(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 963 411**

(51) Int. Cl.:

H04L 9/40 (2012.01)
H04L 9/08 (2006.01)
H04L 9/32 (2006.01)
H04M 7/00 (2006.01)
H04W 4/80 (2008.01)
H04M 3/51 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **13.03.2020 PCT/US2020/022809**

(87) Fecha y número de publicación internacional: **24.09.2020 WO20190788**

(96) Fecha de presentación y número de la solicitud europea: **13.03.2020 E 20718897 (0)**

(97) Fecha y número de publicación de la concesión europea: **25.10.2023 EP 3942788**

(54) Título: **Sistema y método para la preautenticación de llamadas de atención al cliente**

(30) Prioridad:

18.03.2019 US 201916356987

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.03.2024

(73) Titular/es:

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

(72) Inventor/es:

RULE, JEFFREY y
ILINCIC, RAJKO

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Sistema y método para la preautenticación de llamadas de atención al cliente

Solicitudes relacionadas

La presente solicitud reivindica prioridad con respecto a la Solicitud de Patente de los Estados Unidos n.º de serie 16/356,987, titulada "*SYSTEM AND METHOD FOR PRE-AUTHENTICATION OF CUSTOMER SUPPORT CALLS*" presentada el 18 de marzo de 2019.

Antecedentes

Las llamadas de los centros de atención telefónica se proveen normalmente por proveedores de servicios para permitir a los clientes acceder, modificar, eliminar o de otra manera controlar sus cuentas. Desde el punto de vista de la seguridad, los centros de atención telefónica pueden ser las áreas más riesgosas de una empresa dado que las transacciones de los centros de atención telefónica pueden exponer información sensible de los clientes a terceros maliciosos.

Los centros de atención telefónica enfrentan riesgos tanto internos como externos. Los riesgos internos incluyen robo por parte de los empleados de información sensible de los clientes. Durante un proceso de autenticación típico, los empleados de los centros de atención telefónica tienen acceso directo a datos sensibles de los clientes. Los centros de atención telefónica pueden estar tercerizados, y los empleados de los centros de atención telefónica pueden tener una alta tasa de rotación. Como resultado, las compañías están constantemente en riesgo de que empleados que se van de la empresa o empleados remotos puedan retener, de manera inapropiada, información de los clientes.

Los riesgos externos incluyen aquellos que surgen de la suplantación de identidad o fraude informático donde impostores enmascaran o modifican números entrantes, direcciones de correo electrónico, direcciones IP, etc., para hacerse pasar por clientes en un intento por robar información o fondos. Los riesgos externos también surgen de jáqueres que monitorean comunicaciones del proveedor de servicios, en particular, comunicaciones de los centros de atención telefónica, con el fin de robar información de los clientes.

Para abordar estas cuestiones de seguridad, el Consejo de Normas de Seguridad para la Industria de las Tarjetas de Pago (PCI SSC, por sus siglas en inglés) gestiona la evolución en curso de las normas de seguridad para la Industria de las Tarjetas de Pago (PCI, por sus siglas en inglés). Los proveedores de servicio son responsables de reforzar el cumplimiento de las normas de la PCI para proteger datos sensibles de los clientes. Por ejemplo, las normas de la PCI pueden establecer normas de autenticación que deberán seguirse antes de permitir a un cliente acceder a y/o modificar información de la cuenta de cliente. Los centros de atención telefónica pueden requerir la autenticación del cliente en la forma de intercambio de contraseñas, respuestas a preguntas personales, datos biométricos o similares. Puede solicitarse múltiples veces a los clientes que provean información de autenticación en varias formas durante la gestión de una llamada. Este proceso de autenticación y reautenticación no solo puede frustrar a un cliente y degradar la buena voluntad del proveedor de servicios, sino que también cada instancia de autenticación expone potencialmente información sensible de los clientes a partes potencialmente maliciosas.

Los documentos US 2017/017964 A1, US 2009/217039 A1 y US 2014/020073 A1 son técnica anterior relevante.

Compendio

La invención se define por las reivindicaciones independientes. Según un aspecto de la invención, un método para la preautenticación de solicitudes de soporte recibidas por un proveedor de servicios de uno o más dispositivos acoplados incluye las etapas de recibir una solicitud de soporte de un cliente que opera un dispositivo de cliente que se ha autorizado que acceda a una aplicación del proveedor de servicios en respuesta a la primera información de autenticación provista por el cliente. En respuesta a la solicitud de soporte, el método incluye solicitar segunda información de autenticación del cliente, la segunda información de autenticación incluyendo un criptograma y la recepción de la segunda información de autenticación incluyendo el criptograma del dispositivo de cliente. El método incluye validar, de manera selectiva, al cliente mediante el descifrado de al menos una porción de la segunda información de autenticación usando una copia de una clave asociada al cliente y mantenida por el proveedor de servicios. El método incluye las etapas de, en respuesta a la validación del cliente, iniciar una llamada con el dispositivo de cliente y dirigir un servicio de soporte del centro de atención telefónica para evitar una etapa de autorización de un proceso de soporte del centro de atención telefónica para acelerar la gestión de la llamada iniciada. Con dicha disposición, mecanismos de autenticación de múltiples factores del proveedor de servicios pueden aprovecharse para su uso con servicios de atención al cliente y, por consiguiente, aumentar la eficiencia de la resolución de problemas del cliente y aumentar la seguridad de la información del cliente.

Según otro aspecto de la invención, un sistema para preautenticar solicitudes de soporte del servicio de cliente recibidas en un proveedor de servicios de uno o más dispositivos de cliente acoplados incluye una interfaz de cliente adaptada para intercambiar información con uno o más dispositivos de cliente acoplados. El sistema también incluye un dispositivo de almacenamiento y una tabla de claves diversificadas almacenada en el dispositivo de almacenamiento y que comprende una entrada para al menos un cliente del proveedor de servicios, la entrada incluyendo primera y segunda información de autenticación para el cliente. El sistema además incluye una unidad de

autenticación, acoplada a la interfaz de cliente y a la tabla de claves diversificadas, para recuperar una de la primera o segunda información de autenticación tras recibir una solicitud de cliente por la interfaz de cliente y para autorizar la solicitud del cliente en respuesta a la primera o segunda información de autenticación recuperada. Una interfaz de centro de atención telefónica del cliente se acopla a la unidad de autenticación, para reenviar, de manera selectiva, una solicitud de soporte, recibida de un dispositivo de cliente, a un servicio de centro de atención telefónica, la solicitud de soporte reenviada después de la autorización de la solicitud de soporte por la unidad de autenticación, la interfaz del centro de atención telefónica del cliente aumentando la solicitud de soporte para dirigir el servicio del centro de atención telefónica para evitar la autenticación de la solicitud de soporte por un proceso de servicio de centro de atención telefónica.

Según un aspecto adicional de la invención, un método para la preautenticación de solicitudes de soporte recibidas por un proveedor de servicios de uno o más dispositivos de cliente acoplados incluye las etapas de recibir una solicitud de soporte de un dispositivo de cliente que se ha autorizado que acceda a una aplicación del proveedor de servicios en respuesta a la primera información de autenticación provista por el cliente. En respuesta a la recepción de la solicitud de soporte, el método incluye hacer que un cliente asocie una tarjeta al dispositivo de cliente para recuperar segunda información de autenticación de la tarjeta, la segunda información de autenticación incluyendo un criptograma y la recepción de la segunda información de autenticación. El método incluye validar, de manera selectiva, la solicitud de soporte mediante el descifrado de al menos una porción de la segunda información de autenticación usando una clave derivada asociada al cliente y mantenida por el proveedor de servicios. En respuesta a la validación de la solicitud de soporte, el método incluye establecer un enlace de comunicación entre un servicio de soporte del centro de atención telefónica y el dispositivo de cliente mediante el reenvío de información de enlace de comunicación a al menos uno del dispositivo de cliente y servicio de soporte del centro de atención telefónica para hacer que uno del dispositivo de cliente o servicio de soporte del centro de atención telefónica contacte al otro y dirija un servicio de soporte del centro de atención telefónica para evitar una etapa de autorización de un proceso de soporte del centro de atención telefónica para cada llamada entrante que se haya validado previamente por el proveedor de servicios.

Breve descripción de los dibujos

La Figura 1A es un diagrama de bloques de un sistema de transmisión de datos configurado para preautenticar solicitudes de cliente según una realización a modo de ejemplo;

la Figura 1B es un diagrama que ilustra una secuencia para proveer acceso autenticado según una realización a modo de ejemplo;

la Figura 2 es un ejemplo de una tarjeta sin contacto para almacenar información de autenticación que puede usarse en el sistema de la Figura 1A;

la Figura 3 es un diagrama de bloques detallado que ilustra componentes a modo de ejemplo de la tarjeta sin contacto de la Figura 2;

la Figura 4 es un diagrama de campos a modo de ejemplo de mensajes intercambiados entre una tarjeta sin contacto y un dispositivo de cliente de la Figura 1A;

la Figura 5 es un diagrama de bloques detallado de componentes del sistema de la Figura 1A que puede utilizarse para soportar aspectos de la invención;

la Figura 6 es un diagrama de flujo de datos provisto para describir etapas a modo de ejemplo que pueden llevarse a cabo en una realización por los componentes de la Figura 4 durante la autenticación de una llamada según aspectos de la invención;

la Figura 7 es un diagrama de flujo de datos provisto para describir etapas a modo de ejemplo que pueden llevarse a cabo durante la realización de un proceso de enrutamiento de llamada que usa una tarjeta sin contacto de la Figura 2;

la Figura 8 es un diagrama de flujo de datos provisto para describir etapas a modo de ejemplo que pueden llevarse a cabo durante otra realización de un proceso de enrutamiento de llamada que usa una tarjeta sin contacto de la Figura 2; y

la Figura 9 es un diagrama de bloques que ilustra una estructura de gestión de llamadas a modo de ejemplo en un centro de atención telefónica que acepta solicitudes de servicio preautenticadas.

Descripción detallada

Un objetivo de algunas realizaciones de la presente descripción es el uso de una o más claves que se han incorporado a una o más tarjetas sin contacto según se describe en la Solicitud de Patente de los Estados Unidos Número de Serie 16/205,119, presentada el 29 de noviembre de 2018 por Osborn, y otros, titulada "*Systems and Methods for Cryptographic Authentication of Contactless Cards*". La tarjeta sin contacto puede usarse para llevar a cabo la autenticación y numerosas funciones diferentes que pueden de otra manera requerir que el usuario lleve un testigo

físico separado además de la tarjeta sin contacto. La tarjeta sin contacto puede usarse para llevar a cabo la autenticación y numerosas funciones diferentes que pueden de otra manera requerir que el usuario lleve un testigo físico separado además de la tarjeta sin contacto. Mediante el empleo de una interfaz sin contacto, las tarjetas sin contacto pueden estar provistas de un método para interactuar y comunicarse entre el dispositivo de un usuario (como, por ejemplo, un teléfono móvil) y la propia tarjeta. Por ejemplo, el protocolo EMV, que se basa en muchas transacciones con tarjeta de crédito, incluye un proceso de autenticación que es suficiente para sistemas operativos para Android pero presenta desafíos para iOS,®, que es más restrictivo con respecto al uso de la comunicación de campo cercano (NFC, por sus siglas en inglés), dado que puede usarse solamente en forma de solo lectura. A diferencia de RFID que puede usarse para leer dispositivos en movimiento hasta una distancia significativa. Realizaciones a modo de ejemplo de las tarjetas sin contacto descritas en la Solicitud '119 pueden utilizar tecnología NFC.

Se describen un sistema y un método que utilizan características de autenticación de múltiples factores de un proveedor de servicios y enrutamiento de llamadas inteligente para aumentar la seguridad y eficiencia en un centro de atención telefónica de clientes. La preautenticación de solicitudes de soporte de clientes reduce el potencial de apropiación indebida de datos sensibles de los clientes durante la gestión de la llamada. Una tarjeta sin contacto asociada de forma única a un cliente puede proveer un segundo factor de autenticación para reducir el potencial de suplantación del cliente por parte de un tercero malicioso. Las llamadas de atención al cliente preautorizadas se encaminan, de manera inteligente y eficiente, en una manera que reduce la oportunidad de interferencia maliciosa de la llamada y robo de información.

Estas y otras características de la invención se describirán ahora con referencia a las figuras, en donde numerales de referencia iguales se usan para referirse a elementos iguales a lo largo de la presente memoria descriptiva.

Según su uso en la presente solicitud, los términos "sistema", "componente" y "unidad" pretenden referirse a una entidad relacionada con el ordenador, ya sea hardware, una combinación de hardware y software, software, o software en ejecución, ejemplos de los cuales se describen en la presente memoria. Por ejemplo, un componente puede ser, pero sin limitación a, 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, una unidad 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 manera comunicativa, entre sí, mediante varios tipos de medios de comunicaciones para coordinar las operaciones. La coordinación puede implicar el intercambio unidireccional o bidireccional de información. Por ejemplo, los componentes pueden comunicar información en la forma de señales comunicadas en los medios de comunicaciones. La información puede implementarse como señales asignadas a varias líneas de señales. En dichas asignaciones, cada mensaje es una señal. Realizaciones adicionales, sin embargo, pueden emplear, de manera alternativa, mensajes de datos. Dichos mensajes de datos pueden enviarse a lo largo de varias conexiones. Conexiones a modo de ejemplo incluyen interfaces paralelas, interfaces en serie e interfaces de bus.

La Figura 1A ilustra un sistema 100 que incluye uno o más dispositivos 110 de cliente acoplados a un proveedor 120 de servicios mediante una red 115. Según un aspecto, los dispositivos 110 de cliente comprenden ordenadores habilitados por la red y se comunican con el proveedor 120 de servicios mediante redes 115 y 125 para acceder a contenido y servicios del proveedor de servicios.

Según se hace referencia en la presente memoria, un ordenador habilitado por la red puede incluir, pero sin limitación a: p. ej., un dispositivo de ordenador, un dispositivo de comunicaciones que incluya, p. ej., un servidor, un dispositivo de red, un ordenador personal (PC, por sus siglas en inglés), una estación de trabajo, un dispositivo móvil, un teléfono, un PC portátil, un asistente personal digital (PDA, por sus siglas en inglés), un dispositivo de cliente fino, un dispositivo de cliente grueso, un navegador de Internet, u otro dispositivo.

Los dispositivos 110 de cliente, por consiguiente, pueden incluir un procesador y una memoria, y se comprende que los circuitos de procesamiento pueden contener componentes adicionales, incluidos procesadores, memorias, verificadores de errores y paridad/CRC, codificadores de datos, algoritmos anticolisión, controladores, decodificadores de comandos, primitivas de seguridad y hardware a prueba de falsificaciones, según sea necesario para llevar a cabo las funciones descritas en la presente memoria. El dispositivo 110 de cliente puede además incluir una visualización y dispositivos de entrada. La visualización puede ser cualquier tipo de dispositivo para presentar información visual como, por ejemplo, un monitor de ordenador, una pantalla de panel plano, y una pantalla de dispositivo móvil, incluidas las pantallas de cristal líquido, pantallas con diodos emisores de luz, paneles de plasma, y pantallas con tubo de rayos catódicos. Los dispositivos de entrada pueden incluir cualquier dispositivo para ingresar información en el dispositivo de usuario que esté disponible y sea soportada por el dispositivo de usuario como, por ejemplo, una pantalla táctil, un teclado, ratón, dispositivo con control de cursor, micrófono, cámara digital, videograbadora o videocámara. Estos dispositivos pueden usarse para ingresar información e interactuar con el software y otros dispositivos descritos en la presente memoria.

Uno o más dispositivos 110 de cliente también pueden ser un dispositivo móvil, por ejemplo, un iPhone, iPod, iPad de Apple® o cualquier otro dispositivo móvil que ejecute el sistema operativo iOS de Apple, cualquier dispositivo que ejecute

el sistema operativo Windows® Mobile de Microsoft, y/o cualquier otro teléfono inteligente o dispositivo móvil ponible.

Varios dispositivos 110 de cliente de la Figura 1A incluyen un teléfono 142 celular, un ordenador 144 portátil, una tableta 148 y un terminal 146. Los dispositivos 110 de cliente pueden incluir una aplicación de cliente fina específicamente adaptada para la comunicación con el proveedor 120 de servicios. La aplicación de cliente fina puede almacenarse en una memoria del dispositivo de cliente y ser utilizable cuando se ejecuta por el dispositivo de cliente para controlar una interfaz entre el dispositivo de cliente y una aplicación del proveedor de servicios y, por consiguiente, permite a un usuario en el dispositivo de cliente acceder a contenido y servicios del proveedor de servicios.

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 110 de cliente al proveedor 120 de servicios. Por ejemplo, la red 115 puede incluir una o más de una red de fibra óptica, una red óptica pasiva, una red por cable, una red de Internet, una red por satélite, una red de área local (LAN, por sus siglas en inglés) inalámbrica, un Sistema Global para la Comunicación Móvil, un servicio de comunicación personal, una red de área personal, un protocolo de aplicación inalámbrico, servicio de mensajes multimedia, servicio mejorado de mensajes, servicio de mensajes cortos, sistemas basados en la multiplexación por división de tiempo, sistemas basados en el 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, por sus siglas en inglés), Wi-Fi, y/o similares.

Además, la red 115 puede incluir, entre otras, líneas telefónicas, fibras ópticas, IEEE Ethernet 902.3, una red de área amplia ("WAN", por sus siglas en inglés), una red de área personal inalámbrica ("WPAN", por sus siglas en inglés), una red de área local ("LAN"), o una red global como, por ejemplo, Internet. Además, la red 115 puede soportar una red de Internet, una red de comunicación inalámbrica, una red celular, o similar, o cualquier combinación de ellas. La red 115 puede además incluir una red, o cualquier cantidad de los tipos de redes a modo de ejemplo descritos más arriba, que funcionan como una red autónoma o en colaboración entre ellas. La red 115 puede utilizar uno o más protocolos de uno o más elementos de red a los cuales se acopla de manera comunicativa. La red 115 puede traducirse en o de otros protocolos en uno o más protocolos de dispositivos de red.

Debe observarse que, según uno o más ejemplos, la red 115 puede ser parte de múltiples redes interconectadas como, por ejemplo, Internet, una red 125 privada del proveedor de servicios, una red de televisión por cable, redes corporativas como, por ejemplo, redes de asociación de tarjetas de crédito, y redes domésticas. Además, la red 125 privada puede implementarse como una red privada virtual en capas en la red 115.

El proveedor 120 de servicios es, en una realización, una empresa que provee servicios basados en ordenador a clientes en una red 115. Casi todos los proveedores de servicios modernos usan Internet para proveer ofertas de servicio a potenciales consumidores. Las ofertas de servicio se proveen, en general, en la forma de aplicaciones de software que funcionan usando recursos dedicados del proveedor de servicios. La combinación de software y hardware que provee un servicio particular a un cliente se denomina, en la presente memoria, "servidor". Los servidores pueden comunicarse en una red 125 privada del proveedor de servicios, a la que, con frecuencia, se hace referencia como una red corporativa o empresarial. La red 125 privada puede comprender una red inalámbrica, una red cableada o cualquier combinación de red inalámbrica y red cableada según se describe más arriba con respecto a la red 115.

En el sistema de la Figura 1A, el proveedor 120 de servicios incluye un servidor 150 de aplicaciones, un servidor 160 de autenticación y un servidor 140 de Gestión de Relaciones con el Cliente (CRM, por sus siglas en inglés). Aunque cada servidor se ilustra como un dispositivo discreto, se observa que las aplicaciones y los servidores pueden distribuirse a lo largo de la empresa o, en el caso de recursos distribuidos como, por ejemplo, recursos "en la nube", a lo largo de la red 115. El servidor 150 de aplicaciones puede soportar uno o más servicios de aplicaciones provistos por el proveedor 120 de servicios, por ejemplo, servicios de gestión de cuentas. El servidor 140 CRM puede usarse para proveer servicios de atención al cliente a clientes del proveedor 120 de servicios, incluidos el procesamiento y el reenvío de llamadas entrantes de clientes a uno o más agentes de gestión de llamadas en el trabajo en estaciones 132, 135 de trabajo.

La base 130 de datos comprende recursos de almacenamiento de datos que pueden usarse, por ejemplo, para almacenar cuenta del cliente, credenciales u otra información de autenticación, para su uso por el servidor 150 de aplicaciones y el servidor 160 de autenticación. La base 130 de datos puede estar compuesta de recursos de datos acoplados que comprenden cualquier combinación de almacenamiento local, almacenamiento en centros de datos distribuidos, o almacenamiento basado en la nube.

Según un aspecto, una tarjeta 105 sin contacto puede estar presente en una comunicación inalámbrica, por ejemplo, comunicación de campo cercano (NFC), con uno o más dispositivos 110 de cliente. Por ejemplo, la tarjeta 105 sin contacto puede comprender uno o más chips como, por ejemplo, un chip de identificación por radiofrecuencia, configurados mediante NFC u otros protocolos de corto alcance. En otras realizaciones, la tarjeta 105 sin contacto puede comunicarse con dispositivos 110 de cliente a través de otros medios incluidos, entre otros, Bluetooth, satélite y/o WiFi. Como se describe en Aplicación '119, la tarjeta 105 sin contacto puede configurarse para comunicarse con uno de un terminal 146 de lector de tarjeta, un teléfono 142 celular, un ordenador 144 portátil y/o una tableta 148 a través de NFC cuando la tarjeta 105 sin contacto se encuentra dentro del rango del respectivo dispositivo de cliente.

Como se describirá en mayor detalle más abajo, la tarjeta 105 sin contacto puede incluir información de clave y contador que puede transformarse usando algoritmos criptográficos para generar un criptograma que puede usarse por el proveedor de servicios para autenticar el dispositivo de cliente.

La Figura 1B es un diagrama de tiempo que ilustra una secuencia a modo de ejemplo para proveer acceso autenticado según una o más realizaciones de la presente descripción. El sistema 100 puede comprender la tarjeta 105 sin contacto y el dispositivo 110 de cliente, que pueden incluir una aplicación 122 y un procesador 124. La Figura 1B puede hacer referencia a componentes similares a los que se ilustran en la Figura 1A.

En la etapa 102, la aplicación 122 se comunica con la tarjeta 105 sin contacto (p. ej., después de acercarse a la tarjeta 105 sin contacto). La comunicación entre la aplicación 122 y la tarjeta 105 sin contacto puede implicar que la tarjeta 105 sin contacto está suficientemente cerca de un lector de tarjeta (no se muestra) del dispositivo 110 de cliente para permitir la transferencia de datos NFC entre la aplicación 122 y la tarjeta 105 sin contacto.

En la etapa 104, después de que la comunicación se haya establecido entre el dispositivo 110 de cliente y la tarjeta 105 sin contacto, la tarjeta 105 sin contacto genera un criptograma de código de autenticación de mensaje (MAC, por sus siglas en inglés). En algunos ejemplos, esto puede ocurrir cuando la tarjeta 105 sin contacto se lee por la aplicación 122. En particular, esto puede ocurrir tras una lectura como, por ejemplo, una lectura NFC, de una etiqueta de intercambio de datos de campo cercano (NDEF, por sus siglas en inglés), que puede crearse según el Formato de Intercambio de Datos NFC. Por ejemplo, un lector como, por ejemplo, la aplicación 122, puede transmitir un mensaje como, por ejemplo, un mensaje de selección de *applet*, el ID de *applet* de un NDEF produciendo el *applet*. Tras la confirmación de la selección, puede transmitirse una secuencia de mensajes de selección de archivos seguida de mensajes de lectura de archivos. Por ejemplo, la secuencia puede incluir "archivo Seleccionar Capacidades", "archivo Leer Capacidades", y archivo "Seleccionar NDEF". En este punto, un valor de contador mantenido por la tarjeta 105 sin contacto puede actualizarse o aumentarse, y puede seguirse de un archivo "Leer NDFEF". En este punto, puede generarse un mensaje que puede incluir un encabezado y un secreto compartido. Entonces, pueden generarse claves de sesión. El criptograma MAC puede crearse a partir del mensaje, el cual puede incluir el encabezado y el secreto compartido. El criptograma MAC puede entonces concatenarse con uno o más bloques de datos aleatorios, y el criptograma MAC y un número aleatorio (RND, por sus siglas en inglés) pueden cifrarse con la clave de sesión. De allí en adelante, el criptograma y el encabezado pueden concatenarse, y codificarse como ASCII hex y devolverse en formato de mensaje NDEF (en respuesta al mensaje "archivo Leer 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 recurso uniforme (p. ej., como una cadena formateada).

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

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

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

En la etapa 112, el procesador 124 verifica el criptograma MAC según una instrucción de la aplicación 122. Por ejemplo, el criptograma MAC puede verificarse, como se explica más abajo.

En algunos ejemplos, la verificación del criptograma MAC puede llevarse a cabo por un dispositivo diferente del dispositivo 110 de cliente como, por ejemplo, un proveedor 120 de servicios en la comunicación de datos con el dispositivo 110 de cliente (como se muestra en la Figura 1A). Por ejemplo, el procesador 124 puede emitir el criptograma MAC para la transmisión al proveedor 120 de servicios, el cual puede verificar el criptograma MAC.

En algunos ejemplos, el criptograma MAC puede funcionar como una firma digital en aras de la verificación. Otros algoritmos de firma digital como, por ejemplo, algoritmos asimétricos de claves públicas, p. ej., el Algoritmo de Firma Digital y el algoritmo RSA, o protocolos de cero conocimiento, pueden usarse para llevar a cabo esta verificación.

De manera más específica, según un aspecto, una tarjeta 105 sin contacto puede usarse en conjunto con primeras credenciales de autenticación provistas a un proveedor de servicios de aplicaciones para preautenticar una solicitud de soporte de cliente, antes de reenviar la solicitud de soporte al servidor 140 CRM. La preautenticación de solicitudes de soporte de cliente de esta manera provee una doble ventaja; dado que la información de autenticación no se reenvía a la CRM, se obvia la oportunidad de apropiación indebida de dicha información por un agente del centro de atención telefónica. Además, el uso de la tarjeta sin contacto como un segundo factor de autenticación permite la asociación de un dispositivo/número telefónico particular con un individuo específico (a saber, el propietario de la tarjeta) y, por consiguiente, se elimina la probabilidad de que un tercero malicioso "suplante la identidad" del, a saber, se haga pasar por el, cliente. Según otro aspecto de la invención, los protocolos de comunicación de preautenticación descritos más abajo identifican o usan canales de comunicación específicos para la gestión de las llamadas y, de esta manera, reducen la posibilidad de suplantación del cliente.

Realizaciones a modo de ejemplo de sistemas y métodos descritos en la presente memoria pueden configurarse para proveer autenticación de seguridad de múltiples factores que puede usarse para evitar la autenticación en una CRM 140 y, por consiguiente, reducir el potencial de robo de información sensible del cliente durante la gestión de la llamada.

La autenticación del factor seguridad puede comprender múltiples procesos. Un primer proceso de autenticación puede comprender iniciar sesión y validar a un usuario mediante una o más aplicaciones que se ejecutan en un dispositivo. Un segundo proceso de autenticación puede funcionar después del inicio de sesión y validación exitosos 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 seguridad comprende un proceso de autenticación de múltiples factores que puede incluir tanto proveer, de manera segura, la identidad del usuario como alentar al usuario a que participe en uno o más tipos de comportamientos, incluidos, sin limitación, gestos de toque, asociados a la tarjeta sin contacto. En algunos ejemplos, el único o más gestos de toque pueden comprender un toque de la tarjeta sin contacto por el usuario a un dispositivo. En algunos ejemplos, el dispositivo puede comprender un dispositivo móvil, un quiosco, un terminal, una tableta, o cualquier otro dispositivo configurado para procesar un gesto de toque recibido.

Por ejemplo, para proveer una primera capa de autenticación, un cliente puede acceder al sitio web del proveedor de servicios vinculándose a una página web del proveedor de servicios mediante el uso de una aplicación de navegador de Internet que se ejecuta en el dispositivo de cliente. El navegador es una aplicación de software como, por ejemplo, Google® Chrome®, Internet Explorer ®, Safari ®, etc., e incluye un código de programación para traducir páginas web en Lenguaje de Marcas de Hipertexto (HTML, por sus siglas en inglés) de la aplicación del proveedor de servicios en un formato adecuado para que un cliente utilice el dispositivo de cliente. Como parte del acceso al sitio web del proveedor de servicios, el proveedor de servicios puede solicitar primera información de autorización, incluida información de contraseñas, respuestas a consultas prealmacenadas, información biométrica, una imagen, u otro mecanismo de verificación de que un usuario del dispositivo de cliente está autorizado a acceder a contenidos y servicios, incluidas cuentas, gestionados por el proveedor de servicios.

Ciertos servicios de alto riesgo provistos por el proveedor de servicios como, por ejemplo, soporte del centro de atención telefónica, pueden beneficiarse de la autenticación de múltiples factores. Por ejemplo, los proveedores de servicio pueden almacenar información de autenticación de primer nivel dentro del navegador de un cliente como una cookie para acelerar los procesos de autenticación durante el inicio de sesión del cliente. Las cookies del navegador, y la contraseña asociada u otros datos, son vulnerables a descubrimiento y uso indebido. Por consiguiente, antes de permitir al usuario acceder a o modificar información altamente sensible o personal, como puede ocurrir durante las llamadas de atención al cliente, es importante validar que el usuario tiene la autoridad para el acceso.

Según un aspecto, la tarjeta 105 sin contacto puede usarse para proveer una segunda autenticación para un usuario de un dispositivo de cliente. En una realización, y según se describe en mayor detalle más abajo, la tarjeta sin contacto incluye una clave, un contador, y funcionalidad de procesamiento criptográfico que pueden usarse para generar un criptograma que puede usarse para validar a un usuario de un dispositivo de cliente. El contador refleja, de manera ventajosa, comportamientos previos del tenedor de la tarjeta. Por ejemplo, el contador puede reflejar la cantidad de veces que el usuario ha accedido previamente a un servicio particular del proveedor de servicios, información que es virtualmente imposible que un tercero malicioso obtenga con precisión.

Cuando un cliente busca acceder a un servicio de alto riesgo, en algunas realizaciones, dicho servicio provee una aplicación que hace que el usuario provea el segundo nivel de autenticación mediante el uso de la tarjeta 105 sin contacto, por ejemplo, como se describe más arriba, acoplando, de manera comunicativa, la tarjeta 105 a uno de los dispositivos 110 de cliente mediante toques o de otra manera.

Después de la segunda autenticación, y como se describirá en mayor detalle más abajo, el proveedor de servicios devuelve datos al dispositivo de cliente. Los datos pueden incluir datos que permiten al cliente iniciar un enlace de comunicación con el servidor 140 CRM. Dichos datos pueden incluir información de contacto como, por ejemplo, un enlace a una aplicación del proveedor de servicios CRM, o un número de teléfono para un centro de atención telefónica. En algunas realizaciones, la información de contacto puede aumentarse con información de control para la CRM o centro de atención telefónica. Por ejemplo, la información de control puede dirigir la CRM o centro de atención telefónica para que evite cualquier proceso de autenticación o de Respuesta de Voz Interactiva (IVR, por sus siglas en inglés) normalmente llevado a cabo en el centro de atención telefónica para explicar el hecho de que el cliente ya se ha preautenticado por la aplicación del proveedor de servicios/proceso de autenticación de tarjeta sin contacto de múltiples factores.

Debe observarse que, aunque en la descripción de más arriba, la primera autenticación se describe como una que usa información personal, biométrica, preguntas u otra información de autenticación, se reconoce que, en algunos ejemplos, una aplicación de 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 primero como el segundo procesos de autenticación utilizan el proceso de autenticación de tarjeta sin contacto con clave/contador descrito en mayor detalle más abajo. En algunas realizaciones, si la aplicación de lado de cliente no está instalada en un dispositivo de cliente, un toque de la tarjeta sin contacto cerca del lector de tarjeta puede iniciar una descarga de la aplicación (como, por ejemplo, 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, mediante la

aplicación u otra comunicación de soporte, la activación de la tarjeta sin contacto. En algunos ejemplos, la única o más aplicaciones pueden configurarse para determinar que se ha lanzado mediante uno o más gestos de toque de la tarjeta sin contacto, de modo tal que un lanzamiento ha ocurrido a las 3:51 p. m., que una transacción se procesó o tuvo lugar a las 3:56 p. m., con el fin de verificar la identidad del usuario.

En algunos ejemplos, pueden recogerse datos sobre los comportamientos de toque como autenticación biométrica/gestual. Por ejemplo, un identificador único que es criptográficamente seguro y no susceptible de intercepción puede transmitirse a uno o más servicios de soporte. El identificador único puede configurarse para buscar información secundaria sobre el individuo. La información secundaria puede comprender información personalmente identificable sobre el usuario. En algunos ejemplos, la información secundaria puede almacenarse dentro de la tarjeta sin contacto.

La Figura 2 ilustra una o más tarjetas 200 sin contacto, que pueden comprender una tarjeta de pago como, por ejemplo, una tarjeta de crédito, tarjeta de débito, o tarjeta regalo, emitida por un proveedor 205 de servicios que se muestra en la parte frontal o posterior de la tarjeta 200. En algunos ejemplos, la tarjeta 200 sin contacto no está relacionada con una tarjeta de pago, y puede comprender, sin limitación, una tarjeta de identificación. En algunos ejemplos, la tarjeta de pago puede comprender una tarjeta de pago sin contacto de doble interfaz. La tarjeta 200 sin contacto puede comprender un sustrato 210, que puede incluir una única capa, o una o más capas laminadas compuestas de plásticos, metales y otros materiales. Materiales de sustrato a modo de ejemplo incluyen cloruro de polivinilo, acetato de cloruro de polivinilo, acrilonitrilo butadieno estireno, policarbonato, poliésteres, titanio anodizado, paladio, oro, carbón, papel, y materiales biodegradables. En algunos ejemplos, la tarjeta 200 sin contacto puede tener características físicas que cumplen con el formato ID-1 de la norma ISO/IEC 7810, y la tarjeta sin contacto puede, de otra manera, cumplir con la norma ISO/IEC 14443. Sin embargo, se comprende que la tarjeta 200 sin contacto según la presente descripción puede tener diferentes características, y la presente descripción no requiere que una tarjeta sin contacto se implemente en una tarjeta de pago.

La tarjeta 200 sin contacto puede también incluir información 212 de identificación que se muestra en la parte frontal y/o posterior de la tarjeta, y una almohadilla 220 de contacto. La almohadilla 220 de contacto puede configurarse para establecer contacto con otro dispositivo de comunicación como, por ejemplo, un dispositivo de usuario, teléfono inteligente, ordenador portátil, ordenador de sobremesa o tableta. La tarjeta 200 sin contacto puede también incluir circuitos de procesamiento, antenas y otros componentes que no se muestran en la Figura 2. Estos componentes pueden ubicarse detrás de la almohadilla 220 sin contacto o en otra parte en el sustrato 210. La tarjeta 200 sin contacto puede también incluir una tira o cinta magnética, que puede ubicarse en la parte posterior de la tarjeta (no se muestra en la Figura 2).

Como se ilustra en la Figura 3, la almohadilla 220 de contacto puede incluir circuitos de procesamiento para almacenar y procesar información, incluidos un microprocesador 330 y una memoria 335. Se comprende que los circuitos de procesamiento pueden contener componentes adicionales, incluidos procesadores, memorias, verificadores de errores y paridad/CRC, codificadores de datos, algoritmos anticolisión, controladores, decodificadores de comandos, primitivas de seguridad y hardware a prueba de falsificaciones, según sea necesario para llevar a cabo las funciones descritas en la presente memoria.

La memoria 335 puede ser una memoria de solo lectura, memoria de escritura única y múltiple lectura o memoria de lectura/escritura, p. ej., RAM, ROM y EEPROM, y la tarjeta 300 sin contacto puede incluir una o más de estas memorias. Una memoria de solo lectura puede ser programable de fábrica como de solo lectura o programable de una sola vez. La programabilidad de una sola vez provee la oportunidad de escribir una vez y luego leer muchas veces. Una memoria de única escritura/múltiple lectura puede programarse en un punto en el tiempo después de que el chip de la memoria haya abandonado la fábrica. Una vez que la memoria esté programada, no puede reescribirse, pero puede leerse muchas veces. Una memoria de lectura/escritura puede programarse y reprogramarse muchas veces después de abandonar la fábrica. También puede leerse muchas veces.

La memoria 335 puede configurarse para almacenar uno o más *applets* 340, uno o más contadores 345 e información 350 de cliente. El único o más *applets* 340 pueden comprender una o más aplicaciones de software configuradas para ejecutarse en una o más tarjetas sin contacto como, por ejemplo, *applet* de Java Card. Sin embargo, se comprende que los *applets* 340 no se limitan a los *applets* de Java Card y, en cambio, pueden ser cualquier aplicación de software utilizable en tarjetas sin contacto u otros dispositivos que tengan memoria limitada. El único o más contadores 345 pueden comprender un contador numérico suficiente para almacenar un entero. La información 350 de cliente puede comprender un identificador alfanumérico único asignado a un usuario de la tarjeta 200 sin contacto y una o más claves que juntas pueden usarse para distinguir al usuario de la tarjeta sin contacto de otros usuarios de tarjetas sin contacto. En algunos ejemplos, la información 350 de cliente puede incluir información que identifica tanto a un cliente como una cuenta asignada a dicho cliente y puede además identificar la tarjeta sin contacto asociada a la cuenta del cliente.

Los elementos de procesador y memoria de las anteriores realizaciones a modo de ejemplo se describen con referencia a la almohadilla de contacto, pero la presente descripción no se encuentra limitada a ello. Se comprende que estos elementos pueden implementarse fuera de la almohadilla 220 o totalmente separados de ella, o como elementos adicionales además de los elementos de microprocesador 330 y memoria 335 ubicados dentro de la almohadilla 220 de contacto.

En algunos ejemplos, la tarjeta 200 sin contacto puede comprender una o más antenas (no se muestran). La única o más antenas pueden colocarse dentro de la tarjeta 200 sin contacto y alrededor de los circuitos de procesamiento de la almohadilla 220 de contacto. Por ejemplo, la única o más antenas pueden ser integrales con los circuitos de procesamiento y la única o más antenas pueden usarse con una bobina elevadora externa. Como otro ejemplo, la única o más antenas pueden ser externas a la almohadilla 220 de contacto y a los circuitos de procesamiento.

Como se explica más arriba, las tarjetas 200 sin contacto pueden construirse en una plataforma de software utilizable en tarjetas inteligentes u otros dispositivos que comprendan código de programa, capacidad de procesamiento y memoria como, por ejemplo, JavaCard. Los *applets* pueden añadirse a las tarjetas sin contacto para generar una contraseña de un solo uso (OTP, por sus siglas en inglés) para la autenticación de múltiples factores (MFA, por sus siglas en inglés) en varios casos de uso basados en aplicaciones móviles. Los *applets* pueden configurarse para responder una o más solicitudes como, por ejemplo, solicitudes de intercambio de datos de campo cercano (NDEF), de un lector, como, por ejemplo, un lector de comunicación de campo cercano (NFC) móvil, y producen un mensaje NDEF que comprende una OTP criptográficamente segura codificada como una etiqueta de texto NDEF. Por consiguiente, la funcionalidad de la tarjeta sin contacto se adapta para proveer una contraseña única de un solo uso como parte de una comunicación de intercambio de datos de campo cercano como se describe más abajo.

La Figura 4 ilustra una capa 400 de registro corto NDEF a modo de ejemplo (SR=1) según una realización a modo de ejemplo. Un mensaje NDEF provee un método normalizado para que un dispositivo 110 de cliente se comunique con una tarjeta 105 sin contacto. En algunos ejemplos, los mensajes NDEF pueden comprender uno o más registros. El registro 400 NDEF incluye un encabezado 402 que incluye múltiples banderas que definen cómo interpretar el resto del registro, incluidas una bandera 403a Comenzar Mensaje (MB, por sus siglas en inglés), una bandera 403b Finalizar Mensaje (ME, por sus siglas en inglés), una bandera 403c Separar (CF, por sus siglas en inglés), una bandera 403d Registro Corto (SR, por sus siglas en inglés), una bandera 403e Longitud ID (IL, por sus siglas en inglés) y un campo 403f Formato de Nombre de Tipo (TNF, por sus siglas en inglés). Las banderas MB 403a y ME 403b pueden configurarse para indicar los respectivos primero y último registros del mensaje. Las banderas CF 403c e IL 403e proveen información sobre el registro, incluido respectivamente si los datos están `separados' (datos distribuidos entre múltiples registros dentro de un mensaje) o si el campo 408 de longitud de tipo de ID es relevante. La bandera SR 403d puede configurarse cuando el mensaje incluye solo un registro.

El campo TNF 403f identifica el tipo de contenido que contiene el campo, según se define por el protocolo NFC. Estos tipos incluyen vacío, conocido (datos definidos por la Definición de Tipo de Registro (RTD, por sus siglas en inglés) del foro NFC), Extensiones Multipropósito de Correo Internet (MIME, por sus siglas en inglés) [como se define por RFC 2046], Identificador de Recurso Uniforme (URI, por sus siglas en inglés) Absoluto [como se define por RFC 3986], externo (definido por el usuario), desconocido, sin cambios [para separaciones] y reservado.

Otros campos de un registro NFC incluyen longitud 404 de tipo, longitud 406 de carga útil, longitud 408 de ID, Tipo 410, ID 412 y Carga 414 Útil. Contiene la longitud del tipo de carga útil en bytes. El campo 404 longitud de tipo especifica el tipo preciso de datos encontrados en la carga útil. Longitud 406 de Carga Útil contiene la longitud de la carga útil en bytes. Un registro puede contener hasta 4.294.967.295 bytes (o 2^32 — 1 bytes) de datos. Longitud 408 de ID contiene la longitud del campo ID en bytes. Tipo 410 identifica el tipo de datos que contiene la carga útil. El campo 412 ID provee el medio para que aplicaciones externas identifiquen toda la carga útil transportada dentro de un registro NDEF. Carga 414 útil comprende el mensaje.

En algunos ejemplos, los datos pueden inicialmente almacenarse en la tarjeta sin contacto mediante implementación de ALMACENAR DATOS (E2) según un protocolo de canal seguro. Estos datos pueden incluir un ID de Usuario personal (pUID, por sus siglas en inglés) que es único a la tarjeta, así como uno o más de una clave inicial, datos de procesamiento criptográficos que incluyen claves de sesión, claves de cifrado de datos, números aleatorios y otros valores que se describirán en mayor detalle más abajo. Estos valores pueden usarse para generar un código de autenticación de mensaje (MAC) que puede usarse para preautenticar a un cliente antes de la gestión del servicio de cliente.

Información a modo de ejemplo que puede intercambiarse con la tarjeta 105 sin contacto y un servidor 160 de autenticación durante la inicialización para completar la tarjeta sin contacto para soportar la autenticación segura según aspectos de esta invención se muestra en la Tabla 1 más abajo.

TABLA 1:

Elemento	Longitud (bytes)	¿Cifrado?	Notas
pUID	8	No	ID de Tarjeta Único
AutKey	16	Sí	3DES Clave para Derivar claves de sesión MAC
AutKCV	3	No	Valor de Verificación de Clave
DEKKey	16	Sí	3DES Clave para Derivar clave de sesión de Cifrado
DEKKCV	3	No	Valor de Verificación de Clave
Tarjeta Compartida Aleatorio	4 bytes	No	4 Byte número Aleatorio Verdadero (pregenerado)
NTLV	X Bytes	No	datos TLV para mensaje NDEF

Después de la inicialización, tanto la tarjeta sin contacto como el servidor de autenticación almacenan información para identificar, de manera única, al tenedor de la tarjeta. Estas características pueden usarse según un aspecto para autenticar el acceso de clientes a servicios de alto riesgo como se describe más abajo.

La Figura 5 ilustra un sistema de comunicación en el cual una tarjeta 510 sin contacto puede almacenar información como, por ejemplo, la información incluida en la Tabla 1 puede usarse para autenticar a un usuario antes de conectar al usuario con un servicio de alto riesgo del proveedor de servicios. En un aspecto, un "servicio de alto riesgo" es uno que puede beneficiarse de los procesos de autenticación de múltiples factores debido a la oportunidad de que el servicio exponga información sensible del cliente u otra información. Según se describe con respecto a la Figura 3, cada tarjeta sin contacto puede incluir una memoria 516 para almacenar información 518 de cliente, incluidos uno o más tributos de identificación única como, por ejemplo, identificadores, claves, números aleatorios y similares. En un aspecto, la memoria además incluye un *applet* 517 de autenticación utilizable cuando se ejecuta por el microprocesador 512 para controlar procesos de autenticación descritos en la presente memoria. Además, cada tarjeta 510 puede incluir uno o más contadores 514 de transacciones de aplicación (ATC, por sus siglas en inglés), y una interfaz 515. Como se describe más arriba, en una realización, la interfaz opera NFC u otros protocolos de comunicación.

El dispositivo 520 de cliente también incluye una interfaz 525 de tarjeta para comunicarse con la tarjeta sin contacto, y una o más interfaces de red diferentes (no se muestran) que permiten al dispositivo 520 comunicarse con un proveedor de servicios mediante el uso de una variedad de protocolos de comunicación como se describe más arriba. El dispositivo de cliente puede además incluir una interfaz 526 de usuario, que puede incluir uno o más de un teclado o pantalla táctil, que permite la comunicación entre una aplicación del proveedor de servicios y un usuario del dispositivo 520 de cliente. El dispositivo 520 de cliente además incluye una memoria 522 que almacena información y un código de programa que controla el funcionamiento del dispositivo 520 de cliente, incluida, por ejemplo, una aplicación 523 de lado de cliente que puede proveerse al cliente por un proveedor de servicios para facilitar el acceso a y el uso de aplicaciones del proveedor de servicios. En una realización, la aplicación 523 de lado de cliente incluye un código de programa configurado para comunicar información de autenticación de la tarjeta 510 sin contacto a uno o más servicios provistos por el proveedor de servicios. La aplicación 523 de lado de cliente puede controlarse mediante una entrada recibida en una interfaz 527 de aplicación del proveedor de servicios (SP, por sus siglas en inglés) que se muestra en la interfaz 526 de usuario. Por ejemplo, un usuario puede seleccionar un ícono, enlace u otro mecanismo provisto como parte de la interfaz 527 de aplicación SP para lanzar la aplicación de lado de cliente para acceder a servicios de aplicación SP.

Según se describe con respecto a la Figura 1A, el dispositivo 520 de cliente puede conectarse a varios servicios de aquellos provistos por un proveedor 505 de servicios, incluidos un servidor 540 de Gestión de Relaciones con el Cliente (CRM) y un servidor 550 de autenticación. En una realización, el servidor 540 CRM gestiona el enrutamiento de las llamadas de soporte recibidas y la transferencia de las llamadas recibidas a una estructura 542 de gestión de llamadas. El servidor 550 de autenticación incluye una tabla 552 de información de cliente para almacenar información como, por ejemplo, aquella de la Tabla 1 para clientes de un proveedor de servicios. La unidad 554 de autenticación incluye hardware y software para llevar a cabo varios procesos de autenticación para clientes que usan información de la tabla 556. En una realización, el servidor de autenticación además incluye una tabla de la tabla 556 de valores de contador de cliente que puede usarse según se describe más abajo para llevar a cabo la autenticación en conjunto con la tarjeta 510 sin contacto.

La Figura 6 ilustra varias etapas que pueden llevarse a cabo por la tarjeta 601 sin contacto, el dispositivo 611 de cliente y un servicio de autenticación de un proveedor 621 de servicios que se configuran para usar técnicas de diversificación de claves como parte de un protocolo de autenticación de múltiples factores para preautenticar clientes. Por ejemplo, un tenedor de tarjeta de tarjeta 601 sin contacto con acceso a un dispositivo 611 de cliente puede buscar autenticación de un proveedor 621 de servicios para permitir el acceso a servicios, incluida la búsqueda de autenticación de múltiples factores para acceder a servicios de alto riesgo como, por ejemplo, soporte del centro de atención telefónica.

En la etapa 610, el cliente 611 primero accede a una cuenta de cliente mantenida por un proveedor 621 de servicios mediante el intercambio de credenciales de inicio de sesión con el proveedor de servicios, donde las credenciales de inicio de sesión pueden incluir, entre otros, contraseñas, claves, datos biométricos, datos de imágenes, intercambios de consulta/respuesta, etc. En una realización, el cliente puede iniciar este acceso lanzando la aplicación de lado de cliente mediante la interfaz 527 de aplicación SP. El lanzamiento de la aplicación puede incluir mostrar una página web de proveedor de servicios configurada para aceptar primera información de credenciales del usuario.

En algunas realizaciones, la autenticación de primer nivel puede llevarse a cabo usando un proceso de intercambio de criptogramas como se describe más abajo para la autenticación de segundo nivel. La aplicación del proveedor de servicios puede lanzarse dando toques a una tarjeta 601 sin contacto al dispositivo 611 de cliente y, de esta manera, iniciando el intercambio de criptogramas.

El proveedor de servicios recibe las credenciales en la etapa 620 y compara estas credenciales con credenciales para el cliente que se mantienen por el servidor de autorización. Si las credenciales de inicio de sesión no concuerdan en la etapa 622, el proveedor de servicios procede a la etapa 631 para buscar la autenticación del dispositivo de cliente mediante el uso de otros métodos. Si se determina que hay una coincidencia en la etapa 622, el cliente se autentica, y el proveedor de servicios coordina con una aplicación de lado de cliente mantenida por el dispositivo 611 de cliente

mostrar páginas web del proveedor de servicios al cliente para permitir el acceso a uno o más servicios.

En la etapa 614, el dispositivo de cliente solicita acceso a una aplicación de alto riesgo, por ejemplo, una aplicación de servicios de cliente. El cliente puede solicitar acceso, por ejemplo, seleccionando uno de múltiples hipervínculos provistos en un sitio web del proveedor de servicios para dirigir al cliente al servicio seleccionado. El hipervínculo puede incluir, por ejemplo, una dirección web de una página de inicio para el servicio. De manera alternativa, el hipervínculo puede incluir un número de teléfono de un sistema de atención al cliente.

Al recibir la solicitud de servicio de cliente en la etapa 624, el proveedor de servicios determina que el servicio seleccionado es un servicio de alto riesgo que se beneficiará de un segundo nivel de autenticación. Por ejemplo, en una realización que provee la autenticación de un segundo factor mediante el uso de tarjetas sin contacto, el proveedor de servicios puede alentar al cliente a que vincule una tarjeta sin contacto para recuperar un criptograma en aras de la verificación. Dicha indicación puede ser cualquier manera de indicar al cliente que debe vincular la tarjeta sin contacto, incluidas instrucciones de texto, instrucciones visuales, instrucciones audibles y otros mecanismos de indicación disponibles.

El dispositivo 611 de cliente recibe esta solicitud en la etapa 616 y vincula la tarjeta sin contacto. En un aspecto, el dispositivo de cliente usa canales de comunicación NFC como se describe más arriba para intercambiar mensajes con la tarjeta sin contacto; la tarjeta sin contacto colabora para proveer la autenticación de un segundo factor a través de una combinación de claves simétricas, procesamiento criptográfico simétrico y contadores.

En la etapa 602, la tarjeta sin contacto recibe la solicitud de autenticación. En la etapa 604, componentes de procesamiento dentro de la tarjeta sin contacto incrementan un contador de transacción de servicio de aplicación (AST, por sus siglas en inglés) y codifica el contador mediante el uso de la Clave Maestra almacenada en la tarjeta sin contacto mediante el uso de un algoritmo criptográfico simétrico para producir una clave diversificada. El algoritmo criptográfico puede seleccionarse de un grupo que incluye al menos uno de un algoritmo de cifrado simétrico, un algoritmo HMAC y un algoritmo CMAC. En algunos ejemplos, el algoritmo simétrico usado para procesar el valor de diversificación puede comprender cualquier algoritmo criptográfico simétrico usado según sea necesario para generar la clave simétrica diversificada de longitud deseada. Ejemplos no restrictivos del algoritmo simétrico pueden incluir un algoritmo de cifrado simétrico como, por ejemplo, 3DES (Algoritmo de Cifrado de Datos Triple, por sus siglas en inglés) o Estándar de Cifrado Avanzado (AES, por sus siglas en inglés) 128; un algoritmo de Autenticación de Mensajes Basado en Hash (HMAC, por sus siglas en inglés) simétrico, como, por ejemplo, HMAC-SHA-256; y un algoritmo de código de autenticación de mensajes basado en cifrado (CMAC, por sus siglas en inglés) simétrico como, por ejemplo, AES-CMAC. Se comprende que si la salida del algoritmo simétrico seleccionado no genera una clave suficientemente larga, técnicas como, por ejemplo, procesamiento de múltiples iteraciones del algoritmo simétrico con diferentes datos de entrada y la misma clave maestra, pueden producir múltiples salidas que pueden combinarse según sea necesario para producir claves de suficiente longitud.

Los componentes de procesamiento de la tarjeta sin contacto pueden tomar el algoritmo criptográfico seleccionado y, mediante el uso de la clave simétrica maestra, procesar el valor de contador. Por ejemplo, la tarjeta 601 sin contacto puede seleccionar un algoritmo de cifrado simétrico y usar un contador que aumenta con cada transacción de autenticación procesada por la tarjeta sin contacto. La tarjeta 601 sin contacto puede entonces cifrar el valor de contador con el algoritmo de cifrado simétrico seleccionado mediante el uso de la clave simétrica maestra para generar una clave simétrica diversificada.

En un aspecto, la clave simétrica diversificada puede usarse para procesar el contador antes de la transmisión en aras de la autorización. Por ejemplo, la tarjeta 601 sin contacto puede cifrar el valor de contador usando un algoritmo de cifrado simétrico y la clave simétrica diversificada, la salida comprendiendo un criptograma MAC cifrado. La tarjeta 601 sin contacto puede entonces transmitir el criptograma al proveedor 621 de servicios para la autenticación.

En una realización, una plantilla para un mensaje de autenticación que comprende un criptograma puede comprender un primer registro, con un índice conocido para proveer los datos de autenticación dinámica reales. La Tabla II de más abajo es un ejemplo de un mensaje de autenticación que puede intercambiarse entre el dispositivo 611 de cliente y la tarjeta 601 sin contacto.

TABLA II:

Índice Byte	Valor	Comentarios
00	D1	Encabezado {MB, ME, CF, SR, IL, TNF}
02	48	Longitud de Carga Útil que incluye ID de registro
03	54	T
04	02	ID de Registro
05	65 6E EN	(Idioma)
07	43 01 00 76 a6 62 7b 67 a8 cf bb <8 MAC bytes>	

En un ejemplo, si se añaden etiquetas adicionales, el primer byte puede cambiar para indicar el inicio del mensaje, pero no el fin, y un registro posterior puede añadirse. Dado que la longitud de ID es cero, el campo longitud ID e ID se omiten del registro. Un mensaje a modo de ejemplo que se muestra en la Tabla III de más abajo puede incluir: Clave UDK AUT; Clave de sesión AUT derivada (mediante el uso de 0x1234); Versión 1.0; pATC = 0x1234; RND = 76a6627b67a8cfbb; MAC = <ocho bytes computados>. La primera columna puede comprender dirección/índice hacia los datos de mensaje NDEF.

TABLA III:

Formato de Mensaje				
1	2	4	8	8
0x43 (Mensaje Tipo 'A')	Versión	pATC	RND	Criptograma A (MAC)

En la etapa 618, el dispositivo 611 de cliente recibe el criptograma y lo reenvía al proveedor 621 de servicios. En la etapa 626, después de que el proveedor de servicios solicita la autenticación de segundo factor en la etapa 624, en una realización, un servidor de autenticación del proveedor 621 de servicios recupera información del cliente asociada a un tenedor de tarjeta de la tarjeta sin contacto asociada a una cuenta del cliente mediante el uso del dispositivo de cliente. La información de cliente puede incluir una Clave Maestra del cliente y un contador de transacciones de servicio de aplicación de la tarjeta sin contacto. El proveedor 621 de servicios codifica el valor de contador recuperado mediante el uso de la Clave Maestra y un algoritmo criptográfico que coincide con el algoritmo criptográfico usado por la tarjeta sin contacto para producir una copia del proveedor de servicios de una clave diversificada.

En la etapa 628, el proveedor de servicios usa la clave diversificada para descifrar el criptograma para exponer el valor del contador reenviado por la tarjeta sin contacto. En la etapa 629, el proveedor de servicios compara el contador expuesto con el contador recuperado por el proveedor de servicios, lo cual provee una segunda autenticación del usuario. Si no hay coincidencia, no se concede al cliente acceso al servicio, y en la etapa 631, el proveedor 621 de servicios puede buscar autenticar al usuario usando otros métodos. Si en la etapa 629 hay una coincidencia, entonces el proveedor de servicios inicia la gestión de llamada con un servidor CRM en 630. En un aspecto, como se describirá con respecto a la Figura 7 y a la Figura 8, el proveedor de servicios puede generar uno o más mensajes para controlar uno de la CRM o dispositivo de cliente para hacer uso de la preautenticación ya llevada a cabo por el proveedor de servicios.

La próxima vez que se use la tarjeta sin contacto para la autenticación, puede seleccionarse un valor de contador diferente y, de esta manera, producir una clave simétrica diversificada diferente y, por consiguiente, hacer difícil que partes maliciosas monitoreen las comunicaciones para descifrar comunicaciones. Tanto el proveedor de servicios como la tarjeta sin contacto aumentan el contador según un patrón de incremento predeterminado acordado por las partes. Por ejemplo, los contadores pueden aumentar en 1, o en un patrón, por ejemplo, en incrementos de 1 para la primera transacción, en 2 para la segunda, en tres para la tercera o en 5 para cada transacción. Dado que la tarjeta sin contacto y el proveedor de servicios usan un contador común, un patrón de incremento común, una Clave Maestra común y un algoritmo criptográfico común, aunque la clave diversificada cambiará para cada transacción, los dispositivos de transmisión y recepción tendrán la misma clave.

Según se describe más arriba, en algunos ejemplos, el valor de diversificación de clave puede lograrse usando un valor de contador. Otros ejemplos no restrictivos del valor de diversificación de clave incluyen: un *nonce* aleatorio generado cada vez que se necesita una clave nueva diversificada; el valor total de un valor de contador enviado desde el dispositivo de transmisión y dispositivo de recepción; una porción de un valor de contador enviado desde el dispositivo de transmisión y dispositivo de recepción; un contador mantenido independientemente por el dispositivo de transmisión y dispositivo de recepción pero no enviado entre los dos; un código de acceso de una vez intercambiado entre el dispositivo de transmisión y el dispositivo de recepción; y *hash* criptográfico del contador. En algunos ejemplos según se describe en la Aplicación '119, una o más porciones del valor de diversificación de clave pueden usarse por las partes para crear múltiples claves diversificadas. Por ejemplo, un contador puede usarse como el valor de diversificación de clave.

En otro ejemplo, una porción del contador puede usarse como el valor de diversificación de clave. Si múltiples valores de clave maestra se comparten entre las partes, los múltiples valores de clave diversificada pueden obtenerse por el sistema y procesos descritos en la presente memoria. Un nuevo valor de diversificación y, por lo tanto, una nueva clave simétrica diversificada, puede crearse con tanta frecuencia como se necesite. En el caso más seguro, un nuevo valor de diversificación puede crearse para cada intercambio de datos sensibles entre el dispositivo de transmisión y el dispositivo de recepción. En efecto, esto puede crear una clave de un solo uso como, por ejemplo, una clave de sesión única.

Varias técnicas de cifrado/descifrado simétricas que han reemplazado aquellas descritas con respecto a la Figura 6 se describen en la Aplicación '119.

La Figura 7 y la Figura 8 ilustran, cada una, flujos de transacciones a modo de ejemplo que pueden llevarse a cabo después de una autenticación de múltiples factores de un cliente que busca acceso a servicios del centro de atención

telefónica. En una realización, la información de cliente almacenada en la tarjeta sin contacto puede incluir información del centro de atención telefónica específica al cliente. La información del centro de atención telefónica puede incluir un número, por ejemplo. El número puede comprender una dirección IP, número telefónico, u otra dirección de contacto, número aleatorio o cualquier porción o combinación de una dirección IP, número telefónico u otra dirección de contacto o número aleatorio. La Figura 7 ilustra mensajes a modo de ejemplo que pueden ocurrir entre componentes de un proceso 700 de enrutamiento de llamadas mediante el uso de la información del centro de atención telefónica de la tarjeta 701 sin contacto para definir un enlace de comunicación entre el dispositivo 702 de cliente y el agente 705 de atención al cliente.

Después de un proceso de autenticación de múltiples factores que se muestra en la Figura 6, un servidor 703 de aplicación del proveedor de servicios completa la interfaz de cliente con contenido 710 de web de servicio de cliente. El contenido de web puede incluir información de contacto, la información de contacto comprendiendo un URL, número telefónico u otra dirección de contacto para comunicarse con el servidor CRM. Cuando se selecciona el enlace, un enlace de comunicación se genera entre el dispositivo de cliente y el servidor CRM. Según una realización, el contenido de web de servicio de cliente incluye una indicación 711, que solicita la conexión con la tarjeta 701 sin contacto.

La tarjeta 701 sin contacto, tras recibir la indicación, reenvía un número 712 de preautenticación almacenado al dispositivo de cliente, el cual lo pone a disposición del servidor 703 de aplicaciones. En una realización, el número 712 de preautenticación almacenado incluye un número único asociado a la preautenticación de un dispositivo de cliente. Al menos una porción del número de preautenticación puede anexarse a la información de contacto cuando se genera el enlace de comunicación. Por ejemplo, el contenido 710 web puede incluir un enlace a un número telefónico de atención al cliente 1-800-123-4567. La tarjeta sin contacto puede proveer un número de preautenticación de 7777 que el dispositivo de cliente anexa al número telefónico. El dispositivo de cliente inicia una llamada 715 en la red celular al -800-123-4567,,,, 7777. El servidor de aplicaciones alerta a la CRM sobre una llamada entrante con el número anexado de la tarjeta sin contacto en 714. La CRM monitorea llamadas entrantes con números de preautenticación, y evita la autenticación cuando coloca llamadas en 716 en una estructura de agentes de atención al cliente.

Aunque el proceso de la Figura 7 incluye un número de preautenticación almacenado en una tarjeta sin contacto, en algunas realizaciones un dispositivo de cliente puede configurarse para generar el número de preautenticación para anexar a una llamada. El número de preautenticación puede generarse en respuesta a una comunicación con la tarjeta sin contacto, por ejemplo, después de un intercambio de criptograma con la tarjeta sin contacto como se describe en la Figura 6. En algunas realizaciones, el número de preautenticación puede cambiar para cada solicitud de atención al cliente. Dicha disposición asegura las llamadas de atención al cliente frente a la redirección por partes maliciosas, dado que un dispositivo de cliente impostor no posee los números de preautenticación y, por consiguiente, la autenticación no se evitará en el servidor CRM.

En otras realizaciones, según se ilustra en la Figura 8, para proteger aún más la gestión de las llamadas de una interferencia maliciosa, la gestión de las llamadas se inicia por el agente de atención al cliente. Después de la preautenticación mediante el uso del proceso de la Figura 6, el contenido 810 de la web de atención al cliente se provee al dispositivo de cliente. En una realización, el contenido incluye una indicación 811 para alentar la reautorización del dispositivo de cliente. La tarjeta 812 sin contacto genera un criptograma como se describe más arriba, el cual se reenvía mediante el dispositivo 702 de cliente al servidor 703 de autorización para la validación. Una vez que el servidor de autorización valida el criptograma, el servidor de autorización dirige al servidor CRM para que evite la autorización de una llamada en la etapa 815 y en la etapa 814 dirige a la CRM para que inicie una llamada mediante el servidor de soporte al número telefónico del dispositivo de cliente, dirección IP, etc. En 816, la CRM inicia la llamada.

En algunas realizaciones, la etapa de reautenticación puede ocurrir después de iniciar la llamada 816 por el agente 705 de atención al cliente, para garantizar que la llamada no se haya redirigido entre una autenticación previa y la gestión de la llamada. Dichas realizaciones pueden ser beneficiosas cuando hay un retardo entre una autenticación previa y la gestión de la llamada, por ejemplo, una larga espera en la cola de atención al cliente, o una rellamada programada.

La Figura 9 ilustra varios componentes a modo de ejemplo de una realización de un servicio 900 CRM. El servicio 900 CRM se muestra como uno que incluye lógica 906 de autenticación y unidad 910 de asignación de agente. Las llamadas 901 entrantes se reenvían a un filtro 902 de preautenticación. El filtro 902 de preautenticación puede almacenar números de preautenticación recibidos de un servidor de autorización según se describe más arriba. Las llamadas entrantes que no se hayan preautenticado se reenvían a la cola 904 de autenticación. La lógica de autenticación recupera llamadas entrantes de la cola 904 y colabora con un servidor de autenticación (no se muestra) para validar clientes mediante el uso de cualquier combinación de métodos de autenticación descritos más arriba. Una vez autenticadas, las llamadas se reenvían a la cola 908.

Las llamadas entrantes que se determina que se han preautenticado se reenvían directamente del filtro 902 de preautenticación a la cola 908. De manera ventajosa, para minimizar el potencial de interferencia maliciosa, una vez que una llamada que tiene un número de preautenticación almacenado se evita de esta manera, el número de preautenticación se elimina del filtro 902 de preautenticación.

La cola 908, por consiguiente, almacena llamadas autenticadas, que se asignan a agentes 920, 922, 924 para la gestión por la unidad 910 de asignación de agente según la carga de recursos. Con dicha disposición, las llamadas preautenticadas pueden encaminarse de forma inteligente en un centro de atención telefónica de clientes para minimizar los retardos en la gestión.

Por consiguiente, se han descrito un sistema y un método que utilizan características de autenticación de múltiples factores de un proveedor de servicios y enrutamiento de llamadas inteligente para aumentar la seguridad y eficiencia en un centro de atención telefónica de clientes. Algunas realizaciones pueden describirse mediante el uso de la expresión "una realización" junto con sus derivados. Estos términos significan que un aspecto, característica o estructura particular descrita en conexión con la realización se incluye en al menos una realización. Las apariciones de la frase "en una realización" en varios lugares a lo largo de la memoria descriptiva no se refieren todas a la misma realización necesariamente. Además, a menos que se observe lo contrario, se reconoce que las características descritas más arriba son utilizables juntas en cualquier combinación. Por consiguiente, cualquier característica descrita por separado puede emplearse en combinación con otra a menos que se observe que las características son incompatibles entre sí.

Con referencia general a las notaciones y nomenclaturas usadas en la presente memoria, las descripciones detalladas en la presente memoria pueden presentarse en términos de bloques o unidades funcionales que pueden implementarse como procedimientos de programa ejecutados en un ordenador o red de ordenadores. Estas descripciones y representaciones de procedimientos se usan por las personas con experiencia en la técnica para transmitir, de manera más efectiva, la sustancia de su trabajo a otras personas con experiencia en la técnica.

Un procedimiento se concibe aquí, y en general, para ser una secuencia de funciones autocoherentes que llevan a un resultado deseado. Dichas funciones son las que requieren manipulaciones físicas de cantidades físicas. Normalmente, aunque no necesariamente, dichas cantidades toman la forma de señales eléctricas, magnéticas u ópticas que pueden almacenarse, transferirse, combinarse, compararse y de otra manera manipularse. Se ha demostrado que es conveniente a veces, principalmente por motivos de uso común, referirse a dichas señales como bits, valores, elementos, símbolos, caracteres, términos, números o similares. Debe tenerse en cuenta, sin embargo, que todos dichos términos y términos similares se asociarán a las cantidades físicas apropiadas y son etiquetas meramente convenientes aplicadas a dichas cantidades.

Además, las manipulaciones llevadas a cabo se denominan, con frecuencia, en términos como, por ejemplo, añadir o comparar, que se asocian comúnmente a operaciones mentales llevadas a cabo por un operador humano. Tal capacidad de un operador humano no es necesaria, o deseable en la mayoría de los casos, en cualquiera de las funciones descritas en la presente memoria, las cuales forman parte de una o más realizaciones. Más bien, las funciones son operaciones de máquina. Máquinas útiles para llevar a cabo operaciones de varias realizaciones incluyen ordenadores digitales de propósito general o dispositivos similares.

Algunas realizaciones pueden describirse mediante el uso de la expresión "acoplado/a(s)" y "conectado/a(s)" junto con sus derivados. Dichos términos no pretenden necesariamente ser sinónimos entre sí. Por ejemplo, algunas realizaciones pueden describirse mediante el uso de los términos "conectado/a(s)" y/o "acoplado/a(s)" para indicar que dos o más elementos están en contacto físico o eléctrico directo entre sí. El término "acoplado/a(s)", sin embargo, puede significar también que dos o más elementos no están en contacto directo entre sí, pero colaboran o interactúan entre sí.

Varias realizaciones también se refieren a un aparato o sistemas para llevar a cabo estas operaciones. Este aparato puede construirse especialmente para los propósitos requeridos, o puede comprender un ordenador de propósito general selectivamente activado o reconfigurado por un programa de ordenador almacenado en el ordenador. Los procedimientos presentados en la presente memoria no están inherentemente relacionados con un ordenador particular u otro aparato. Varias máquinas de propósito general pueden usarse con programas escritos según las enseñanzas de la presente memoria, o puede ser conveniente construir aparatos más especializados para llevar a cabo las etapas requeridas del método. La estructura requerida para una variedad de estas máquinas surgirá de la descripción provista.

Se enfatiza que el Resumen de la Descripción se provee para permitir a un lector establecer rápidamente la naturaleza de la descripción técnica. Se presenta en el entendimiento de que no se usará para limitar o interpretar el alcance o significado de las reivindicaciones. Además, en la Descripción Detallada anterior, varias características se agrupan juntas en una sola realización con el fin de optimizar la descripción. El presente método de descripción no se interpretará como uno que refleja una intención de que las realizaciones reivindicadas requieren más características que las enumeradas expresamente en cada reivindicación. Más bien, como las siguientes reivindicaciones reflejan, el objeto de la invención reside en menos que todas las características de una sola realización descrita. Por consiguiente, las siguientes reivindicaciones se incorporan a la Descripción Detallada, siendo cada reivindicación independiente como una realización separada. En las reivindicaciones anexas, los términos "que incluye(n)" y "en el/la cual" se usan como equivalentes de los términos respectivos "que comprende(n)" y "en donde". Además, los términos "primer/a/o(s)", "segundo/a(s)", "tercer/a/o(s)", etc., se usan meramente como etiquetas, y no pretenden imponer requisitos numéricos a sus objetos.

La descripción de más arriba incluye ejemplos de la arquitectura descrita. Por supuesto, no es posible describir cada combinación concebible de componentes y/o metodologías, pero una persona con experiencia en la técnica puede reconocer que son posibles muchas combinaciones y permutaciones adicionales. Por consiguiente, la arquitectura novedosa pretende abarcar todas las alteraciones, modificaciones y variaciones que caigan dentro del alcance de las reivindicaciones anexas.

REIVINDICACIONES

1. Un método implementado por ordenador, que comprende:

recibir, por un sistema de proveedor de servicios, después de una autenticación de múltiples factores para preautenticar un dispositivo de cliente que busca acceder a servicios del centro de atención telefónica ofrecido por el proveedor de servicios mediante el uso de primera información de autenticación, una solicitud de soporte para acceder a una aplicación del proveedor de servicios que ejecuta servicios del centro de atención telefónica;

en respuesta a la solicitud de soporte, enviar al dispositivo de cliente por el proveedor de servicios, una solicitud de segunda información de autenticación de una tarjeta sin contacto;

recibir, por el sistema de proveedor de servicios del dispositivo de cliente, la segunda información de autenticación que incluye un criptograma de una tarjeta sin contacto mediante el dispositivo de cliente;

obtener una validación del criptograma según un proceso de autenticación ejecutado por el sistema de proveedor de servicios;

recibir por el sistema de proveedor de servicios una llamada entrante del dispositivo de cliente, en donde la llamada entrante ha anexado al menos una porción de un número de preautenticación que incluye un número único asociado a la preautenticación del dispositivo de cliente, el número de preautenticación indicando que el dispositivo de cliente y la llamada entrante están preautenticados;

filtrar, por el sistema de proveedor de servicios, la llamada entrante para el número de preautenticación; y

según la llamada entrante preautenticada, avanzar la llamada entrante a una posición en una cola de gestión de llamadas que evita una cola de autenticación.

2. El método de la reivindicación 1, en donde la primera información de autenticación incluye una de credenciales, información biométrica, una clave o combinación de ellas.

3. El método de la reivindicación 1, que además comprende:

mantener por el sistema de proveedor de servicios una copia de una clave maestra usada para generar una clave de diversidad que se usa para validar el criptograma.

4. El método de la reivindicación 3, que además comprende:

descifrar, por el sistema de proveedor de servicios, información en el criptograma recibido del dispositivo de cliente mediante el uso de la clave diversificada generada a partir de la copia de la clave maestra mantenida por el sistema de proveedor de servicios para exponer un valor de contador de la tarjeta sin contacto, en donde el valor de contador se incluye con la segunda información de autenticación de la tarjeta sin contacto;

comparar el valor de contador incluido en el criptograma recibido del dispositivo de cliente con otro valor de contador recuperado por el sistema de proveedor de servicios; y

en respuesta a la comparación, indicar una coincidencia y, de esta manera, generar la validación.

5. El método de la reivindicación 1, en donde la llamada entrante es una llamada de atención al cliente al sistema de proveedor de servicios.

6. El método de la reivindicación 1, en donde la solicitud de la segunda información de autenticación hace que el dispositivo de cliente presente una indicación en una visualización de dar un toque a una tarjeta sin contacto al dispositivo de cliente.

7. Un sistema de proveedor de servicios, que comprende:

un procesador;

una memoria que comprende instrucciones ejecutables por el procesador, el procesador configurado para ejecutar las instrucciones para:

recibir, de un dispositivo de cliente por el sistema de proveedor de servicios después de una autenticación de múltiples factores para preautenticar el dispositivo de cliente que busca acceder a servicios del centro de atención telefónica ofrecido por el proveedor de servicios, una solicitud de soporte para acceder a una aplicación del proveedor de servicios que ejecuta servicios del centro de atención telefónica;

autenticar el dispositivo de cliente con primera información de autenticación;

enviar al dispositivo de cliente por el proveedor de servicios, una solicitud de segunda información de

autenticación de una tarjeta sin contacto;

recibir, del dispositivo de cliente, la segunda información de autenticación que incluye un criptograma de la tarjeta sin contacto mediante el dispositivo de cliente;

validar el criptograma según un proceso de autenticación ejecutado por el sistema de proveedor de servicios;

recibir una llamada entrante del dispositivo de cliente, en donde la llamada entrante ha anexado al menos una porción de un número de preautenticación que incluye un número único asociado a la preautenticación del dispositivo de cliente, el número de preautenticación indicando que el dispositivo de cliente y la llamada entrante están preautenticados según la primera y segunda información de autenticación;

filtrar la llamada entrante para el número de preautenticación; y

según la llamada entrante preautenticada, avanzar la llamada entrante a una posición en una cola de gestión de llamadas que evita una cola de autenticación.

8. El sistema de la reivindicación 7, en donde la primera información de autenticación incluye una de credenciales, información biométrica, una clave o combinación de ellas.

9. El sistema de la reivindicación 7, las instrucciones configuradas además para hacer que el procesador mantenga una copia de una clave maestra usada para generar una clave de diversidad que se usa para validar el criptograma.

10. El sistema de la reivindicación 9, las instrucciones configuradas además para hacer que el procesador:

descifre el criptograma usando la clave diversificada generada a partir de la copia de la clave maestra para exponer un valor de contador de la tarjeta sin contacto;

compare el valor de contador incluido en el criptograma con otro valor de contador recuperado de un almacenamiento; y

en respuesta a la coincidencia del valor de contador con el otro valor de contador, valide el criptograma.

11. El sistema de la reivindicación 7, en donde la llamada entrante es una llamada de atención al cliente al sistema de proveedor de servicios.

12. El sistema de la reivindicación 7, en donde la solicitud de la segunda información de autenticación hace que el dispositivo de cliente presente una indicación en una visualización de dar un toque a una tarjeta sin contacto al dispositivo de cliente.

13. Un medio de almacenamiento legible por ordenador, que comprende instrucciones que, cuando se ejecutan por circuitos de procesamiento, hacen que:

se procese, por un sistema de proveedor de servicios después de una autenticación de múltiples factores para preautenticar un dispositivo de cliente que busca acceder a servicios del centro de atención telefónica ofrecidos por el proveedor de servicios, una solicitud de soporte del dispositivo de cliente para acceder a una aplicación de proveedor de servicios que ejecuta los servicios del centro de atención telefónica;

se autentique el dispositivo de cliente con primera información de autenticación;

se envíe al dispositivo de cliente por el proveedor de servicios, una solicitud de segunda información de autenticación de una tarjeta sin contacto;

se reciba, del dispositivo de cliente, la segunda información de autenticación que incluye un criptograma de la tarjeta sin contacto;

se valide el criptograma según un proceso de autenticación ejecutado por el sistema de proveedor de servicios;

se reciba una llamada entrante del dispositivo de cliente, en donde la llamada entrante ha anexado al menos una porción de un número de preautenticación que incluye un número único asociado a la preautenticación del dispositivo de cliente, el número de preautenticación indicando que el dispositivo de cliente y la llamada entrante están preautenticados según la primera y segunda información de autenticación;

se filtre la llamada entrante para el número de preautenticación; y

según la llamada entrante preautenticada, se haga avanzar la llamada entrante a una posición en una cola de gestión de llamadas que evita una cola de autenticación.

14. El medio de almacenamiento de la reivindicación 13, las instrucciones configuradas además para hacer que los circuitos de procesamiento mantengan una copia de una clave maestra usada para generar una clave de diversidad

que se usa para validar el criptograma.

15. El medio de almacenamiento de la reivindicación 14, las instrucciones configuradas además para hacer que los circuitos de procesamiento:

descifren el criptograma usando la clave diversificada generada a partir de la copia de la clave maestra para exponer un valor de contador de la tarjeta sin contacto;

comparen el valor de contador incluido en el criptograma con otro valor de contador recuperado de un almacenamiento; y

en respuesta a la coincidencia del valor de contador con el otro valor de contador, validen el criptograma.

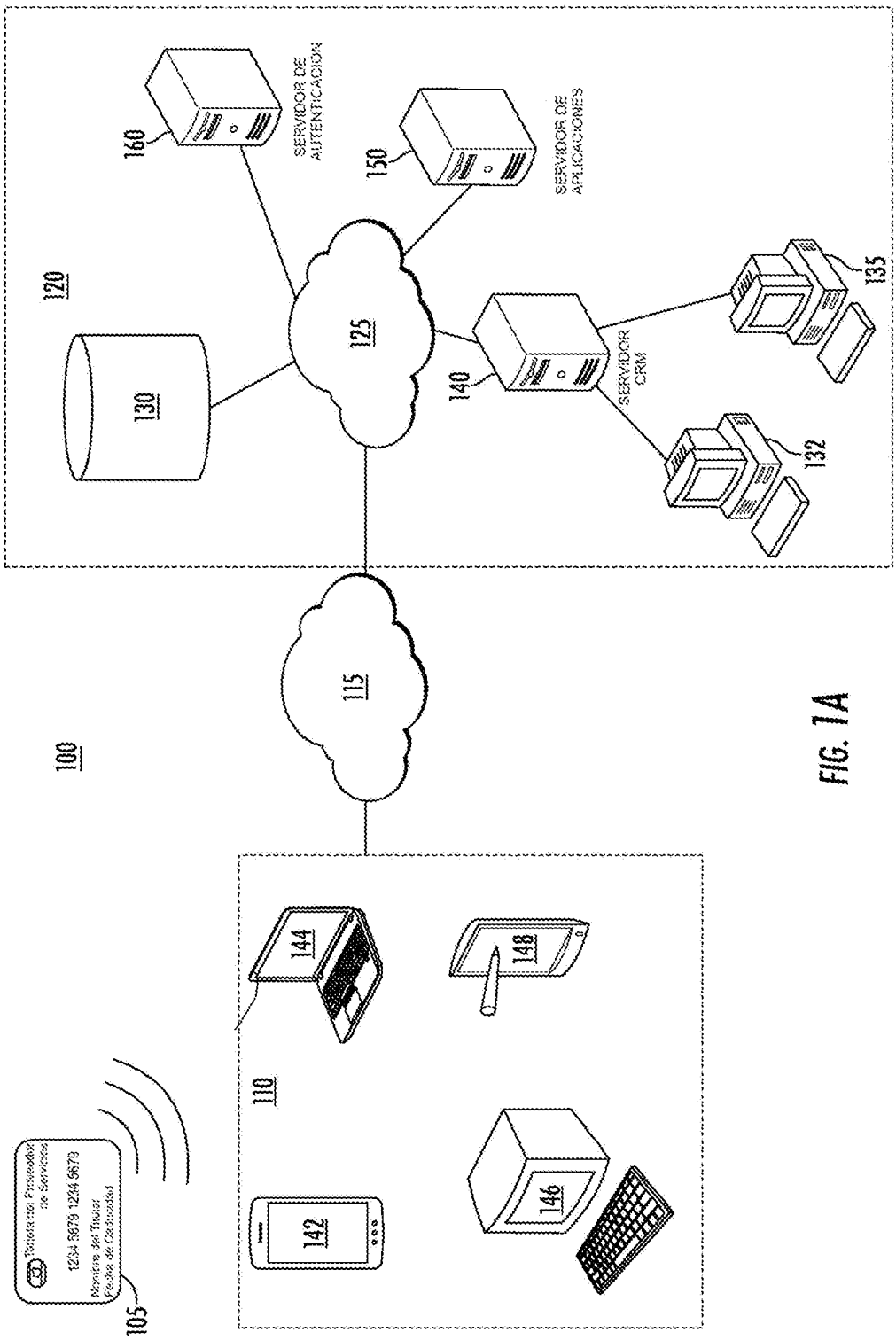
100
105
110
115
120
125
130
132
135
140
142
144
146
148
150
160
SERVIDOR DE AUTENTICACIÓN
SERVIDOR DE APLICACIONES
SERVIDOR CRM
Tarjeta del Proveedor de Servicios
1234 5678 1234 5678
Nombre del Titular
Fecha de Caducidad

FIG. 1A

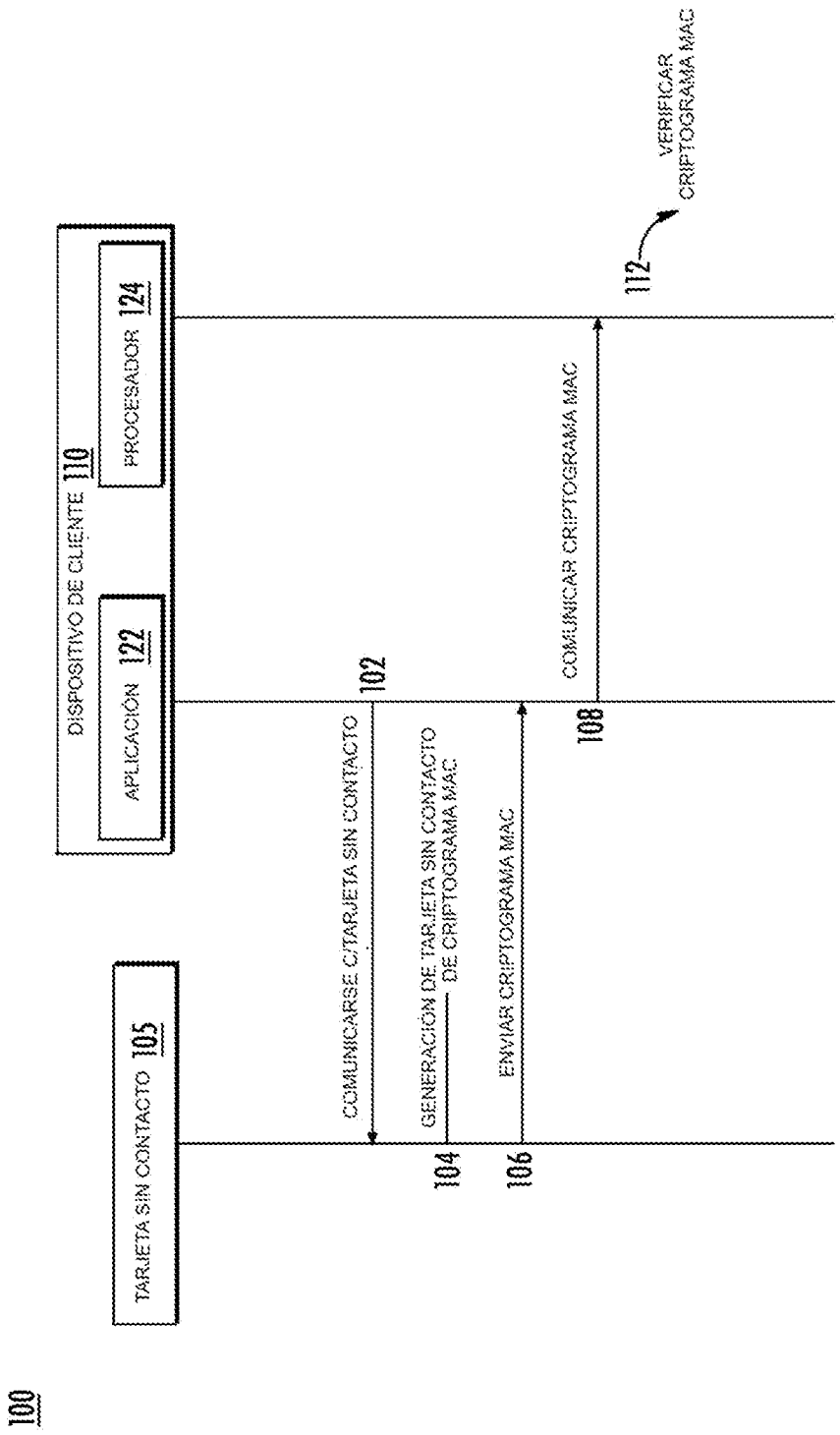
100
TARJETA SIN CONTACTO 105
DISPOSITIVO DE CLIENTE 110
APLICACIÓN 122
PROCESADOR 124
COMUNICARSE C/TARJETA SIN CONTACTO
102
GENERACIÓN DE TARJETA SIN CONTACTO DE CRIPTOGRAMA MAC
104
ENVIAR CRIPTOGRAMA MAC
106
COMUNICAR CRIPTOGRAMA MAC
108
VERIFICAR CRIPTOGRAMA MAC
112

FIG. 1B

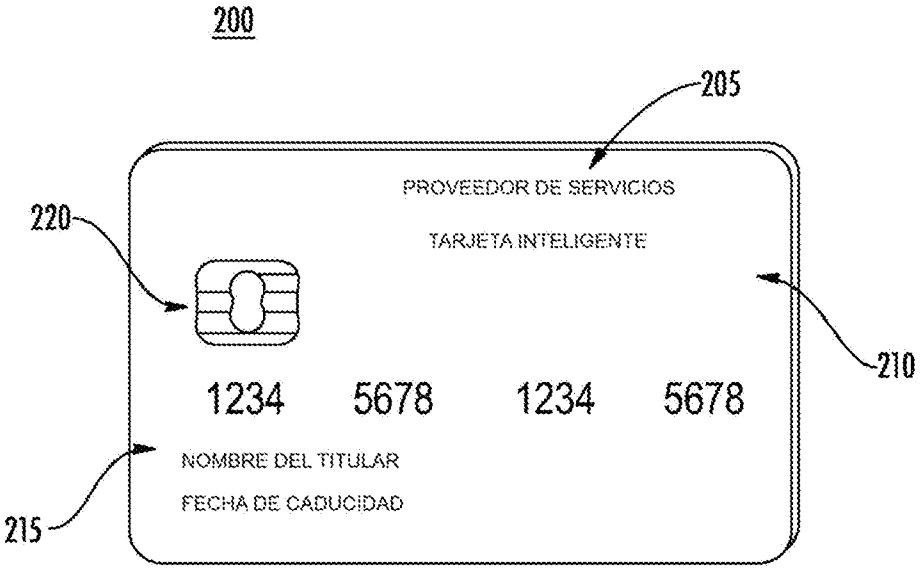
200
205
PROVEEDOR DE SERVICIOS
TARJETA INTELIGENTE
220
210
1234 5678 1234 5678
NOMBRE DEL TITULAR
FECHA DE CADUCIDAD
215

FIG. 2

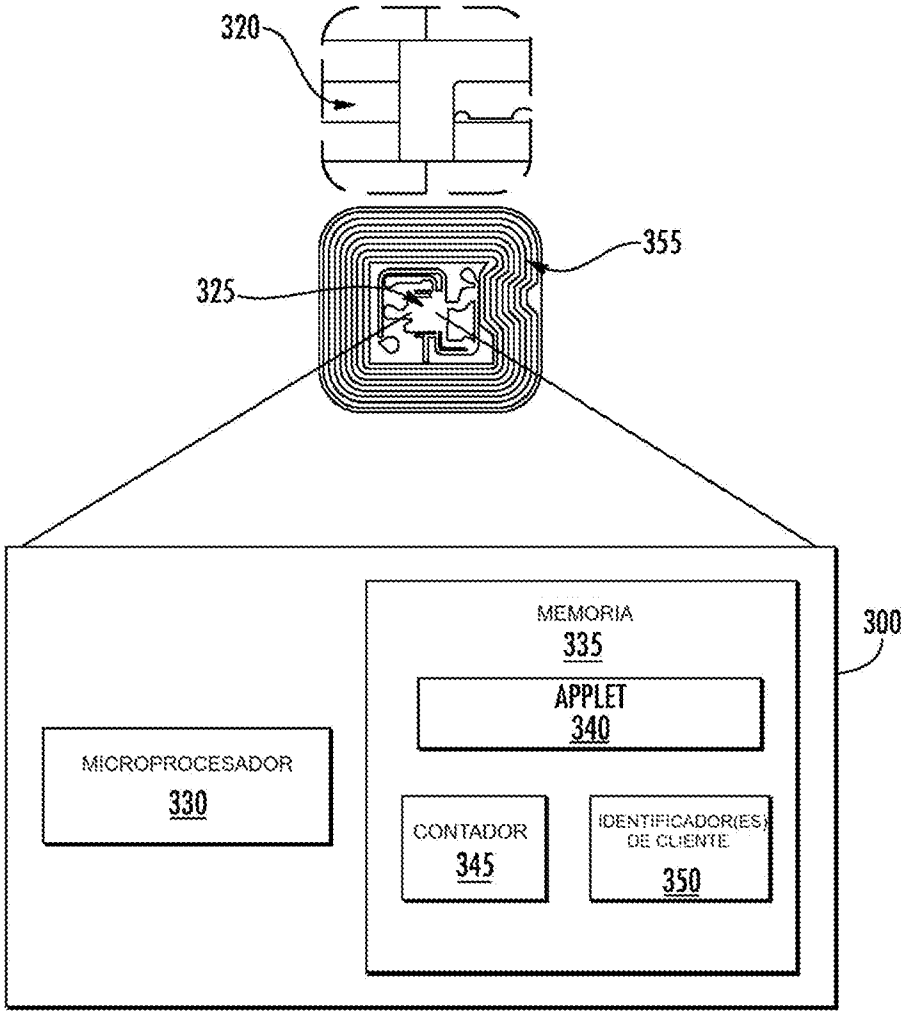
320
355
325
300
MEMORIA
335
APPLET
340
MICROPROCESADOR
330
CONTADOR
345
IDENTIFICADOR(ES) DE CLIENTE
350

FIG. 3

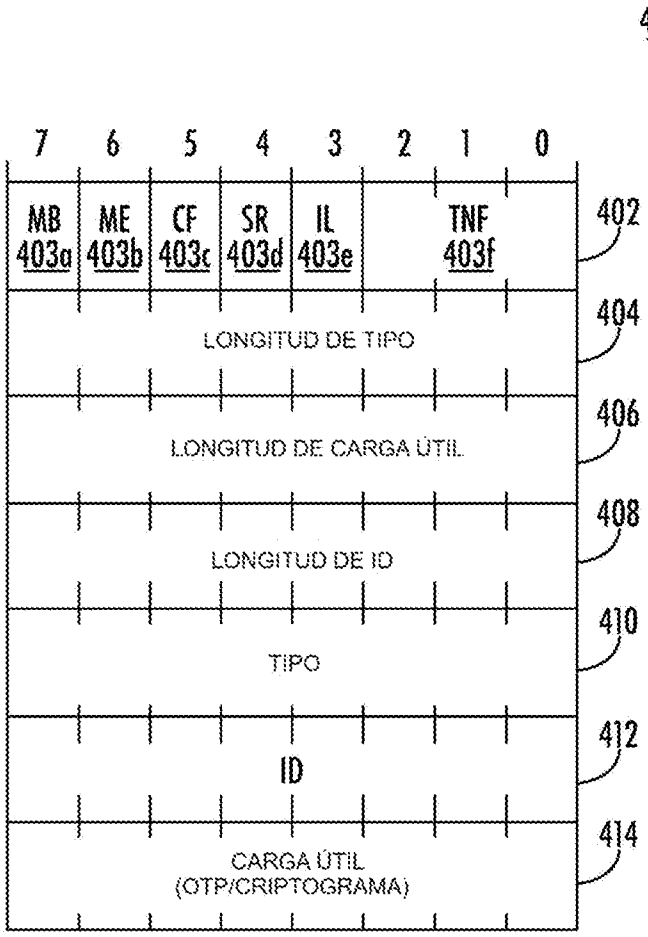
400
7 6 5 4 3 2 1 0
MB 403a
ME 403b
CF 403c
SR 403d
IL 403e
TNF 403f
402
LONGITUD DE TIPO
404
LONGITUD DE CARGA ÚTIL
406
LONGITUD DE ID
408
TIPO
410
ID
412
CARGA ÚTIL (OTP/CRIPTOGRAMA)
414

FIG. 4

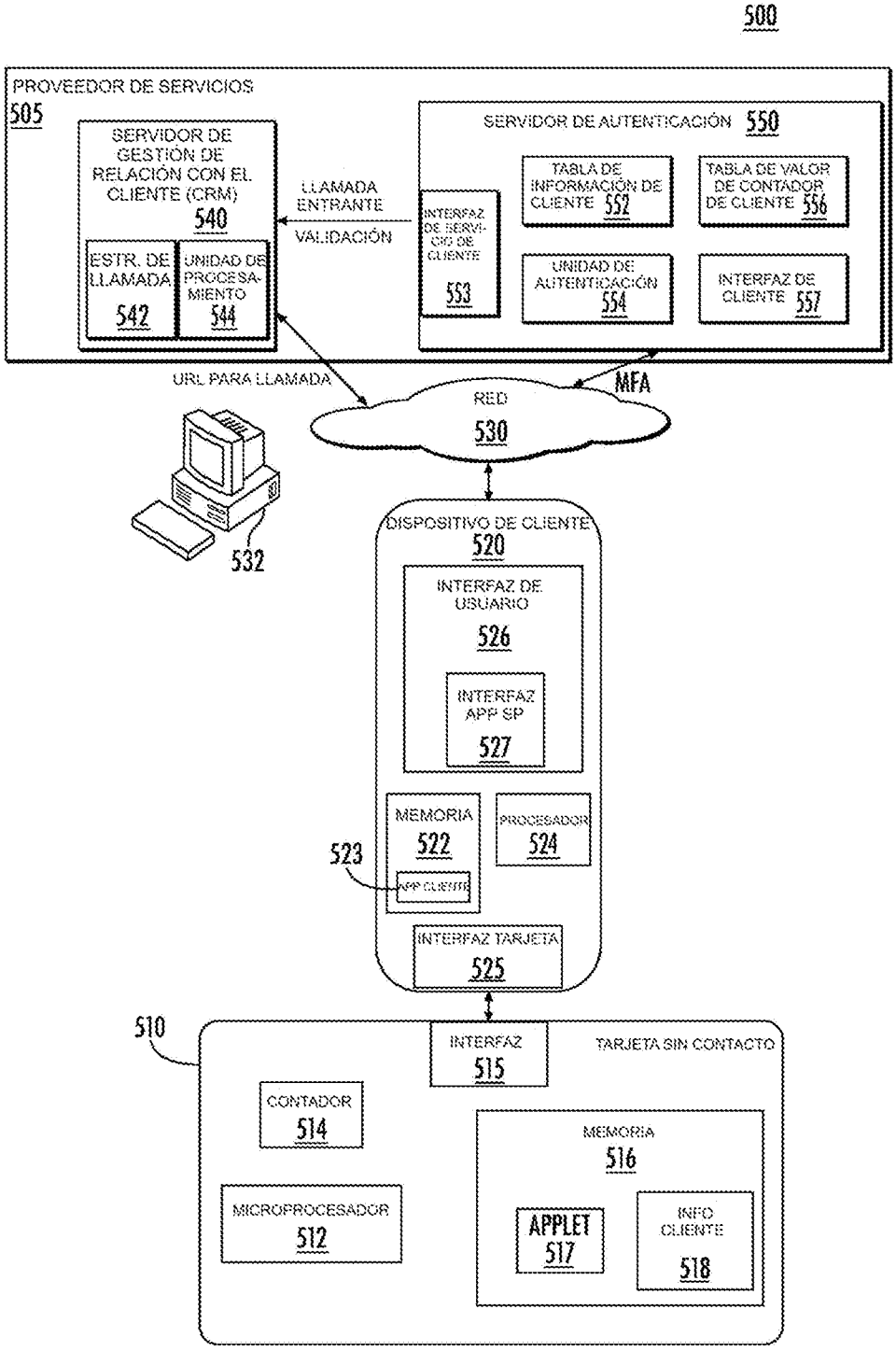
500
PROVEEDOR DE SERVICIOS
505
SERVIDOR DE GESTIÓN DE RELACIÓN CON EL CLIENTE (CRM)
540
ESTR. DE LLAMADA
542
UNIDAD DE PROCESAMIENTO
544
LLAMADA ENTRANTE
VALIDACIÓN
SERVIDOR DE AUTENTICACIÓN 550
INTERFAZ DE SERVICIO DE CLIENTE
553
TABLA DE INFORMACIÓN DE CLIENTE 552
TABLA DE VALOR DE CONTADOR DE CLIENTE 556
UNIDAD DE AUTENTICACIÓN
554
INTERFAZ DE CLIENTE 557
URL PARA LLAMADA
MFA
RED
530
532
DISPOSITIVO DE CLIENTE
520
INTERFAZ DE USUARIO
526
INTERFAZ APP SP
527
MEMORIA
522
PROCESADOR
524
523
APP CLIENTE
INTERFAZ TARJETA
525
510
INTERFAZ
515
TARJETA SIN CONTACTO
CONTADOR
514
MEMORIA
516
MICROPROCESADOR
512
APPLET
517
INFO CLIENTE
518

FIG. 5

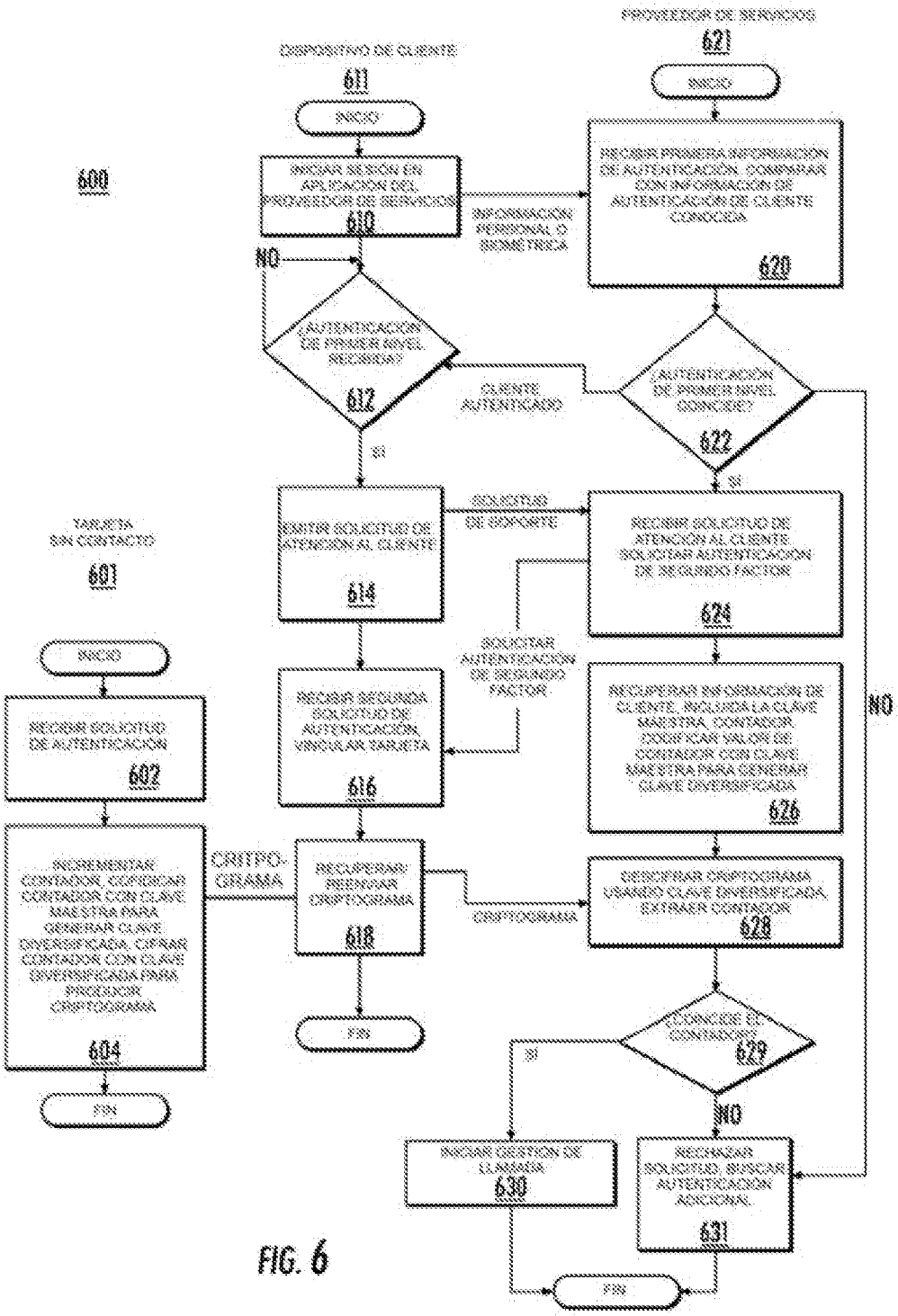
600
DISPOSITIVO DE CLIENTE
611
INICIO
INICIAR SESIÓN EN APLICACIÓN DEL PROVEEDOR DE SERVICIOS
610
INFORMACIÓN PERSONAL O BIOMÉTRICA
NO
¿AUTENTICACIÓN DE PRIMER NIVEL RECIBIDA?
612
SI
CLIENTE AUTENTICADO
PROVEEDOR DE SERVICIOS
621
INICIO
RECIBIR PRIMERA INFORMACIÓN DE AUTENTICACIÓN, COMPARAR CON INFORMACIÓN DE AUTENTICACIÓN DE CLIENTE CONOCIDA
620
¿AUTENTICACIÓN DE PRIMER NIVEL CONOCIDA?
622
SI
NO
EMITIR SOLICITUD DE ATENCIÓN AL CLIENTE
614
SOLICITUD DE SOPORTE
RECIBIR SOLICITUD DE ATENCIÓN AL CLIENTE, SOLICITAR AUTENTICACIÓN DE SEGUNDO FACTOR
624
SOLICITAR AUTENTICACIÓN DE SEGUNDO FACTOR
RECIBIR SEGUNDA SOLICITUD DE AUTENTICACIÓN, VINCULAR TARJETA
616
RECUPERAR INFORMACIÓN DE CLIENTE, INCLUIDA LA CLAVE MAESTRA, CONTADOR, CODIFICAR VALOR DE CONTADOR CON CLAVE MAESTRA PARA GENERAR CLAVE DIVERSIFICADA
626
TARJETA SIN CONTACTO
601
INICIO
RECIBIR SOLICITUD DE AUTENTICACIÓN
602
INCREMENTAR CONTADOR, CODIFICAR CONTADOR CON CLAVE MAESTRA PARA GENERAR CLAVE DIVERSIFICADA, CIFRAR CONTADOR CON CLAVE DIVERSIFICADA PARA PRODUCIR CRIPTOGRAMA
604
FIN
CRIPTO-GRAMA
RECUPERAR/ RENVIAR CRIPTOGRAMA
618
FIN
CRIPTOGRAMA
DESCIFRAR CRIPTOGRAMA USANDO CLAVE DIVERSIFICADA, EXTRAER CONTADOR
628
¿CONTADOR DE CONTADOR?
629
SI
NO
INICIAR GESTIÓN DE LLAMADA
630
RECHAZAR SOLICITUD, BUSCAR AUTENTICACIÓN ADICIONAL
631
FIN

FIG. 6

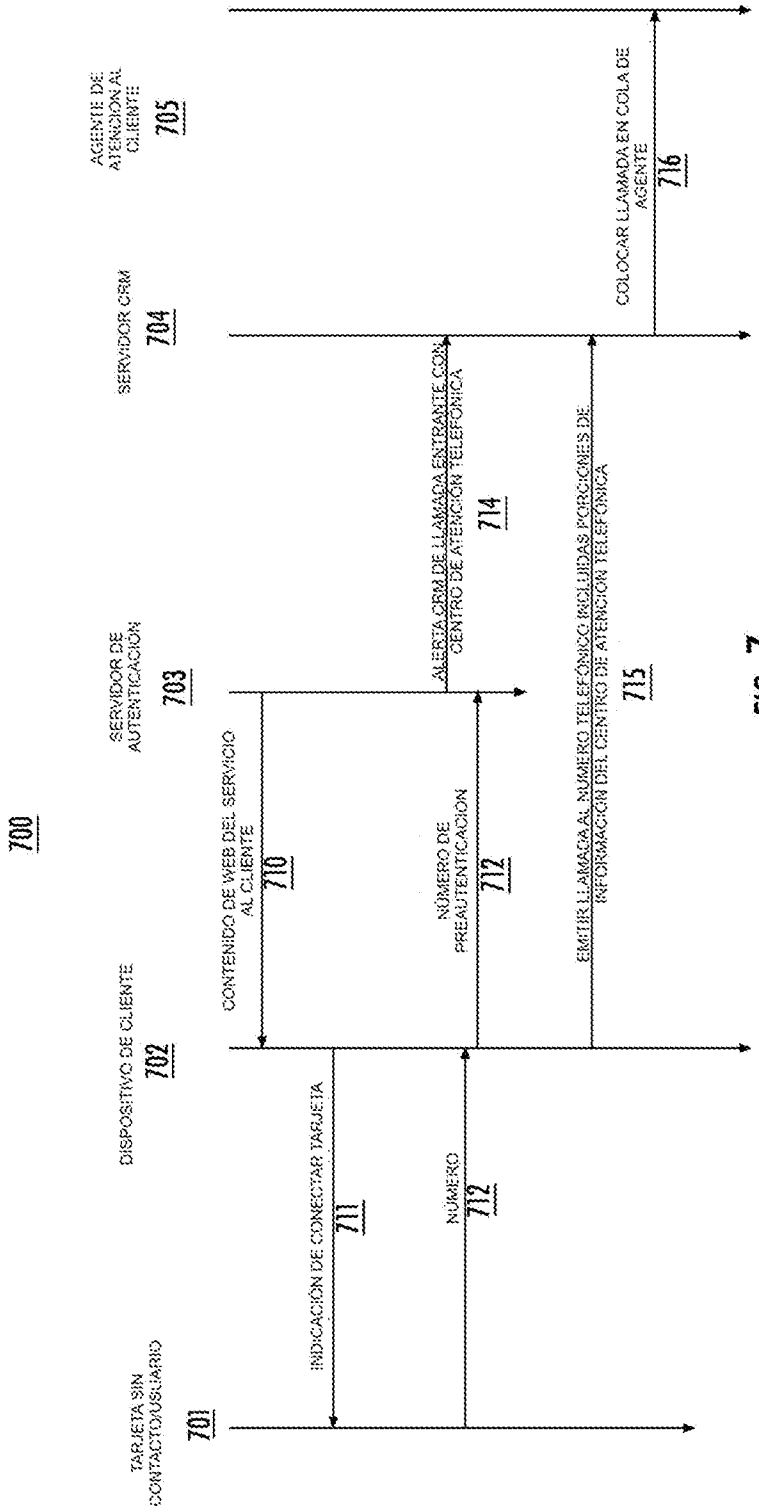
700
TARJETA SIN CONTACTO/USUARIO
701
DISPOSITIVO DE CLIENTE
702
SERVIDOR DE AUTENTICACIÓN
703
SERVIDOR CRM
704
AGENTE DE ATENCIÓN AL CLIENTE
705
INDICACIÓN DE CONECTAR TARJETA
711
NÚMERO
712
CONTENIDO DE WEB DEL SERVICIO AL CLIENTE
710
NÚMERO DE PREAUTENTICACIÓN
712
ALERTA CRM DE LLAMADA ENTRANTE CON CENTRO DE ATENCIÓN TELEFÓNICA
714
EMITIR LLAMADA AL NÚMERO TELEFÓNICO INCLUIDAS PORCIONES DE INFORMACIÓN DEL CENTRO DE ATENCIÓN TELEFÓNICA
715
COLOCAR LLAMADA EN COLA DE AGENTE
716

FIG. 7

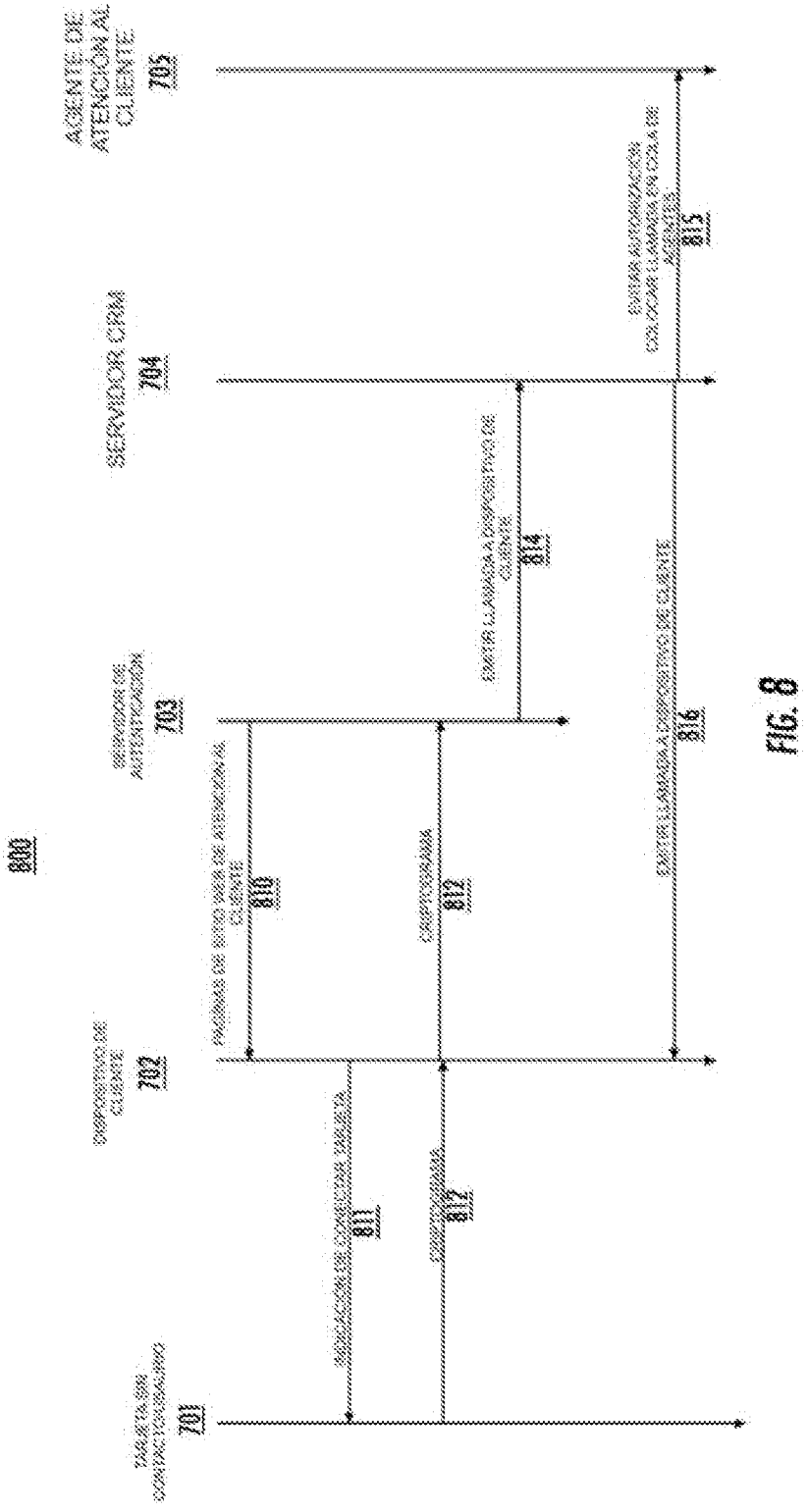
800
TARJETA SIN CONTACTO/SIN CONTACTO
701
DISPOSITIVO DE CLIENTE
702
SERVIDOR DE AUTENTICACIÓN
703
SERVIDOR CRM
704
AGENTE DE ATENCIÓN AL CLIENTE
705
INDICACIÓN DE SOLICITUD TARJETA
811
CRIPTOGRAMA
812
CRIPTOGRAMA
812
PANTALLA DE BIENVENIDA DE ATENCIÓN AL CLIENTE
810
ENVÍA LLAMADA A DISPOSITIVO DE CLIENTE
814
ENVÍA LLAMADA A DISPOSITIVO DE CLIENTE
816
ENVÍA NOTIFICACIÓN COLOCAR LLAMADA EN COLA DE AGENTES
815

FIG. 8

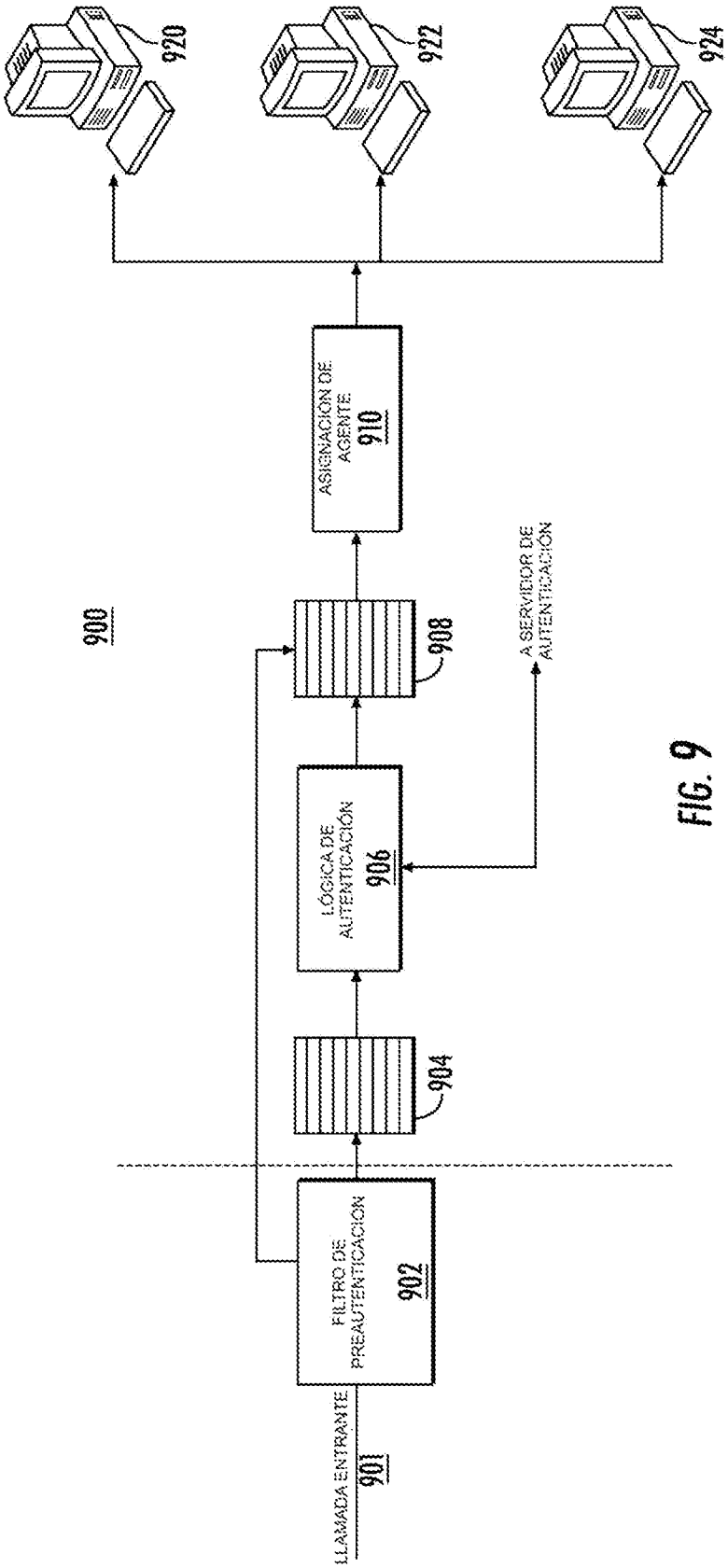
920
922
924
ASIGNACIÓN DE AGENTE
910
900
908
A SERVIDOR DE AUTENTICACIÓN
LÓGICA DE AUTENTICACIÓN
906
904
FILTRO DE PREAUTENTICACIÓN
902
LLAMADA ENTRANTE
901

FIG. 9