas, incluidos intentos de fraude, lleguen al cliente receptor, mejorando así la seguridad de su información. En algunas realizaciones, la conexión selectiva de un primer dispositivo cliente y de un segundo dispositivo cliente para una comunicación basada en los resultados de la autenticación o de la autenticación multifactor puede reducir la carga de comunicaciones no deseadas en los clientes y mejorar así la experiencia del cliente.

De este modo, las realizaciones descritas en la presente memoria aprovechan las características de autenticación de, al menos, un dispositivo cliente y/o proveedor de servicios en aplicaciones prácticas para aumentar la seguridad de las comunicaciones de red y/o mejorar la confianza del cliente en la autenticidad de las comunicaciones recibidas. En varias realizaciones, los componentes descritos en la presente memoria pueden proporcionar formas específicas y particulares de autenticar comunicaciones y/o gestionar comunicaciones en función de los resultados de la autenticación. En muchas realizaciones, uno o más de los componentes descritos en la presente memoria pueden implementarse como un conjunto de reglas que mejoran la tecnología informática permitiendo una función que un ordenador no podía realizar previamente y que permite lograr un resultado tecnológico mejorado. Por ejemplo, autenticar una comunicación en función de la información de identificación relacionada con el iniciador de la comunicación es un resultado tecnológico mejorado. En otro ejemplo, la función puede incluir autenticación multifactor segura a través de aprovechar las características de un dispositivo cliente y/u objeto separado, como una tarjeta sin contacto. En otro ejemplo, la función puede incluir gestionar las comunicaciones conectando, de forma selectiva, dispositivos para la comunicación según los resultados de la autenticación multifactor.

Estas y otras características de la invención se describirán ahora con referencia a las figuras, en donde se utilizan números de referencia similares para referirse a elementos similares en todas partes.

Tal como se utilizan en esta solicitud, los términos "sistema", "componente" y "unidad" pretenden referirse a una entidad informática, ya sea hardware, una combinación de hardware y software, software, o software en ejecución, ejemplos de los cuales se describen en la presente memoria. Por ejemplo, un componente puede ser, pero no se limita a ser, un proceso que se ejecuta en un procesador, un procesador, una unidad de disco duro, múltiples unidades de

almacenamiento (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 hilo de ejecución, y un componente puede localizarse en un ordenador y/o distribuirse entre dos o más ordenadores.

Además, los componentes pueden acoplarse, de forma comunicativa, 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 dichas asignaciones, cada mensaje es una señal. Sin embargo, otras realizaciones pueden emplear, alternativamente, mensajes de datos. Dichos mensajes de datos pueden enviarse a través de varias conexiones. Las conexiones ejemplares incluyen interfaces paralelas, interfaces serie, e interfaces de bus.

La **FIG. 1** ilustra un sistema 100 que incluye 2 o más dispositivos cliente 125 y 130 acoplados a través de una red 115. En diversas realizaciones, los dispositivos cliente 125 y 130 comprenden ordenadores conectados a la red y se comunican entre sí a través de la red 115. Específicamente, diversas realizaciones incluyen que cada dispositivo cliente esté asociado a una clave privada y a una clave pública. En realizaciones, un dispositivo cliente 125 que inicia una comunicación puede enviar un mensaje 140 que comprende un número de teléfono y una carga útil cifrada con su propia clave privada 126. El mensaje puede pasarse a través de un router 120 de autenticación que es parte de la red 115. La carga útil cifrada del mensaje 140 puede descifrarse utilizando la clave pública 127 asociada al dispositivo cliente 125. La comunicación puede pasarse al dispositivo cliente 130. Las realizaciones no están limitadas en este contexto.

En diversas realizaciones, un primer dispositivo cliente 125 puede iniciar una comunicación con la intención de llegar a uno o más dispositivos cliente 130. Aunque solo se ilustra un dispositivo en la **FIG. 1,** se entenderá que la comunicación podría tener una pluralidad de destinatarios, por ejemplo, como en un mensaje grupal, una llamada de conferencia, o un chat de video grupal. Las realizaciones no están limitadas en este contexto.

Los dispositivos cliente 125 y 130 pueden incluir un procesador y una memoria, y se entiende que el circuito de procesamiento puede contener componentes adicionales, que incluyen procesadores, memorias, comprobadores de errores y de 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 la presente memoria. Los dispositivos cliente 125 y 130 pueden incluir además, una pantalla y dispositivos de entrada. La pantalla puede ser cualquier tipo de dispositivo para presentar información visual, como un monitor de ordenador, una pantalla plana, y una pantalla de dispositivo móvil, incluidas pantallas de cristal líquido, pantallas de diodos emisores de luz, paneles de plasma, y pantallas de tubos de rayos catódicos. Los dispositivos de entrada pueden incluir cualquier dispositivo para ingresar información en el dispositivo del usuario que esté disponible y admitido por el dispositivo del usuario, como una pantalla táctil, un teclado, un ratón, un dispositivo de control del cursor, pantalla táctil, micrófono, cámara digital, grabadora de video o videocámara. Estos dispositivos pueden utilizarse para ingresar información e interactuar con el software y otros dispositivos descritos en la presente memoria.

Uno o más dispositivos cliente 125 y 130 también pueden ser un dispositivo móvil, por ejemplo, como un iPhone, iPod, iPad de Apple® o cualquier otro dispositivo móvil que ejecute el sistema operativo iOS de Apple, cualquier dispositivo que ejecute el sistema operativo Windows® Móvil de Microsoft y/o cualquier otro teléfono inteligente o dispositivo móvil portátil similar.

Los dispositivos cliente 125 y 130 pueden incluir una aplicación de cliente ligera adaptada, específicamente, para la comunicación con un proveedor de servicios. Un proveedor de servicios puede ser una empresa u otra entidad que proporciona servicios informáticos a través de una red. La aplicación de cliente ligera puede almacenarse en una memoria del dispositivo cliente y ser operativa cuando el dispositivo cliente la ejecuta para controlar una interfaz entre el dispositivo cliente y una aplicación del proveedor de servicios, que permite a un usuario en el dispositivo cliente acceder al contenido y los servicios del proveedor de servicios.

En realizaciones, el dispositivo cliente 125 está asociado a una clave privada 126 y a una clave pública 127. La clave privada 126 y la clave pública 127 pueden estar relacionadas para poder cifrar y descifrar datos, como en el cifrado de clave simétrica o el cifrado de clave asimétrica (también conocido como cifrado de clave pública). En realizaciones, la clave privada 126 y la clave pública 127 pueden ser diferentes, con la clave pública 127 estando disponible para sistemas externos al dispositivo cliente 125 y la clave privada 126 destinada a ser conocida sólo por el dispositivo cliente 125. En dichas realizaciones, el sistema 100 puede ser dirigido para utilizar cifrado de clave asimétrica. En algunas realizaciones, la misma clave pública puede estar disponible para y/o asociada a múltiples dispositivos cliente, por ejemplo, al dispositivo cliente 125 y al dispositivo cliente 130.

En diversas realizaciones, la clave privada 126 puede ser persistente o estática. En otras realizaciones, la clave privada puede ser una clave dinámica. Por ejemplo, una clave privada 126 puede ser una clave evolutiva. Una clave privada 126 puede cambiarse, por ejemplo, en función del tiempo, de un contador, u otra condición dinámica. En diversas realizaciones, un contador mediante el cual se actualiza una clave privada 126 puede avanzar por el uso por parte de un cliente del dispositivo cliente 125 o de un objeto separado, como una tarjeta sin contacto como se describe en la

solicitud '119 y con más detalle en la presente memoria. Se entenderá, fácilmente, que una clave dinámica puede actualizarse en respuesta a otros eventos, cambios de circunstancias, y/o una combinación de cualquiera de los descritos anteriormente.

En diversas realizaciones, la asociación de la clave privada 126 y/o de la clave pública 127 con el dispositivo cliente 125 puede establecerse en, o antes de, la emisión del dispositivo cliente 125 al cliente. Por ejemplo, las claves pueden ser establecidas por el fabricante del dispositivo, por un proveedor de servicios, u otra entidad. En otras realizaciones, la clave privada 126 y/o la clave pública 127 pueden vincularse al dispositivo más tarde. Por ejemplo, un dispositivo cliente 125 puede recibir las claves 126 y 127 actualizadas. En diversas realizaciones, la clave privada 126 y/o la clave pública 127 pueden almacenarse en la memoria del dispositivo cliente 125 o en un servidor o base de datos externa. En diversas realizaciones, la clave privada 126 y/o la clave pública 127 pueden actualizarse utilizando una aplicación en el dispositivo cliente y/o utilizando un ordenador separado. Por ejemplo, la clave privada 126 y/o la clave pública 127 pueden actualizarse o diversificarse de acuerdo con datos dinámicos como un contador. Dichos ejemplos se encuentran en la referencia '119, incorporada en la presente memoria por referencia.

El dispositivo cliente 125 puede iniciar una comunicación con otro dispositivo cliente 130 generando un mensaje 140. En realizaciones, el mensaje 140 puede comprender una carga útil cifrada y un número de teléfono. La carga útil cifrada puede cifrarse utilizando la clave privada 126. El número de teléfono puede comprender el número de teléfono del dispositivo cliente 125 y/o del dispositivo cliente 130. En realizaciones, la carga útil cifrada como la carga útil cifrada del mensaje 140 puede comprender datos de texto, numéricos, de audio, o de otro tipo, o una combinación de los mismos La carga útil puede comprender información de identificación, exclusivamente, para el cliente, el dispositivo cliente 125, o una combinación de los mismos. Además, la carga útil cifrada puede contener datos hash. Dicha información puede almacenarse en una memoria accesible al dispositivo cliente 125, por ejemplo, local al dispositivo cliente o accesible a través de una conexión de red. En diversas realizaciones, la carga útil cifrada puede comprender información dinámica relacionada con el cliente, con el dispositivo cliente 125, o con un objeto separado, por ejemplo, una tarjeta sin contacto como se describe con mayor detalle en la presente memoria. La información dinámica puede cambiar con cada comunicación enviada por el dispositivo cliente 125 o a otro tasa. En algunas realizaciones, la clave pública 127 puede incluirse en el mensaje 140.

En algunas realizaciones, la carga útil cifrada y/o el mensaje 140 pueden agregarse a una comunicación del dispositivo cliente 125. Por ejemplo, la carga útil cifrada puede agregarse a un flujo de datos de la llamada. En algunas realizaciones, una comunicación del dispositivo cliente 125 puede incluirse en la carga útil cifrada.

El mensaje 140 puede enviarse desde el dispositivo cliente 125. En diversas realizaciones, el mensaje 140 puede pasar a través de un router 120 de autenticación. El router 120 de autenticación puede estar asociado a una red 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 125 al proveedor 320 de servicios. Por ejemplo, la red 115 puede incluir una o más de una red de fibra óptica, una red óptica pasiva, una red de cable, una red de Internet, una red satelital, una red de área local inalámbrica (LAN), un Sistema Global para Comunicaciones Móviles, un Servicio de Comunicación Personal, una Red de Área Personal, Protocolo de Aplicaciones Inalámbricas, Servicio de Mensajería Multimedia, Servicio de Mensajería Mejorado, Servicio de Mensajes Cortos, sistemas basados en Multiplexación por División en el 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, Ethernet 902.3 del IEEE, una red de área amplia ("WAN"), una red de área personal inalámbrica ("WPAN"), una red de área local ("LAN"), o una red global como Internet. Además, la red 115 puede soportar una red de Internet, una red de comunicación inalámbrica, una red celular, o similares, o cualquier combinación de las mismas. La red 115 puede incluir además, una red, o cualquier número de los tipos de redes ejemplares mencionados anteriormente, que funcionan como una red independiente o en cooperación entre sí. La red 115 puede utilizar uno o más protocolos de uno o más elementos de red a los que está acoplada, de forma comunicativa. La red 115 puede traducir hacia o desde otros protocolos a uno o más protocolos de los dispositivos de red.

Además, debe apreciarse que según uno o más ejemplos, la red 115 puede ser parte de una pluralidad de redes interconectadas, como, por ejemplo, Internet, una red privada del proveedor de servicios, una red de televisión por cable, redes corporativas, como redes de asociaciones de tarjetas de crédito, y redes domésticas. En algunas realizaciones, el router 120 de autenticación y/o la red 115 pueden estar asociados a un proveedor de servicios de comunicación. Además, puede implementarse una red privada como una red privada virtual superpuesta a la red 115.

Por ejemplo, la red 115 puede comprender una red telefónica pública conmutada (PSTN), y el router de autenticación puede estar asociado al proveedor de servicios de comunicación utilizado por el cliente del dispositivo cliente 125 y/o del dispositivo cliente 130.

El router 120 de autenticación puede tener acceso a la clave pública 127 asociada al dispositivo cliente 125. En algunos casos, el router 120 de autenticación puede recibir la clave pública 127 del dispositivo cliente 125 a través del mensaje

140. En otras realizaciones, el router 120 de autenticación puede tener acceso a una base de datos, tabla, u otro almacenamiento o memoria en la que se almacena la clave pública 127. En estas realizaciones, la memoria puede ser local al router 120 de autenticación o estar disponible, de otro modo, a través de la red 115.

En algunas realizaciones, el router 120 de autenticación tiene acceso al almacenamiento como se describió anteriormente, que incluye información dinámica perteneciente a la carga útil cifrada del mensaje 140. Por ejemplo, la información dinámica incluida en la carga útil cifrada puede reflejarse mediante la información disponible para el router de autenticación. Por ejemplo, si la carga útil comprende información actual sobre una cuenta del cliente con un proveedor de servicios de comunicación, la memoria puede comprender información actual, mantenida por separado, sobre la cuenta del cliente con el proveedor de servicios. En otro ejemplo, si la carga útil cifrada comprende un contador que aumenta cada vez que un cliente utiliza el dispositivo cliente 125 para realizar una llamada, el contador puede actualizarse en la memoria accesible al router 120 de autenticación cada vez que el dispositivo cliente 125 realice una llamada.

Dicha información relativa al cliente y/o al dispositivo cliente 125 puede ponerse, inicialmente, a disposición del router 120 de autenticación tras la activación de un dispositivo cliente 125 o la emisión de un dispositivo cliente 125 a un cliente. Además, dicha información debe estar asociada al cliente y/o al dispositivo cliente. Por ejemplo, un contador asociado a un dispositivo cliente puede establecerse en cero o en algún otro número predeterminado en respuesta a la activación de un dispositivo, o un empleado del proveedor de servicios de comunicación puede ingresar la información inicial de la cuenta para un cliente en respuesta a la creación de una cuenta para el cliente. Sin embargo, dicha información se actualiza, independientemente, del contenido del mensaje 140.

En algunas realizaciones, la clave pública 127 se almacena en dicha memoria accesible al router 120 de autenticación. En realizaciones, la clave pública 127 puede ingresarse con una ubicación de memoria asociada al cliente y/o al dispositivo cliente 125 tras la emisión del dispositivo cliente 125 al cliente y/o el comienzo del servicio por parte del proveedor de servicios de comunicación. Si la clave pública se actualiza, por ejemplo, para que coincida con una clave privada actualizada, la clave pública 127 en la memoria puede actualizarse. En algunas realizaciones, esta actualización puede ser automática. En otras realizaciones, esta actualización puede realizarse en respuesta a un evento, por ejemplo, el envío de un mensaje 140 desde el dispositivo cliente 125. En algunas realizaciones, la clave pública 127 puede actualizarse en respuesta a ser recibida como parte de un mensaje 140.

En diversas realizaciones, el router 120 de autenticación puede descifrar el mensaje 140 utilizando la clave pública 127. En realizaciones en donde la carga útil cifrada comprende datos hash, puede aplicarse una función hash a la carga útil descifrada para extraer información, por ejemplo, un identificador. En realizaciones, el contenido de la carga útil descifrada del mensaje 140 puede entonces compararse con información conocida por el router de autenticación perteneciente al cliente y/o al dispositivo cliente. Por ejemplo, si la carga útil comprende un contador, ese contador puede compararse con el contador conocido por el router de autenticación. La coincidencia de la información de la carga útil descifrada y la información conocida por el router 120 de autenticación permite la autenticación del mensaje 140 como enviado, de forma genuina, desde el dispositivo cliente 125.

Como la clave pública 127 está relacionada con la clave privada 126, que es conocida sólo por el dispositivo cliente 125, el descifrado con éxito del mensaje 140 utilizando la clave pública 127 indica que el mensaje 140 fue enviado, de hecho, desde el dispositivo cliente 125. Sin embargo, una discrepancia entre la carga útil cifrada de un mensaje enviado desde un dispositivo cliente y la información disponible para el router de autenticación perteneciente al cliente y/o al dispositivo cliente 125 puede indicar una actividad nefasta. Por ejemplo, un pirata informático o un impostor puede haber obtenido acceso a la clave privada 126 del dispositivo cliente 125 y el mensaje recibido por el router de autenticación puede no ser del dispositivo cliente 125 identificado. En los casos donde no se pudo descifrar un mensaje entrante utilizando la clave pública 127 y/o la carga útil descifrada del mensaje no se pudo autenticar, la comunicación puede marcarse para el dispositivo cliente destinatario 130. En algunas realizaciones, la conexión para la comunicación entre los dispositivos cliente 125 y 130 puede no completarse en base a dicho fallo de autenticación. La información perteneciente al dispositivo cliente 125 y/o al mensaje 140 puede marcarse, almacenarse en una base de datos, y/o enviarse al proveedor de servicios u otra entidad, por ejemplo, las fuerzas del orden, en base a dicho fallo de autenticación. En algunas realizaciones, los dispositivos cliente 125 y 130 pueden conectarse para una comunicación en base a la autenticación con éxito del dispositivo cliente iniciador 125.

En algunas realizaciones, el dispositivo cliente 130 tiene una clave privada 136 asociada y una clave pública 137 propia. Se entenderá que estas claves pueden permitir una comunicación devuelta desde el dispositivo cliente 130 al dispositivo cliente 125 mediante los mismos métodos descritos con respecto a las comunicaciones desde el dispositivo cliente 125 al dispositivo cliente 130.

En diversas realizaciones, los procesos de autenticación pueden tener lugar, localmente, en el dispositivo cliente destinatario 130 en lugar de, localmente, en un router 120 de autenticación. Específicamente, la red 115 puede enrutar un mensaje 140 al dispositivo cliente 130 mientras aún está cifrado.

En dichas realizaciones, el dispositivo cliente 130 puede tener acceso a la clave pública 127 asociada al dispositivo cliente 125. En algunos casos, el dispositivo cliente 130 puede recibir la clave pública 127 del dispositivo cliente 125 a través del mensaje 140. En otras realizaciones, el dispositivo cliente 130 puede tener acceso a una base de datos,

tabla, u otro almacenamiento o memoria en la que se almacena la clave pública 127. En estas realizaciones, la memoria puede ser local al dispositivo cliente 130 o estar disponible, de otro modo, a través de la red 115.

En algunas realizaciones, el dispositivo cliente 130 tiene acceso al almacenamiento como se describió anteriormente, que incluye información dinámica perteneciente a la carga útil cifrada del mensaje 140. Por ejemplo, la información dinámica incluida en la carga útil cifrada puede reflejarse mediante la información disponible para el router de autenticación. Por ejemplo, si la carga útil comprende información actual sobre una cuenta del cliente con un proveedor de servicios de comunicación, la memoria puede comprender información actual, mantenida por separado, sobre la cuenta del cliente con el proveedor de servicios. En otro ejemplo, si la carga útil cifrada comprende un contador que aumenta cada vez que un cliente utiliza el dispositivo cliente 125 para realizar una llamada, el contador puede actualizarse en la memoria accesible al dispositivo cliente 130 cada vez que el dispositivo cliente 125 realice una llamada. En dicho ejemplo, los contadores relacionados con el dispositivo cliente 125 locales al dispositivo cliente 125 y locales al dispositivo cliente 130 pueden actualizarse, específicamente, en respuesta a las comunicaciones entre el dispositivo cliente 125 y el dispositivo cliente 130.

Dicha información relativa al cliente y/o al dispositivo cliente 125 puede ponerse, inicialmente, a disposición del dispositivo cliente 130 tras la activación de un dispositivo cliente 125 o la emisión de un dispositivo cliente 125 a un cliente. Además, dicha información debe estar asociada al cliente y/o al dispositivo cliente. Por ejemplo, un contador asociado a un dispositivo cliente 125 puede establecerse en cero o en otro número predeterminado en respuesta a la activación del dispositivo cliente 125, o un empleado del proveedor de servicios de comunicación puede ingresar la información inicial de la cuenta para un cliente en respuesta a la creación de una cuenta para el cliente. En este ejemplo, la información puede almacenarse en una memoria externa al dispositivo cliente 130, como una base de datos ubicada en un servidor de red. Sin embargo, dicha información se actualiza, independientemente, del contenido del mensaje 140.

En algunas realizaciones, la clave pública 127 se almacena en dicha memoria accesible al dispositivo cliente 130. En realizaciones, la clave pública 127 puede ingresarse en la memoria en asociación con el cliente y/o el dispositivo cliente 125 tras la emisión del dispositivo cliente 125 al cliente y/o el comienzo del servicio por parte del proveedor de servicios de comunicación. Si la clave pública se actualiza, por ejemplo, para que coincida con una clave privada evolutiva, la clave pública 127 en la memoria puede actualizarse. En algunas realizaciones, esta actualización puede ser automática. En otras realizaciones, esta actualización puede realizarse en respuesta a un evento, por ejemplo, el envío de un mensaje 140 desde el dispositivo cliente 125 al dispositivo cliente 130. En algunas realizaciones, la clave pública 127 puede actualizarse en la memoria disponible para el dispositivo cliente 130 en respuesta a ser recibida como parte de un mensaje 140.

En diversas realizaciones, el dispositivo cliente 130 puede descifrar el mensaje 140 utilizando la clave pública 127. En realizaciones, la carga útil descifrada del mensaje 140 puede entonces compararse con información conocida por el dispositivo cliente 130 perteneciente al cliente y/o al dispositivo cliente. Por ejemplo, si la carga útil comprende un contador, ese contador puede compararse con el contador conocido por el dispositivo cliente 130. La coincidencia de la información de la carga útil descifrada y la información conocida por el dispositivo cliente 130 permite la autenticación del mensaje 140 como enviado, de forma genuina, desde el dispositivo cliente 125.

Como la clave pública 127 está relacionada con la clave privada 126, que es conocida sólo por el dispositivo cliente 125, el descifrado con éxito del mensaje 140 utilizando la clave pública 127 indica que el mensaje 140 fue enviado, de hecho, desde el dispositivo cliente 125. Sin embargo, una discrepancia entre la carga útil cifrada de un mensaje enviado desde un dispositivo cliente y la información disponible para el router de autenticación perteneciente al cliente y/o al dispositivo cliente 125 puede indicar una actividad nefasta. Por ejemplo, un pirata informático o un impostor puede haber obtenido acceso a la clave privada 126 del dispositivo cliente 125 y el mensaje recibido por el router de autenticación puede no ser del dispositivo cliente 125 identificado. En los casos donde no se pudo descifrar un mensaje entrante utilizando la clave pública 127 y/o la carga útil descifrada del mensaje no se pudo autenticar, la comunicación puede marcarse para el dispositivo cliente destinatario 130. En algunas realizaciones, la conexión para la comunicación entre los dispositivos cliente 125 y 130 puede no completarse o continuarse en base a dicho fallo de autenticación. La información perteneciente al dispositivo cliente 125 y/o al mensaje 140 puede marcarse, almacenarse en una base de datos, y/o enviarse al proveedor de servicios u otra entidad, por ejemplo, las fuerzas del orden, en base a dicho fallo de autenticación. En algunas realizaciones, los dispositivos cliente 125 y 130 pueden conectarse para una comunicación en base a la autenticación con éxito del dispositivo cliente iniciador 125.

La **FIG. 2** es un diagrama de bloques que ilustra varios componentes ejemplares que pueden ser útiles para implementar métodos como los discutidos con respecto a la **FIG. 1.** El sistema 200 puede, por ejemplo, implementarse para permitir el cifrado y/o descifrado de datos. Como tal, pueden implementarse componentes similares como el dispositivo cliente 125, el router 120 de autenticación, y/o el dispositivo cliente 130. El sistema 200 está dirigido, particularmente, a comunicaciones que comprenden llamadas telefónicas. Las realizaciones no están limitadas de esta manera.

En realizaciones, el sistema 200 puede incluir un procesador 210. Se entiende que el circuito de procesamiento puede contener componentes adicionales, que incluyen procesadores, memorias, comprobadores de errores y de 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 la presente memoria. Además, el procesador 210 puede ser cualquiera de varios procesadores informáticos disponibles comercialmente, que incluyen, sin limitación, procesadores Athlon®, Duron® y Opteron® de AMD®; una aplicación ARM®, procesadores integrados y seguros; procesadores IBM® y DragonBall® y PowerPC® de Motorola®; procesadores IBM y Celulares de Sony®; procesadores Celeron®, Core®, Core (2) Duo®, Itanium®, Pentium®, Xeón®, y XScale® de Intel®; y procesadores similares. También pueden emplearse como el procesador 210 microprocesadores duales, procesadores de múltiples núcleos, y otras arquitecturas multiprocesador. Un procesador de este tipo puede permitir que un dispositivo conectado a la red se comunique con otros dispositivos conectados a la red mediante el uso de una interfaz PSTN 215 gestionada por un interfaz 220 de red SS7.

Específicamente, la interfaz PSTN 215 permite que el sistema 200 se conecte con una red 115 y sus servicios asociados. Una interfaz de red no. 7 del sistema de señalización (SSN) se utiliza para gestionar el uso de la red 115 por parte del sistema 200 a través de la interfaz PSTN 215 utilizando una ruta y una instalación distintas del canal de voz para señalar el establecimiento y la liberación de una comunicación.

Los sistemas de memoria como aquellos a los que se hace referencia con respecto al dispositivo cliente 125, al router 120 de autenticación, y al dispositivo cliente 130 pueden incorporarse como una memoria 225, en algunos ejemplos. La memoria 225 puede ser una memoria de sólo lectura, una memoria de lectura múltiple de una sola escritura o una memoria de lectura/escritura, p. ej., RAM, ROM, y EEPROM, y el sistema 200 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 de una sola vez brinda la oportunidad de escribir una vez y luego leer muchas veces. Puede programarse una memoria de escritura única/lectura múltiple en un momento dado después de que el chip de memoria haya salido de la fábrica. Una vez programada la memoria, es posible que no se reescriba, pero sí se puede leer muchas veces. Una memoria de lectura/escritura puede programarse y reprogramarse muchas veces después de salir de la fábrica. Una memoria de lectura/escritura también puede leerse muchas veces después de salir de la fábrica.

La memoria 225 puede configurarse para almacenar uno o más de los datos 230 de la clave, el código 235 de cifrado/descifrado, y el código 240 de validación de clave. Los datos de la clave pueden comprender claves utilizadas para cifrar y/o descifrar información como un mensaje, como el mensaje 140, una carga útil de identificación, u otra información. Por ejemplo, los datos 230 de la clave pueden comprender una clave privada 126 y una clave pública 127.

El código 235 de cifrado/descifrado puede comprender código para cifrar y/o descifrar información como un mensaje, como el mensaje 140, una carga útil de identificación, u otra información utilizando los datos 230 de la clave.

El código 240 de validación de clave puede comprender código para validar el cifrado y/o descifrado de información como un mensaje, como el mensaje 140, una carga útil de identificación, u otra información utilizando los datos 230 de la clave según el código 235 de cifrado/descifrado. En algunas realizaciones, el código 240 de validación de clave puede comprender una carga útil que identifica al cliente y/o al dispositivo cliente, por ejemplo, una carga útil de identificación del mensaje 140.

La **FIG. 3** es un diagrama de bloques que ilustra un sistema 300 en el que un dispositivo cliente 125 está acoplado, a través de una red 315, a un proveedor 320 de servicios. Las realizaciones no están limitadas de esta manera.

El proveedor 320 de servicios es, en una realización, una empresa que proporciona servicios informáticos a clientes a través de una red 115. Casi todos los proveedores de servicios modernos utilizan Internet para proporcionar ofertas de servicios a consumidores potenciales. Las ofertas de servicios se proporcionan, generalmente, en forma de aplicaciones de software que funcionan utilizando recursos dedicados del proveedor de servicios. La combinación de software y hardware que proporciona un servicio en particular a un cliente se denomina en la presente memoria "servidor". Los servidores pueden comunicarse a través de una red privada 350 del proveedor de servicios, a menudo denominada red corporativa o de empresa. La red privada 350 puede comprender una red inalámbrica, una red cableada o cualquier combinación de red inalámbrica y red cableada como se describió anteriormente con respecto a la red 115.

En el sistema 300, se muestra un proveedor 320 de servicios que incluye un servidor 360 de autenticación. Aunque el servidor se ilustra como un dispositivo discreto, se aprecia que las aplicaciones y servidores pueden distribuirse por toda la empresa o, en el caso de recursos distribuidos, como recursos 'en la nube', por toda la red 115.

La base de datos 330 comprende recursos de almacenamiento de datos que pueden utilizarse, por ejemplo, para almacenar la cuenta del cliente, credenciales y otra información de autenticación para su uso por parte del servidor 360 de autenticación. La base de datos 330 puede estar compuesta de recursos de datos acoplados que comprenden cualquier combinación de almacenamiento local, almacenamiento distribuido en centros de datos o almacenamiento basado en la nube.

Una tarjeta sin contacto 305 puede comprender una tarjeta de pago, como una tarjeta de crédito, tarjeta de débito, o tarjeta regalo, emitida por un proveedor 320 de servicios mostrada en el anverso o el reverso de la tarjeta 305. En algunos ejemplos, la tarjeta sin contacto 305 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 sin contacto 305 puede comprender un sustrato, 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 sin contacto 305 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 sin contacto 305 según la presente descripción puede tener características diferentes, y la presente descripción no requiere que se implemente una tarjeta sin contacto en una tarjeta de pago.

La tarjeta sin contacto 305 también puede incluir información de identificación mostrada en el anverso y/o el reverso de la tarjeta, y una almohadilla de contacto. La almohadilla de contacto puede configurarse para establecer contacto con otro dispositivo de comunicación, como un dispositivo de usuario, teléfono inteligente, ordenador portátil, de escritorio, o tableta. La tarjeta sin contacto 305 también puede incluir un circuito de procesamiento, antena y otros componentes no mostrados en la **FIG. 3.** Estos componentes pueden estar ubicados detrás de la almohadilla de contacto, o en cualquier otro lugar del sustrato. La tarjeta sin contacto 305 también puede incluir una tira o cinta magnética, que puede estar ubicada en el reverso de la tarjeta (no mostrada en la FIG. 3).

Según un aspecto, una tarjeta sin contacto 305 puede estar en comunicación inalámbrica, por ejemplo, NFC, con uno o más dispositivos cliente 125. Por ejemplo, la tarjeta sin contacto 305 puede comprender uno o más chips, como un chip de identificación por radiofrecuencia, configurado para comunicarse a través de NFC u otros protocolos de corto alcance. En otras realizaciones, la tarjeta sin contacto 305 puede comunicarse con los dispositivos cliente 410 a través de otros medios que incluyen, pero no se limitan a, Bluetooth, satélite, y/o WiFi. Como se describe en la solicitud `119, la tarjeta sin contacto 305 puede configurarse para comunicarse con uno de los dispositivos cliente 125 a través de NFC cuando la tarjeta sin contacto 305 está dentro del alcance del respectivo dispositivo cliente. Como se describirá con más detalle a continuación, la tarjeta sin contacto 305 puede generar un criptograma para su uso por parte del proveedor de servicios para autenticar el dispositivo cliente.

La tarjeta sin contacto 305 puede utilizarse para generar un criptograma del código de autenticación de mensaje (MAC) que puede funcionar como una firma digital con fines de verificación. Pueden utilizarse para realizar esta verificación otros algoritmos de firma digital, como algoritmos asimétricos de clave pública, p. ej., el Algoritmo de Firma Digital y el algoritmo RSA, o protocolos de conocimiento cero.

Más específicamente, la tarjeta sin contacto 305 puede utilizarse para generar una clave de sesión. La clave de sesión puede recibirse a través de la comunicación entre la tarjeta sin contacto 305 y el dispositivo cliente 125 y actuar como una clave privada como se describe con respecto a la **FIG. 1.** En realizaciones, este proceso puede ser una alternativa a la generación de, o almacenamiento de, una clave privada local para el dispositivo cliente 125 como se describe con respecto a la **FIG. 1.**

En realizaciones, la tarjeta sin contacto 305 puede utilizarse para pasar un identificador al dispositivo cliente 125. Un identificador podría ser un contador, por ejemplo. En diversas realizaciones, una clave privada asociada al dispositivo cliente 125 puede diversificarse utilizando el contador y/o utilizarse para cifrar el identificador de la tarjeta sin contacto 305 como parte de una carga útil de identificación cifrada.

El dispositivo cliente 125 puede enviar un mensaje, por ejemplo, el mensaje 140. En realizaciones, el mensaje puede adjuntarse a un flujo de datos de una llamada. El mensaje puede comprender una carga útil del identificador cifrada asociada al cliente y/o al dispositivo cliente 125. La carga útil del identificador puede comprender datos de audio, por ejemplo, un mensaje de voz. El mensaje puede comprender además, al menos, un número de teléfono, por ejemplo, como se encuentra en el mensaje 140.

En realizaciones, los datos de audio pueden grabarse a partir de una voz humana, por ejemplo, del cliente o de un empleado del proveedor de servicios. En algunas realizaciones, los datos de audio pueden comprender un mensaje de voz personalizado. En otras realizaciones, los datos de audio pueden ser generados por un ordenador. En dichas realizaciones, los datos de audio pueden generarse en respuesta a una interpretación del dispositivo informático de los datos de texto y/o numéricos, por ejemplo, mediante una aplicación o programa de conversión de texto a voz. La interpretación de los datos de texto y/o numéricos puede realizarse, localmente, al dispositivo cliente 125 o en otro dispositivo conectado a la red. Los datos interpretados pueden comprender información de identificación del cliente y/o del dispositivo cliente. Dicha información puede almacenarse en una memoria accesible al dispositivo cliente 125, por ejemplo, local al dispositivo cliente, local a la tarjeta sin contacto, o accesible a través de una conexión de red. Por ejemplo, la información para un cliente en particular puede encontrarse en una base de datos en asociación con el número de teléfono del dispositivo cliente desde el que se envió el mensaje. En algunas realizaciones, la información puede comprender información dinámica, como un contador.

La carga útil puede comprender además, información que incluye, al menos, un identificador, en algunas realizaciones. Un identificador de este tipo puede comprender un contador de la tarjeta sin contacto 305, por ejemplo, como se describe con más detalle en la presente memoria y en la solicitud '119.

En realizaciones, una red 315 puede incluir un sistema habilitado con respuesta de voz interactiva (IVR). El sistema IVR puede recibir y descifrar la carga útil de identificación cifrada enviada por el dispositivo cliente 125. El descifrado puede tener lugar mediante los métodos necesarios, por ejemplo, mediante los métodos descritos en la solicitud '119 o mediante los métodos descritos con respecto a la **FIG. 1.**

El identificador de la carga útil descifrada, por ejemplo, un contador, puede compararse con un identificador esperado asociado al dispositivo cliente desde el que se envió el mensaje. En realizaciones, el identificador esperado puede asociarse al dispositivo cliente mediante referencia a un número de teléfono asociado a ese dispositivo cliente. En realizaciones, el identificador esperado puede actualizarse, independientemente, del contenido de las comunicaciones entrantes desde el dispositivo asociado. Por ejemplo, puede aumentarse un contador tras la recepción de una comunicación desde el dispositivo cliente, pero, independientemente, del contenido de los mensajes recibidos del dispositivo cliente. En otro ejemplo, puede aumentarse un contador por cada mensaje recibido desde el dispositivo cliente cuando un mensaje contiene un determinado tipo de información. La comparación del identificador de la carga útil descifrada con el identificador esperado puede ser realizada por el sistema IVR, por otro dispositivo conectado a la red, por una aplicación al respecto, u otro procesador capaz. Las realizaciones no están limitadas de esta manera.

La coincidencia del identificador de la carga útil descifrada con el identificador esperado puede determinar una coincidencia de autenticación de primer factor. Esta autenticación añade una capa de seguridad más allá de la autenticación de clave simétrica o de clave asimétrica sola, al requerir no sólo un descifrado con éxito, sino también la coincidencia de un identificador conocido sólo por el dispositivo cliente 125 y la memoria en la que está almacenado el identificador esperado. Por ejemplo, un valor de contador de un número X coincidente de la carga útil descifrada con un valor esperado puede indicar no solo que la carga útil se pudo descifrar correctamente, sino que el dispositivo cliente emisor tenía el mismo registro de las comunicaciones pasadas del número X de con el servidor, como registro del servidor.

En realizaciones, el sistema IVR puede realizar una autenticación de segundo factor utilizando los datos de audio incluidos en la carga útil de identificación. En particular, el sistema IVR puede interpretar los datos de audio incluidos en la carga útil de identificación. En algunas realizaciones, los datos de audio de la carga útil descifrada pueden interpretarse mediante un programa de transcripción de voz, como una aplicación de conversión de voz a texto. En algunas realizaciones, los datos de audio pueden analizarse para determinar las características de los propios datos de audio. En realizaciones, los atributos, como atributos del mensaje de voz, pueden identificarse a partir de los datos de audio. Los atributos del mensaje de voz pueden incluir palabras reconocidas, habla humana versus voz generada por ordenador, características de la voz como tono, idioma, acento, cadencia, ruido de fondo, volumen y otras características reconocibles en los datos de audio por un ordenador. Dichos atributos pueden identificarse utilizando métodos conocidos en la técnica de procesamiento del lenguaje, por ejemplo, identificación o reconocimiento de palabras clave de acuerdo con un modelo entrenado por uno o más algoritmos de aprendizaje automático, redes neuronales, u otro método de entrenamiento. En algunas realizaciones, puede calcularse, al menos, un nivel de confianza según la probabilidad de que los datos de audio contengan, al menos, un atributo.

Los datos de audio interpretados pueden, en realizaciones, ser recibidos por un proveedor 320 de servicios. El proveedor 320 de servicios puede incluir una red empresarial privada 350, un servidor 360 de autenticación, y una base de datos 330. En realizaciones, aspectos del análisis de los datos de audio pueden tener lugar en la red empresarial 350 en contraposición a la red pública 315. En los casos donde el análisis se realiza como se describió anteriormente en la red 315, los atributos identificados de los datos de audio pueden enviarse a la red empresarial.

Un servidor 360 de autenticación puede comparar los atributos identificados de los datos de audio de la carga útil descifrada con atributos esperados de los datos de audio de un cliente y/o dispositivo cliente 125 en particular. Dichos atributos pueden almacenarse en asociación con un cliente y/o dispositivo cliente en la base de datos 330. Por ejemplo, un mensaje de voz personalizado de la carga útil descifrada puede compararse con un mensaje de voz personalizado, previamente conocido, asociado al dispositivo cliente 125 en la base de datos 330. En algunas realizaciones, puede utilizarse un análisis binario de la coincidencia de los atributos. En otras realizaciones, los atributos pueden ser coincidentes según un nivel de confianza dentro de un cierto rango. Dicho nivel de confianza puede ser calculado por uno o más métodos de aprendizaje automático, métodos de identificación de palabras clave, y/u otros métodos conocidos en la técnica, por ejemplo. En base a la comparación de los atributos identificados con los atributos esperados de los datos de audio, el servidor 360 de autenticación puede o no ser capaz de establecer una coincidencia de autenticación de segundo factor. Como dicha coincidencia de autenticación de segundo factor puede basarse en información y/o datos de audio que son únicos para el usuario esperado del dispositivo cliente 125, la autenticación puede proporcionar confianza de que el usuario real del dispositivo cliente 125 es el usuario esperado, en lugar de un impostor.

En algunas realizaciones, el sistema IVR puede establecer, de forma selectiva, una conexión entre el primer dispositivo cliente 125 y el segundo dispositivo cliente 130 en función de los resultados de la coincidencia de autenticación de primer y/o de segundo factor. En algunas realizaciones, el servidor 360 de autenticación puede comunicar al sistema IVR los resultados de la coincidencia de autenticación de primer y/o de segundo factor. En algunas realizaciones, el servidor 360 de autenticación puede comunicar, además, instrucciones para conectar o no conectar el primer dispositivo cliente 125 y el segundo dispositivo cliente 130 en función del resultado de las coincidencias de autenticación de uno o más de factores. En otras realizaciones, el sistema PSTN o IVR en la red 315 puede recibir los

resultados de la primera y/o de la segunda coincidencia de autenticación y determinar si se conecta o no el primer dispositivo cliente 125 y el segundo dispositivo cliente 130 para una comunicación en función de los resultados de las coincidencias de autenticación de uno o más factores. En algunas realizaciones, el sistema IVR puede utilizarse para limitar el acceso del primer dispositivo cliente 125 al segundo dispositivo cliente 130 en base a que el primer dispositivo cliente 125 esté autenticado como uno de, al menos uno, los interlocutores validados conocidos. Por ejemplo, dichos interlocutores validados pueden ser conocidos y/o marcados en el sistema por realizar llamadas no solicitadas problemáticas.

La **FIG. 4** es un diagrama de tiempos que ilustra una secuencia de ejemplo para proporcionar acceso autenticado según una o más realizaciones de la presente descripción. El sistema 400 puede comprender una tarjeta sin contacto 305 y un dispositivo cliente 410, que puede incluir una aplicación 422 y un procesador 424. Las realizaciones no están limitadas de esta manera.

En el paso 402, la aplicación 422 se comunica con la tarjeta sin contacto 305 (p. ej., después de acercarse a la tarjeta sin contacto 305). La comunicación entre la aplicación 422 y la tarjeta sin contacto 305 puede implicar que la tarjeta sin contacto 305 esté lo suficientemente cerca de un lector de tarjetas (no mostrado) del dispositivo cliente 410 para permitir una transferencia de datos NFC entre la aplicación 422 y la tarjeta sin contacto 305.

En el paso 404, después de que se haya establecido una comunicación entre el dispositivo cliente 410 y la tarjeta sin contacto 305, la tarjeta sin contacto 305 genera un criptograma MAC. En algunos ejemplos, esto puede ocurrir cuando la aplicación 422 lee la tarjeta sin contacto 305. En particular, esto puede ocurrir tras una lectura, como una lectura NFC, de una etiqueta de intercambio de datos de campo cercano (NDEF), que puede crearse de acuerdo con el Formato de Intercambio de Datos NFC. Por ejemplo, un lector, como la aplicación 422, puede transmitir un mensaje, como un mensaje de selección de subprograma, con el ID del subprograma de un subprograma productor de NDEF. Tras la confirmación de la selección, puede transmitirse 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, puede actualizarse o incrementarse un valor de contador mantenido por la tarjeta sin contacto 305, lo que puede ir seguido de "Leer archivo NDEF". En este punto, puede generarse el mensaje que puede incluir una cabecera y un secreto compartido. Luego pueden generarse las claves de sesión. El criptograma MAC puede crearse a partir del mensaje, que puede incluir la cabecera y el secreto compartido. Luego, el criptograma MAC puede concatenarse con uno o más bloques de datos aleatorios, y el criptograma MAC y un número aleatorio (RND) pueden cifrarse con la clave de sesión. A partir de entonces, el criptograma y la cabecera pueden concatenarse, y codificarse como ASCII hexadecimal y devolverse en el formato del 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 (p. ej., como una cadena formateada).

En algunos ejemplos, la aplicación 422 puede configurarse para transmitir una solicitud a la tarjeta sin contacto 305, comprendiendo la solicitud una instrucción para generar un criptograma MAC.

En el paso 406, la tarjeta sin contacto 305 envía el criptograma MAC a la aplicación 422. 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 408, la aplicación 422 comunica el criptograma MAC al procesador 424.

En el paso 412, el procesador 424 verifica el criptograma MAC con arreglo a una instrucción de la aplicación 422. Por ejemplo, el criptograma MAC puede verificarse, como se explica a continuación.

En algunos ejemplos, la verificación del criptograma MAC puede ser realizada por un dispositivo distinto del dispositivo cliente 410, como un proveedor 320 de servicios en comunicación de datos con el dispositivo cliente 410. Por ejemplo, el procesador 424 puede emitir el criptograma MAC para su transmisión al proveedor de servicios. 320, que puede verificar el criptograma MAC.

En algunos ejemplos, el criptograma MAC puede funcionar como una firma digital con fines de verificación. Pueden utilizarse para realizar esta verificación otros algoritmos de firma digital, como algoritmos asimétricos de clave pública, p. ej., el Algoritmo de Firma Digital y el algoritmo RSA, o protocolos de conocimiento cero.

Más específicamente, según un aspecto, puede utilizarse una tarjeta sin contacto 305 junto con las primeras credenciales de autenticación proporcionadas a un proveedor de servicios, como el proveedor 320 de servicios, para autenticar una comunicación desde un dispositivo cliente 410, por ejemplo, una llamada. El uso de la tarjeta sin contacto como segundo factor de autenticación permite la asociación de un dispositivo/número de teléfono en particular con un individuo específico (es decir, el propietario de la tarjeta), eliminando así la capacidad de falsificar de un tercero malintencionado, es decir, suplantar al cliente. Según otro aspecto de la invención, los protocolos de la comunicación de autenticación descritos en la presente memoria identifican o utilizan canales de comunicación específicos para el manejo de llamadas, reduciendo así la posibilidad de suplantación del cliente.

La autenticación del factor de seguridad puede comprender una pluralidad de procesos. En algunas realizaciones, un primer proceso de autenticación puede comprender iniciar sesión y validar a un usuario a través de una o más aplicaciones que se ejecutan en un dispositivo. Un segundo proceso de autenticación puede operar después del inicio de sesión y de la validación con éxito, para hacer que un usuario participe en uno o más comportamientos asociados a una o más tarjetas sin contacto. En efecto, el proceso de autenticación del factor de seguridad comprende un proceso de autenticación multifactor que puede incluir, tanto probar, de forma segura, la identidad del usuario como alentar al usuario a participar en uno o más tipos de comportamientos, que incluyen, pero no se limitan a, uno o más gestos de toque, asociados a la tarjeta sin contacto. En algunos ejemplos, el uno o más gestos de toque pueden comprender un toque de la tarjeta sin contacto por parte del usuario a un dispositivo. En algunos ejemplos, el dispositivo puede comprender un dispositivo móvil, un terminal, una tableta, o cualquier otro dispositivo configurado para procesar un gesto de toque recibido.

Por ejemplo, para proporcionar una primera capa de autenticación, un cliente puede acceder a una aplicación que opera en el dispositivo cliente. En otros ejemplos, el cliente puede acceder al sitio web del proveedor de servicios mediante un enlace a una página web del proveedor de servicios utilizando una aplicación de navegador de Internet que se ejecuta en el dispositivo cliente. El navegador es una aplicación de software como Google® Chrome®, Internet Explorer ®, Safari ®, etc., e incluye código de programación para traducir páginas web en Lenguaje de Marcado de Hipertexto (HTML) de la aplicación del proveedor de servicios a un formato adecuado para un cliente que opera el dispositivo cliente.

Como parte del acceso a la aplicación o al sitio web del proveedor de servicios, el proveedor de servicios puede solicitar información de la primera autorización, que incluye información de contraseña, respuestas a consultas previamente almacenadas, información biométrica, una imagen, u otro mecanismo para verificar que un usuario del dispositivo cliente está autorizado a acceder a contenidos y servicios, incluidas cuentas, gestionadas por el proveedor de servicios. Además, este nivel de autenticación proporciona la confianza de que el usuario del dispositivo cliente 125 es el cliente esperado. En otras palabras, mientras que los métodos descritos anteriormente pueden ser, particularmente útiles, para, al menos, autenticar que una comunicación proviene de un dispositivo autenticado, estos pasos pueden autenticar aún más que una comunicación proviene de un usuario autenticado de dicho dispositivo.

Según un aspecto, la tarjeta sin contacto 305 puede utilizarse para proporcionar una segunda autenticación para un usuario de un dispositivo cliente. En una realización, y como se describe con más detalle a continuación, la tarjeta sin contacto incluye una clave, un contador, y una funcionalidad de procesamiento criptográfico que puede utilizarse para generar un criptograma que puede utilizarse para validar a un usuario de un dispositivo cliente. El contador refleja, de forma ventajosa, comportamientos previos del titular de la tarjeta. Por ejemplo, el contador puede reflejar el número de veces que el usuario se ha comunicado, previamente, con una parte en particular, información que es prácticamente imposible de obtener con precisión para un tercero malintencionado.

Puede realizarse un nivel adicional de autenticación utilizando la tarjeta sin contacto 305, por ejemplo, acoplando, de forma comunicativa, la tarjeta 305 a uno de los dispositivos cliente 410 mediante toques o de otro modo, como se mencionó anteriormente. En algunas realizaciones, esto constituye la segunda autenticación. En otras realizaciones, la segunda autenticación continúa con un análisis adicional de una carga útil de identificación, por ejemplo, como se describe con respecto a la **FIG. 3.**

Después de la segunda autenticación, y como se describe con más detalle en la presente memoria, los datos pueden devolverse al dispositivo cliente. Por ejemplo, los datos pueden incluir datos que permitan al cliente iniciar un enlace de comunicación con el segundo dispositivo cliente o información sobre el éxito o el fracaso del intento de autenticación.

Cabe señalar que, aunque en la descripción anterior la primera autenticación se describe como el uso de información personal, biométrica, preguntas u otra información de autenticación, se reconoce que en algunos ejemplos, una aplicación cliente que se ejecuta en un dispositivo puede responder a un toque de una tarjeta sin contacto para activar o lanzar, inicialmente, la aplicación del dispositivo. En dichos ejemplos, tanto el primer como el segundo proceso de autenticación utilizan el proceso de autenticación de tarjeta sin contacto con llave/contador que se describe con más detalle a continuación.

En algunas realizaciones, si la aplicación del lado del cliente no está instalada en un dispositivo cliente, un toque de la tarjeta sin contacto cerca del lector de tarjetas puede iniciar una descarga de la aplicación (como una navegación a una página de descarga de la aplicación). Después de la instalación, un toque de la tarjeta sin contacto puede activar o lanzar la aplicación y luego iniciar, por ejemplo a través de la aplicación o de otra comunicación de backend, la activación de la tarjeta sin contacto. En algunos ejemplos, la una o más aplicaciones pueden configurarse para determinar que se lanzó a través de uno o más gestos de toque de la tarjeta sin contacto, de modo que el lanzamiento se produjo a las 3:51 p.m., que una transacción se procesó o tuvo lugar a las 3:56 PM, con el fin de verificar la identidad del usuario.

En algunos ejemplos, pueden recopilarse datos sobre comportamientos de toque como autenticación biométrica/gestual. Por ejemplo, un identificador único que sea, criptográficamente, seguro y no susceptible de interceptación, puede transmitirse a uno o más servicios de backend. El identificador único puede configurarse para

buscar información secundaria sobre el individuo. La información secundaria puede comprender información de identificación personal sobre el usuario. En algunos ejemplos, la información secundaria puede almacenarse dentro de la tarjeta sin contacto.

La **FIG.** 5 ilustra un sistema ejemplar 500 en el que puede realizarse una llamada autenticada. El sistema 500 comprende dos o más dispositivos cliente 125 y 130. Como se ilustra, un único dispositivo cliente 125 es el dispositivo utilizado para iniciar la comunicación y un único dispositivo cliente 130 es el dispositivo utilizado para recibir la comunicación. Sin embargo, se entenderá fácilmente que la comunicación podría transmitirse desde el dispositivo cliente 130 al dispositivo cliente 125 y/o que cada dispositivo cliente como se ilustra puede comprender una pluralidad de dispositivos cliente, como en una llamada grupal. Las realizaciones no están limitadas de esta manera.

El dispositivo cliente 125 puede estar asociado a una clave privada 126 y a una clave pública 127. El dispositivo cliente 130 puede estar asociado a una clave privada 136 y a una clave pública 137. En realizaciones en las que, al menos, uno del dispositivo cliente 125 o del dispositivo cliente 130 representa una pluralidad de dispositivos cliente, cada dispositivo cliente puede estar asociado a una clave privada y a una clave pública.

Para cada dispositivo cliente, la clave privada y la clave pública pueden estar relacionadas de modo que una descifre los datos cifrados por la otra. En algunas realizaciones, la clave privada y la clave pública para un dispositivo pueden ser la misma, lo que permite el cifrado de clave simétrica. En otras realizaciones, la clave privada y la clave pública pueden ser diferentes, lo que permite el cifrado de clave asimétrica. Las claves pueden ser persistentes o dinámicas. En algunas realizaciones, una clave privada puede ser una clave de sesión diversificada mediante el uso de información dinámica local al dispositivo cliente o proporcionada por un objeto o dispositivo externo, como una tarjeta sin contacto, como se describió anteriormente.

En diversas realizaciones, el dispositivo cliente 125 puede iniciar una comunicación con el dispositivo cliente 130, por ejemplo, un flujo de datos de una llamada. Puede adjuntarse un mensaje 505 a la comunicación. El mensaje 505 puede comprender una carga útil cifrada, al menos, un número de teléfono, comprendiendo el, al menos uno, número de teléfono un número de teléfono asociado al dispositivo cliente destinatario 130, y una nota de voz. En realizaciones, el propietario del dispositivo cliente emisor 125 puede personalizar la nota de voz, por ejemplo, una frase o un saludo. En algunas realizaciones, el mensaje 505 puede incluir, además, la clave pública 127 del dispositivo cliente 125.

La carga útil cifrada puede cifrarse utilizando la clave privada del dispositivo cliente 125. La carga útil cifrada puede comprender, al menos, un identificador. En algunos casos, la nota de voz puede incluirse en la carga útil cifrada.

El segundo dispositivo cliente 130 puede tener acceso a la clave pública 127 del primer dispositivo cliente 125 en asociación con el número de teléfono u otros datos de identificación para el dispositivo cliente 125. Por ejemplo, la clave pública 127 del primer dispositivo cliente 125 puede recibirse con el mensaje 505, almacenarse, localmente, en la memoria del dispositivo cliente 130 después de una comunicación previa entre los dos dispositivos, o estar disponible a través de otra memoria o base de datos, como una base de datos vinculada a Internet. Además, el segundo dispositivo cliente 130 puede tener acceso a un identificador esperado en asociación con el dispositivo cliente 125. Por ejemplo, la misma base de datos puede utilizarse para almacenar, al menos, un dispositivo cliente 125, una clave pública asociada, y un identificador esperado asociado a ese dispositivo cliente 125.

El mensaje 505 puede ser recibido por el dispositivo cliente 130. El dispositivo cliente 130 puede recuperar la clave pública 127 asociada al dispositivo cliente 125 y utilizar la clave pública 127 para descifrar la carga útil cifrada del mensaje 505.

El fallo en el descifrado de la carga útil con la clave pública 127 puede indicar un posible comportamiento fraudulento. Como resultado, la conexión de comunicación que, supuestamente, proviene del dispositivo cliente 125 puede ser denegada. En algunas realizaciones, puede proporcionarse retroalimentación al usuario del dispositivo cliente 130, a un proveedor de servicios, o a un tercero, por ejemplo, fuerzas policiales.

En algunas realizaciones, la nota de voz del mensaje 505 puede presentarse al usuario del dispositivo cliente 130, por ejemplo, a través de una interfaz de usuario reproduciendo los datos de audio de la nota de voz al usuario del dispositivo cliente 130, cuando responde la llamada entrante. La interfaz de usuario puede ser una parte de una aplicación en el dispositivo cliente 130. En algunas realizaciones, la nota de voz del mensaje 505 sólo puede presentarse al usuario en base a una primera autenticación con éxito del identificador de la carga útil cifrada.

El dispositivo cliente 130 puede entonces recibir retroalimentación de su usuario si reconoce o no la nota de voz del usuario del primer dispositivo cliente 125. Por ejemplo, la retroalimentación puede recibirse a través de una interfaz de usuario. Esta verificación del reconocimiento de la nota de voz del primer cliente por parte del segundo cliente proporciona una capa adicional de autenticación. En algunas realizaciones, el dispositivo cliente 130 puede recibir instrucciones del usuario a través de la interfaz de usuario que dirige la continuación o denegación de la conexión de comunicación entre los dispositivos cliente 125 y 130.

En función de la retroalimentación relativa al reconocimiento de la nota de voz recibida del usuario, el dispositivo cliente 130 puede establecer, de forma selectiva, una conexión entre el dispositivo cliente 125 y el dispositivo cliente 130. En algunas realizaciones, en función de la retroalimentación, el dispositivo cliente 130 puede salvar la clave pública 127

del dispositivo cliente 125 en la memoria local o agregar el dispositivo cliente 125 a una lista de dispositivos reconocidos y/o de confianza.

En algunas realizaciones, la comunicación continua entre dispositivos reconocidos y/o de confianza puede tener lugar con métodos de autenticación simplificados. Por ejemplo, es posible que sólo se requiera un primer nivel de autenticación.

La **FIG. 6** es un flujo lógico 600 que ilustra un método para conectar, de forma selectiva, un primer dispositivo cliente y un segundo dispositivo cliente para una comunicación en base a los resultados de la autenticación. Específicamente, **FIG. 6** ilustra un ejemplo en el que el primer y el segundo dispositivo cliente son ambos dispositivos de telefonía móvil y la comunicación es un flujo de datos de una llamada. Las realizaciones no están limitadas en la presente memoria.

En el paso 610, se recibe un flujo de datos de una llamada entrante de un primer dispositivo de telefonía móvil. El flujo de la llamada entrante comprende un número de teléfono asociado a un segundo dispositivo de telefonía móvil y una carga útil cifrada. La carga útil cifrada se cifra utilizando una clave privada asociada al primer dispositivo móvil. En realizaciones, la carga útil cifrada puede adjuntarse al flujo de datos de la llamada entrante. Los datos de la carga útil pueden comprender información perteneciente al primer cliente y/o dispositivo cliente.

En el paso 620, el flujo de datos de la llamada entrante puede autenticarse en respuesta a una coincidencia entre la información de la carga útil cifrada y la información almacenada relacionada con el primer dispositivo de telefonía móvil. En diversas realizaciones, la coincidencia entre la información de la carga útil cifrada y la información almacenada relacionada con el primer dispositivo de telefonía móvil puede juzgarse mediante el descifrado con éxito de la carga útil. Por ejemplo, una carga útil puede haber sido cifrada con una clave pública diversificada utilizando un contador. En este ejemplo, el descifrado con éxito de la carga útil con una clave pública diversificada por un contador, mantenido de forma independiente, puede indicar una autenticación adecuada.

En el paso 630, el sistema puede establecer una conexión de llamada entre el primer dispositivo de telefonía móvil y el segundo dispositivo de telefonía móvil en respuesta al paso de autenticación.

En algunas realizaciones, un fallo del sistema para autenticar, adecuadamente, una llamada puede provocar la denegación de la llamada u otro método de desestimación de la llamada. En algunas realizaciones, puede notificarse a un primer dispositivo cliente y/o a un segundo dispositivo cliente del intento fallido y proporcionar detalles del intento, como el número de teléfono de la persona que llama y/o del destinatario. En algunas realizaciones, puede solicitarse a un destinatario, a través de la interfaz de usuario del segundo dispositivo cliente, que agregue el número de teléfono del primer dispositivo cliente que llama a una lista de números a bloquear. En diversas realizaciones, el sistema puede proporcionar a un proveedor de servicios o a un tercero, por ejemplo, fuerzas policiales, información relacionada con la llamada no autenticada.

En algunas realizaciones, una autenticación con éxito de una llamada por parte del sistema puede provocar el establecimiento de una conexión entre el primer dispositivo móvil y el segundo dispositivo móvil. En diversas realizaciones, la información sobre el primer dispositivo móvil puede guardarse en y/o mediante el segundo dispositivo móvil, que identifica que el primer dispositivo móvil ha sido contactado a través de una llamada autenticada. Puede hacerse referencia a dicho registro en comunicaciones posteriores entre los dos dispositivos cliente para verificar, de forma eficiente, la probable autenticidad de las comunicaciones posteriores en función de la autenticación de una comunicación anterior.

En algunas realizaciones, puede realizarse una conexión de llamada entre un primer y un segundo dispositivo de telefonía móvil en respuesta al paso de autenticación, y los resultados del paso de autenticación pueden indicarse al destinatario, por ejemplo, a través de una interfaz de usuario del segundo dispositivo cliente. Por ejemplo, puede realizarse una conexión de llamada a pesar de un fallo en la autenticación, pero puede comunicarse al destinatario una advertencia a través de la interfaz de usuario de su teléfono móvil de que la llamada no está autenticada. En otro ejemplo, puede realizarse una conexión de llamada en respuesta al éxito de la autenticación, comunicándose al destinatario una verificación a través de la interfaz de usuario de su teléfono móvil de que la llamada ha sido autenticada.

La **FIG. 7** es un flujo lógico 700 que ilustra un método para conectar, de forma selectiva, un primer dispositivo cliente y un segundo dispositivo cliente para una comunicación en base a los resultados de una autenticación multifactor. Específicamente, la **FIG. 7** ilustra un ejemplo en el que el primer y el segundo dispositivo cliente son ambos dispositivos de telefonía móvil y la comunicación es un flujo de datos de una llamada. Las realizaciones no están limitadas de esta manera.

El paso 710 describe la recuperación de una clave pública del número de la llamada entrante de un dispositivo de almacenamiento de datos. En algunas realizaciones, el dispositivo de almacenamiento de datos puede ser local al segundo dispositivo cliente. En otras realizaciones, el dispositivo de almacenamiento de datos puede ser una memoria externa, como la discutida anteriormente con referencia al router 120 de autenticación o a la base de datos 330, por ejemplo.

El paso 720 describe el descifrado de la carga útil cifrada utilizando la clave pública del número de la llamada entrante, recuperada en el paso 710, para producir una carga útil descifrada que comprende un identificador. La carga útil cifrada puede recibirse con el número de la llamada entrante, por ejemplo, como en el mensaje 140. El identificador puede estar relacionado con el cliente emisor y/o con el primer dispositivo cliente.

El paso 730 describe la comparación del identificador de la carga útil descifrada con un identificador esperado asociado al número de la llamada entrante para determinar una coincidencia de autenticación de primer factor. En diversas realizaciones, el identificador esperado asociado al número de la llamada entrante puede recuperarse de la memoria, que puede ser el mismo dispositivo de almacenamiento de datos referenciado en el paso 710 o un dispositivo de almacenamiento de datos separado.

El paso 740 describe la comparación del atributo de un mensaje de voz con un atributo del mensaje de voz esperado para identificar una coincidencia de autenticación de segundo factor. El mensaje de voz puede recibirse en asociación con, o como parte de, la carga útil cifrada.

El paso 750 describe el establecimiento selectivo de una conexión entre el primer dispositivo de telefonía móvil y el segundo dispositivo de telefonía móvil en respuesta a la autenticación del primer factor y a la coincidencia de autenticación de segundo factor.

En algunas realizaciones, un fallo del sistema para autenticar, adecuadamente, una llamada a través de las coincidencias de autenticación de primer factor y/o de segundo factor puede provocar la denegación de la llamada, el abandono de la llamada, u otro método de desestimación de la llamada. En algunas realizaciones, puede notificarse a un primer dispositivo cliente y/o a un segundo dispositivo cliente del intento fallido y proporcionarse detalles del intento, como el número de teléfono de la persona que llama y/o del destinatario. En algunas realizaciones, puede solicitarse a un destinatario, a través de la interfaz de usuario del segundo dispositivo cliente, agregar el número de teléfono del primer dispositivo cliente que llama a una lista de números a bloquear. En diversas realizaciones, el sistema puede proporcionar a un proveedor de servicios o a un tercero, por ejemplo, fuerzas policiales, información relacionada con la llamada no autenticada. Dicha información puede especificar qué factor de autenticación falló e incluir más detalles del intento.

En algunas realizaciones, una autenticación con éxito de una llamada por parte del sistema a través de las coincidencias de autenticación de primer factor y/o de segundo factor puede provocar el establecimiento de una conexión entre el primer dispositivo móvil y el segundo dispositivo móvil. En diversas realizaciones, la información sobre el primer dispositivo móvil puede guardarse en y/o mediante el segundo dispositivo móvil, que identifica que el primer dispositivo móvil ha sido contactado a través de una llamada con autenticación multifactor. Puede hacerse referencia a dicho registro en comunicaciones posteriores entre los dos dispositivos cliente para verificar, de forma eficiente, la probable autenticidad de las comunicaciones posteriores en función de la autenticación multifactor de una comunicación anterior.

En algunas realizaciones, puede realizarse una conexión de llamada entre un primer y un segundo dispositivo de telefonía móvil en respuesta a las coincidencias de autenticación de primer factor y/o de segundo factor, y los resultados del paso de autenticación pueden indicarse al destinatario, por ejemplo, a través de una interfaz de usuario del segundo dispositivo cliente. Por ejemplo, puede realizarse una conexión de llamada a pesar de un fallo en la autenticación multifactor, pero puede comunicarse al destinatario una advertencia a través de la interfaz de usuario de su teléfono móvil de que la llamada no está autenticada o solo está parcialmente autenticada. En otro ejemplo, puede realizarse una conexión de llamada en respuesta al éxito de la autenticación multifactor, comunicándose al destinatario una verificación a través de la interfaz de usuario de su teléfono móvil de que la llamada ha sido autenticada a través de autenticación multifactor.

Pueden implementarse varias realizaciones utilizando elementos de hardware, elementos de software, o una combinación de ambos. Los ejemplos de elementos de hardware pueden incluir procesadores, microprocesadores, circuitos, elementos del circuito (p. ej., transistores, resistencias, condensadores, inductores, etc.), circuitos integrados, circuitos integrados de aplicación específica (ASIC), dispositivos lógicos programables (PLD), procesadores de señales digitales (DSP), matriz de puertas programables en campo (FPGA), puertas lógicas, registros, dispositivos semiconductores, chips, microchips, conjuntos de chips, etc. Los ejemplos de software pueden incluir componentes de software, programas, aplicaciones, programas informáticos, programas de la aplicación, programas del sistema, programas de la máquina, software del sistema operativo, middleware, firmware, módulos de software, rutinas, subrutinas, funciones, métodos, procedimientos, interfaces de software, interfaces del programa de la aplicación (API), conjuntos de instrucciones, código de computación, código informático, segmentos de código, segmentos de código informático, palabras, valores, símbolos, o cualquier combinación de los mismos. Determinar si una realización se implementa utilizando elementos de hardware y/o elementos de software puede variar de acuerdo con cualquier número de factores, como la tasa computacional deseada, niveles de potencia, tolerancias térmicas, presupuesto del ciclo de procesamiento, tasas de datos de entrada, tasas de datos de salida, recursos de memoria, velocidades del bus de datos y otras limitaciones de diseño o rendimiento.

Uno o más aspectos de, al menos, una realización, pueden implementarse mediante instrucciones representativas almacenadas en un medio legible por máquina, que representa diversas lógicas dentro del procesador, que cuando

son leídas por una máquina hacen que la máquina produzca lógicas para realizar las técnicas descritas en la presente memoria. Dichas representaciones, conocidas como "núcleos IP", pueden almacenarse en un medio tangible, legible por máquina, y suministrarse a varios usuarios o instalaciones de fabricación para que las carguen en las máquinas de fabricación que realmente hacen la lógica o el procesador. Algunas realizaciones pueden implementarse, por ejemplo, utilizando un medio o artículo legible por máquina que puede almacenar una instrucción o un conjunto de instrucciones que, si son ejecutadas por una máquina, pueden hacer que la máquina realice un método y/u operaciones de acuerdo con las realizaciones. Dicha máquina puede incluir, por ejemplo, cualquier plataforma de procesamiento, plataforma informática, dispositivo informático, dispositivo de procesamiento, sistema informático, sistema de procesamiento, ordenador, procesador, o similar, adecuado, y puede implementarse utilizando cualquier combinación adecuada de hardware y/o software. El medio o artículo legible por máquina puede incluir, por ejemplo, cualquier tipo adecuado de unidad de memoria, dispositivo de memoria, artículo de memoria, medio de memoria, dispositivo de almacenamiento, artículo de almacenamiento, medio de almacenamiento y/o unidad de almacenamiento, por ejemplo, memoria, medios extraíbles o no extraíbles, medios borrables o no borrables, medios grabables o regrabables, medios digitales o analógicos, disco duro, disquete, Memoria de Sólo Lectura en Disco Compacto (CD-ROM), Disco Compacto Grabable (CD-R), Disco Compacto Regrabable (CD-RW), disco óptico, medios magnéticos, medios magneto-ópticos, tarjetas o discos de memoria extraíbles, varios tipos de Disco Versátil Digital (DVD), una cinta, un casete, o similares. Las instrucciones pueden incluir cualquier tipo adecuado de código, como código fuente, código compilado, código interpretado, código ejecutable, código estático, código dinámico, código cifrado, y similares, implementado utilizando cualquier lenguaje de programación adecuado de alto nivel, bajo nivel, orientado a objetos, visual, compilado y/o interpretado.

REIVINDICACIONES

1. Un método para autenticar llamadas entre dispositivos móviles (125, 130), que comprende:

recibir un flujo de datos de una llamada entrante de un primer dispositivo (125) de telefonía móvil, comprendiendo el flujo de datos de la llamada entrante un número de la llamada entrante asociado a un segundo dispositivo (130) de telefonía móvil, una carga útil que comprende un criptograma recuperado de una tarjeta sin contacto (305), en donde, al menos, una parte de la carga útil está cifrada con una clave privada de la tarjeta sin contacto (305);

recuperar (710) una clave pública del número de la llamada entrante de un dispositivo de almacenamiento de datos, la clave pública asociada a la clave privada;

descifrar (720) el criptograma utilizando la clave pública del número de la llamada entrante para producir una carga útil descifrada que comprende un identificador;

comparar (730) el identificador de la carga útil descifrada con un identificador esperado asociado al número de la llamada entrante para determinar una coincidencia de autenticación; y

establecer (750), de forma selectiva, una conexión entre el primer dispositivo (125) de telefonía móvil y el segundo dispositivo (130) de telefonía móvil en respuesta a la coincidencia de autenticación.

2. El método de la reivindicación 1, en donde el identificador comprende un identificador único de la tarjeta sin contacto (305).

3. El método de la reivindicación 2, en donde el identificador comprende un valor de contador mantenido por la tarjeta sin contacto (305).

4. El método de la reivindicación 1, en donde la carga útil comprende, además, un atributo del mensaje de voz, y el método comprende comparar (740) el atributo del mensaje de voz con un atributo del mensaje de voz esperado para identificar una coincidencia de autenticación de segundo factor, el método para establecer, sólo de forma selectiva, la conexión en respuesta a la coincidencia de autenticación de segundo factor.

5. El método de la reivindicación 1, en donde la carga útil comprende, además, información biométrica asociada al usuario, y el método comprende comparar la información biométrica con la información biométrica almacenada para identificar una coincidencia de autenticación de segundo factor, el método para establecer, sólo de forma selectiva, la conexión en respuesta a la coincidencia de autenticación de segundo factor.

6. El método de la reivindicación 1, en donde la carga útil cifrada comprende datos hash, y en donde el método incluye el paso de aplicar una función hash a la carga útil descifrada para extraer el identificador.

7. El método de la reivindicación 1, en donde la clave privada es mantenida por la tarjeta sin contacto (305) asociada al primer dispositivo (125) de telefonía móvil.

8. Un aparato que comprende:

una memoria configurada para almacenar instrucciones:

un procesador acoplado a la memoria, el procesador configurado para procesar las instrucciones, que cuando son ejecutadas hacen que el procesador:

procese un flujo de datos de una llamada entrante de un primer dispositivo (125) de telefonía móvil, comprendiendo el flujo de datos de la llamada entrante un número de la llamada entrante asociado a un segundo dispositivo (130) de telefonía móvil, y una carga útil que comprende un criptograma recuperado de una tarjeta sin contacto (305), en donde el criptograma está cifrado con una clave privada de la tarjeta sin contacto (305);

determine (710) una clave pública del número de la llamada entrante de un dispositivo de almacenamiento de datos, la clave pública asociada a la clave privada;

descifre (720) el criptograma utilizando la clave pública del número de la llamada entrante para producir una carga útil descifrada que comprende un identificador;

compare (730) el identificador de la carga útil descifrada con un identificador esperado asociado al número de la llamada entrante para determinar una coincidencia de autenticación; y

establezca (740), de forma selectiva, una conexión entre el primer dispositivo de telefonía móvil y el segundo dispositivo de telefonía móvil en respuesta a la coincidencia de autenticación.

9. El aparato de la reivindicación 8, en donde el identificador comprende un identificador único de la tarjeta sin contacto (305).

10. El aparato de la reivindicación 9, en donde el identificador único comprende un valor de contador mantenido por la tarjeta sin contacto (305).

11. El aparato de la reivindicación 8, en donde la carga útil comprende, además, un atributo del mensaje de voz, y el procesador para comparar (740) el atributo del mensaje de voz con un atributo del mensaje de voz esperado para identificar una coincidencia de autenticación de segundo factor, y el procesador para establecer, sólo de forma selectiva, la conexión en respuesta a la coincidencia de autenticación de segundo factor y a la coincidencia de autenticación.

12. El aparato de la reivindicación 8, en donde la carga útil comprende, además, información biométrica asociada al usuario, y el procesador para comparar la información biométrica con la información biométrica almacenada para identificar una coincidencia de autenticación de segundo factor, y el procesador para establecer, sólo de forma selectiva, la conexión en respuesta a la coincidencia de autenticación de segundo factor y a la coincidencia de autenticación.

13. El aparato de la reivindicación 8, en donde la carga útil cifrada comprende datos hash, y el procesador para aplicar una función hash a la carga útil descifrada para extraer el identificador.

14. El aparato de la reivindicación 8, en donde la clave privada es mantenida por la tarjeta sin contacto (305) asociada al primer dispositivo (125) de telefonía móvil.

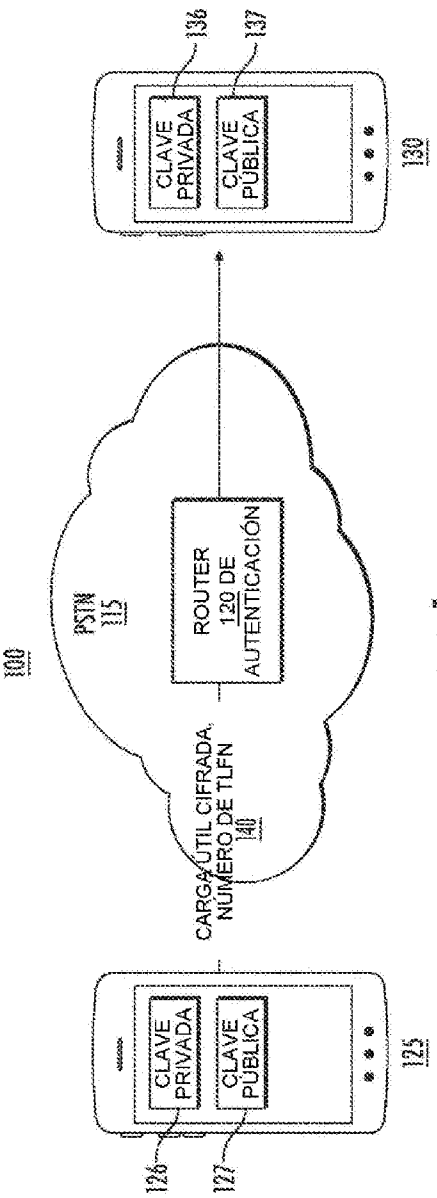
100
PSTN
115
ROUTER
120 DE
AUTENTICACIÓN
CARGA ÚTIL CIFRADA,
NÚMERO DE TLFN
140
CLAVE
PRIVADA
CLAVE
PÚBLICA
125
126
127
130
136
137

FIG. 1

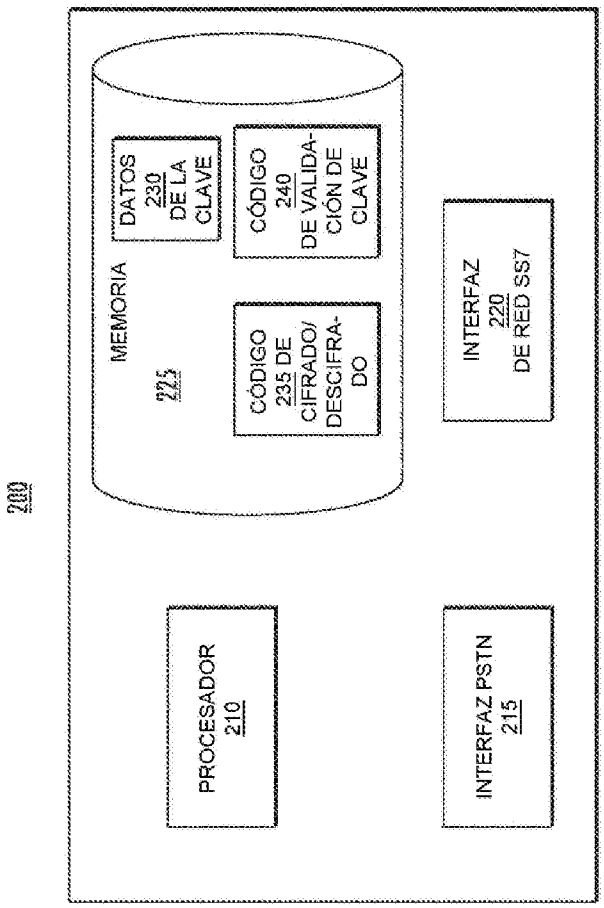
200
MEMORIA
225
DATOS 230 DE LA CLAVE
CÓDIGO 240 DE VALIDACIÓN DE CLAVE
CÓDIGO 235 DE CIFRADO/DESCIFRADO
INTERFAZ 220 DE RED SS7
PROCESADOR 210
INTERFAZ PSTN 215

FIG. 2

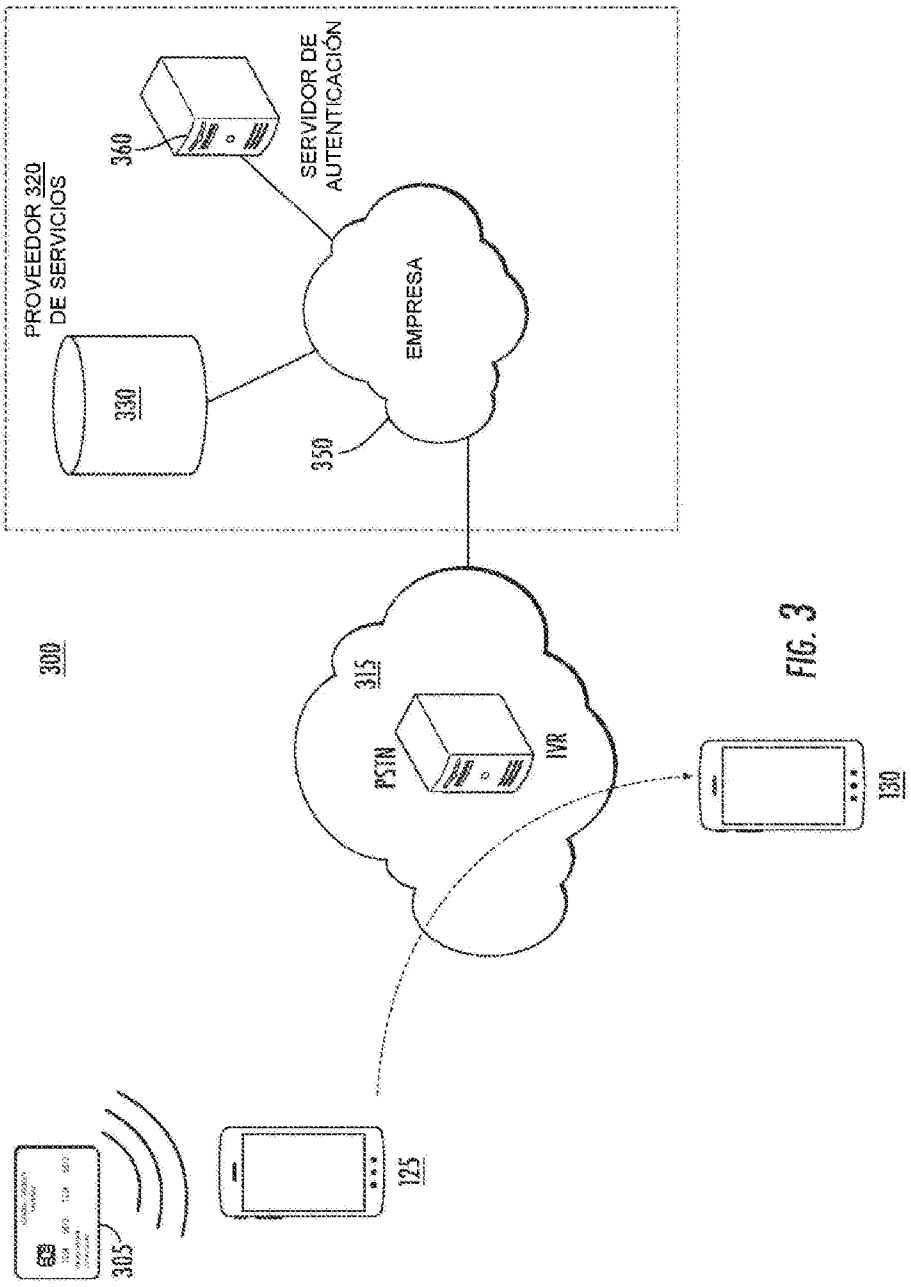
PROVEEDOR 320
DE SERVICIOS
360
SERVIDOR DE
AUTENTICACIÓN
330
EMPRESA
350
300
315
PSTN
IVR
130
125
305

FIG. 3

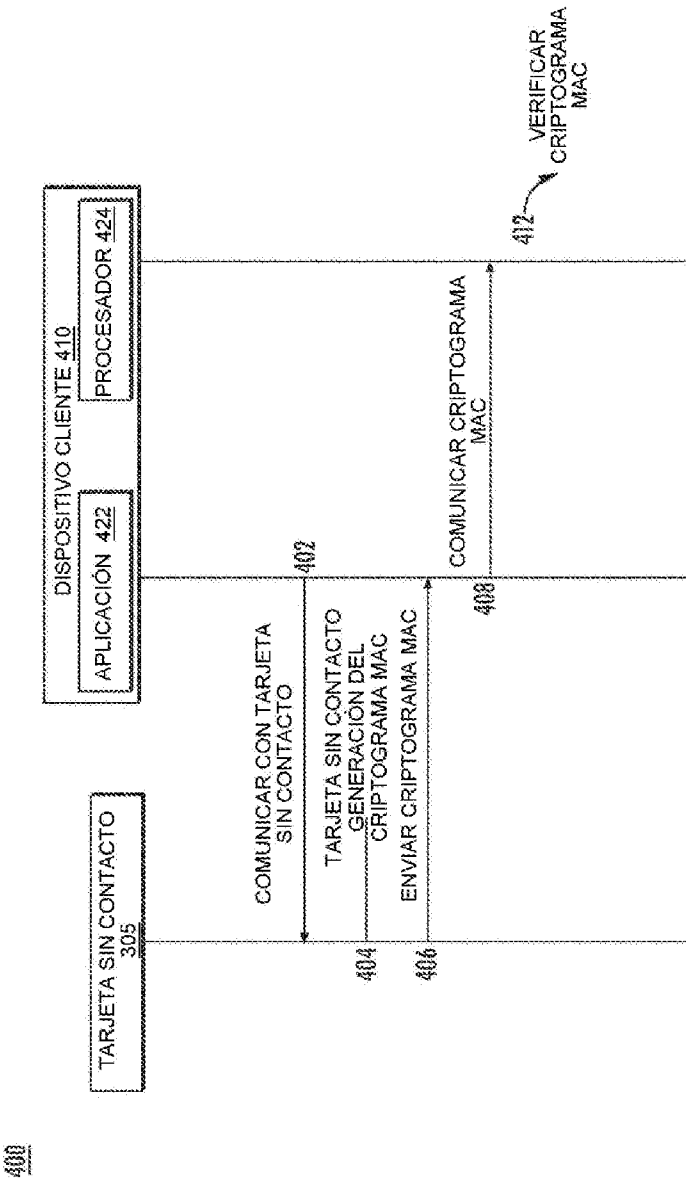
400
TARJETA SIN CONTACTO
305
DISPOSITIVO CLIENTE 410
APLICACIÓN 422
PROCESADOR 424
COMUNICAR CON TARJETA SIN CONTACTO
402
TARJETA SIN CONTACTO GENERACIÓN DEL CRIPTOGRAMA MAC
404
ENVIAR CRIPTOGRAMA MAC
406
COMUNICAR CRIPTOGRAMA MAC
408
VERIFICAR CRIPTOGRAMA MAC
412

FIG. 4

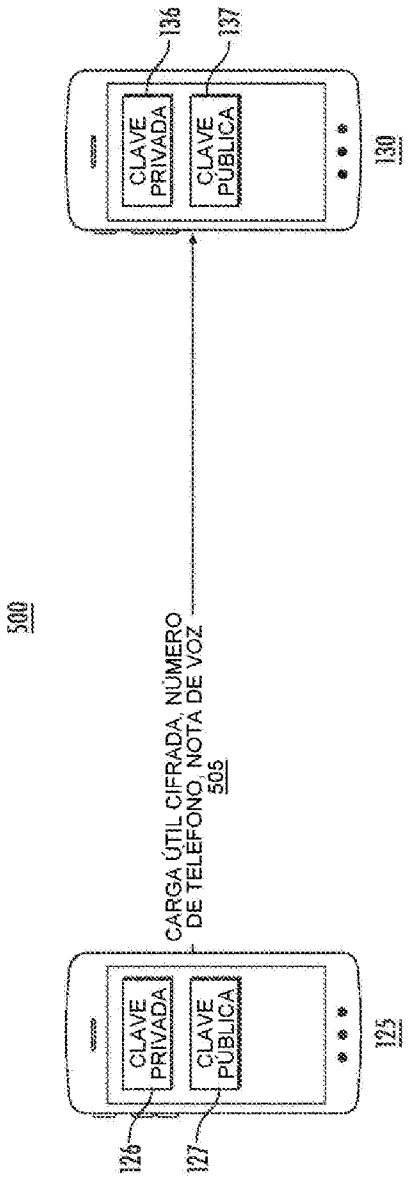
500
CARGA ÚTIL CIFRADA, NÚMERO DE TELEFONO, NOTA DE VOZ
505
CLAVE PRIVADA
CLAVE PÚBLICA
125
126
127
130
136
137

FIG. 5

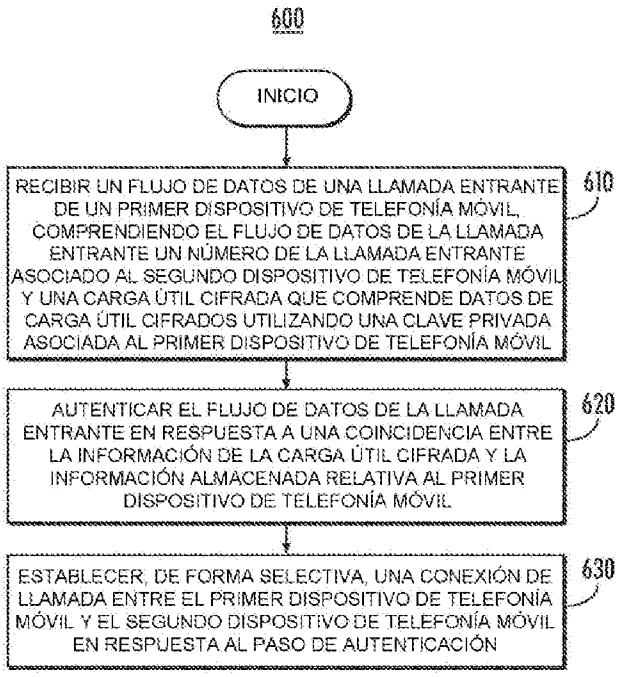
600
INICIO
RECIBIR UN FLUJO DE DATOS DE UNA LLAMADA ENTRANTE DE UN PRIMER DISPOSITIVO DE TELEFONÍA MÓVIL, COMPRENDIENDO EL FLUJO DE DATOS DE LA LLAMADA ENTRANTE UN NÚMERO DE LA LLAMADA ENTRANTE ASOCIADO AL SEGUNDO DISPOSITIVO DE TELEFONÍA MÓVIL Y UNA CARGA ÚTIL CIFRADA QUE COMPRENDE DATOS DE CARGA ÚTIL CIFRADOS UTILIZANDO UNA CLAVE PRIVADA ASOCIADA AL PRIMER DISPOSITIVO DE TELEFONÍA MÓVIL
610
AUTENTICAR EL FLUJO DE DATOS DE LA LLAMADA ENTRANTE EN RESPUESTA A UNA COINCIDENCIA ENTRE LA INFORMACIÓN DE LA CARGA ÚTIL CIFRADA Y LA INFORMACIÓN ALMACENADA RELATIVA AL PRIMER DISPOSITIVO DE TELEFONÍA MÓVIL
620
ESTABLECER, DE FORMA SELECTIVA, UNA CONEXIÓN DE LLAMADA ENTRE EL PRIMER DISPOSITIVO DE TELEFONÍA MÓVIL Y EL SEGUNDO DISPOSITIVO DE TELEFONÍA MÓVIL EN RESPUESTA AL PASO DE AUTENTICACIÓN
630

FIG. 6

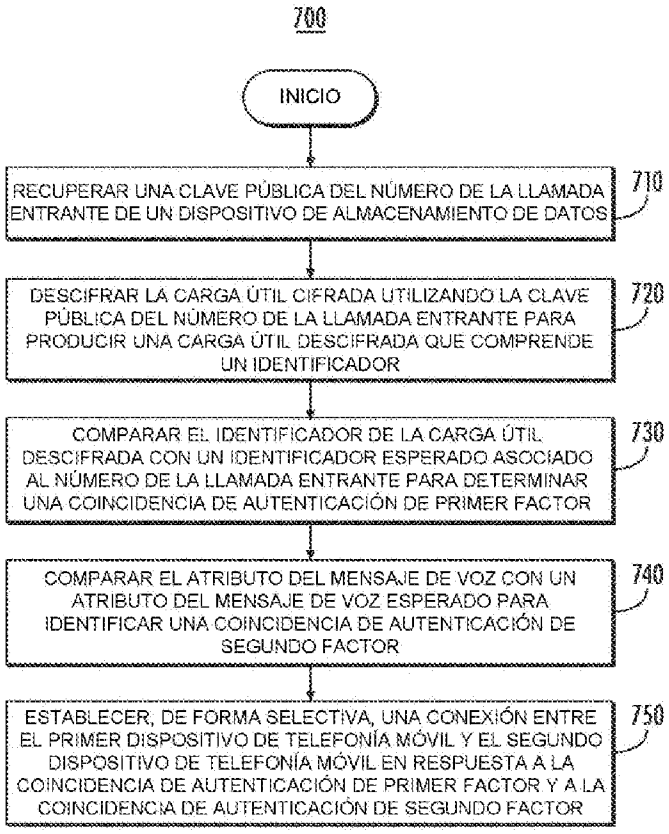
700
INICIO
RECUPERAR UNA CLAVE PÚBLICA DEL NÚMERO DE LA LLAMADA ENTRANTE DE UN DISPOSITIVO DE ALMACENAMIENTO DE DATOS
710
DESCIFRAR LA CARGA ÚTIL CIFRADA UTILIZANDO LA CLAVE PÚBLICA DEL NÚMERO DE LA LLAMADA ENTRANTE PARA PRODUCIR UNA CARGA ÚTIL DESCIFRADA QUE COMPRENDE UN IDENTIFICADOR
720
COMPARAR EL IDENTIFICADOR DE LA CARGA ÚTIL DESCIFRADA CON UN IDENTIFICADOR ESPERADO ASOCIADO AL NÚMERO DE LA LLAMADA ENTRANTE PARA DETERMINAR UNA COINCIDENCIA DE AUTENTICACIÓN DE PRIMER FACTOR
730
COMPARAR EL ATRIBUTO DEL MENSAJE DE VOZ CON UN ATRIBUTO DEL MENSAJE DE VOZ ESPERADO PARA IDENTIFICAR UNA COINCIDENCIA DE AUTENTICACIÓN DE SEGUNDO FACTOR
740
ESTABLECER, DE FORMA SELECTIVA, UNA CONEXIÓN ENTRE EL PRIMER DISPOSITIVO DE TELEFONÍA MÓVIL Y EL SEGUNDO DISPOSITIVO DE TELEFONÍA MÓVIL EN RESPUESTA A LA COINCIDENCIA DE AUTENTICACIÓN DE PRIMER FACTOR Y A LA COINCIDENCIA DE AUTENTICACIÓN DE SEGUNDO FACTOR
750

FIG. 7