(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 583 156**

(51) Int. CI.:

H04L 29/06 (2006.01)
G06F 21/41 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **05.04.2008 E 08745189 (4)**

(97) Fecha y número de publicación de la concesión europea: **11.05.2016 EP 2156306**

(54) Título: **Procedimiento y sistema para llamadas pre-autenticadas en aplicaciones de voz**

(30) Prioridad:

26.04.2007 US 789846

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
19.09.2016

(73) Titular/es:

MICROSOFT CORPORATION (100.0%)
ONE MICROSOFT WAY
REDMOND, WA 98052-6399, US

(72) Inventor/es:

SARAF, TAL;
PALL, GURDEEP SINGH y
RAMAKRISHNA, ANAND

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

DESCRIPCIÓN

Procedimiento y sistema para llamadas pre-autenticadas en aplicaciones de voz

Antecedentes

Los avances tecnológicos en las comunicaciones digitales han revolucionado la telefonía proporcionando medios de comunicaciones de voz alternativos a los proporcionados por los sistemas de telefonía analógica tradicional. Por ejemplo, la telefonía IP (protocolo de internet) es una forma de telefonía que usa el conjunto de protocolos TCP/IP popularizados por las redes IP, tales como internet, para transmitir datos de voz digitalizados. El encaminamiento de conversaciones de voz a través de internet u otras redes IP se denomina habitualmente voz sobre IP (VoIP). La telefonía digital se presentó para mejorar los servicios de voz, pero posteriormente se descubrió que era muy útil en la creación de nuevos servicios de red, debido a la transferencia de datos más rápida a través de líneas telefónicas.

Los protocolos de sesión de medios, tales como el protocolo de inicio de sesión (SIP), pueden usarse para crear, modificar, y terminar sesiones IP con uno o más participantes. Las sesiones SIP pueden incluir llamadas telefónicas IP, distribución multimedia, y conferencias multimedia. El protocolo SIP resuelve una necesidad de un protocolo de aviso y establecimiento de llamada para comunicaciones basadas en IP que soporte las funciones y las características de procesamiento de llamada presentes en la red de telefonía pública conmutada usando servidores intermediarios y agentes de usuario.

Sin embargo, en tales sistemas digitales, la autenticación es importante para evitar que los usuarios no autorizados accedan a las redes y los servicios de red. La autenticación (o verificación de identidad) de los solicitantes de llamada telefónica y/o los dispositivos de solicitante de llamada es un problema general para los servicios de telefonía, automatizados o no. Puesto que la implementación de la ANI (identificación automática de número) o el número de teléfono desde el que se origina la llamada (habitualmente denominado “identificación de solicitante de llamada”) muchas veces no está disponible, o más importante, puede suplantarse, las aplicaciones y los servicios de voz tienen habitualmente que implementar procedimientos de autenticación del solicitante de llamada que son tan costosos de desarrollar como incómodos para el usuario. Tales procedimientos incluyen diálogos interactivos en los que el usuario necesita proporcionar un PIN, información confidencial y/o verificación del hablante automática (una tecnología costosa en sí misma).

El “inicio de comunicación único” es un concepto que gana popularidad en el que un módulo de autenticación proporciona acceso a una multiplicidad de servicios basados en un procedimiento de inicio de comunicación único o autenticación. Aunque esto también tiene el objetivo de reducir la necesidad de proporcionar credenciales a múltiples servicios, todavía se requiere que tenga lugar al menos un inicio de comunicación. Dada la naturaleza ubicua de los dispositivos móviles (por ejemplo, los teléfonos móviles) y los dispositivos informáticos, los vendedores podrían obtener una significativa ventaja comercial proporcionando un mecanismo de autenticación más eficiente y eficaz. El documento WO 2007/035846 A2 se refiere a una técnica de inicio de comunicación único que permite múltiples accesos a una o más aplicaciones u otros recursos usando un módulo de prueba de autenticación que opera junto con un componente de autenticación convencional. La aplicación, u otro recurso, emite una solicitud de información de autenticación al componente de autenticación convencional en respuesta a una solicitud de acceso del usuario. La aplicación, u otro recurso, recibe un valor de prueba de autenticación del componente de autenticación convencional en respuesta a la solicitud de información de autenticación, y autentica al usuario basándose en el valor de prueba de autenticación. El componente de autenticación convencional interactúa con el módulo de prueba de autenticación para obtener el valor de prueba de autenticación. El módulo de prueba de autenticación está configurado para generar múltiples valores de prueba de autenticación para la autenticación de las solicitudes de acceso respectivas del usuario.

El documento US 2006/0069914 A1 se refiere a un procedimiento para autenticar a un usuario en una red por medio de una contraseña temporal y/o de un solo uso. La contraseña temporal y/o de un solo uso se proporciona por un proveedor de servicios al que puede accederse por medio de un dispositivo de telecomunicaciones móviles. La contraseña temporal se proporciona bajo demanda, cuando el usuario recurre a una solicitud de acceso correspondiente que se transmite al proveedor de servicios por medio del dispositivo de telecomunicaciones móviles. El proveedor de servicios comprueba y confirma una solicitud de acceso recibida y genera la contraseña temporal haciendo uso de un procedimiento criptográfico especializado. La contraseña temporal generada se muestra finalmente al usuario por medio del dispositivo de telecomunicaciones móviles y, a continuación, el usuario puede introducir manualmente la contraseña temporal en el dispositivo informático con el fin de autenticar la red.

El documento US 2005/0144482 A1 se refiere a un sistema compatible con internet, para su uso en la autenticación de acceso de usuario a la información, que incluye un repositorio y un procesador de autenticación. El repositorio asocia un identificador de usuario inicial con una aplicación ejecutable específica y con una información de credenciales. La información de credenciales incluye un primer identificador de usuario y una primera contraseña correspondiente, que permite el acceso del usuario a la aplicación ejecutable específica. El procesador de autenticación recibe los datos que representan el identificador de usuario inicial. El procesador de autenticación detecta una solicitud iniciada de aplicación de navegador para la información de credenciales en respuesta a una orden de usuario a la aplicación de navegador para acceder a una aplicación ejecutable específica. El procesador de

autenticación valida si la información de credenciales obtenida del repositorio, usando el identificador de usuario recibido inicial, autoriza a un usuario a acceder a la aplicación ejecutable específica en respuesta a una solicitud iniciada de aplicación de navegador detectada. El procesador de autenticación proporciona una información de credenciales autorizada validada obtenida del repositorio para la aplicación de navegador para permitir a un usuario acceder a la aplicación ejecutable específica en respuesta a la validación correcta.

El documento US 2005/0096048 A1 se refiere a una red de comunicaciones para gestionar identificadores de usuario de los usuarios que acceden a aplicaciones de datos en al menos dos redes diferentes, a cada una de las cuales puede accederse a través de un proveedor de servicios, y proporcionar un inicio de comunicación continuo cuando se accede a una aplicación de datos desde una estación móvil.

Sumario

El objeto de la presente invención es proporcionar un sistema y un procedimiento para evitar el inicio de comunicación de un teléfono basado en IP en unas comunicaciones de voz basadas en IP.

Este objeto se resuelve por la materia objeto de las reivindicaciones independientes.

Las realizaciones preferidas se definen por las reivindicaciones dependientes.

A continuación, se presenta un sumario simplificado con el fin de proporcionar una comprensión básica de las realizaciones novedosas descritas en el presente documento. Este sumario no es una extensa visión general, y no está destinado a identificar elementos clave/críticos o a delinear el ámbito de los mismos. Su único fin es presentar algunos conceptos de una forma simplificada como un preludio a la descripción más detallada que se presenta a continuación.

La arquitectura desvelada incluye un módulo o aplicación de pre-autenticación que elimina la necesidad de diálogos de autenticación que requieren la interacción del usuario utilizando credenciales disponibles a partir de un punto final (por ejemplo, un servidor SIP apto) pre-autenticado o de confianza. Esto también puede incluir la seguridad conocida del protocolo de sesión de medios, que puede ser una conexión de protocolo de inicio de sesión (SIP). En el contexto de las comunicaciones de voz basadas en IP, en el que ahora puede hacerse una llamada de un cliente que sea pre-autenticable, ya no es necesario que se inscriba un teléfono basado en IP.

En general, el módulo de pre-autenticación de la arquitectura puede ser una aplicación que facilita la utilización de información de usuario y/o información de punto final en mensajes de protocolo de medios (por ejemplo, basados en SIP) para reemplazar información que de otro modo se recopilaría a través de un diálogo, con el fin de mejorar la eficiencia de la comunicación y mejorar la seguridad/privacidad de las comunicaciones.

Además, puede accederse a la información de perfil de usuario y la información de personalidad, por ejemplo, para proporcionar una implementación más robusta, en particular en el contexto de un operador automático y un diálogo asociado.

Para el cumplimiento de lo anterior y los fines relacionados, se describen en el presente documento ciertos aspectos ilustrativos en relación con la siguiente descripción y los dibujos adjuntos. Estos aspectos solo son indicativos, sin embargo, de algunas de las diversas maneras en las que pueden emplearse los principios desvelados en el presente documento y se pretende incluir todos estos aspectos y sus equivalentes. Otras ventajas y características novedosas serán evidentes a partir de la siguiente descripción detallada cuando se considera en relación con los dibujos.

Breve descripción de los dibujos

La figura 1 ilustra un sistema de autenticación implementado por ordenador de acuerdo con la nueva arquitectura.
La figura 2 ilustra una implementación más detallada de un sistema para el procesamiento de pre-autenticación.
La figura 3 ilustra un sistema para aplicar una selección a los servicios o funcionalidades de aplicaciones basándose en las credenciales pre-autenticadas.
La figura 4 ilustra un sistema en el que puede accederse a diferentes servicios de diferentes aplicaciones correspondientes basándose en la información de credenciales pre-autenticadas.
La figura 5 ilustra un sistema que emplea un componente de aprendizaje y de razonamiento (LR) de máquina que facilita la automatización de una o más características.
La figura 6 ilustra una o más fuentes de información de credenciales que pueden recibirse y procesarse por el componente de confianza para las credenciales de autenticación.
La figura 7 ilustra un procedimiento de procesamiento de pre-autenticación.
La figura 8 ilustra un procedimiento de procesamiento de información de perfil de usuario asociada con las credenciales autenticadas.
La figura 9 ilustra un procedimiento de procesamiento de llamadas que usa un operador automático y unas credenciales pre-autenticadas.
La figura 10 ilustra un procedimiento de procesamiento de información de interacción y comportamiento de

usuario basado en las credenciales pre-autenticadas.
La figura 11 ilustra un procedimiento de procesamiento de llamadas que usa un asistente virtual privado.
La figura 12 ilustra un procedimiento de procesamiento de información de llamadas de usuario basado en las credenciales pre-autenticadas.
La figura 13 ilustra un diagrama de bloques de un sistema informático operativo para ejecutar la creación y/o el procesamiento de credenciales de pre-autenticación de acuerdo con la arquitectura desvelada.
La figura 14 ilustra un diagrama de bloques esquemático de un entorno informático ejemplar que puede facilitar ejecutar la creación y/o el procesamiento de credenciales de pre-autenticación de acuerdo con la arquitectura desvelada.

Descripción detallada

La arquitectura desvelada elimina la necesidad requerida anteriormente de interactuar con sistemas de diálogo, por ejemplo, para proporcionar información para obtener acceso a una red y/o servicios de red. Convencionalmente, por ejemplo, las aplicaciones de llamada de conferencia requieren habitualmente la entrada de un código de participante y/o un código de coordinador con el fin de unirse y/o permitir la conferencia. Estas son etapas de autenticación de usuario incómodas y, a menudo, molestas. Contrariamente a los mecanismos convencionales, la arquitectura desvelada implementa una aplicación de llamada o comunicaciones que puede incluir un módulo de pre-autenticación que elimina las etapas de autenticación convencionales, al menos para los solicitantes de llamada basados en IP. El módulo puede suministrar la identidad del solicitante de llamada en las comunicaciones de protocolo de sesión de medios (por ejemplo, el protocolo de inicio de sesión (SIP)) con la aplicación a través de una conexión segura (por ejemplo, usando TLS (capa de seguridad de transporte)).

Ahora se hace referencia a los dibujos, en los que se usan los mismos números de referencia para referirse a los mismos elementos en todas partes. En la siguiente descripción, con fines de explicación, se exponen numerosos detalles específicos con el fin de proporcionar una comprensión completa de la misma. Puede ser evidente, sin embargo, que las nuevas realizaciones pueden ponerse en práctica sin estos detalles específicos. En otros casos, se muestran estructuras y dispositivos bien conocidos en forma de diagrama de bloques con el fin de facilitar una descripción de los mismos.

Haciendo referencia inicialmente a los dibujos, la figura 1 ilustra un sistema 100 de autenticación implementado por ordenador de acuerdo con la nueva arquitectura. El sistema 100 puede incluir un componente 102 de confianza para recibir y procesar las credenciales de una entidad 104 de confianza que ya se han autenticado (por lo tanto, credenciales pre-autenticadas). Por ejemplo, la entidad 104 de confianza puede ser una fuente de información de acceso tal como el nombre de usuario, la contraseña, el PIN, los servicios de red, y así sucesivamente. En otras palabras, la entidad 104 de confianza es un componente que ya ha autenticado un usuario y/o un dispositivo de usuario y proporciona la base para la comunicación de esa confianza en la forma de credenciales pre-autenticadas.

Sobre la base de la entidad 104, que es una entidad de confianza, el componente 102 de confianza procesa las credenciales pre-autenticadas y envía al menos la información de identidad extraída de las mismas o asociada con las mismas a un componente 106 de aplicación. El componente 106 de aplicación puede ser una sola aplicación o múltiples aplicaciones de uno o más sistemas, pudiendo asociarse cada aplicación del mismo con un servicio o funcionalidad que se expone en función de la información de identidad correcta. Una vez expuesto, el servicio facilita las comunicaciones entre una fuente 110 y un destino 112.

En una implementación, la entidad 104 de confianza puede ser un servicio de red (por ejemplo, un servicio de acceso de red) que ya ha procesado el acceso por la fuente 110 (por ejemplo, un ordenador portátil) a, por ejemplo, una red. De este modo, utilizando esta relación de confianza ya existente, el componente 102 de confianza considerará la fuente 110 una entidad autenticada. En consecuencia, en una implementación general, el componente 102 de confianza puede avisar al componente 106 de aplicación para exponer la funcionalidad deseada, permitiendo de este modo la conectividad y/o un cierto nivel de comunicaciones entre la fuente 110 y el destino 112.

En una implementación alternativa, el componente 102 de confianza envía información más detallada que una señal general para exponer la funcionalidad de aplicación, de tal manera que el componente 106 de aplicación puede usar la información más detallada para controlar o gestionar internamente los procedimientos o servicios de aplicación para la fuente 110. Por ejemplo, cuando el componente 106 de aplicación es un conjunto de aplicaciones diseñadas para trabajar conjuntamente, la información más detallada puede incluir datos que exponen la funcionalidad para solo una de las aplicaciones pero no para otra, o expone una interfaz limitada de una sola aplicación, en lugar de toda la funcionalidad de una sola aplicación. En otras palabras, en función de la cantidad y el tipo de información comunicada en las credenciales pre-autenticadas, o que se almacena y puede recuperarse usando las credenciales pre-autenticadas, puede obtenerse una amplia diversidad de gestión y de control.

En otra implementación, el sistema 100 se emplea en el contexto de las comunicaciones de voz móviles o basadas en IP. En este caso, la entidad 104 de confianza puede ser un servidor de comunicaciones dispuesto en una red, las credenciales pre-autenticadas incluyen al menos uno de un dato de identidad de dispositivo basado en IP o un dato de identidad de usuario, y el servicio 108 de aplicación facilita las comunicaciones de voz entre la fuente 110, que

puede ser un dispositivo telefónico o móvil apto basado en IP (por ejemplo, un teléfono inteligente) y el destino 112, que puede ser otro teléfono. En otras palabras, el usuario ha accedido al servidor de comunicaciones (o entidad 104 de confianza) directamente (por ejemplo, a través de internet) o indirectamente a través del componente 106 de aplicación (por ejemplo, una interfaz de aplicación de comunicaciones de cliente para el servidor de comunicaciones) para iniciar la conversación telefónica basada en IP con el destino 112.

Como parte de este procedimiento, el usuario tendría que haberse autenticado con éxito en el servidor de comunicaciones (o entidad 104 de confianza). Por lo tanto, una vez autenticado con éxito en el servidor de comunicaciones, el usuario no estaría obligado a someterse a otro procedimiento de acceso, por ejemplo, pero se le permitiría obtener la funcionalidad de la aplicación cliente y completar la llamada a través del destino 112 sin obstáculos por tales procedimientos convencionales de múltiples accesos.

Las credenciales pre-autenticadas pueden comunicarse usando un protocolo de sesión de medios tal como un SIP. Por lo tanto, las credenciales pre-autenticadas pueden incluir información más allá de, por ejemplo, un nombre de usuario, contraseña, correo electrónico, o PIN, pero también la información de calidad de servicio (QoS) relacionada con el paquete de suscripción de abonado y los niveles de servicio. Por ejemplo, la información QoS, que puede recuperarse en función de las credenciales pre-autenticadas, puede incluir la duración de la llamada (por ejemplo, solo veinte minutos), cómo facturar la llamada basada en IP (por ejemplo, tarjeta de crédito, tarjeta de llamada), dónde enviar la información de factura de la llamada (por ejemplo, a través de correo electrónico al usuario), y así sucesivamente. Otra información, que puede enviarse en las credenciales pre-autenticadas o a la que puede accederse usando las credenciales pre-autenticadas, puede incluir información de personalidad para la implementación de la llamada dada. Esto se describe a continuación.

En otras palabras, una plataforma de comunicaciones (la entidad 104 de confianza) que está pasando el audio de la llamada telefónica (por ejemplo, basada en SIP) a una aplicación de recepción también puede proporcionar o validar la información de identidad de autenticación del usuario de origen. Esto permite la aplicación de recepción para tratar la conexión como autenticada. Un escenario es que el usuario inicia una llamada de voz/datos desde un dispositivo (por ejemplo, un teléfono SIP, un teléfono inteligente que ejecuta una aplicación de comunicaciones, un PC que ejecuta una aplicación de comunicaciones, etc.). Puesto que el usuario está autenticado debido a la autenticación previa de la plataforma de comunicaciones o como un usuario SIP, la aplicación local o de dispositivo puede omitir el procedimiento de acceso basándose en la identidad existente recibida desde la plataforma de comunicaciones. A continuación, la aplicación local o de dispositivo puede proporcionar una experiencia diferente sin requerir las etapas convencionales adicionales de autorización, ya que las aplicaciones de voz actuales deben hacerse hoy.

Por lo tanto, un “inicio de comunicación único” es una de las ventajas obtenidas por la implementación de un sistema 100 de autenticación que permite el acceso a una multiplicidad de servicios basado en un procedimiento de “inicio de comunicación único” o autenticación. Aunque esto también tiene el objetivo de reducir la necesidad de proporcionar credenciales a múltiples servicios, se requiere que tenga lugar un inicio de comunicación. En un ejemplo, ya no se requiere un inicio de comunicación de teléfono cuando se realiza una llamada desde un cliente que se ha pre-autenticado.

La figura 2 ilustra una implementación más detallada de un sistema 200 para el procesamiento de pre-autenticación. En este caso, la entidad 106 de confianza de la figura 1 se ilustra como un componente 202 de nivel intermedio (o nivel medio) (por ejemplo, un servidor de comunicaciones accesible en la web basado en IP), en el que puede tener lugar una autenticación inicial. El componente 202 de nivel medio puede incluir un componente 204 de autenticación a través del que un usuario 206 de un sistema 208 cliente (por ejemplo, un ordenador) ha interactuado previamente (por ejemplo, para un procedimiento de acceso) para la creación de las credenciales de autenticación. Por ejemplo, el usuario 206 cliente puede acceder al componente 202 de nivel medio a través de un componente 210 de aplicación cliente para configurar una llamada basada en IP (por ejemplo, voz sobre IP (VoIP)). El componente 210 de aplicación cliente puede incluir una aplicación con una interfaz adecuada para interconectarse a una aplicación 212 de nivel medio. La aplicación 212 de nivel medio puede configurarse, por ejemplo, para solicitar al usuario información de acceso. Basándose en la información de acceso, el componente 204 de autenticación de nivel medio crea credenciales de autenticación.

Después de configurar el procedimiento deseado (por ejemplo, una llamada basada en IP) en el componente 202 de nivel medio, el usuario 206 en el sistema 208 cliente puede iniciar las comunicaciones IP a través del sistema 208 cliente a través de una red 214 IP con el dispositivo 112 de destino (por ejemplo, un teléfono móvil, un teléfono VoIP). En respuesta a ello, un componente 216 de confianza cliente puede recibir las credenciales pre-autenticadas del componente 202 de nivel medio, permitiendo automáticamente de este modo al usuario 206 realizar comunicaciones de voz IP desde el sistema 208 cliente al destino 112. El componente 216 de confianza cliente puede desencadenarse para buscar las credenciales autenticadas por el usuario interactuando con el componente 210 de aplicación cliente. Esto proporciona un procedimiento de autenticación transparente para el usuario 206.

En otro ejemplo más, el usuario 206 desea usar un teléfono 218 IP por cable/inalámbrico para comunicarse con el destino 112. En este escenario, una vez que el usuario 206 ha configurado las comunicaciones a través del sistema 208 cliente con el componente 202 de nivel medio, las credenciales pre-autenticadas se pasan al componente 216

de confianza cliente que, a continuación, puede convertirse en la entidad de confianza en relación con el teléfono 218 IP. En otras palabras, las credenciales pre-autenticadas pueden incluir información relacionada con el teléfono 218 IP de tal manera que el uso del teléfono 218 desencadena automáticamente una comparación de la información telefónica única con la información telefónica proporcionada en las credenciales pre-autenticadas. Basándose en una verificación exitosa, ahora puede usarse el teléfono 218 para comunicarse a través del sistema 208 cliente con el destino 112. El teléfono IP puede comunicarse a través de diferentes tecnologías inalámbricas convencionales, tales como Bluetooth, WiFi, WiMax, y tecnologías por cable tales como USB, IEEE 1394, IEEE 802.3, y así sucesivamente. El teléfono 218 también puede incluir un componente 220 de confianza de teléfono que recibe el mismo conjunto de credenciales pre-autenticadas recibidas por el sistema 208 cliente desde el componente 202 de nivel medio, o un conjunto modificado que también incluye información del sistema cliente que facilita el establecimiento de una relación de confianza entre el teléfono 218 y el sistema 208 cliente.

Los componentes (216 y 220) de confianza cliente puede estar en forma de componentes de software individuales y descargables que facilitan la obtención de las ventajas de las credenciales pre-autenticadas descritas en el presente documento. Los componentes de confianza clientes pueden diseñarse para la implementación adecuada de diferentes tipos de sistemas, tales como sistemas informáticos y teléfonos celulares, teléfonos IP, etc., esencialmente cualquier dispositivo que incluya al menos la capacidad de comunicaciones de voz.

La figura 3 ilustra un sistema 300 para aplicar una selección a los servicios o funcionalidades de aplicaciones basándose en las credenciales pre-autenticadas. En este caso, la aplicación 210 cliente incluye múltiples servicios o funcionalidades 302 (indicados como $SERVICIO_1$,..., $SERVICIO_N$, donde N es un número entero positivo), uno o más de los cuales puede utilizarse para facilitar la experiencia de usuario para las comunicaciones deseadas. Las credenciales pre-autenticadas obtenidas a partir de la entidad 104 de confianza por el componente 216 de confianza pueden incluir, además, datos o información de perfil que definen el acceso a los servicios o funcionalidades 302. La información de permisos puede incluirse y procesarse por un componente 304 de permisos del componente 210 cliente que extrae la información de permisos para determinar finalmente cuál de los servicios 302 puede exponerse y/o el nivel (o grado) de un servicio determinado a exponer. Un componente 306 de selección facilita la selección de los uno o más servicios 302 que finalmente se emplean para las comunicaciones entre la fuente 110 y el destino.

El sistema 300 ilustra un almacén 308 de datos de los datos 310 de perfil de usuario a los que puede accederse basándose en una o más piezas de datos en las credenciales pre-autenticadas que se proporcionan después de la autenticación, o en preparación del montaje de las credenciales pre-autenticadas. El almacén 308 de datos puede residir como un nodo de red independiente o en asociación con la entidad 104 de confianza. Los datos 310 de perfil pueden incluir información QoS, información contable, información de personalidad, y así sucesivamente, en cualquier cantidad que pueda transmitirse en las credenciales pre-autenticadas o junto con las mismas.

En un ejemplo, en el caso de un sistema de operador automático (o respuesta de voz interactiva (IVR)), la aplicación puede incluir la oferta de características de autorización de gran alcance aprovechando la identidad del usuario. Un usuario puede preconfigurar una piel de personalidad, que incluye atributos asociados a ser locuaz, aburrido, animado, hablador, etc., así como otros. A continuación, esta información puede activarse automáticamente como parte del diálogo de operador después de que el sistema de usuario recibe las credenciales pre-autenticadas. Otros datos pueden incluir un servicio de confianza de larga distancia basado en la autenticación de un plan de marcado mejorado. Además, un comportamiento diferente puede basarse en planes de marcado (esencialmente proporcionar al solicitante de llamada una experiencia de solicitante de llamada interna que es diferente de cuando el solicitante de llamada es un interlocutor externo al que no se permite marcar llamadas de larga distancia).

Otros ejemplos incluyen ejecutar automáticamente los datos usados más recientemente (MRU), de tal manera que el solicitante de llamada siempre se presenta con el John Smith correcto en lugar de tener que navegar por listas de múltiples instancias del mismo nombre. Otras capacidades incluyen, por ejemplo, aprovechar las normas ejecutadas en el sistema de nivel medio, emplear la acumulación probabilística de edificios/localizaciones, aprender y razonar sobre el comportamiento del solicitante de llamada y/o el destinatario de llamada, las interacciones de llamadas, la información de localización de llamadas, acceder y buscar información de contactos o listas de amigos desde otras aplicaciones, y así sucesivamente.

La figura 4 ilustra un sistema 400, desde el que puede accederse a diferentes servicios de diferentes aplicaciones correspondientes basándose en la información de credenciales pre-autenticadas. El componente 102 de confianza (similar al componente 216 de confianza de la figura 2) recibe y procesa las credenciales pre-autenticadas, y reenvía partes de las mismas y/o información de perfil asociada a uno o ambos del componente 304 de permisos y el componente 306 de selección para la selección y la exposición, en el componente 210 de aplicación cliente, de las funcionalidades o servicios de las múltiples aplicaciones 402 cliente (indicadas como $APLICACIONES_1$, ..., $APLICACIONES_{1S}$) que tienen los servicios correspondientes (indicados como $SERVICIOS(S)_1$, ..., $SERVICIOS(S)_S$).

Los permisos pueden incluir la exposición de un servicio de una de las aplicaciones 402 y otro servicio de otra de las aplicaciones 402, que se facilitan por el componente 306 de selección. Además, como se ha descrito anteriormente, puede seleccionarse un servicio, pero el nivel del servicio se reduce o se aumenta en función de las credenciales y/o los datos de perfil asociados. En otras palabras, el permiso para exponer un servicio no es un permiso para utilizar la funcionalidad completa del servicio; sin embargo, puede facilitar la exposición completa, como se ha configurado.

Cuando la fuente 110 se activa por el usuario cliente, esta puede desencadenar automáticamente la búsqueda de las credenciales pre-autenticadas accediendo a fuentes conocidas de tal información, por ejemplo, la entidad de confianza, u otras fuentes indicadas de manera similar. En una implementación alternativa, cierta interacción del usuario con el componente 210 cliente facilita la búsqueda y la recuperación de las credenciales. Esta interacción puede incluir la búsqueda de ciertos servicios, marcar un cierto número o dirección, y otros tipos de información que pueden usarse para deducir la intención del usuario.

La figura 5 ilustra un sistema 500 que emplea un componente 502 de aprendizaje y de razonamiento (LR) de máquina lo que facilita la automatización de una o más características. La arquitectura objeto (por ejemplo, en relación con la selección) puede emplear diversos esquemas basados en LR para realizar diversos aspectos de la misma. Por ejemplo, un procedimiento para determinar qué información incluir en las credenciales pre-autenticadas o en asociación con las mismas puede facilitarse a través de un sistema y procedimiento clasificador automático.

Un clasificador es una función que mapea un vector de atributo de entrada, x = (x1, x2, x3, x4, *xn*), en una etiqueta de clase *clase* (x). El clasificador también puede emitir una confidencia de que la entrada pertenece a una clase, es decir, f(x) = *confidencia* (*clase*(x)). Dicha clasificación puede emplear un análisis probabilístico y/u otro análisis estadístico (por ejemplo, una factorización en el análisis de las utilidades y los costes para maximizar el valor esperado en una o más personas) para pronosticar o deducir una acción que un usuario desea realizar automáticamente.

Tal como se usa en el presente documento, los términos “inferir” e “inferencia” se refieren, en general, al procedimiento de razonamiento acerca de, o la inferencia de estados sobre, el sistema, el entorno y/o usuario a partir de un conjunto de observaciones que se captan a través de eventos y/o datos. Una inferencia puede emplearse para identificar un contexto o una acción específicos, o puede generar, por ejemplo, una distribución de probabilidades sobre los estados. La inferencia puede ser probabilística, es decir, el cálculo de una distribución de probabilidades sobre estados de interés basándose en una consideración de datos y eventos. La inferencia también puede referirse a las técnicas empleadas para la composición de eventos de alto nivel a partir de un conjunto de eventos y/o datos. Tal inferencia da como resultado la construcción de nuevos eventos o acciones a partir de un conjunto de eventos observados y/o datos de eventos almacenados, si los eventos se correlacionan o no en estrecha proximidad temporal, y si los eventos y los datos provienen de una o varias fuentes de eventos y de datos.

Una máquina de vectores de soporte (SVM) es un ejemplo de un clasificador que puede emplearse. La SVM opera mediante la búsqueda de una hipersuperficie en el espacio de posibles entradas que divide los eventos de entrada de desencadenamiento a partir de los eventos no desencadenados de una manera óptima. Intuitivamente, esto hace la clasificación correcta para comprobar los datos que están próximos, pero no son idénticos, a los datos de prueba. Otros enfoques de clasificación modelo dirigida y no dirigida incluyen, por ejemplo, diversas formas de regresión estadística, el clasificador ingenuo de Bayes, redes bayesianas, árboles de decisión, redes neuronales, modelos de lógica difusa, y pueden emplearse otros modelos de clasificación estadística que representan diferentes patrones de independencia. La clasificación, tal como se usa en el presente documento, también incluye los procedimientos utilizados para asignar rango y/o prioridad.

Como se apreciará fácilmente a partir de la especificación objeto, la arquitectura objeto puede emplear clasificadores que están explícitamente probados (por ejemplo, a través de una comprobación genérica de datos), así como implícitamente probados (por ejemplo, a través de la observación del comportamiento del usuario, la recepción de información extrínseca). Por ejemplo, las SVM se configuran a través de una fase de aprendizaje o de entrenamiento dentro de un constructor de clasificadores y un módulo de selección de características. Por lo tanto, el o los clasificadores pueden emplearse para aprender y realizar automáticamente una serie de funciones de acuerdo con unos criterios predeterminados.

Por ejemplo, con el tiempo, una configuración de autorización necesaria o de rechazo puede cambiarse y/o desencadenarse en función del comportamiento de interacción de usuario aprendido. En otras palabras, en función del número de veces que los usuarios interactúan con el sistema, el nivel de experiencia puede aumentarse de acuerdo con una mejora aprendida o computada en la interacción de usuario. A lo largo de estas líneas, a medida que el usuario progresa en experiencia, se presentarán un menor número de sugerencias o indicaciones de ayuda, proporcionando de este modo una experiencia eficiente y eficaz de manera progresiva con el tiempo. Un usuario que progresa a un nivel de experto no será molestado ni obstaculizado con las mismas indicaciones o información de nivel principiante que ya se han superado. Como alternativa, las sugerencias o indicaciones pueden aumentar en complejidad o ser más complicadas a medida que el usuario progresa para presentar información más detallada acerca del comportamiento sobre el que el usuario parece interesarse con más frecuencia.

En otro ejemplo de aprendizaje y de razonamiento, si el usuario ha solicitado o expresado de manera rutinaria, recientemente, o durante las dos últimas semanas al operador automático un usuario específico, puede presentarse una lista de usuarios que, por ejemplo, esté más centrada en, y que pueda ser más específica para, un grupo de productos que se presentará. Esta información puede extraerse automáticamente, por ejemplo, de los contactos de usuario o de otras fuentes de información del usuario. Esto también puede aprenderse en función de la interacción del usuario con el sistema y/o las aplicaciones.

La acumulación de la información presentada al usuario cuando el usuario debe presentarse con una lista de opciones potenciales puede basarse en la localización geográfica. Por ejemplo, la acumulación probabilística puede facilitarse razonando sobre un Joe Smith localizado a 8,05 kilómetros de distancia, en un edificio corporativo frente a un Joe Smith localizado en un edificio adyacente, y que con toda probabilidad, estaría en el mismo grupo de trabajo, en contacto físico más a menudo, y así sucesivamente.

De nuevo, estas son características que pueden comunicarse como parte de las credenciales o en asociación con las mismas cuando se reciben por el componente 216 de confianza (o el componente 102 de confianza de la figura 1).

La figura 6 ilustra un sistema 600 de una o más fuentes 602 de información de credenciales que pueden recibirse y procesarse por el componente 102 de confianza para credenciales de pre-autenticación. Las fuentes 602 incluyen el sistema 202 de nivel medio de la figura 2 para obtener y generar las credenciales de pre-autenticación para su uso por el componente 106 de aplicación. Además de, o con independencia de, las capacidades de autenticación del sistema de nivel medio, puede emplearse una verificación 604 de hablante como un medio de crear y de proporcionar las credenciales de pre-autenticación para el componente 102 de confianza. De nuevo, además de, o con independencia de, las capacidades de autenticación del sistema de nivel medio y la verificación 604 de hablante, puede emplearse la verificación 606 basada en PIN como un medio para crear y proporcionar las credenciales de pre-autenticación para el componente 102 de confianza. Pueden emplearse otras fuentes que incluyen la biométrica, y así sucesivamente.

El componente 102 de confianza se muestra como un componente que puede tomar una entrada de cualquiera o todas estas fuentes 602. Sin embargo, en la práctica, cada una de las fuentes 602 puede tener un componente de confianza especializado. La salida del componente 102 de confianza es la validación de la identidad para la aplicación 106 que, a continuación, puede tratar las comunicaciones (o la sesión) como autenticadas, y aplicar la autorización, según sea necesario, a un solicitante de llamada en términos de acceso a la información y capacidades transaccionales.

La figura 7 ilustra un procedimiento de procesamiento de autenticación. Mientras que, por motivos de simplicidad de la explicación, la una o más metodologías mostradas en el presente documento, por ejemplo, en forma de una gráfica de flujo o un diagrama de flujo, se muestran y se describen como una serie de acciones, debe entenderse y apreciarse que las metodologías no están limitadas por el orden de las acciones, ya que algunas acciones pueden, de acuerdo con ello, producirse en un orden diferente y/o simultáneamente con otras acciones que las mostradas y descritas en el presente documento. Por ejemplo, los expertos en la materia entenderán y apreciarán que una metodología podría representarse alternativamente como una serie de estados o de eventos interrelacionados, tal como en un diagrama de estados. Además, no todas las acciones ilustradas en una metodología pueden ser necesarias para una implementación novedosa.

En 700, un primer cliente de un usuario se autentica para los servicios de comunicaciones en una localización remota. En 702, se crean credenciales de autenticación en la localización remota para el primer cliente. En 704, se recibe una solicitud de servicios de comunicaciones de un segundo cliente del usuario. En 706, las credenciales se transmiten al segundo cliente en función de la autenticación del primer cliente. En 708, se habilitan comunicaciones para el segundo cliente en función de las credenciales pre-autenticadas.

La figura 8 ilustra un procedimiento de procesamiento de la información de perfil de usuario asociada con las credenciales autenticadas. En 800, se generan credenciales autenticadas en función de la autenticación de un primer usuario. En 802, una primera información de perfil de usuario se asocia con las credenciales. En 804, las credenciales y la información de perfil se envían a un segundo cliente del primer usuario. En 806, las credenciales pre-autenticadas y la información de perfil se procesan en el segundo cliente del primer usuario para exponer la funcionalidad del primer cliente para el beneficio del segundo cliente.

La figura 9 ilustra un procedimiento de procesamiento de llamadas que usa un operador automático y las credenciales pre-autenticadas. En 900, se generan credenciales autenticadas en función de la autenticación del primer usuario. En 902, el primer usuario accede al operador. En 904, las credenciales pre-autenticadas se envían al operador. En 906, el operador accede a la información de perfil de usuario asociada con las credenciales pre-autenticadas. El operador procesa y presenta un diálogo al primer usuario basándose en la información de perfil de usuario.

La figura 10 ilustra un procedimiento de procesamiento de información de interacción y de comportamiento de usuario basándose en las credenciales pre-autenticadas. En 1000, se generan credenciales autenticadas en función de la autenticación de un primer usuario. En 1002, el primer usuario accede al operador. En 1004, las credenciales pre-autenticadas se envían al operador. En 1006, el operador accede a la información de interacción y de comportamiento de usuario basándose en las credenciales. En 1008, el operador presenta un diálogo basado en los datos MRU y/o la acumulación probabilística debida a la información de geolocalización extraída de la información de interacción y de comportamiento.

La figura 11 ilustra un procedimiento de procesamiento de llamadas que usa un asistente virtual privado. En 1100, se generan credenciales autenticadas en una entidad de confianza basándose en la autenticación del primer cliente de un usuario. En 1102, las comunicaciones de llamada se inician a través de un segundo cliente del usuario a un destinatario de llamada. La llamada puede ser una llamada VoIP que usa SIP. En 1104, las credenciales autenticadas se envían, a continuación, desde la entidad al segundo cliente basándose en la relación de confianza entre el primer cliente y la entidad. En 1106, se autoriza la llamada del segundo cliente. En 1108, se inicia un asistente virtual privado basado en la información de perfil en las credenciales. En 1110, la información de destinatario de llamada más probable se presenta en función de los datos de la lista de contactos y/o de amigos del usuario. En 1112, la llamada se conecta en función de la información de destinatario de llamada seleccionada por el usuario.

La figura 12 ilustra un procedimiento de procesamiento de la información de llamada de usuario en función de las credenciales pre-autenticadas. En 1200, se generan credenciales autenticadas en una entidad de confianza en función de la autenticación del primer cliente de un usuario. En 1202, las comunicaciones de llamadas se inician a través de un segundo cliente del usuario con un destinatario de llamada. En 1204, las credenciales autenticadas se envían, a continuación, desde la entidad al segundo cliente basándose en la relación de confianza entre el primer cliente y la entidad. En 1206, las credenciales se procesan para recuperar la información de llamada de usuario de un almacén de datos. En 1208, se gestiona la llamada por el usuario en función de la información de llamada de usuario.

Tal como se usa en la presente solicitud, los términos “componente” y “sistema” están previstos para referirse a un entidad relacionada con ordenadores, o bien un hardware, una combinación de hardware y software, un software, o un software en ejecución. Por ejemplo, un componente puede ser, pero no se limita a ser, un procedimiento que se ejecuta en un procesador, un procesador, una unidad de disco duro, múltiples unidades de almacenamiento (de un medio óptico y/o de almacenamiento magnético), un objeto, un ejecutable, un hilo de ejecución, un programa, y/o un ordenador. A modo de ilustración, tanto una aplicación que se ejecuta en un servidor como el servidor pueden ser un componente. Uno o más componentes pueden residir dentro de un procedimiento y/o un hilo de ejecución, y un componente puede localizarse en un ordenador y/o distribuirse entre dos o más ordenadores.

Haciendo ahora referencia a la figura 13, se ilustra un diagrama de bloques de un sistema 1300 informático que puede operarse para ejecutar la creación y/o el procesamiento de credenciales de pre-autenticación de acuerdo con la arquitectura desvelada. Con el fin de proporcionar un contexto adicional para diversos aspectos de la misma, la figura 13 y el análisis siguiente están previstos para proporcionar una breve descripción general de un sistema 1300 informático adecuado en el que pueden implementarse los diversos aspectos. Aunque la descripción anterior pertenece al contexto general de las instrucciones ejecutables por ordenador que pueden desarrollarse en uno o más ordenadores, los expertos en la materia reconocerán que también puede implementarse una realización novedosa en combinación con otros módulos de programa y/o como una combinación de hardware y software.

En general, los módulos de programa incluyen rutinas, programas, componentes, estructuras de datos, etc., que realizan tareas específicas o implementan tipos de datos abstractos específicos. Además, los expertos en la materia apreciarán que los procedimientos de la invención pueden ponerse en práctica con otras configuraciones de sistemas informáticos, incluyendo sistemas informáticos de un único procesador o de multiprocesador, miniordenadores, ordenadores centrales, así como ordenadores personales, dispositivos informáticos de mano, productos electrónicos basados en microprocesador o programables, y similares, cada uno de los cuales puede acoplarse operativamente a uno o más dispositivos asociados.

Los aspectos ilustrados también pueden ponerse en práctica en entornos informáticos distribuidos en los que se realizan ciertas tareas mediante dispositivos de procesamiento remotos que están vinculados a través de una red de comunicaciones. En un entorno informático distribuido, los módulos de programa pueden localizarse en dispositivos de almacenamiento de memoria tanto locales como remotos.

Habitualmente, un ordenador incluye una diversidad de medios legibles por ordenador. Los medios legibles por ordenador pueden ser cualquier medio disponible al que puede accederse por el ordenador e incluyen medios volátiles y no volátiles, medios extraíbles y no extraíbles. A modo de ejemplo, y no de limitación, los medios legibles por ordenador pueden comprender medios de almacenamiento en ordenador y medios de comunicación. Los medios de almacenamiento en ordenador incluyen medios volátiles y no volátiles, medios extraíbles y no extraíbles implementados en cualquier procedimiento o tecnología para el almacenamiento de información, tales como instrucciones legibles por ordenador, estructuras de datos, módulos de programa u otros datos. Los medios de almacenamiento en ordenador incluyen, pero sin limitarse a, una memoria RAM, ROM, EEPROM, flash u otra tecnología de memoria, un CD-ROM, un disco de vídeo digital (DVD) u otro almacenamiento de disco óptico, casetes magnéticos, cintas magnéticas, dispositivos de almacenamiento de disco magnético u otros dispositivos de almacenamiento magnético, o cualquier otro medio que pueda usarse para almacenar la información deseada y al que pueda accederse por ordenador.

Con referencia de nuevo a la figura 13, el sistema 1300 informático ejemplar para implementar diversos aspectos incluye un ordenador 1302, incluyendo el ordenador 1302 una unidad 1304 de procesamiento, una memoria 1306 de sistema y un bus 1308 de sistema. El bus 1308 de sistema proporciona una interfaz para los componentes de

sistema que incluye, pero sin limitarse a, la memoria 1306 de sistema para la unidad 1304 de procesamiento. La unidad 1304 de procesamiento puede ser cualquiera de los diversos procesadores comercialmente disponibles. Los microprocesadores duales y otras arquitecturas de multiprocesador también pueden emplearse como la unidad 1304 de procesamiento.

El bus 1308 de sistema puede ser cualquiera de varios tipos de estructura de bus que pueden interconectarse adicionalmente a un bus de memoria (con o sin un controlador de memoria), un bus periférico, y un bus local usando cualquiera de una diversidad de arquitecturas de bus comercialmente disponibles. La memoria 1306 de sistema incluye una memoria 1310 de solo lectura (ROM) y una memoria 1312 de acceso aleatorio (RAM). Un sistema de entrada/salida básico (BIOS) se almacena en una memoria 1310 no volátil, tal como ROM, EPROM, EEPROM, conteniendo el BIOS las rutinas básicas que ayudan a transferir información entre los elementos dentro del ordenador 1302, tal como durante el arranque. La RAM 1312 también puede incluir una RAM de alta velocidad, tal como una RAM estática para datos en caché.

El ordenador 1302 incluye, además, una unidad 1314 de disco duro interno (HDD) (por ejemplo, EIDE, SATA), una unidad 1314 de disco duro interno que también puede configurarse para uso externo en un chasis adecuado (no mostrado), una unidad 1316 de disco flexible magnético (FDD), (por ejemplo, para leer o escribir en un disquete 1318 extraíble) y una unidad 1320 de disco óptico, (por ejemplo, para leer un disco 1322 CD-ROM o, para leer o escribir en otros medios ópticos de alta capacidad como el DVD). La unidad 1314 de disco duro, la unidad 1316 de disco magnético y la unidad 1320 de disco óptico pueden conectarse al bus 1308 de sistema por una interfaz 1324 de unidad de disco duro, una interfaz 1326 de unidad de disco magnético y una interfaz 1328 de unidad óptica, respectivamente. La interfaz 1324 para implementaciones de unidades externas incluye al menos una o ambas tecnologías de interfaz 1394 de bus serie universal (USB) e IEEE.

Las unidades y sus medios legibles por ordenador asociados proporcionan un almacenamiento no volátil de datos, estructuras de datos, instrucciones ejecutables por ordenador, y así sucesivamente. Para el ordenador 1302, las unidades y los medios admiten el almacenamiento de cualquier dato en un formato digital adecuado. Aunque la descripción de los medios legibles por ordenador anterior se refiere a un HDD, un disquete magnético extraíble y un medio óptico extraíble, tal como un CD o un DVD, debería apreciarse por los expertos en la materia que otros tipos de medios que son legibles por un ordenador, tales como unidades zip, casetes magnéticos, tarjetas de memoria flash, cartuchos, y similares, también pueden usarse en el entorno operativo ejemplar y, además, que cualquiera de tales medios puede contener instrucciones ejecutables por ordenador para la realización de nuevos procedimientos de la arquitectura desvelada.

Una serie de módulos de programa pueden almacenarse en las unidades y la RAM 1312, incluyendo un sistema 1330 operativo, uno o más programas 1332 de aplicación, otros módulos 1334 de programa y los datos 1336 de programa. El uno o más programas 1332 de aplicación y los otros módulos 1334 de programa pueden incluir, por ejemplo, el componente 102 de confianza, la entidad 104 de confianza, y el componente 106 de aplicación de la figura 1, el componente 212 de aplicación de nivel medio, el componente 204 de autenticación, los componentes (216 y 220) de confianza cliente, y el componente 210 de aplicación cliente de la figura 2, el componente 304 de permisos, el componente 306 de selección, y los servicios 302 de la figura 3 y el componente 503 de aprendizaje y de razonamiento de la figura 5.

Todas o algunas de las partes del sistema operativo, las aplicaciones, los módulos, y/o los datos también pueden almacenarse en caché en la RAM 1312. Debe apreciarse que la arquitectura desvelada puede implementarse con diversos sistemas operativos comercialmente disponibles o combinaciones de sistemas operativos.

Un usuario puede introducir órdenes e información en el ordenador 1302 a través de uno o más dispositivos de entrada por cable/inalámbricos, por ejemplo, un teclado 1338 y un dispositivo de puntero, como un ratón 1340. Otros dispositivos de entrada (no mostrados) pueden incluir un micrófono, un control remoto IR, una palanca de mando, un control de mando, un lápiz óptico, una pantalla táctil, o similares. Estos y otros dispositivos de entrada se conectan a menudo a la unidad 1304 de procesamiento a través de una interfaz 1342 de dispositivo de entrada que está acoplada al bus 1308 de sistema, pero pueden conectarse por otras interfaces, tales como un puerto paralelo, un puerto 1394 serie IEEE, un puerto de juegos, un puerto USB, una interfaz IR, etc.

Un monitor 1344 u otro tipo de dispositivo de visualización también se conectan al bus 1308 de sistema a través de una interfaz, tal como un adaptador 1346 de vídeo. Además del monitor 1344, un ordenador incluye habitualmente otros dispositivos de salida periféricos (no mostrados), tales como altavoces, impresoras, etc.

El ordenador 1302 puede operar en un entorno de red usando conexiones lógicas a través de comunicaciones por cable y/o inalámbricas en uno o más ordenadores remotos, tal como uno o unos ordenadores 1348 remotos. El o los ordenadores 1348 remotos pueden ser una estación de trabajo, un ordenador servidor, un encaminador, un ordenador personal, un ordenador portátil, un aparato de entretenimiento basado en microprocesador, un dispositivo parejo u otro nodo de red común, y habitualmente incluye muchos o todos los elementos descritos en relación con el ordenador 1302, aunque, por motivos de brevedad, solo se ilustra un dispositivo 1350 de memoria/almacenamiento. Las conexiones lógicas representadas incluyen una conectividad por cable/inalámbrica a una red 1352 de área local (LAN) y/o a redes más grandes, por ejemplo, una red 1354 de área amplia (WAN). Tales entornos de red LAN y

WAN son habituales en oficinas y empresas, y facilitan redes informáticas amplias de empresa, tales como intranets, pudiendo conectarse todas ellas a una red de comunicaciones global, por ejemplo, internet.

Cuando se usa en un entorno de red LAN, el ordenador 1302 se conecta a la red 1352 local a través de una interfaz o adaptador 1356 de red de comunicaciones por cable y/o inalámbrica. El adaptador 1356 puede facilitar la comunicación por cable o inalámbrica con la LAN 1352, que también puede incluir un punto de acceso inalámbrico dispuesto en el mismo para comunicarse con el adaptador 1356 inalámbrico.

Cuando se usa en un entorno de red WAN, el ordenador 1302 puede incluir un módem 1358, o está conectado a un servidor de comunicaciones en la WAN 1354, o tiene otros medios para establecer comunicaciones a través de la WAN 1354, tal como por medio de internet. El módem 1358, que puede ser interno o externo, y un dispositivo por cable o inalámbrico, se conecta al bus 1308 de sistema a través de la interfaz 1342 de puerto serie. En un entorno de red, los módulos de programa representados en relación con el ordenador 1302, o partes de los mismos, pueden almacenarse en el dispositivo 1350 de memoria/almacenamiento remoto. Se apreciará que las conexiones de red mostradas son ejemplos y que pueden usarse otros medios para establecer un enlace de comunicaciones entre los ordenadores.

El ordenador 1302 puede funcionar para comunicarse con cualquier dispositivo o entidad inalámbrica dispuesta operativamente en una comunicación inalámbrica, por ejemplo, una impresora, un escáner, un escritorio y/o un ordenador portátil, un asistente de datos portátil, un satélite de comunicaciones, cualquier pieza de equipo o localización asociada con una etiqueta detectable de manera inalámbrica (por ejemplo, un quiosco, un puesto de prensa, un baño), y un teléfono. Esto incluye al menos las tecnologías inalámbricas Wi-Fi y Bluetooth™. Por lo tanto, la comunicación puede ser una estructura predefinida con una red convencional o simplemente una comunicación ad hoc entre al menos dos dispositivos.

La Wi-Fi, o fidelidad inalámbrica, permite la conexión a internet desde un sofá en casa, una cama en una habitación de hotel, o una sala de conferencias en el trabajo, sin necesidad de cables. Wi-Fi es una tecnología inalámbrica similar a la usada en un teléfono móvil que permite que tales dispositivos, por ejemplo, ordenadores, envíen y reciban datos en interiores y exteriores; en cualquier lugar dentro del alcance de una estación base. Las redes Wi-Fi usan las tecnologías de radio denominadas IEEE 802.11x(a, b, g, etc.) para proporcionar una conectividad inalámbrica segura, fiable y rápida. Una red Wi-Fi puede usarse para conectar los ordenadores entre sí, a internet, y a redes por cable (que usan IEEE 802.3 o ethernet).

Haciendo ahora referencia a la figura 14, se ilustra un diagrama de bloques esquemático de un entorno 1400 informático ejemplar que puede facilitar la ejecución de la creación y/o el procesamiento de credenciales de pre-autenticación de acuerdo con la arquitectura desvelada. El sistema 1400 incluye uno o más clientes 1402. El o los clientes 1402 pueden ser un hardware y/o un software (por ejemplo, hilos, procedimientos, dispositivos informáticos). El o los clientes 1402 pueden albergar, por ejemplo, un o unos chivatos y/o información contextual asociada.

El sistema 1400 también incluye uno o más servidores 1404. El o los servidores 1404 también pueden ser un hardware y/o un software (por ejemplo, hilos, procedimientos, dispositivos informáticos). Los servidores 1404 pueden albergar hilos para realizar transformaciones empleando, por ejemplo, la arquitectura. Una posible comunicación entre un cliente 1402 y un servidor 1404 puede ser en forma de un paquete de datos adaptado para transmitirse entre dos o más procedimientos informáticos. El paquete de datos puede incluir, por ejemplo, un chivato y/o información contextual asociada. El sistema 1400 incluye una infraestructura 1406 de comunicaciones (por ejemplo, una red de comunicaciones global, tal como internet) que puede emplearse para facilitar las comunicaciones entre el o los clientes 1402 y el o los servidores 1404.

Pueden facilitarse las comunicaciones a través de una tecnología por cable (incluyendo la fibra óptica) y/o inalámbrica. El o los clientes 1402 están conectados operativamente a uno o más almacenes 1408 de datos de cliente que pueden emplearse para almacenar información local para el o los clientes 1402 (por ejemplo, un o unos chivatos y/o información contextual asociada). De manera similar, el o los servidores 1404 están conectados operativamente a uno o más almacenes 1410 de datos de servidor que pueden emplearse para almacenar información local en los servidores 1404.

Lo que se ha descrito anteriormente incluye ejemplos de la arquitectura desvelada. Por supuesto, no es posible describir todas las combinaciones imaginables de componentes y/o metodologías, pero los expertos en la materia pueden reconocer que son posibles muchas otras combinaciones y permutaciones. En consecuencia, la nueva arquitectura está prevista para abarcar todas esas alteraciones, modificaciones y variaciones que se incluyen dentro del ámbito de las reivindicaciones adjuntas. Además, en la medida en que se usa el término “incluye”, tanto en la descripción detallada como en las reivindicaciones, se pretende que tal término sea inclusivo de una manera similar a la expresión “que comprende”, ya que “que comprende” se interpreta cuando se emplea como una palabra de transición en una reivindicación.

La siguiente es una lista de realizaciones preferidas adicionales de la invención:

Realización 1: Un sistema (100) de autenticación implementado por ordenador, que comprende:

un componente (102) de confianza para recibir credenciales pre-autenticadas de una entidad de confianza; y

un componente (106) de aplicación para proporcionar un servicio de aplicación basado en las credenciales pre-autenticadas.

Realización 2: El sistema de la realización 1, en el que las credenciales pre-autenticadas se reciben a través de un protocolo de sesión de medios que es un protocolo de inicio de sesión (SIP).

Realización 3: El sistema de la realización 2, en el que el protocolo de sesión de medios es un protocolo de inicio de sesión (SIP).

Realización 4: El sistema de la realización 1, en el que la entidad de confianza es un servidor de comunicaciones, las credenciales pre-autenticadas incluyen al menos uno de un dato de identidad de dispositivo o un dato de identidad de usuario, y el servicio de aplicación facilita las comunicaciones de voz entre un dispositivo móvil y el servidor de comunicaciones.

Realización 5: El sistema de la realización 1, en el que las credenciales pre-autenticadas incluyen un nivel de permiso relacionado con un tipo del servicio de aplicación que se proporciona por el componente de aplicación.

Realización 6: El sistema de la realización 1, en el que la entidad de confianza recibe las credenciales pre-autenticadas de otra entidad de confianza.

Realización 7: El sistema de la realización 1, que comprende además un componente de permisos para seleccionar el servicio de aplicación de una o más aplicaciones basándose en un permiso asociado con las credenciales pre-autenticadas.

Realización 8: El sistema de la realización 1, en el que el componente de confianza y el componente de aplicación son de un cliente que recibe las credenciales pre-autenticadas para la conexión de una llamada telefónica basada en IP a través del cliente con un destino remoto.

Realización 9: El sistema de la realización 1, que comprende además un componente de aprendizaje y de razonamiento de máquina que emplea un análisis probabilístico y/o basado en estadística para pronosticar o deducir una acción que es deseable que se realice automáticamente.

Realización 10: El sistema de la realización 1, en el que las credenciales pre-autenticadas incluyen la información de perfil de usuario que define un servicio de calidad para la comunicación con un dispositivo de destino.

Realización 11: Un procedimiento implementado por ordenador del procesamiento de autenticación, que comprende:

autenticar a un primer cliente de un usuario para los servicios de comunicaciones en una localización remota (700);

generar credenciales autenticadas en la localización remota para el primer cliente (702);

recibir una solicitud para servicios de comunicaciones de un segundo cliente del usuario (704);

transmitir las credenciales autenticadas al segundo cliente basándose en la autenticación del primer cliente (706); y

habilitar los servicios de comunicaciones para el segundo cliente basándose en las credenciales autenticadas (708).

Realización 12: El procedimiento de la realización 11, que comprende además el acceso a la localización remota a través de una interfaz web, localización remota que es un servidor de comunicaciones de nivel medio basado en red que procesa las comunicaciones basadas en SIP del primer cliente.

Realización 13: El procedimiento de la realización 11, en el que al menos uno del primer cliente o el segundo cliente es parte de un dispositivo de comunicaciones de voz sobre IP.

Realización 14: El procedimiento de la realización 11, que comprende además incluir información de personalidad en las credenciales autenticadas que cambia la forma en que el segundo cliente, que es un operador automático, interactúa con un usuario.

Realización 15: El procedimiento de la realización 11, que comprende además emplear la información usada más recientemente basándose en las credenciales autenticadas para presentar la información al usuario para la selección.

Realización 16: El procedimiento de la realización 11, que comprende además controlar los parámetros de calidad de servicio para el segundo cliente basándose en las credenciales autenticadas.

Realización 17: El procedimiento de la realización 11, que comprende además exponer de manera automática la funcionalidad de un asistente personal virtual basándose en las credenciales autenticadas, estando la funcionalidad expuesta basada en el conocimiento de una lista de contactos o una lista de amigos.

Realización 18: El procedimiento de la realización 11, que comprende además seleccionar los servicios de diferentes aplicaciones del primer cliente basándose en las credenciales autenticadas y que proporcionan los servicios seleccionados para las comunicaciones por el segundo cliente.

Realización 19: El procedimiento de la realización 11, que comprende además el aprendizaje y el razonamiento sobre el comportamiento interactivo del cliente o el usuario y la presentación automática de información al usuario basándose en el mismo.

Realización 20: Un sistema implementado por ordenador, que comprende:

medios (202) implementados por ordenador para autenticar a un primer cliente de un usuario para los servicios de comunicaciones en una localización remota;

medios (204) implementados por ordenador para generar credenciales autenticadas en la localización remota para el primer cliente;

medios (208) implementados por ordenador para recibir una solicitud de servicios de comunicaciones de un segundo cliente del usuario;

medios (216) implementados por ordenador para transmitir las credenciales autenticadas al segundo cliente basándose en la autenticación del primer cliente; y

medios (210) implementados por ordenador para habilitar los servicios de comunicaciones para el segundo cliente.

REIVINDICACIONES

1. Un sistema de autenticación implementado por ordenador para evitar el inicio de comunicación de un teléfono (110, 218) basado en IP, protocolo de internet, que inicia una conversación telefónica basada en IP con un destino (112) remoto en unas comunicaciones (100) de voz basadas en IP una vez que un usuario del teléfono basado en IP se ha autenticado previamente con éxito con los datos de identidad de usuario en un servidor (104) de comunicaciones que comprende:

un cliente (208) para conectar una llamada del teléfono basado en IP a través del cliente al destino (112) remoto sin necesidad de que el usuario se someta a un procedimiento de acceso complementario en un componente (102, 216) de aplicación, comprendiendo el cliente:

un componente (102, 216) de confianza adaptado para recibir unas credenciales pre-autenticadas que contienen los datos de identidad de usuario procedentes del servidor de comunicaciones a través de un protocolo de sesión de medios que es un protocolo de inicio de sesión, SIP; y
el componente (106, 210) de aplicación adaptado para proporcionar una comunicación de voz entre el teléfono basado en IP y el destino remoto, a la vez que elude el procedimiento de acceso basándose en los datos de identidad de usuario contenidos en las credenciales pre-autenticadas.

2. El sistema de la reivindicación 1, en el que las credenciales pre-autenticadas incluyen al menos uno de los datos de identidad de usuario.

3. El sistema de la reivindicación 1, en el que las credenciales pre-autenticadas incluyen uno o más de un nivel de permiso relativo a un tipo de la comunicación de voz que se proporciona por el componente de aplicación, y una información de perfil de usuario que define un servicio de calidad para la comunicación con el destino remoto.

4. El sistema de la reivindicación 1, que comprende además el servidor de comunicaciones adaptado para recibir las credenciales pre-autenticadas de una entidad de confianza.

5. El sistema de la reivindicación 1, que comprende además un componente (304) de permisos para seleccionar la comunicación de voz de una o más aplicaciones basándose en un permiso asociado con las credenciales pre-autenticadas.

6. El sistema de la reivindicación 1, que comprende además un componente (502) de aprendizaje y de razonamiento de máquina que emplea un análisis probabilístico y/o basado en estadística para pronosticar o deducir una acción que es deseable que se realice automáticamente.

7. Un procedimiento implementado por ordenador de procesamiento de autenticación para evitar el inicio de comunicación de un teléfono basado en IP, protocolo de internet, en las comunicaciones de voz basadas en IP, que comprende:

pre-autenticar a un usuario del teléfono basado en IP con los datos de identidad de usuario para los servicios de comunicaciones en un servidor (104, 202) de comunicaciones remoto antes de iniciar una conversación telefónica basada en IP por el teléfono basado en IP con un destino (112) remoto sin necesidad de que el usuario se someta a un procedimiento de acceso complementario en un componente (102, 216) de aplicación;
generar credenciales pre-autenticadas que contienen los datos de identidad de usuario en el servidor de comunicaciones remoto para el usuario;
recibir una solicitud para las comunicaciones de voz en el teléfono (110, 218) basado en IP del usuario;
buscar las credenciales pre-autenticadas accediendo al servidor de comunicaciones remoto;
transmitir, desde el servidor de comunicaciones remoto, a través de un protocolo de inicio de sesión, SIP, las credenciales pre-autenticadas al teléfono basado en IP basándose en la pre-autenticación del usuario; y
habilitar, por el componente de aplicación, las comunicaciones de voz entre el teléfono basado en IP y el destino (112) a la vez que se elude el procedimiento de acceso basándose en los datos de identidad de usuario contenidos en las credenciales pre-autenticadas.

8. El procedimiento de la reivindicación 7, que comprende además acceder al servidor de comunicaciones remoto a través de una interfaz web, en el que el servidor de comunicaciones remoto es un servidor de comunicaciones de nivel intermedio basado en la red que procesa las comunicaciones basadas en SIP procedentes del usuario.

9. El procedimiento de la reivindicación 7, que comprende además uno o más de:

emplear la información usada más recientemente basándose en las credenciales pre-autenticadas para presentar información al usuario para la selección; y
aprender y razonar sobre el comportamiento interactivo del cliente o del usuario y automatizar la presentación de la información al usuario basándose en el mismo.

10. El procedimiento de la reivindicación 7, que comprende además uno o más de:

controlar los parámetros de calidad de servicio para el teléfono basado en IP basándose en las credenciales pre-

autenticadas; y
seleccionar servicios de diferentes aplicaciones basándose en las credenciales autenticadas y proporcionar los servicios seleccionados para las comunicaciones por el teléfono basado en IP.

11. El procedimiento de la reivindicación 7, que comprende además exponer automáticamente la funcionalidad de un asistente personal virtual basándose en las credenciales pre-autenticadas, estando la funcionalidad expuesta basada en el conocimiento de una lista de contactos o una lista de amigos.

12. Un medio legible por ordenador que almacena en el mismo unas instrucciones legibles por ordenador que, cuando se llevan a cabo por un procesador, hacen que el procesador realice el procedimiento de una de las reivindicaciones 7 a 11.

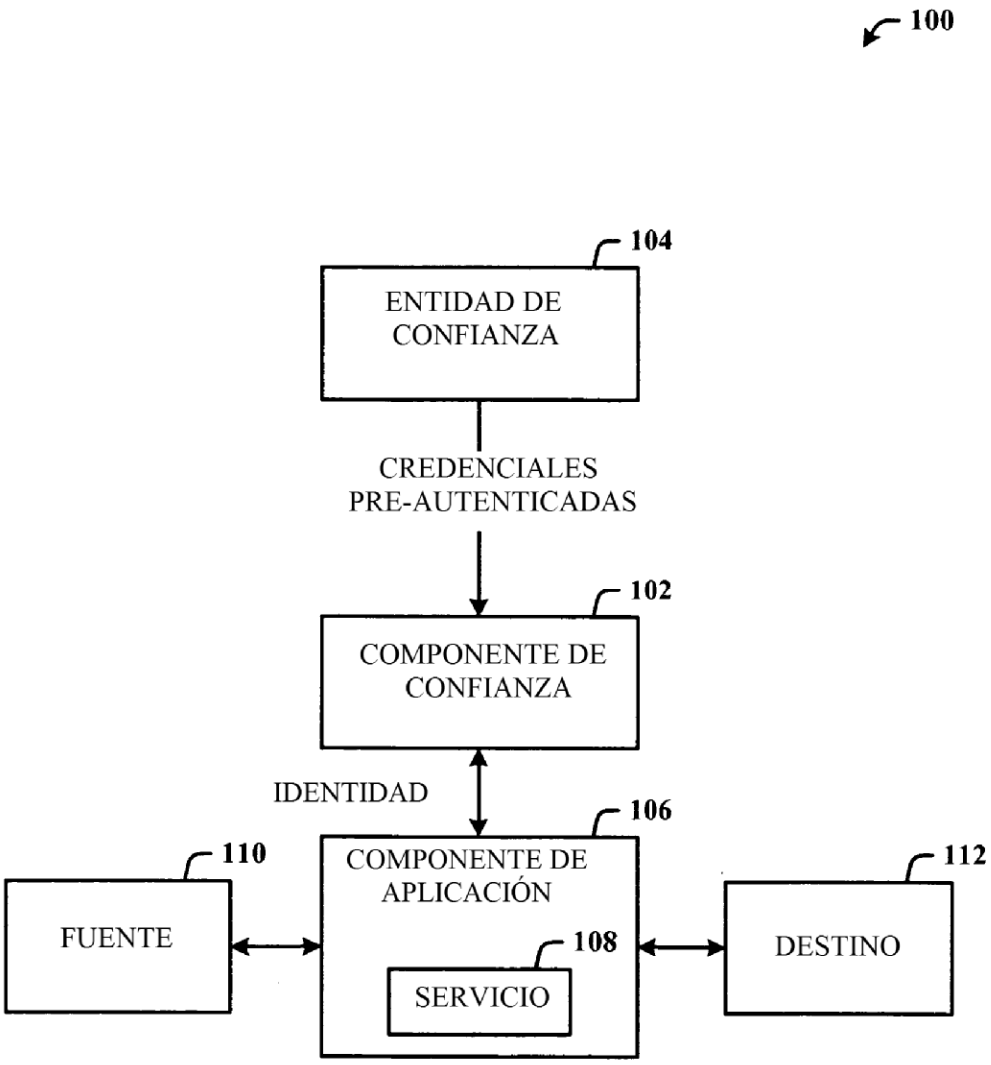
100
104
ENTIDAD DE CONFIANZA
CREDENCIALES PRE-AUTENTICADAS
102
COMPONENTE DE CONFIANZA
IDENTIDAD
106
110
COMPONENTE DE APLICACIÓN
112
FUENTE
108
SERVICIO
DESTINO

FIG. 1

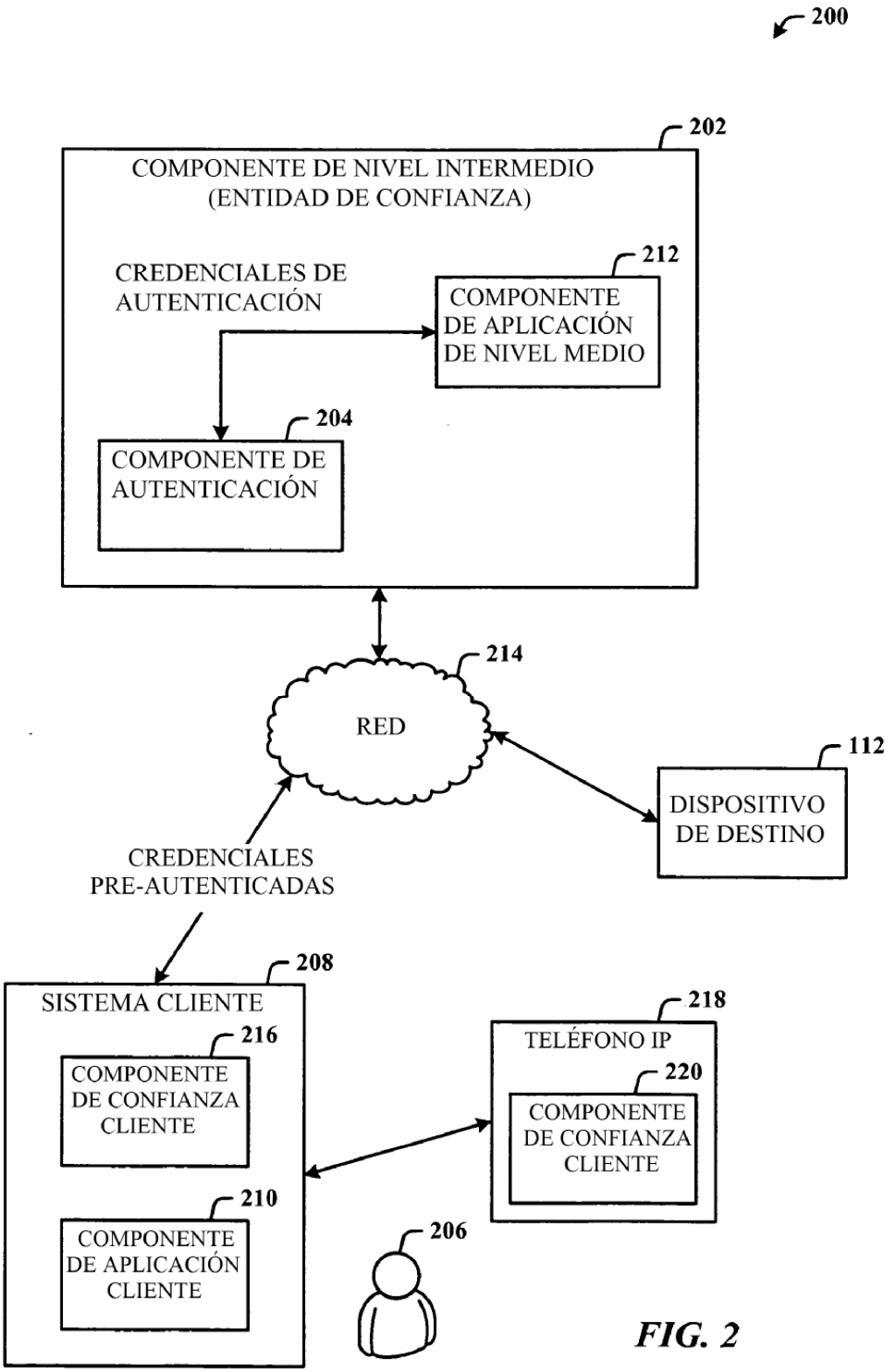
200
202
COMPONENTE DE NIVEL INTERMEDIO
(ENTIDAD DE CONFIANZA)
212
CREDENCIALES DE
AUTENTICACIÓN
COMPONENTE
DE APLICACIÓN
DE NIVEL MEDIO
204
COMPONENTE DE
AUTENTICACIÓN
214
RED
112
DISPOSITIVO
DE DESTINO
CREDENCIALES
PRE-AUTENTICADAS
208
SISTEMA CLIENTE
216
COMPONENTE
DE CONFIANZA
CLIENTE
218
TELÉFONO IP
220
COMPONENTE
DE CONFIANZA
CLIENTE
210
COMPONENTE
DE APLICACIÓN
CLIENTE
206

FIG. 2

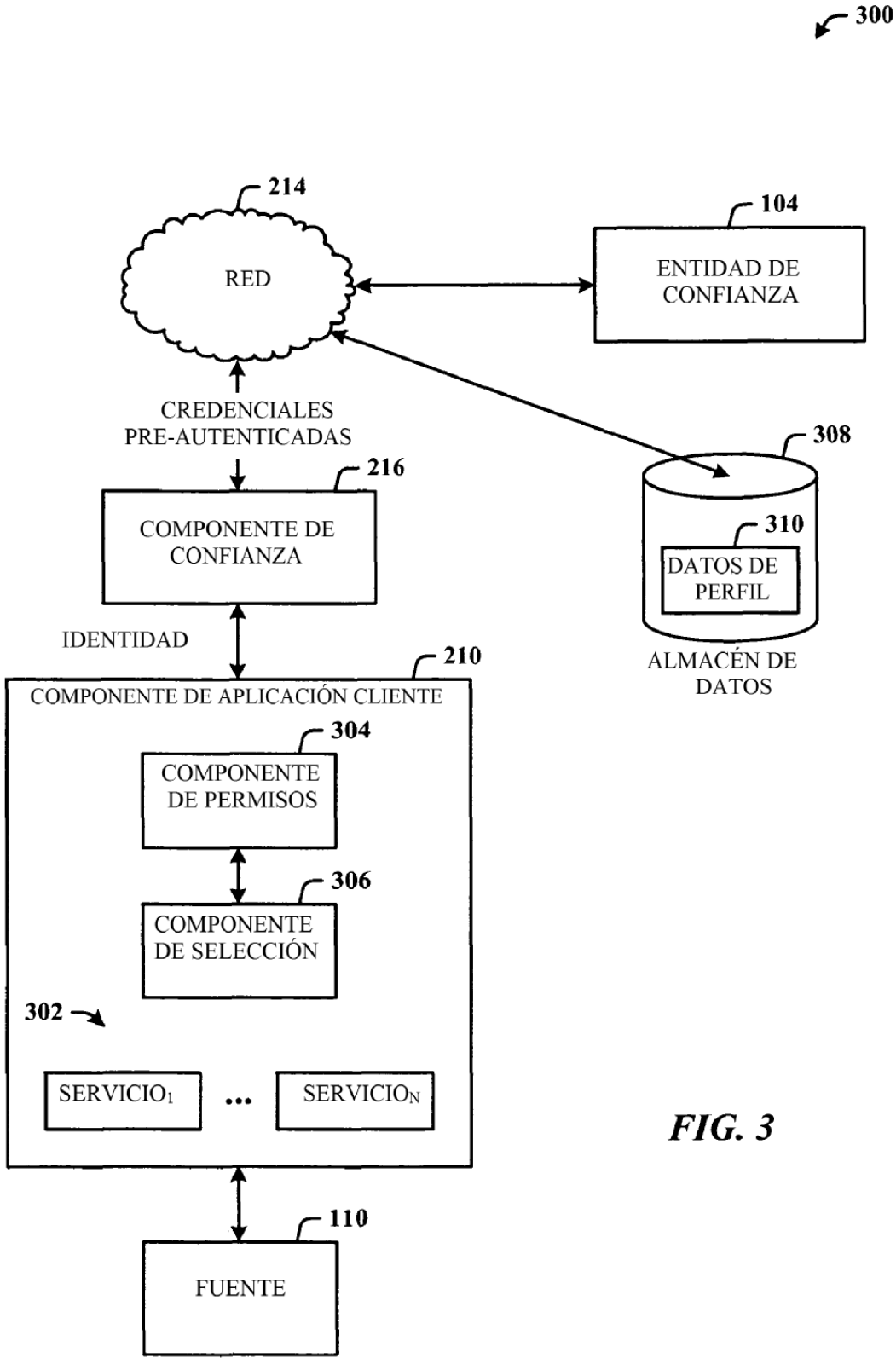
300
214
RED
104
ENTIDAD DE CONFIANZA
CREDENCIALES PRE-AUTENTICADAS
308
216
COMPONENTE DE CONFIANZA
310
DATOS DE PERFIL
IDENTIDAD
ALMACÉN DE DATOS
210
COMPONENTE DE APLICACIÓN CLIENTE
304
COMPONENTE DE PERMISOS
306
COMPONENTE DE SELECCIÓN
302
SERVICIO1
...
SERVICION
110
FUENTE

FIG. 3

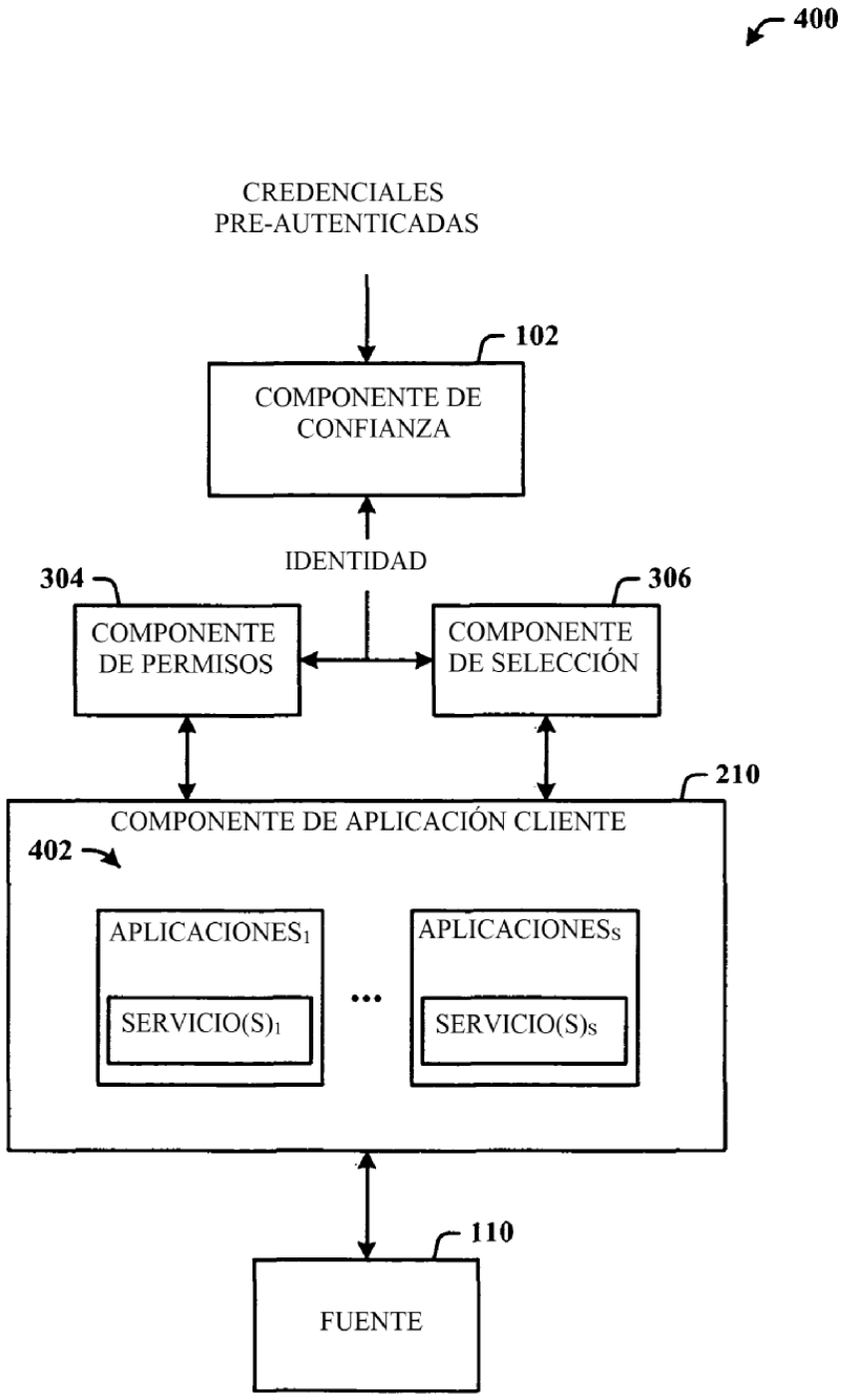
400
CREDENCIALES
PRE-AUTENTICADAS
102
COMPONENTE DE
CONFIANZA
IDENTIDAD
304
COMPONENTE
DE PERMISOS
306
COMPONENTE
DE SELECCIÓN
210
COMPONENTE DE APLICACIÓN CLIENTE
402
APLICACIONES1
SERVICIO(S)1
...
APLICACIONESs
SERVICIO(S)s
110
FUENTE

FIG. 4

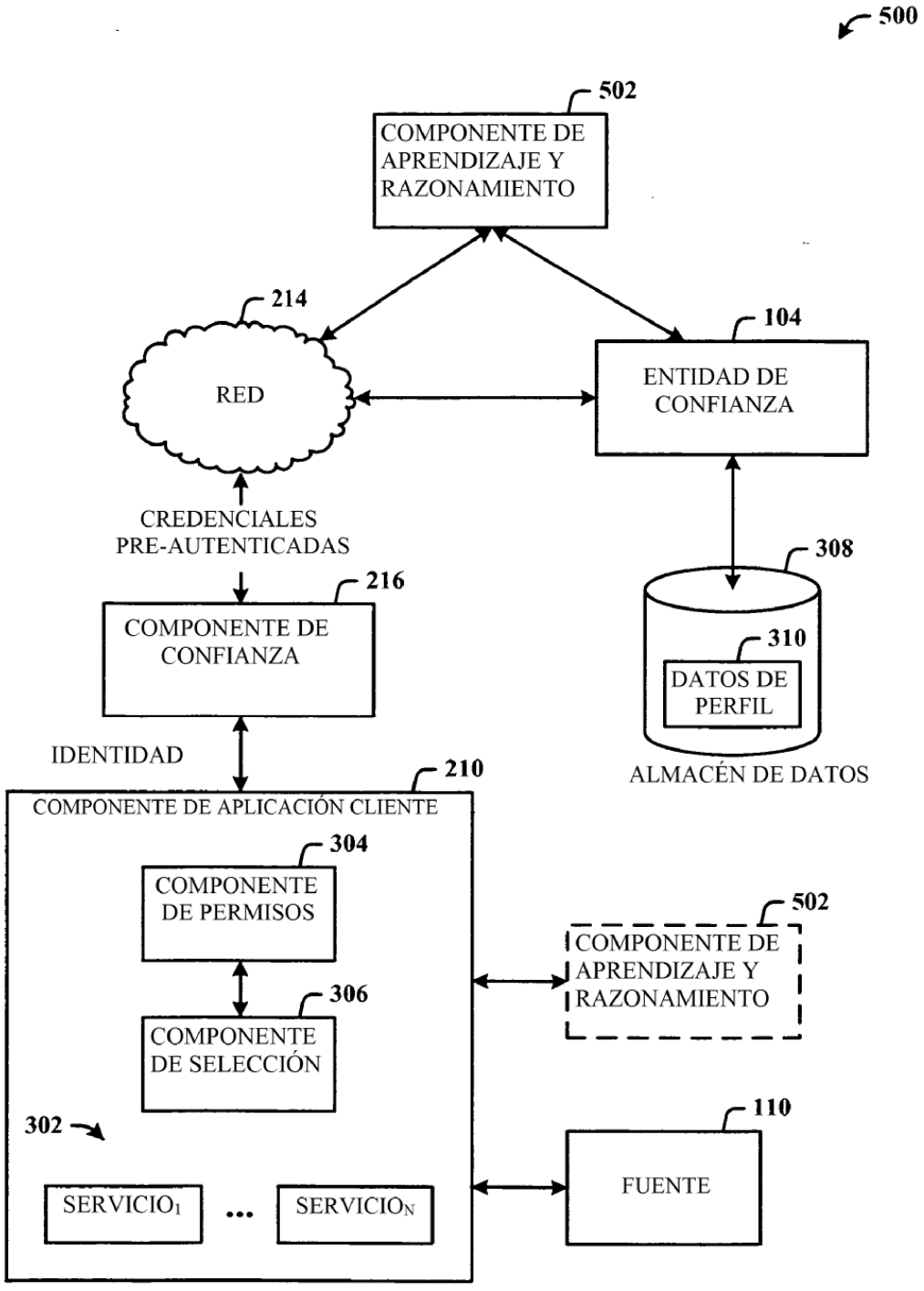
500
502
COMPONENTE DE APRENDIZAJE Y RAZONAMIENTO
214
RED
104
ENTIDAD DE CONFIANZA
CREDENCIALES PRE-AUTENTICADAS
308
216
COMPONENTE DE CONFIANZA
310
DATOS DE PERFIL
IDENTIDAD
ALMACÉN DE DATOS
210
COMPONENTE DE APLICACIÓN CLIENTE
304
COMPONENTE DE PERMISOS
502
COMPONENTE DE APRENDIZAJE Y RAZONAMIENTO
306
COMPONENTE DE SELECCIÓN
302
110
FUENTE
SERVICIO1
...
SERVICION

FIG. 5

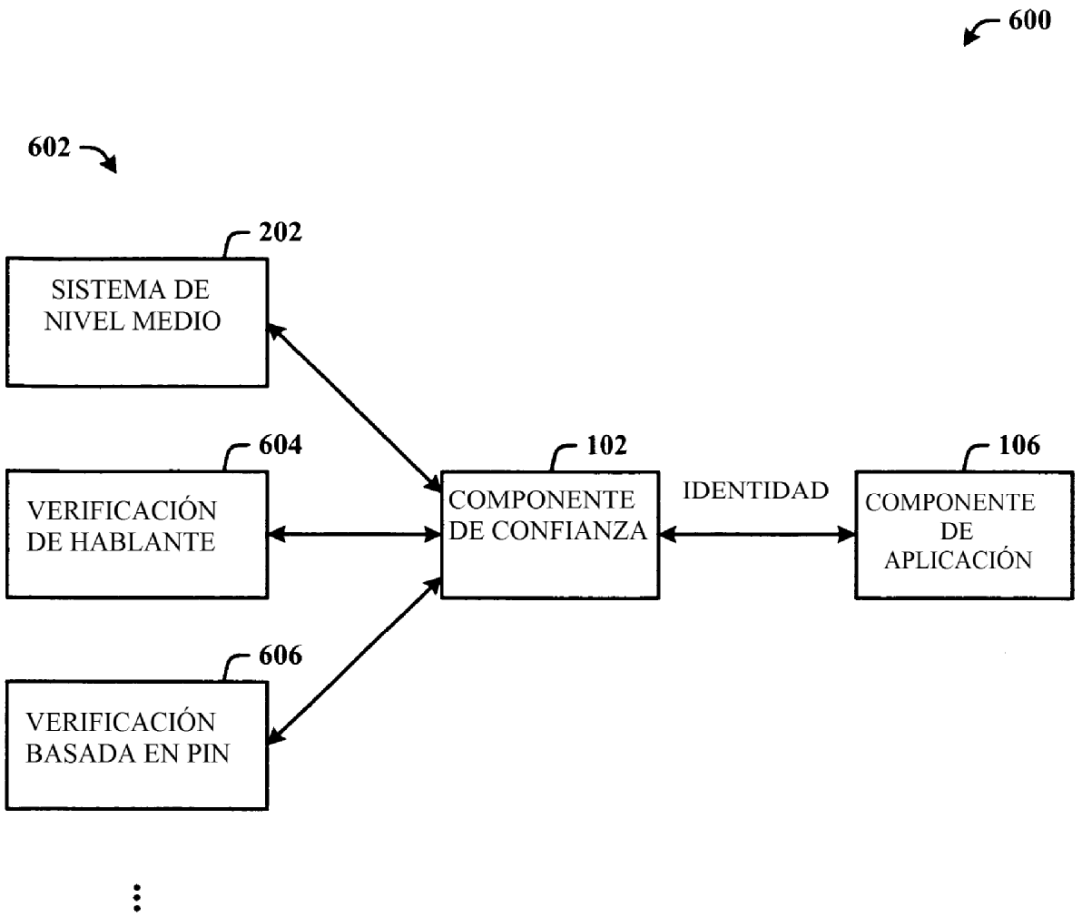
600
602
202
SISTEMA DE NIVEL MEDIO
604
VERIFICACIÓN DE HABLANTE
606
VERIFICACIÓN BASADA EN PIN
102
COMPONENTE DE CONFIANZA
IDENTIDAD
106
COMPONENTE DE APLICACIÓN

FIG. 6

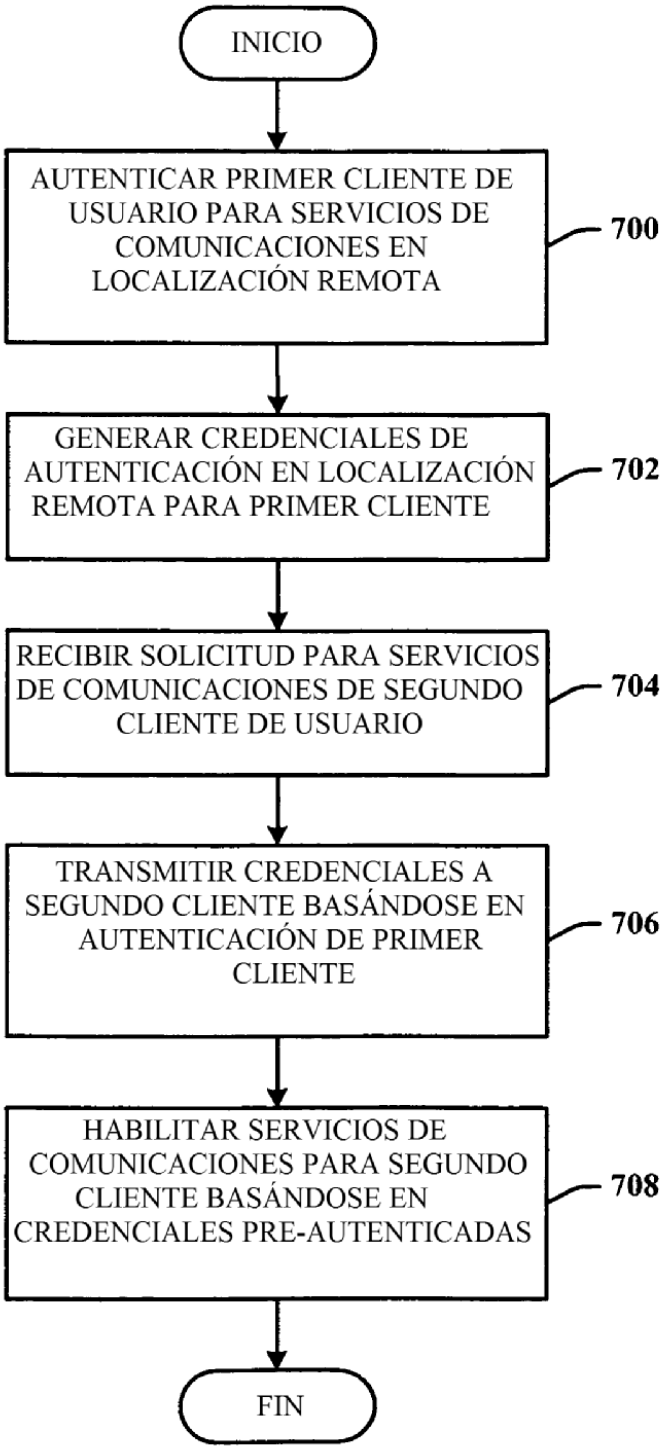
INICIO
AUTENTICAR PRIMER CLIENTE DE USUARIO PARA SERVICIOS DE COMUNICACIONES EN LOCALIZACIÓN REMOTA
700
GENERAR CREDENCIALES DE AUTENTICACIÓN EN LOCALIZACIÓN REMOTA PARA PRIMER CLIENTE
702
RECIBIR SOLICITUD PARA SERVICIOS DE COMUNICACIONES DE SEGUNDO CLIENTE DE USUARIO
704
TRANSMITIR CREDENCIALES A SEGUNDO CLIENTE BASÁNDOSE EN AUTENTICACIÓN DE PRIMER CLIENTE
706
HABILITAR SERVICIOS DE COMUNICACIONES PARA SEGUNDO CLIENTE BASÁNDOSE EN CREDENCIALES PRE-AUTENTICADAS
708
FIN

FIG. 7

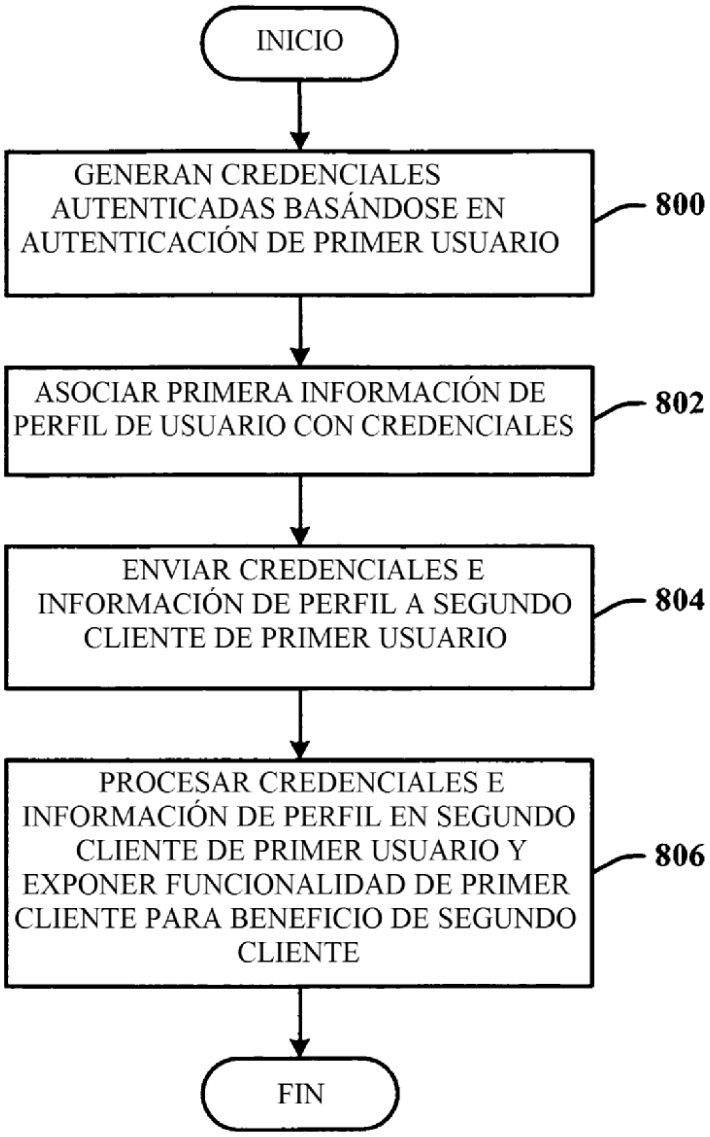
INICIO
GENERAN CREDENCIALES AUTENTICADAS BASÁNDOSE EN AUTENTICACIÓN DE PRIMER USUARIO
800
ASOCIAR PRIMERA INFORMACIÓN DE PERFIL DE USUARIO CON CREDENCIALES
802
ENVIAR CREDENCIALES E INFORMACIÓN DE PERFIL A SEGUNDO CLIENTE DE PRIMER USUARIO
804
PROCESAR CREDENCIALES E INFORMACIÓN DE PERFIL EN SEGUNDO CLIENTE DE PRIMER USUARIO Y EXPONER FUNCIONALIDAD DE PRIMER CLIENTE PARA BENEFICIO DE SEGUNDO CLIENTE
806
FIN

FIG. 8

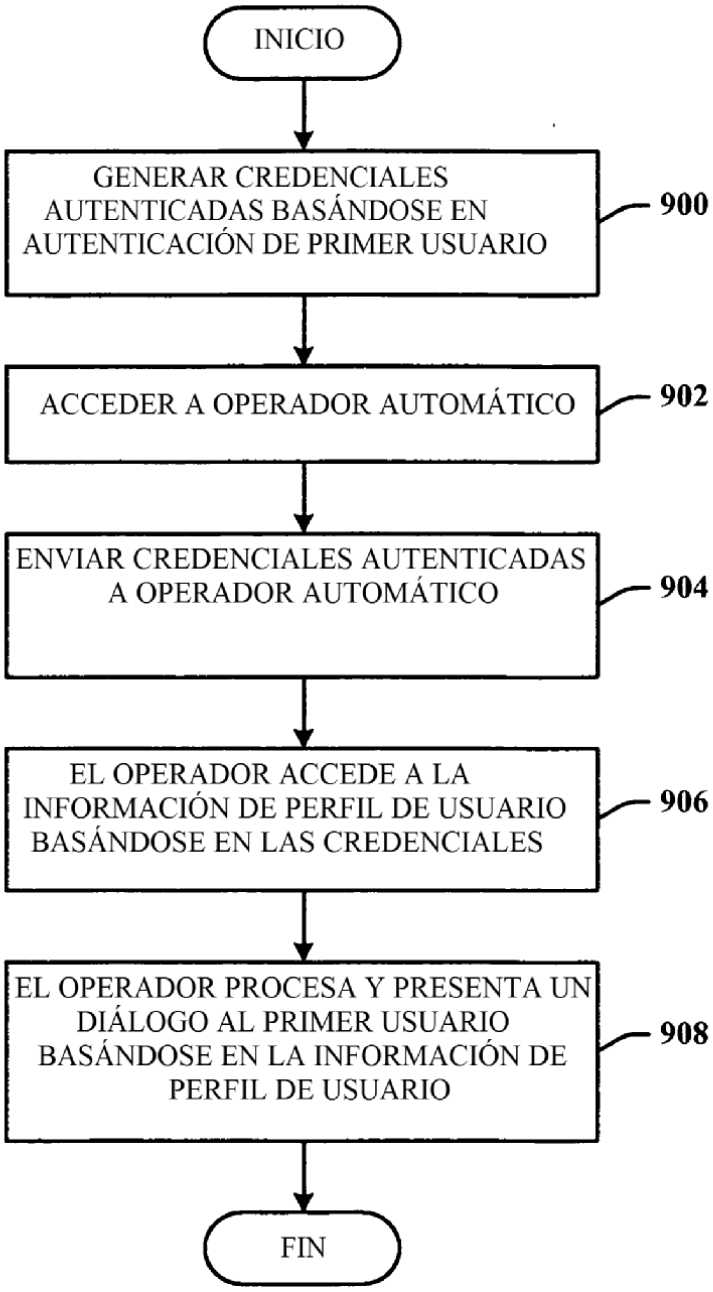
INICIO
GENERAR CREDENCIALES AUTENTICADAS BASÁNDOSE EN AUTENTICACIÓN DE PRIMER USUARIO
900
ACCEDER A OPERADOR AUTOMÁTICO
902
ENVIAR CREDENCIALES AUTENTICADAS A OPERADOR AUTOMÁTICO
904
EL OPERADOR ACCEDE A LA INFORMACIÓN DE PERFIL DE USUARIO BASÁNDOSE EN LAS CREDENCIALES
906
EL OPERADOR PROCESA Y PRESENTA UN DIÁLOGO AL PRIMER USUARIO BASÁNDOSE EN LA INFORMACIÓN DE PERFIL DE USUARIO
908
FIN

FIG. 9

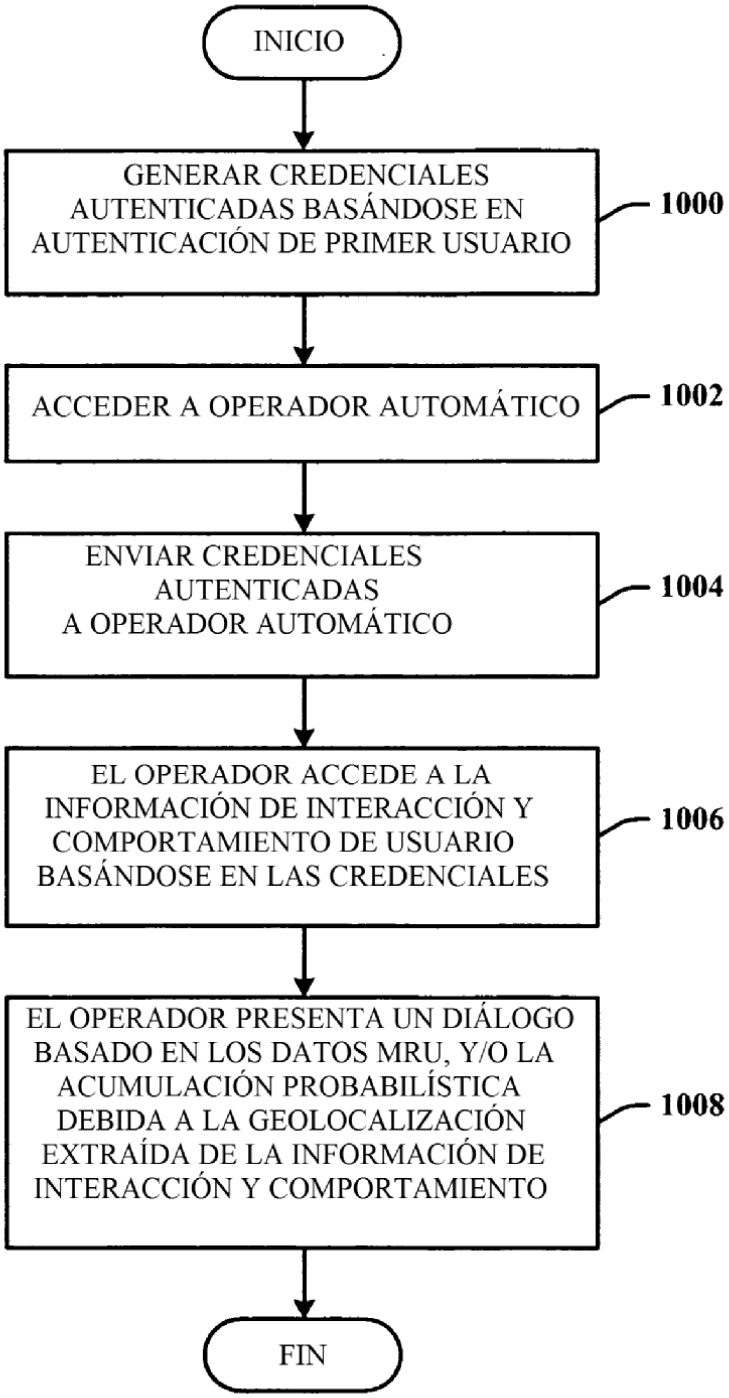
INICIO
GENERAR CREDENCIALES AUTENTICADAS BASÁNDOSE EN AUTENTICACIÓN DE PRIMER USUARIO
1000
ACCEDER A OPERADOR AUTOMÁTICO
1002
ENVIAR CREDENCIALES AUTENTICADAS A OPERADOR AUTOMÁTICO
1004
EL OPERADOR ACCEDE A LA INFORMACIÓN DE INTERACCIÓN Y COMPORTAMIENTO DE USUARIO BASÁNDOSE EN LAS CREDENCIALES
1006
EL OPERADOR PRESENTA UN DIÁLOGO BASADO EN LOS DATOS MRU, Y/O LA ACUMULACIÓN PROBABILÍSTICA DEBIDA A LA GEOLOCALIZACIÓN EXTRAÍDA DE LA INFORMACIÓN DE INTERACCIÓN Y COMPORTAMIENTO
1008
FIN

FIG. 10

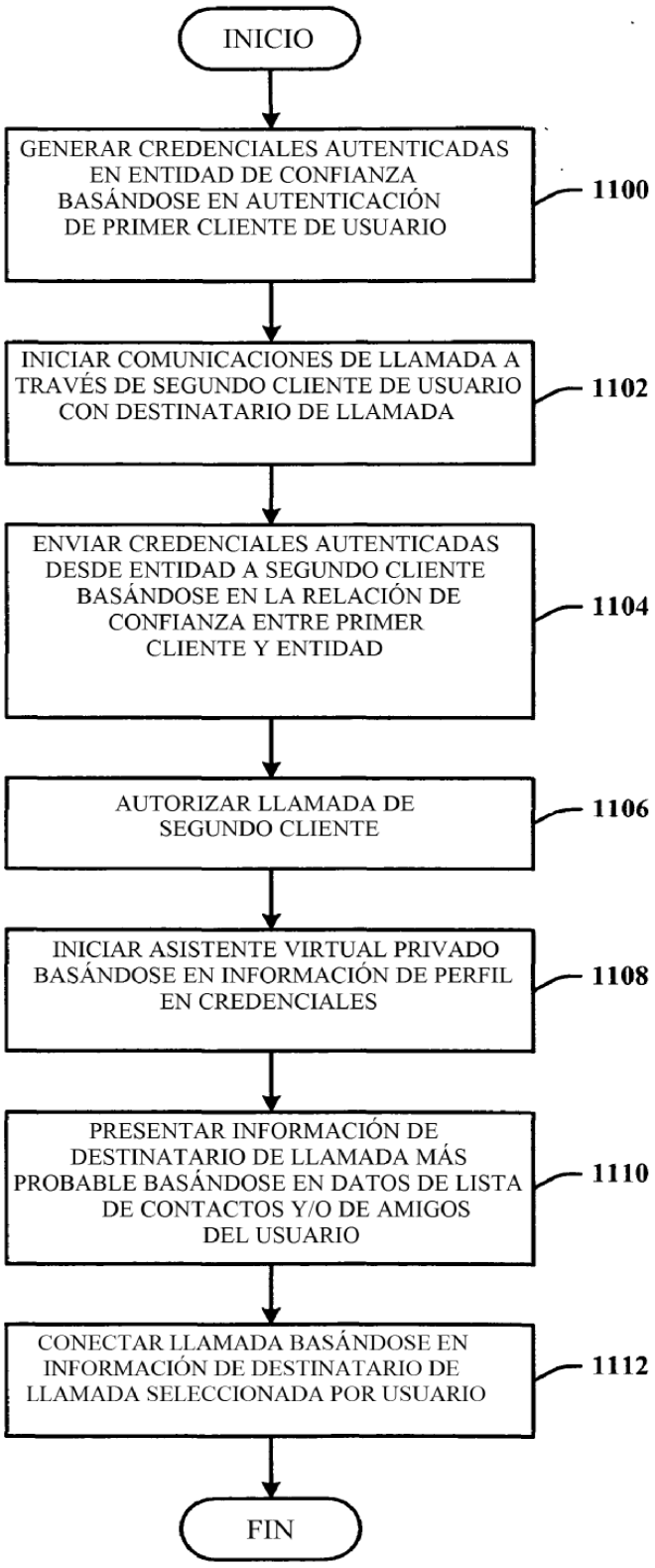
INICIO
GENERAR CREDENCIALES AUTENTICADAS EN ENTIDAD DE CONFIANZA BASÁNDOSE EN AUTENTICACIÓN DE PRIMER CLIENTE DE USUARIO
1100
INICIAR COMUNICACIONES DE LLAMADA A TRAVÉS DE SEGUNDO CLIENTE DE USUARIO CON DESTINATARIO DE LLAMADA
1102
ENVIAR CREDENCIALES AUTENTICADAS DESDE ENTIDAD A SEGUNDO CLIENTE BASÁNDOSE EN LA RELACIÓN DE CONFIANZA ENTRE PRIMER CLIENTE Y ENTIDAD
1104
AUTORIZAR LLAMADA DE SEGUNDO CLIENTE
1106
INICIAR ASISTENTE VIRTUAL PRIVADO BASÁNDOSE EN INFORMACIÓN DE PERFIL EN CREDENCIALES
1108
PRESENTAR INFORMACIÓN DE DESTINATARIO DE LLAMADA MÁS PROBABLE BASÁNDOSE EN DATOS DE LISTA DE CONTACTOS Y/O DE AMIGOS DEL USUARIO
1110
CONECTAR LLAMADA BASÁNDOSE EN INFORMACIÓN DE DESTINATARIO DE LLAMADA SELECCIONADA POR USUARIO
1112
FIN

FIG. 11

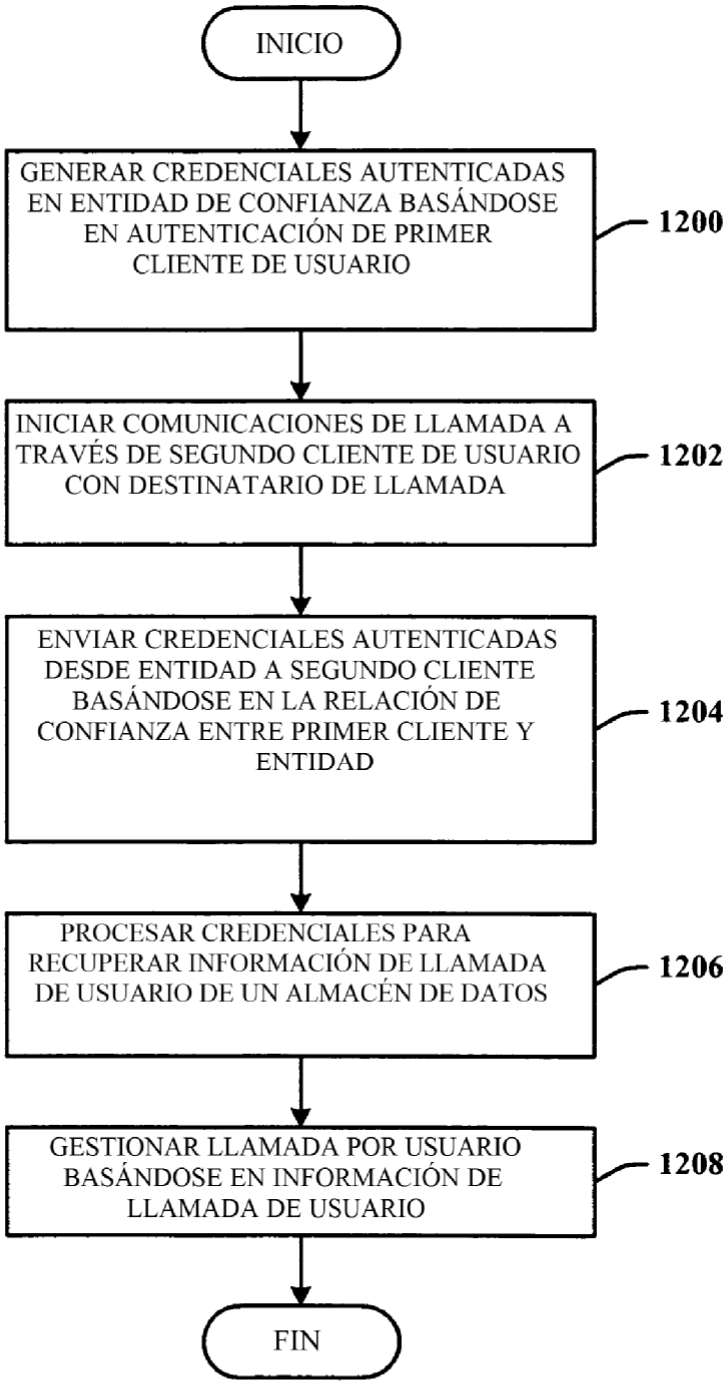
INICIO
GENERAR CREDENCIALES AUTENTICADAS EN ENTIDAD DE CONFIANZA BASÁNDOSE EN AUTENTICACIÓN DE PRIMER CLIENTE DE USUARIO
1200
INICIAR COMUNICACIONES DE LLAMADA A TRAVÉS DE SEGUNDO CLIENTE DE USUARIO CON DESTINATARIO DE LLAMADA
1202
ENVIAR CREDENCIALES AUTENTICADAS DESDE ENTIDAD A SEGUNDO CLIENTE BASÁNDOSE EN LA RELACIÓN DE CONFIANZA ENTRE PRIMER CLIENTE Y ENTIDAD
1204
PROCESAR CREDENCIALES PARA RECUPERAR INFORMACIÓN DE LLAMADA DE USUARIO DE UN ALMACÉN DE DATOS
1206
GESTIONAR LLAMADA POR USUARIO BASÁNDOSE EN INFORMACIÓN DE LLAMADA DE USUARIO
1208
FIN

FIG. 12

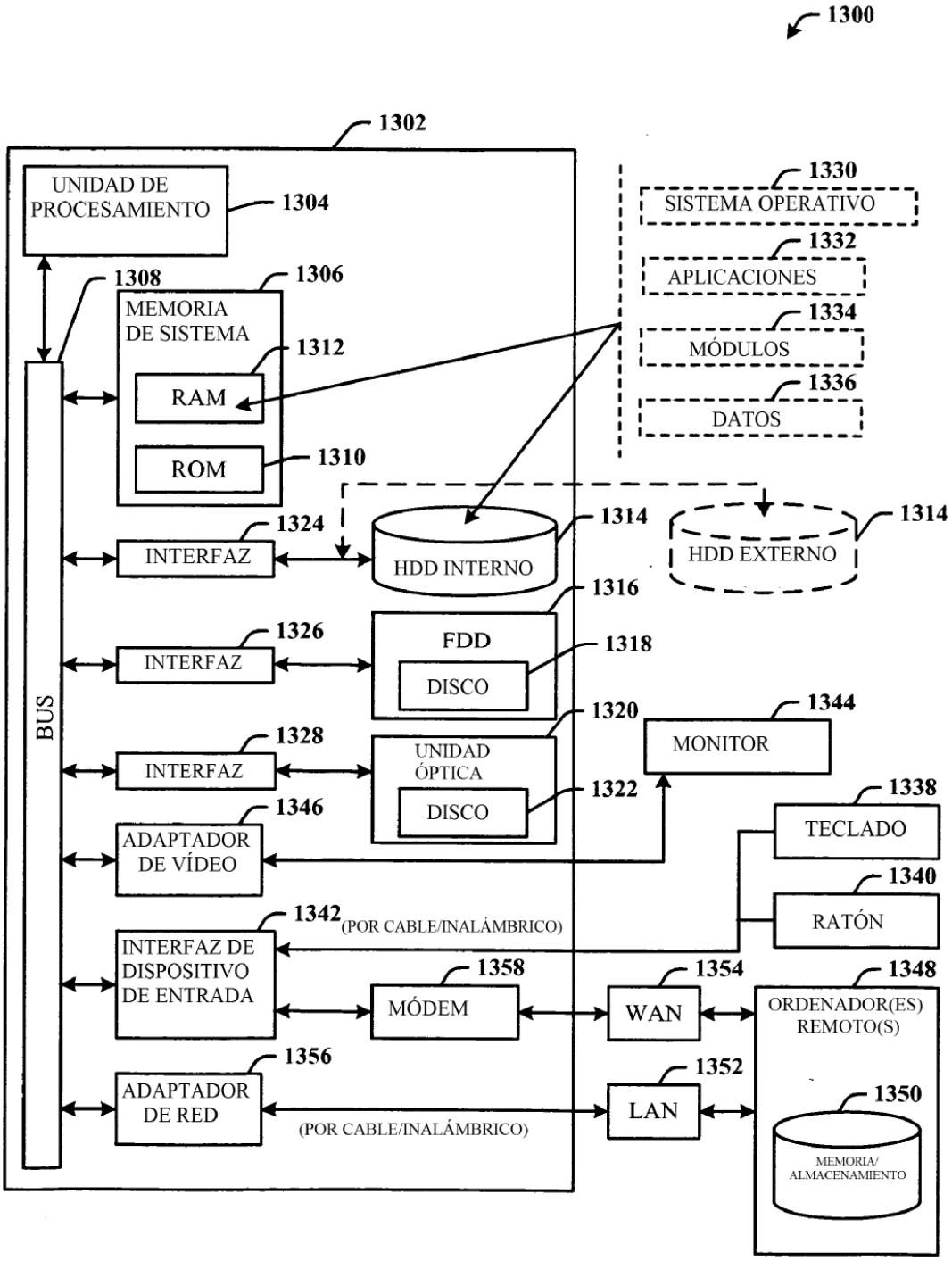
1300
1302
UNIDAD DE PROCESAMIENTO
1304
1308
1306
MEMORIA DE SISTEMA
1312
RAM
ROM
1310
BUS
1330
SISTEMA OPERATIVO
1332
APLICACIONES
1334
MÓDULOS
1336
DATOS
1324
INTERFAZ
HDD INTERNO
1314
HDD EXTERNO
1314
1316
1326
INTERFAZ
FDD
DISCO
1318
1320
1328
INTERFAZ
UNIDAD ÓPTICA
DISCO
1322
1344
MONITOR
1346
ADAPTADOR DE VÍDEO
1338
TECLADO
1340
RATÓN
1342
(POR CABLE/INALÁMBRICO)
INTERFAZ DE DISPOSITIVO DE ENTRADA
1358
MÓDEM
1354
WAN
1348
ORDENADOR(ES) REMOTO(S)
1356
ADAPTADOR DE RED
(POR CABLE/INALÁMBRICO)
1352
LAN
1350
MEMORIA/ ALMACENAMIENTO

FIG. 13

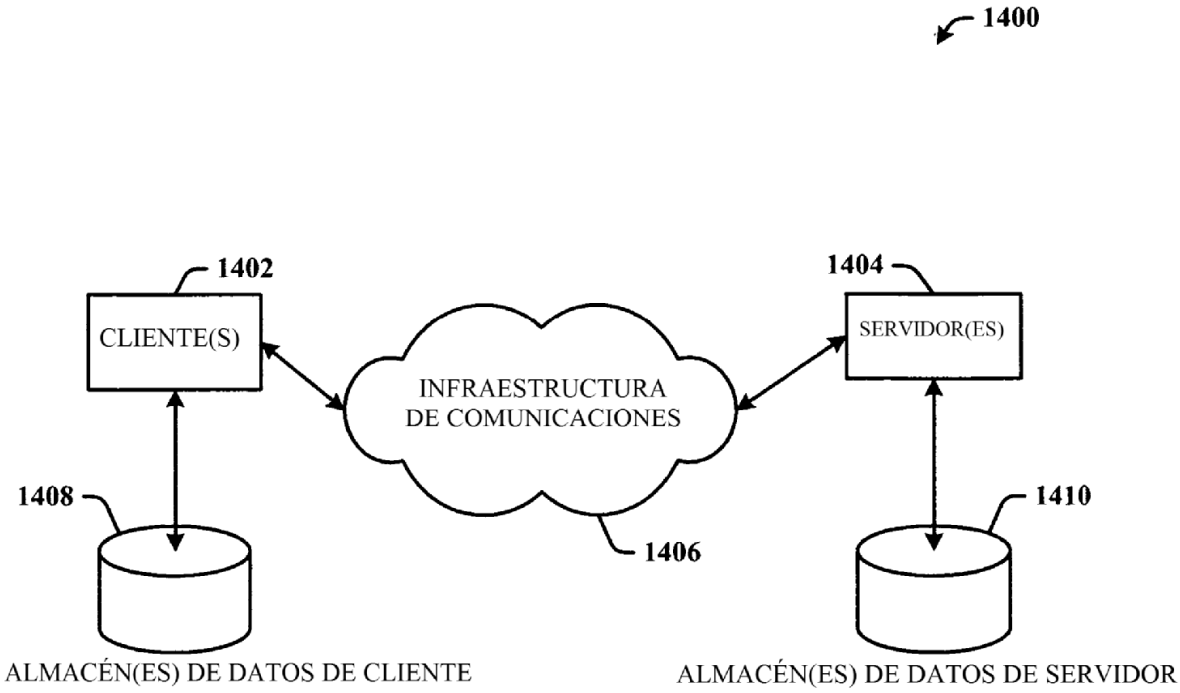
1400
1402
CLIENTE(S)
1404
SERVIDOR(ES)
INFRAESTRUCTURA
DE COMUNICACIONES
1406
1408
1410
ALMACÉN(ES) DE DATOS DE CLIENTE
ALMACÉN(ES) DE DATOS DE SERVIDOR

FIG. 14