(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 758 124**

(51) Int. CI.:

H04L 12/58 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **15.09.2015 E 15185202 (7)**

(97) Fecha y número de publicación de la concesión europea: **28.08.2019 EP 2996288**

(54) Título: **Sistema de mensajes no retenidos**

(30) Prioridad:

15.09.2014 US 201414486833

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
04.05.2020

(73) Titular/es:

THORPE, JOHN R. (100.0%)
3902 Buffington Drive
Columbia, MO 65203, US

(72) Inventor/es:

THORPE, JOHN R.

(74) Agente/Representante:

ARIAS SANZ, Juan

DESCRIPCIÓN

Sistema de mensajes no retenidos

Antecedentes

La especificación se refiere a mensajería electrónica. En particular la especificación se refiere a mensajería electrónica no retenida. Los sistemas de correo electrónico existentes, implican el envío de mensajes a través de una red compleja de servidores tales como servidores SMTP, IMAP y POP. Cuando los mensajes se envían a través de estos servidores, copias de los mensajes a menudo se almacenan y retienen con el propósito de entrega. Incluso después de que se hayan entregado los mensajes, es altamente probable que se retengan numerosas copias del mensaje en la red, o bien como copias de seguridad, copias de correos electrónicos basadas en la nube, archivos, bandejas de entrada, correo basura, elementos de basura, etc. En muchas circunstancias, especialmente cuando están siendo transmitidos mensajes o documentos altamente sensibles o confidenciales, el objetivo es solamente comunicarse con la parte de recepción y no tener ninguna información retenida en ningún otro lugar en todo el sistema. Tener mensajes o documentos retenidos, muchas veces de manera permanente, significa que las partes comunicantes han perdido el control de esos mensajes y documentos. Tal pérdida de control puede conducir a resultados perjudiciales, incluyendo la divulgación accidental de información, indicaciones no deseadas de comunicaciones y otras numerosas consecuencias no deseadas.

De manera similar, sitios de redes sociales tales como Facebook, Twitter, Google+, etc., retienen contenido tal como fotografías, vídeos, texto y otro contenido de usuario permanentemente o durante un periodo fuera del control del creador. Puede haber casos en los que a un creador de contenido le gustaría publicar contenido con el propósito de compartir, pero no desea que el contenido sea retenido indefinidamente o fuera del control del creador.

El documento EP 2 974 162 A1 se refiere a un sistema y a un método para mensajería electrónica no retenida. El sistema incluye un módulo receptor de mensajes, un módulo de almacenamiento de mensajes y generación de identificador, un módulo de recuperación de mensajes y un módulo de eliminación. El módulo receptor de mensajes recibe un mensaje. El módulo de almacenamiento de mensajes y generación de identificador almacena el mensaje en una memoria no transitoria y no persistente de uno o más dispositivos informáticos, genera un identificador de mensaje y envía el identificador de mensaje a un dispositivo destinatario. El módulo de recuperación de mensaje, recibe una selección del identificador de mensaje desde el dispositivo destinatario, recupera el mensaje de la memoria no transitoria y no persistente, y envía el mensaje al dispositivo destinatario para su presentación. El módulo de eliminación elimina el mensaje de uno o más dispositivos en respuesta al envío del mensaje al dispositivo destinatario para su presentación.

El documento US 2013/194301 A1 se refiere a un sistema y a un método para transmitir de manera segura información sobre una red de comunicaciones que comprende recibir una notificación de mensaje de que un destinatario tiene un mensaje en un dispositivo cliente del destinatario de un servidor basado en procesador tras la recepción del mensaje desde un dispositivo cliente del remitente. El mensaje del dispositivo cliente del remitente se almacena en un dispositivo de almacenamiento por el servidor. El destinatario accede al servidor para ver el mensaje usando el dispositivo cliente del destinatario. El mensaje se representa y muestra en la pantalla por el dispositivo cliente del destinatario según un método de visualización seleccionado por el remitente del mensaje para presentar solamente una parte del mensaje en un momento dado al destinatario. Esto evita que el mensaje sea registrado o capturado.

El documento US 2010/057869 A1 se refiere a revocación de correo electrónico en la que se proporciona que el correo electrónico transmitido se pueda retirar antes de que un destinatario sea capaz de leer el correo electrónico transmitido. Un servidor de eventos almacena un correo electrónico transmitido durante un período de tiempo dado o hasta que se recupere por un cliente de correo electrónico de recepción. Si el período de tiempo dado expira o se retira el correo electrónico, el cliente de correo electrónico de recepción es incapaz de recuperar el correo electrónico.

El documento US 2009/075630 A1 se refiere a un método y a un sistema para proteger datos en un aparato de teléfono móvil cuando se activa remotamente por un usuario que implican cifrar los datos usando una clave de cifrado, almacenar los datos cifrados y borrar los datos no cifrados junto con la clave de cifrado. También se pueden cargar datos en un servidor a través de datos celulares exigidos para su uso en copia de seguridad del aparato de teléfono móvil. Una aplicación de aparato de teléfono móvil configura el aparato de teléfono para recibir comandos de activación desde un servidor para cifrar, cargar o descargar datos. La clave de cifrado se recibe o bien desde el servidor o bien se genera por el aparato de teléfono móvil y se comunica al servidor. Se pueden generar y almacenar archivos de datos simulados en el aparato de teléfono móvil para permitir que las aplicaciones del aparato de teléfono funcionen normalmente después de que se hayan cifrado los archivos de datos.

Compendio

La especificación supera las deficiencias y limitaciones de la técnica anterior, al menos en parte, proporcionando un sistema y método para mensajería electrónica no retenida.

La presente invención se define en las reivindicaciones independientes. Las reivindicaciones dependientes definen las realizaciones de la presente invención.

La especificación describe un sistema, método y producto de programa de ordenador para mensajería electrónica no retenida según algunas realizaciones. El sistema comprende un módulo receptor de mensajes, un módulo de almacenamiento de mensajes e identificador, un módulo de recuperación de mensajes y un módulo de eliminación. El módulo receptor de mensajes recibe un mensaje. El módulo de almacenamiento de mensajes y generación de identificador almacena el mensaje en una memoria no transitoria y no persistente de uno o más dispositivos informáticos, genera un identificador de mensaje y envía el identificador de mensaje a un dispositivo destinatario. El módulo de recuperación de mensajes recibe una selección del identificador de mensaje desde el dispositivo destinatario, recupera el mensaje de la memoria no transitoria y no persistente y envía el mensaje al dispositivo destinatario para su presentación. El módulo de eliminación elimina el mensaje del uno o más dispositivos en respuesta al módulo de recuperación de mensajes que envía el mensaje al dispositivo destinatario para su presentación.

El módulo de eliminación elimina el identificador de mensaje del uno o más dispositivos informáticos en respuesta al envío del identificador de mensaje al dispositivo destinatario. El identificador de mensaje y el mensaje se envían de manera anónima en base a una preferencia del usuario asociada con un remitente del mensaje. El identificador de mensaje es un URL. El sistema carece de una memoria escribible y persistente. El identificador de mensaje y el mensaje se envían a un cliente de correo electrónico a través de un protocolo de correo electrónico estándar.

El sistema incluye un módulo de generación de claves para generar una clave globalmente única. El identificador de mensaje se basa, al menos en parte, en la clave globalmente única. El módulo de eliminación elimina la clave globalmente única del uno o más dispositivos informáticos en respuesta al envío del identificador de mensaje al dispositivo destinatario, y recibir la selección del identificador de mensaje incluye recibir la clave globalmente única.

El sistema incluye un módulo de comprobación aleatoria de índice para generar un índice hash en base, al menos en parte, a la clave globalmente única, y el mensaje se almacena en la memoria no transitoria y no persistente usando el índice hash. El índice se comprueba aleatoriamente en base, al menos en parte, a una clave de dispositivo, la clave de dispositivo asociada con un dispositivo informático que comprende la memoria no transitoria y no persistente en la que se almacena el mensaje. El módulo de eliminación elimina el índice hash del uno o más dispositivos informáticos en respuesta al envío del identificador de mensaje al dispositivo destinatario.

El sistema incluye un módulo de generación de índice para generar un índice globalmente único en respuesta a la recepción del mensaje. El índice hash generado por el módulo de comprobación aleatoria de índice se basa, al menos en parte, en el índice globalmente único, el módulo de eliminación elimina el índice globalmente único del uno o más dispositivos informáticos en respuesta al envío del identificador de mensaje al dispositivo destinatario, el identificador de mensaje se basa, al menos en parte, en el índice globalmente único y recibir la selección del identificador de mensaje incluye recibir el índice globalmente único.

El sistema incluye un módulo de cifrado de mensajes para cifrar el mensaje antes de almacenar el mensaje en la memoria no transitoria y no persistente. Un módulo de generación de claves genera una clave globalmente única, el módulo de cifrado de mensajes cifra el mensaje usando una clave de cifrado antes de almacenar el mensaje en la memoria no transitoria y no persistente, en donde la clave de cifrado se basa, al menos en parte, en la clave globalmente única, y descifra el mensaje recuperado de la memoria no transitoria y no persistente antes de enviar el mensaje al dispositivo destinatario para su presentación, y el módulo de eliminación elimina la clave globalmente única y la clave de cifrado del uno o más dispositivos informáticos en respuesta al envío del identificador de mensaje al dispositivo destinatario, el identificador de mensaje en base, al menos en parte, a la clave globalmente única, y en donde recibir la selección del identificador de mensaje incluye recibir la clave globalmente única.

El módulo de eliminación establece un temporizador en base a un período de tiempo definido por el usuario y elimina el mensaje de la memoria no transitoria y no persistente del uno o más dispositivos informáticos en respuesta a un fallo al recibir la selección del identificador de mensaje desde el dispositivo destinatario dentro del período de tiempo definido por el usuario. El módulo de eliminación establece un temporizador en base a un período de tiempo definido por el sistema para el sistema y elimina el mensaje de la memoria no transitoria y no persistente del uno o más dispositivos informáticos en respuesta a un fallo al recibir la selección del identificador de mensaje desde el dispositivo destinatario dentro del período de tiempo definido por el sistema.

Las características y ventajas descritas en la presente memoria no incluyen todo y muchas características y ventajas adicionales serán evidentes en vista de las figuras y la descripción. Además, se debería observar que el lenguaje usado en la especificación se ha seleccionado principalmente con propósitos de legibilidad e instrucción, y no para limitar el alcance del tema descrito en la presente memoria.

Breve descripción de los dibujos

Las realizaciones se ilustran a modo de ejemplo, y no a modo de limitación en las figuras de los dibujos que se acompañan en los que se usan números de referencia iguales para referirse a elementos similares.

La Figura 1 ilustra un sistema para mensajería electrónica no retenida según una realización.

La Figura 2A es un diagrama de bloques que ilustra un dispositivo informático para mensajería no retenida según una realización.

La Figura 2B es un diagrama de bloques que ilustra un servidor de mensajería de no retención según una realización.

La Figura 3 es un diagrama de bloques que ilustra un módulo de mensajería no retenida según una realización.

La Figura 4 es un diagrama de flujo que ilustra un método para mensajería electrónica no retenida según una realización.

La Figura 5 es un diagrama de flujo que ilustra un método para mensajería electrónica no retenida según otra realización.

La Figura 6A-6B es un diagrama de flujo que ilustra un método para mensajería electrónica no retenida según otra realización más.

La Figura 7 es un diagrama de flujo que ilustra un método para verificación de un destinatario según una realización.

La Figura 8 es un diagrama de flujo que ilustra un método para generar un registro y una notificación de un evento según una realización.

Descripción detallada

Un sistema y un método para mensajería electrónica no retenida. En la siguiente descripción, con propósitos de explicación, se exponen numerosos detalles específicos con el fin de proporcionar una comprensión minuciosa de las realizaciones. Será evidente, no obstante, que las realizaciones se pueden practicar sin estos detalles específicos. En otros casos, las estructuras y dispositivos se muestran en forma de diagrama de bloques con el fin de evitar oscurecer las realizaciones. Por ejemplo, se describe a continuación una realización con referencia a interfaces de usuario y hardware particular. No obstante, las presentes realizaciones pueden aplicarse a diferentes tipos de dispositivos informáticos que pueden recibir datos y comandos, y dispositivos periféricos que proporcionan servicios.

Una referencia en la especificación a “una realización” significa que un rasgo, estructura o característica particular descrito en conexión con la realización se incluye en al menos una realización. Las apariciones de la frase “en una realización” en diversos lugares de la especificación no están refiriéndose todas necesariamente a la misma realización.

Algunas partes de las descripciones detalladas que siguen se presentan en términos de algoritmos y representaciones simbólicas de operaciones en bits de datos dentro de una memoria de ordenador. Estas descripciones y representaciones algorítmicas son los medios usados por los expertos en las técnicas de procesamiento de datos para transportar lo más eficazmente la sustancia de su trabajo a otros expertos en la técnica. Un algoritmo está aquí, y generalmente, concebido para ser una secuencia consistente en sí misma de pasos que conducen a un resultado deseado. Los pasos son aquellos que requieren manipulaciones físicas de cantidades físicas. Normalmente, aunque no necesariamente, estas cantidades toman la forma de señales eléctricas o magnéticas capaces de ser almacenadas, transferidas, combinadas, comparadas y manipuladas de otro modo. Ha demostrado ser conveniente a veces, principalmente por razones de uso común, hacer referencia a estas señales como bits, valores, elementos, símbolos, caracteres, términos, números o similares.

Se debería tener en cuenta, no obstante, que todos estos términos y otros similares se han de asociar con las cantidades físicas apropiadas y son meramente etiquetas convenientes aplicadas a estas cantidades. A menos que se exprese específicamente de otro modo, como es evidente a partir de la siguiente discusión, se aprecia que en toda la descripción, las discusiones que utilizan términos que incluyen, por ejemplo, “procesamiento” o “computación” o “cálculo” o “determinación” o “visualización” o similares, se refieren a la acción y los procesos de un sistema informático, o dispositivo informático electrónico similar, que manipula y transforma datos representados como cantidades físicas (electrónicas) dentro de los registros del sistema informático y las memorias en otros datos representados de manera similar como cantidades físicas dentro de la memorias o registros del sistema informático u otros de tales dispositivos de almacenamiento, transmisión o visualización de información.

Las presentes realizaciones también se refieren a un aparato para realizar las operaciones en la presente memoria. Este aparato se puede construir especialmente con los propósitos requeridos, o puede comprender un ordenador de propósito general activado selectivamente o reconfigurado por un programa de ordenador almacenado en el ordenador. Tal programa de ordenador se puede almacenar en un medio de almacenamiento legible por ordenador, incluyendo, pero no limitado a, cualquier tipo de disco, incluyendo discos flexibles, discos ópticos, CD-ROM y discos magnéticos, memorias de sólo lectura (ROM), memorias de acceso aleatorio (RAM), EPROM, EEPROM, tarjetas

magnéticas u ópticas, memorias rápidas incluyendo llaves USB con memoria no volátil o cualquier tipo de medio adecuado para almacenar instrucciones electrónicas, cada uno acoplado a un bus del sistema informático.

Las realizaciones pueden tomar la forma de una realización completamente de hardware, una realización completamente de software o una realización que contiene tanto elementos de hardware como de software. Una realización ejemplar se implementa en software, que incluye pero no se limita a microprogramas, software residente, microcódigo, etc.

Además, las realizaciones pueden tomar la forma de un producto de programa de ordenador accesible desde un medio utilizable por ordenador o legible por ordenador que proporciona código de programa para su uso por o en conexión con un ordenador o cualquier sistema de ejecución de instrucciones. Con los propósitos de esta descripción, un medio utilizable por ordenador o legible por ordenador puede ser cualquier aparato que pueda contener, almacenar, comunicar, propagar o transportar el programa para su uso por o en conexión con el sistema, aparato o dispositivo de ejecución de instrucciones.

Un sistema de procesamiento de datos adecuado para almacenar y/o ejecutar un código de programa incluirá al menos un procesador acoplado directa o indirectamente a elementos de memoria a través de un bus del sistema. Los elementos de memoria pueden incluir memoria local empleada durante una ejecución real del código de programa, almacenamiento masivo y memorias caché que proporcionan almacenamiento temporal de al menos algún código de programa con el fin de reducir el número de veces que el código se debe recuperar del almacenamiento masivo durante su ejecución.

Los dispositivos de entrada/salida o I/O (incluyendo, pero no limitados a, teclados, visualizadores, dispositivos de apuntamiento, etc.) se pueden acoplar al sistema o bien directamente o bien a través de controladores de I/O intervinientes.

Los adaptadores de red también se pueden acoplar al sistema para permitir que el sistema de procesamiento de datos llegue a ser acoplado a otros sistemas de procesamiento de datos o impresoras remotas o dispositivos de almacenamiento a través de redes públicas o privadas intervinientes. Módems, módem de cable y tarjetas Ethernet son sólo unos pocos de los tipos de adaptadores de red disponibles actualmente.

Finalmente, los algoritmos y visualizadores presentados en la presente memoria no están inherentemente relacionados con ningún ordenador u otro aparato en particular. Diversos sistemas de propósito general se pueden usar con programas según las enseñanzas en la presente memoria, o puede resultar conveniente construir un aparato más especializado para realizar los pasos requeridos del método. La estructura requerida para una variedad de estos sistemas aparecerá a partir de la descripción a continuación. Además, las presentes realizaciones no se describen con referencia a ningún lenguaje de programación particular. Se apreciará que se pueden usar una variedad de lenguajes de programación para implementar las enseñanzas de las realizaciones que se describen en la presente memoria.

Descripción general del sistema

La Figura 1 ilustra un diagrama de bloques de un sistema 100 para mensajería electrónica no retenida. El sistema 100 ilustrado incluye dispositivos cliente 115a, 115b y 115n (a los que también se hace referencia colectivamente como dispositivos cliente 115 o individualmente como dispositivo cliente 115) a los que se accede por los usuarios 125a, 125b y 125n (a los que también se hace referencia colectivamente como usuarios 125 o individualmente como usuario 125), servidores de mensajes no retenidos (NRM) 101a, 101b y 101c (a los que también se hace referencia colectivamente como servidores NRM 101 o individualmente como servidor NRM 101), un servidor de directorio de mensajes no retenidos 180, un servidor de terceros 190 y un servidor de autorizaciones 107. En la realización ilustrada, estas entidades se acoplan comunicativamente a través de una red 105. Aunque se ilustran tres dispositivos cliente 115, cualquier número de dispositivos cliente 115 está disponible para cualquier número de usuarios 125.

Los dispositivos cliente 115 en la Figura 1 se usan a modo de ejemplo. Mientras que la Figura 1 ilustra tres dispositivos cliente 115, la presente especificación se aplica a cualquier arquitectura de sistema que tenga uno o más dispositivos cliente 115. Además, aunque solamente una red 105 está acoplada a los dispositivos cliente 115, los servidores NRM 101 y el servidor de autorización 107, en la práctica, se puede conectar a las entidades cualquier número de redes 105. Además, aunque solamente se muestra un servidor de directorio de mensajes no retenidos 180, el sistema 100 puede incluir cualquier número de servidores de directorio de mensajes no retenidos 180. Además, aunque solamente se muestra un servidor de terceros 190, el sistema 100 puede incluir cualquier número de servidores de terceros 190.

Además, aunque solamente se muestra un servidor de autorización 107, el sistema 100 puede incluir cualquier número de servidores de autorización 107. En una realización, el sistema 100 incluye múltiples servidores de autorización 107 direccionados por un único URL, dirección o nombre de dominio. En una realización, el sistema 100 incluye múltiples servidores de autorización 107 al frente de un balanceador de carga (no mostrado).

Además, aunque la Figura 1 ilustra tres servidores NRM 101, la presente especificación se aplica a cualquier arquitectura de sistema que tenga uno o más servidores NRM 101. En una realización, el sistema 100 incluye servidores NRM 101 direccionados por un único URL, dirección o nombre de dominio. En una realización, el sistema 100 incluye múltiples servidores NRM 101 al frente de un balanceador de carga.

En una realización, se incluye un módulo de mensajería no retenida 220a en el servidor NRM 101a y es operable en el servidor NRM 101a, que se conecta a la red 105 a través de la línea de señal 104. En otra realización, el módulo de mensajería no retenida 220b está incluido en el servidor NRM 101b y es operable en el servidor NRM 101b, que se conecta a la red 105 a través de la línea de señal 106. En otra realización más, el módulo de mensajería no retenida 220c está incluido en el servidor NRM 101c y es operable en el servidor NRM 101c, que se conecta a la red 105 a través de la línea de señal 108. Se reconocerá que el módulo de mensajería no retenida 220a/220b/220c (al que se hace referencia generalmente como el módulo de mensajería no retenida 220) se puede almacenar en cualquier combinación de uno o más servidores NRM 101. En algunas realizaciones, el módulo de mensajería no retenida 220 incluye múltiples módulos distribuidos que cooperan unos con otros para realizar las funciones descritas a continuación. Los detalles que describen la funcionalidad y los componentes del módulo de mensajería no retenida 220 se explican con detalle adicional a continuación con respecto a la Figura 3.

La red 105 permite las comunicaciones entre los dispositivos cliente 115, los servidores NRM 101 y el servidor de autorización 107. De este modo, la red 105 puede incluir enlaces que usan tecnologías que incluyen, por ejemplo, Wi-Fi, Wi-Max, 2G, Sistema Universal de Telecomunicaciones Móviles (UMTS), 3G, Ethernet, 802.11, red digital de servicios integrados (RDSI), línea de abonado digital (DSL), modo de transferencia asíncrono (ATM), InfiniBand, Conmutación Avanzada Rápida PCI, etc. De manera similar, los protocolos de interconexión de redes usados en la red 105 pueden incluir el protocolo de control de transmisión/protocolo de Internet (TCP/IP), conmutación de etiquetas multiprotocolo (MPLS), el Protocolo de Datagramas de Usuario (UDP), el protocolo de transporte de hipertexto (HTTP), el protocolo simple de transferencia de correo (SMTP), el protocolo de transferencia de archivos (FTP), el protocolo ligero de acceso a directorios (LDAP), Acceso Múltiple por División de Código (CDMA), Acceso Múltiple por División de Código de Banda Ancha (WCDMA), Sistema Global para Comunicaciones Móviles (GSM), Acceso a Paquetes de Enlace Descendente de Alta Velocidad (HSDPA), etc. Los datos intercambiados sobre la red 105 se pueden representar usando tecnologías y/o formatos que incluyen el lenguaje de marcado de hipertexto (HTML), el lenguaje de marcado extensible (XML), la Notación de Objetos JavaScript (JSON), los Valores Separados por Comas (CSV), etc. Además , todos o algunos de los enlaces se pueden cifrar usando tecnologías de cifrado convencionales, por ejemplo, la capa de conexiones seguras (SSL), HTTP seguro (HTTPS) y/o redes privadas virtuales (VPN) o seguridad de Protocolo de Internet (IPsec). En otra realización, las entidades pueden usar tecnologías de comunicaciones de datos personalizadas y/o dedicadas en lugar de, o además de, las descritas anteriormente. Dependiendo de la realización, la red 105 también puede incluir enlaces a otras redes.

En una realización, la red 105 es una red parcialmente pública o totalmente pública, por ejemplo, Internet. La red 105 también puede ser una red privada o incluir una o más redes privadas distintas o lógicas (por ejemplo, redes privadas virtuales, Redes de Área Extensa (“WAN”) y/o Redes de Área Local (“LAN”)). Además, los enlaces de comunicación hacia y desde la red 105 pueden ser cableados o inalámbricos (es decir, transceptores terrestres o basados en satélites). En una realización, la red 105 es una red de área extensa o metropolitana basada en IP.

En la realización ilustrada, los dispositivos cliente 115a, 115b y 115n se acoplan a la red 105 a través de las líneas de señal 108, 112 y 114, respectivamente. El usuario 125a puede interactuar con el dispositivo cliente 115a. De manera similar, el usuario 125b puede interactuar con el dispositivo cliente 115b, y el usuario 125n puede interactuar con el dispositivo cliente 115n. El servidor NRM 101a se acopla comunicativamente con la red 105 a través de la línea de señal 104. El servidor NRM 101b se acopla comunicativamente con la red 105 a través de la línea de señal 106. El servidor NRM 101c se acopla comunicativamente con la red 105 a través de la línea de señal 108. El servidor de autorización 107 se acopla comunicativamente con la red 105 a través de la línea de señal 116. En una realización, el servidor de autorización 107 se acopla comunicativamente con el almacenamiento de datos 130 a través de la línea de señal 102. En una realización, el servidor de directorio de mensajes no retenidos 180 se acopla comunicativamente con la red 105 a través de la línea de señal 118. En una realización, los servidores de terceros 190 se acoplan comunicativamente con la red a través de la línea de señal 122.

En una realización, el almacenamiento de datos 130 almacena datos e información de cada usuario 125 del sistema 100. En una realización, los datos e información almacenados incluyen credenciales asociadas con cada usuario 125. Las credenciales se pueden basar, al menos en parte, en uno o más de lo que un usuario 125 sabe (por ejemplo, una contraseña), lo qué un usuario 125 es y lo que un usuario 125 posee. Ejemplos de credenciales incluyen, pero no se limitan a, un nombre de usuario y/o contraseña, un alias de usuario, una dirección de correo electrónico, un identificador biométrico, un identificador electrónico o cualquier otra cosa capaz de identificar a un usuario 125 y/o a una cuenta de usuario asociada. En una realización, que se trata a continuación, se incluye un dispositivo de almacenamiento 214 (véase la Figura 2) en el servidor de autorización 107 (es decir, una realización de un dispositivo informático 200) y el dispositivo de almacenamiento 214 almacena los datos e información de los usuarios 125 del servidor de autorizaciones 107.

En una realización, un dispositivo cliente 115a/115b/115n es un dispositivo electrónico que tiene un cliente de mensajería 120a/120b/120n (al que también se hace referencia colectivamente como clientes de mensajería 120 o

individualmente como cliente de mensajería) para interactuar con los diversos servidores 101, 107 y dispositivos cliente 115 del sistema 100 a través de la red 105. El dispositivo cliente 115 puede ser, por ejemplo, un ordenador portátil, un ordenador de sobremesa, una tableta, un teléfono móvil, un asistente digital personal (PDA), un dispositivo de correo electrónico móvil, un reproductor portátil de juegos, un reproductor portátil de música, un televisor con uno o más procesadores integrados en el mismo o acoplados al mismo, o cualquier otro dispositivo electrónico capaz de acceder a una red. Se reconocerá que son posibles otros tipos de dispositivos cliente 115. En una realización, el sistema 100 comprende una combinación de diferentes tipos de dispositivos cliente 115. Por ejemplo, una combinación de un ordenador personal, un teléfono móvil y una tableta. En una realización, el sistema comprende una combinación de diferentes clientes de mensajería 120. Por ejemplo, el cliente de mensajería 120a es el Cliente de Mensajería A ofrecido por la Compañía A, el cliente de mensajería 120b es el Cliente de Mensajería B ofrecido por la Compañía B y el cliente de mensajería 120c es el Cliente de Mensajería C ofrecido por la Compañía C. En una realización, el dispositivo cliente incluye un navegador web (no mostrado). El usuario 125 es un usuario humano del dispositivo cliente 115.

En una realización, el servidor de directorio de mensajes no retenidos 180 localiza un servidor NRM 101 para el almacenamiento y la recuperación de un mensaje por un servidor NRM 101. En una realización, el servidor de directorio de mensajes no retenidos 180 se comunica con los servidores NRM 101 para determinar qué servidores NRM almacenarán copias redundantes de un mensaje para copia de seguridad. En una realización, el servidor de directorio de mensajes no retenidos 180 no es un servidor separado, sino que se incorpora en un servidor NRM 101. Por ejemplo, el módulo de copia de seguridad de mensajes 322, tratado a continuación en referencia a la Figura 3, determina qué servidores NRM 101 almacenarán copias redundantes de un mensaje para copia de seguridad.

En una realización, los servidores de terceros 190 son un servidor asociado con un sistema de mensajería tradicional (por ejemplo, correo electrónico, mensaje instantáneo, redes sociales, microblogs, servicios de mensajes cortos (SMS), etc.) y proporciona servicios de mensajería tradicional (por ejemplo, correo electrónico, mensajería instantánea, redes sociales, microblogs, mensajes SMS, etc.). En una realización, el servidor de terceros 190 se usa por el sistema de mensajería no retenida 100 para enviar un identificador de mensaje (no el mensaje en sí mismo) a un destinatario. Por ejemplo, un identificador de mensaje se puede enviar como un “tweet” en Twitter, una publicación en Facebook, como un mensaje en LinkedIn, como un correo electrónico a través de Gmail, como un mensaje de texto SMS, etc. Se debería reconocer que los anteriores son meramente ejemplos de servicios de mensajería tradicionales y que existen otros. El identificador de mensaje se trata a continuación en referencia a la Figura 3. En una realización, el almacenamiento y envío de mensajes es exclusivo para los servidores NRM 101 y un servidor de terceros 190 u otro servidor (por ejemplo, el servidor de autorización 107) no se usa para enviar o almacenar un mensaje.

Ejemplo de dispositivo informático 200

La Figura 2A es un diagrama de bloques de un dispositivo informático 200 para mensajería no retenida según una realización. Como se ilustra en la Figura 2A, el dispositivo informático 200 incluye un adaptador de red 202 acoplado a un bus 204. Según una realización, también acoplado al bus 204 están al menos un procesador 206, una memoria 208, un adaptador de gráficos 210, un dispositivo de entrada 212, un dispositivo de almacenamiento 214. La memoria 208 almacena uno o más módulos, que se ejecutan por el procesador 206. En una realización, la funcionalidad del bus 204 se proporciona por un conjunto de chips de interconexión. El dispositivo informático 200 también incluye un visualizador 218, que se acopla al adaptador de gráficos 210.

El procesador 206 puede ser cualquier procesador de propósito general. El procesador 206 comprende una unidad de lógica aritmética, un microprocesador, un controlador de propósito general o alguna otra agrupación de procesadores para realizar cálculos y ejecutar código y rutinas. El procesador 206 se acopla al bus 204 para comunicación con los otros componentes del dispositivo informático 200. El procesador 206 procesa señales de datos y puede comprender diversas arquitecturas informáticas que incluyen una arquitectura de ordenador de conjunto de instrucciones complejas (CISC), una arquitectura de ordenador de conjunto de instrucciones reducidas (RISC), o una arquitectura que implementa una combinación de conjuntos de instrucciones. Aunque solamente se muestra un único procesador en la Figura 2A, se pueden incluir múltiples procesadores. La capacidad de procesamiento se puede limitar para soportar la visualización de imágenes y la captura y transmisión de imágenes. La capacidad de procesamiento podría ser suficiente para realizar tareas más complejas, incluyendo diversos tipos de extracción de características y muestreo. El dispositivo informático 200 también incluye un sistema operativo ejecutable por el procesador que incluye, pero no se limita a, sistemas operativos basados en WINDOWS®, MacOS X, Android o UNIX®. Se reconocerá que son posibles otros procesadores, sistemas operativos, sensores, visualizadores y configuraciones físicas.

La memoria 208 es un medio de almacenamiento no transitorio. La memoria 208 contiene instrucciones y/o datos que se pueden ejecutar por el procesador 206. En una realización, las instrucciones y/o datos almacenados en la memoria 208 comprenden código para realizar cualquiera y/o todas las técnicas descritas en la presente memoria. La memoria 208 puede ser un dispositivo de memoria de acceso aleatorio dinámica (DRAM), un dispositivo de memoria de acceso aleatorio estática (SRAM), memoria rápida u algún otro dispositivo de memoria. En una realización, la memoria 208 también incluye una memoria no volátil o dispositivo de almacenamiento permanente similar y medios, por ejemplo, una unidad de disco duro, una unidad de disco flexible, un dispositivo CD-ROM, un

dispositivo DVD-ROM, un dispositivo DVD-RAM, un dispositivo DVD-RW, un dispositivo de memoria rápida o algún otro dispositivo de almacenamiento masivo conocido para almacenar información sobre una base más permanente. En algunas realizaciones, la memoria 208 incluye solamente una memoria volátil. La memoria 208 se acopla por el bus 204 para comunicación con los otros componentes del dispositivo informático 200. En una realización, el dispositivo informático 200 es un servidor NRM 101 y un módulo de mensajería no retenida 220 se almacena en la memoria 208 y es ejecutable por el procesador 206. En una realización, el dispositivo informático 200 es un módulo de autorización 107 y un módulo de autenticación 240 se almacena en la memoria 208 y es ejecutable por el procesador 206. En una realización, el dispositivo informático 200 es un dispositivo cliente 115 y el cliente de mensajería 120 se almacena en la memoria 208 y es ejecutable por el procesador 206.

En una realización, el dispositivo informático 200 es un servidor NRM 101 e incluye un módulo de mensajería no retenida 220. El módulo de mensajería no retenida 220, al que se hace referencia ocasionalmente en la presente memoria como “módulo NRM 220”, incluye código y rutinas ejecutables por el procesador 206 para mensajería electrónica no retenida. En una realización, el módulo de mensajería no retenida 220 es un conjunto de instrucciones ejecutables por el procesador 206. En otra realización, el módulo de mensajería no retenida 220 se almacena en la memoria 208 y es accesible y ejecutable por el procesador 206. Los detalles que describen la funcionalidad y los componentes del módulo de mensajería no retenida 220 se explican en más detalle a continuación en referencia a la Figura 3.

En una realización, el dispositivo informático 200 es un servidor de autorización 107 e incluye un módulo de autenticación 240. El módulo de autenticación 240 incluye código y rutinas ejecutables por el procesador 206 para autenticar credenciales y autorizar el uso del sistema de mensajería no retenida 100. En una realización, el módulo de autenticación 240 es un conjunto de instrucciones ejecutables por el procesador 206. En otra realización, el módulo de autenticación 240 se almacena en la memoria 208 y es accesible y ejecutable por el procesador 206.

El módulo de autenticación 240 autentica las credenciales y autoriza el uso del sistema de mensajería no retenida 100. En una realización, el módulo de autenticación 240 compara las credenciales de usuario proporcionadas por un usuario con las almacenadas por el servidor de autorización 107 (por ejemplo, en un almacén de datos 130 o dispositivo de almacenamiento 214 del servidor de autorización 107), y autentica al usuario si hay una coincidencia. En una realización, las credenciales de usuario incluyen un nombre de usuario y contraseña y el nombre de usuario y la contraseña de comprobación aleatoria de cada usuario se almacenan (por ejemplo, como un archivo plano o una base de datos relacional) en el almacén de datos 130 o el dispositivo de almacenamiento 214 del servidor de autorización 107. En una realización, las contraseñas se comprueban aleatoriamente para evitar la adquisición y explotación ilegítimas de las contraseñas por parte de un pirata informático u otro usuario malvado. En una realización, se incluyen múltiples servidores de autorización 107 en el sistema de mensajería no retenida 100 y los múltiples servidores de autorización 107 comparten una base de datos común de credenciales de usuario. Se reconocerá que otras realizaciones pueden incluir credenciales distintas de, o diferentes de, nombre de usuario y contraseña.

En una realización, el dispositivo informático 200 es un dispositivo cliente 115 e incluye un cliente de mensajería 120. El cliente de mensajería 120 incluye código y rutinas ejecutables por el procesador 206 para enviar y recibir mensajes sobre el sistema de mensajería electrónica no retenida 100. En una realización, el cliente de mensajería 120 es un conjunto de instrucciones ejecutables por el procesador 206. En otra realización, el cliente de mensajería 120 se almacena en la memoria 208 y es accesible y ejecutable por el procesador 206.

Un cliente de mensajería 120 puede incluir uno o más de un cliente de correo electrónico, cliente de mensajería instantánea o cualquier otro cliente de mensajería. Con propósitos de claridad y simplificación, muchos de los ejemplos contenidos en la presente memoria suponen que el cliente de mensajería 120 es un cliente de correo electrónico. No obstante, se reconocerá que la descripción se puede aplicar también a otros tipos de clientes de mensajería 120.

En una realización, el usuario configura el cliente de mensajería 120 de la misma forma que lo haría el usuario para un servicio de mensajería típico. Por ejemplo, en una realización, el remitente añade una cuenta de servidor de correo electrónico al cliente de correo electrónico de la misma manera que cualquier otra cuenta de correo electrónico, excepto que el servidor de correo saliente para la cuenta sea la dirección, o el nombre de dominio, de los servidores NRM 101.

En una realización, el cliente de mensajería 120 permite que el usuario redacte un mensaje (por ejemplo, que incluya uno o más de un asunto, texto, audio, video, imágenes, archivos, archivos adjuntos, etc.), identifique a un destinatario y envíe el mensaje. En una realización, las interfaces de usuario para redactar un mensaje a ser enviado usando el sistema de mensajería no retenida 100 pueden ser idénticas, o casi idénticas, a aquéllas para enviar un mensaje tradicional usando el cliente de mensajería 120. En una realización, el cliente de mensajería 120 formatea el mensaje igual que un mensaje a ser enviado en un sistema de mensajería tradicional (por ejemplo, correo electrónico, mensaje instantáneo, etc.). Por ejemplo, supongamos que el cliente de mensajería 120 es un cliente de correo electrónico; en una realización, el cliente de correo electrónico formatea el mensaje usando un protocolo de correo electrónico estándar (por ejemplo, SMTP) para enviar a través del sistema de mensajería no retenida 100. Se reconocerá que lo anterior es meramente un ejemplo de un formato y que existen otros.

En una realización, el cliente de mensajería 120 recibe y almacena las preferencias de usuario localmente en el dispositivo cliente 115. Ejemplos de preferencias de usuario incluyen, pero no se limitan a, uno o más de si el remitente de un mensaje se identifica con el destinatario, un período de tiempo definido por el usuario que define la vida útil de un mensaje en el servidor o servidores NRM 101 y un evento del que se mide la vida útil. Algunos de estos ejemplos se tratan aún más a continuación. Se reconocerá que los anteriores son meramente ejemplos y existen otros ejemplos de preferencias de usuario. En una realización, el cliente de mensajería 120 permite que un usuario destinatario guarde o imprima localmente un mensaje enviado a través del sistema de mensajes no retenidos 100. En una realización, suponiendo que un usuario decida no guardar o imprimir localmente un mensaje entregado a través del sistema 100, ese mensaje se pierde permanentemente y es irrecuperable, debido a que los mensajes se eliminan automáticamente del sistema 100 después de la recuperación/entrega.

El dispositivo de almacenamiento 214 es cualquier dispositivo capaz de contener datos, como un disco duro, una memoria de sólo lectura de disco compacto (CD-ROM), DVD, o un dispositivo de memoria de estado sólido. El dispositivo de almacenamiento 214 es un dispositivo de memoria no volátil o un dispositivo y medios de almacenamiento permanente similares. El dispositivo de almacenamiento 214 almacena datos e instrucciones para el procesador 206 y comprende uno o más dispositivos que incluyen una unidad de disco duro, una unidad de disco flexible, un dispositivo CD-ROM, un dispositivo DVD-ROM, un dispositivo DVD-RAM, un dispositivo DVD-RW, un dispositivo de memoria rápida o algún otro dispositivo de almacenamiento masivo. En una realización, el dispositivo de almacenamiento 214 almacena datos e información de un usuario 125. Por ejemplo, en una realización, el dispositivo informático 200 es un servidor de autorización 107 y el dispositivo de almacenamiento 214 almacena los datos de usuario y la información tratada anteriormente en referencia al almacenamiento de datos 130 (por ejemplo, credenciales). En otro ejemplo, en una realización, el dispositivo informático 200 es un dispositivo cliente 115 y el dispositivo de almacenamiento 214 almacena mensajes.

El dispositivo de entrada 212 puede incluir un ratón, una bola de seguimiento u otro tipo de dispositivo de apuntamiento para introducir datos en el dispositivo informático 200. El dispositivo de entrada 212 también puede incluir un teclado, por ejemplo, un teclado QWERTY, un escáner de código gráfico o cualquier otro teclado físico o virtual en cualquier idioma. El dispositivo de entrada 212 también puede incluir un micrófono, una cámara web o un dispositivo similar de captura de audio o video. El adaptador de gráficos 210 muestra imágenes y otra información en el visualizador 218. El visualizador 218 es de un tipo convencional, por ejemplo, un visualizador de cristal líquido (LCD) o cualquier otro dispositivo de visualización, pantalla, pantalla táctil o monitor equipado de manera similar. El visualizador 218 representa cualquier dispositivo equipado para mostrar imágenes y datos electrónicos como se describe en la presente memoria. El adaptador de red 202 acopla el dispositivo informático 200 a una red de área local o extensa.

Como se conoce en la técnica, un dispositivo informático 200 puede tener diferentes componentes y/u otros distintos de los mostrados en la Figura 2A. Por ejemplo, el dispositivo informático 200 puede tener altavoces u otra forma de salida de audio. Además, el dispositivo informático 200 puede carecer de ciertos componentes ilustrados. Por ejemplo, en una realización, el dispositivo informático 200 es un servidor de autorización 107 y carece de un dispositivo de entrada 212, adaptador de gráficos 210 y/o visualizador 218. Además, el dispositivo de almacenamiento 214 puede ser local y/o remoto del dispositivo informático 200 (por ejemplo, una red de área de almacenamiento (SAN)).

Ahora con referencia a la Figura 2B, que ilustra un diagrama de bloques de un servidor NRM 101 según una realización. En un ejemplo, el dispositivo informático 200 es un servidor NRM 101 y, según la realización ilustrada, carece de un dispositivo de entrada 212, dispositivo de almacenamiento 214, adaptador de gráficos 210 y un visualizador 218. Además, según una realización, un servidor NRM 101 incluye una memoria no persistente 207 y una memoria persistente 205. Las memorias 205, 207 se acoplan por el bus 204 para su comunicación con los otros componentes del servidor NRM 101.

En una realización, la memoria no persistente 207 almacena un mensaje 230a, 230n enviado usando el sistema de mensajería no retenida 100 pendiente de entrega al destinatario. En una realización, la memoria no persistente 207 es una memoria volátil. Ejemplos de memoria volátil incluyen, pero no se limitan a, un dispositivo de memoria de acceso aleatorio dinámica (DRAM), un dispositivo de memoria de acceso aleatorio estática (SRAM), una memoria caché de procesador, etc.

En una realización, el servidor NRM 101 incluye una memoria persistente 205 para almacenar el módulo de mensajería no retenida 220. Ejemplos de memoria persistente incluyen una memoria no volátil o dispositivos y medios de almacenamiento permanente similares, por ejemplo, una unidad de disco duro, una unidad de disco flexible, un dispositivo CD-ROM, un dispositivo DVD-ROM, un dispositivo DVD-RAM, un dispositivo DVD-RW, un dispositivo de memoria rápida u algún otro dispositivo de almacenamiento masivo para almacenar información sobre una base más permanente. En una realización ejemplar, la memoria persistente 205 es una memoria de sólo lectura (ROM) e incapaz de almacenar mensajes enviados usando el sistema de mensajería no retenida 100. En una realización, el dispositivo informático 200 es un servidor NRM 101 y un módulo de mensajería no retenida 220 se almacena en la memoria persistente 205 y es ejecutable por el procesador 206. Dado que la memoria no persistente 207 (por ejemplo, RAM) no es permanente y generalmente es más costosa y proporciona menos capacidad que la memoria persistente 205 (por ejemplo, una unidad de disco duro), las realizaciones en las que el servidor NRM 101

carece de una memoria escribible y persistente o una memoria totalmente persistente pueden disminuir las posibilidades y desincentivar mensajes de retención indefinidamente en el sistema de mensajería no retenida 100.

Como es sabido en la técnica, el dispositivo informático 200 está adaptado para ejecutar módulos de programas informáticos para proporcionar la funcionalidad descrita en la presente memoria. Como se usa en la presente memoria, el término “módulo” se refiere a lógica de programa de ordenador utilizada para proporcionar la funcionalidad especificada. De este modo, un módulo se puede implementar en hardware, microprogramas y/o software. En una realización, los módulos de programa se ejecutan por el procesador 206.

Las realizaciones de las entidades descritas en la presente memoria pueden incluir otros módulos y/o diferentes que los descritos aquí. Además, la funcionalidad atribuida a los módulos se puede realizar por otros módulos o diferentes en otras realizaciones. Además, esta descripción omite ocasionalmente el término “módulo” con propósitos de claridad y comodidad.

Ejemplo de módulo de mensajería no retenida 220

Con referencia ahora a la Figura 3, el módulo de mensajería no retenida 220 se muestra con más detalle según una realización. La Figura 3 es un diagrama de bloques del módulo de mensajería no retenida 220 incluido en un servidor NRM 101.

En una realización, el módulo de mensajería no retenida 220 comprende una interfaz de comunicaciones 302, un módulo receptor de mensajes 304, un módulo de almacenamiento de mensajes y generación de identificador 318, un módulo de recuperación de mensajes 322 y un módulo de eliminación 324. En algunas realizaciones, el módulo de mensajería no retenida 220 también incluye opcionalmente uno o más de un módulo de solicitud de autenticación 306, un módulo de generación de claves 308, un módulo de generación de índices 310, un módulo de comprobación aleatoria de índice 312, un módulo de generación de claves de cifrado 314, un módulo de cifrado de mensajes 316 y un módulo de copia de seguridad de mensajes 320, un módulo de verificación de destinatario 326 y un módulo de registro y notificación 328.

Se reconocerá que los módulos 302, 304, 306, 308, 310, 312, 314, 316, 318, 320, 322, 324, 326, 326 comprendidos en el módulo de mensajería no retenida 220 no están necesariamente todos en el mismo servidor NRM 101. En una realización, los módulos 302, 304, 306, 308, 310, 312, 314, 316, 318, 320, 322, 324, 326, 326 se distribuyen a través de múltiples servidores NRM 101. Por ejemplo, en una realización, el módulo de copia de seguridad de mensajes 316 se incluye en el servidor NRM 101a y los otros módulos 302, 304, 306, 308, 310, 312, 314, 318, 320, 322, 324, 326 y 328 se incluyen en el servidor NRM 101b. Se reconocerá que lo anterior es meramente un ejemplo de distribución de módulos a través de múltiples servidores NRM 101 y que existen otros ejemplos.

La interfaz de comunicación 302 incluye código y rutinas para manejar las comunicaciones entre el módulo receptor de mensajes 304, el módulo de solicitud de autenticación 306 (dependiendo de la realización), el módulo de generación de claves 308 (dependiendo de la realización), el módulo de generación de índices 310 (dependiendo de la realización), el módulo de comprobación aleatoria de índice 312 (dependiendo de la realización), el módulo de generación de claves de cifrado 314 (dependiendo de la realización), el módulo de cifrado de mensajes 316 (dependiendo de la realización), el módulo de almacenamiento de mensajes y generación de identificador 318, el módulo de copia de seguridad de mensajes 320 (dependiendo de la realización), el módulo de recuperación de mensajes 322, el módulo de eliminación 324, el módulo de verificación de destinatario 326 (dependiendo de la realización), el módulo de registro y notificación 328 (dependiendo de la realización) y otros componentes del servidor NRM 101. En una realización, la interfaz de comunicación 302 es un conjunto de instrucciones ejecutables por el procesador 206. En otra realización, la interfaz de comunicación 302 se almacena en la memoria persistente 205 y es accesible y ejecutable por el procesador 206. En cualquier realización, la interfaz de comunicación 302 está adaptada para cooperación y comunicación con el procesador 206, otros componentes del servidor NRM 101 y otros componentes del módulo de mensajería no retenida 220.

La interfaz de comunicación 302 maneja las comunicaciones entre el módulo receptor de mensajes 304, el módulo de solicitud de autenticación 306 (dependiendo de la realización), el módulo de generación de claves 308 (dependiendo de la realización), el módulo de generación de índices 310 (dependiendo de la realización), el módulo de comprobación aleatoria de índice 312 (dependiendo de la realización), el módulo de generación de claves de cifrado 314 (dependiendo de la realización), el módulo de cifrado de mensajes 316 (dependiendo de la realización), el módulo de almacenamiento de mensajes y generación de identificador 318, el módulo de copia de seguridad de mensajes 320 (dependiendo de la realización), el módulo de recuperación de mensajes 322, el módulo de eliminación 324, el módulo de verificación de destinatario 326 (dependiendo de la realización), el módulo de registro y notificación 328 (dependiendo de la realización) y otros componentes del servidor NRM 101. Por ejemplo, en una realización, la interfaz de comunicación 202 se comunica con el módulo de generación de claves 308 y el módulo de comprobación aleatoria de índice 312 para pasar la salida del módulo de generación de claves 308 (es decir, una clave globalmente única) al módulo de comprobación aleatoria de índice 312. No obstante, esta descripción puede omitir ocasionalmente la mención de la interfaz de comunicación 302 con propósitos de claridad y comodidad. Por ejemplo, con propósitos de claridad y comodidad, el escenario anterior se puede describir como el módulo de generación de claves 308 que pasa la clave globalmente única al módulo de comprobación aleatoria de índice 312.

El módulo receptor de mensajes 304 incluye código y rutinas para recibir un mensaje. En una realización, el módulo receptor de mensajes 304 es un conjunto de instrucciones ejecutables por el procesador 206. En otra realización, el módulo receptor de mensajes 304 se almacena en la memoria persistente 205 y es accesible y ejecutable por el procesador 206. En cualquier realización, el módulo receptor de mensajes 304 se adapta para cooperación y comunicación con el procesador 206, otros componentes del servidor NRM 101 y otros componentes del módulo de mensajería no retenida 220.

El módulo receptor de mensajes 304 recibe un mensaje. En una realización, el módulo receptor de mensajes 304 recibe un mensaje del cliente de mensajería de un usuario remitente 120. Por simplicidad y claridad, se hace referencia ocasionalmente a un usuario 125 que envía un mensaje como “remitente”. Por ejemplo, el módulo receptor de mensajes 304 se acopla comunicativamente para recibir el mensaje desde el cliente de mensajería 120 del dispositivo de cliente de un remitente 115 a través de la red 105.

Un cliente de mensajería 120 puede incluir uno o más de un cliente de correo electrónico, cliente de mensajería instantánea o cualquier otro cliente de mensajería. En una realización, el módulo receptor de mensajes 304 recibe un mensaje desde un cliente de mensajería 120 con poca o ninguna modificación al cliente de mensajería 120. Por ejemplo, en una realización, el módulo receptor de mensajes 304 recibe mensajes de un cliente de correo electrónico, tal como Microsoft Outlook, Mozilla Thunderbird, Opera Mail, etc. Ejemplos de pequeñas modificaciones incluyen la introducción de un servidor de correo electrónico saliente, la introducción de una cuenta de correo electrónico, la instalación de un enchufable, un complemento, un paquete de expansión, etc. Se reconocerá que los ejemplos anteriores son meramente ejemplos de clientes de correo electrónico existentes y disponibles comercialmente y que existen otros ejemplos de clientes de mensajería y clientes de correo electrónico.

En una realización, el módulo receptor de mensajes 304 recibe un mensaje que incluye un identificador de destinatario y un cuerpo de mensaje. El identificador de destinatario es un identificador único asociado con el destinatario deseado del mensaje del remitente. Ejemplos de un identificador de destinatario incluyen, pero no se limitan a, direcciones de correo electrónico, números de teléfono, nombres de usuario o cualquier otro identificador asociado con un usuario y único dentro del sistema de mensajería no retenida 100. El cuerpo de un mensaje incluye el contenido, el cual el remitente desea comunicar al destinatario. El cuerpo de mensaje puede incluir, por ejemplo, uno o más de texto, audio, video, imágenes, archivos, archivos adjuntos, etc.

En una realización, el mensaje recibido tiene un formato idéntico al de un mensaje enviado usando un sistema de mensajería tradicional. Por ejemplo, supongamos que el cliente de mensajería 120 es un cliente de correo electrónico; en una realización, el módulo receptor de mensajes 304 recibe un mensaje formateado usando un protocolo de correo electrónico estándar (por ejemplo, SMTP). Se reconocerá que lo anterior es meramente un ejemplo de un formato y que existen otros y se puede usar sin apartarse de las enseñanzas en la presente memoria.

En una realización, el módulo receptor de mensajes 304 pasa el mensaje recibido al módulo de almacenamiento de mensajes y generación de identificador 318. Por ejemplo, el módulo receptor de mensajes 304 se acopla comunicativamente al módulo de almacenamiento de mensajes y generación de identificador 318 para enviar el mensaje recibido al módulo de almacenamiento de mensajes y generación de identificador 318. En otra realización, el módulo receptor de mensajes 304 pasa el mensaje recibido al módulo de cifrado de mensajes 316. Por ejemplo, el módulo receptor de mensajes 304 se acopla comunicativamente al módulo de cifrado de mensajes 316 para enviar el mensaje recibido al módulo de cifrado de mensajes 316.

En algunas realizaciones, puede ser deseable autenticar usuarios. Por ejemplo, puede ser deseable autenticar a un usuario con el fin de que el usuario acceda al sistema 100 y/o a un rasgo o funcionalidad del mismo. Por ejemplo, puede ser deseable autenticar al usuario antes de uno o más de redactar un mensaje, enviar un mensaje, enviar un identificador de mensaje, etc. En una realización tal, el módulo de mensajería no retenida 220 incluye un módulo de solicitud de autenticación 306 opcional.

El módulo de solicitud de autenticación 306 incluye código y rutinas para solicitar autenticación de usuario. En una realización, el módulo de solicitud de autenticación 306 es un conjunto de instrucciones ejecutables por el procesador 206. En otra realización, el módulo de solicitud de autenticación 306 se almacena en la memoria persistente 205 y es accesible y ejecutable por el procesador 206. En cualquier realización, el módulo de solicitud de autenticación 306 se adapta para cooperación y comunicación con el procesador 206, otros componentes del servidor NRM 101 y otros componentes del módulo de mensajería no retenida 220.

El módulo de solicitud de autenticación 306 solicita autenticación de usuario. En algunas realizaciones, la autenticación de usuario se basa en credenciales. En una realización, el módulo de solicitud de autenticación 306 solicita autenticación de usuario desde un servidor de autorización 107. Por ejemplo, supongamos que el servidor NRM 101 no almacena credenciales debido a que, por ejemplo, el servidor NRM 101 carece de un dispositivo de almacenamiento 214 y una memoria persistente escribible 205.

En una realización, el módulo de solicitud de autenticación 306 solicita las credenciales de usuario y pasa las credenciales, recibidas desde el usuario 125, al servidor de autorización 107 como parte de la solicitud de autenticación de usuario. En otra realización, el módulo de solicitud de autenticación 306 pasa una solicitud de

autenticación de usuario al servidor de autorización 107, y el servidor de autorización 107 solicita y recibe las credenciales de usuario. En cualquier realización, el servidor de autorización 107 determina si el usuario está autorizado en base, al menos en parte, a las credenciales e informa al módulo de solicitud de autenticación 306. Por ejemplo, el servidor de autorización 107 determina si el usuario está autorizado en base a si un nombre de usuario y una contraseña proporcionados por el usuario coinciden con un nombre de usuario y contraseña asociados almacenados por el servidor de autorización 107 y notifica al módulo de solicitud de autenticación 306 si el usuario está autenticado o no.

En algunas realizaciones, uno o más de los módulos del módulo de mensajería no retenida 220 se ejecutan sujetos a la autenticación de usuario. Por ejemplo, en una realización, el módulo receptor de mensajes 304 se ejecuta pendiente de la autenticación de usuario del usuario remitente. En otro ejemplo, en una realización, el módulo de almacenamiento de mensajes y generación de identificador 318 se ejecuta pendiente de la autenticación de usuario del usuario remitente.

En una realización, el módulo de solicitud de autenticación 306 pasa la autenticación de usuario a uno o más de los otros módulos del módulo de mensajería no retenida 220. Por ejemplo, el módulo de solicitud de autenticación 306 se acopla comunicativamente a uno o más de los otros módulos del módulo de mensajería no retenida 220 para enviar la autenticación de usuario a uno o más de los otros módulos del módulo de mensajería no retenida 220.

El módulo de generación de claves 308 opcional incluye código y rutinas para generar una clave globalmente única para cada mensaje. En una realización, el módulo de generación de claves 308 es un conjunto de instrucciones ejecutables por el procesador 206. En otra realización, el módulo de generación de claves 308 se almacena en la memoria persistente 205 y es accesible y ejecutable por el procesador 206. En cualquier realización, el módulo de generación de claves 308 se adapta para cooperación y comunicación con el procesador 206, otros componentes del servidor NRM 101 y otros componentes del módulo de mensajería no retenida 220.

El módulo de generación de claves 308 genera una clave globalmente única para cada mensaje. Una clave globalmente única es un sólo objeto único que es único en el mundo en todos los dispositivos informáticos. Por ejemplo, en una realización, la clave globalmente única es un número aleatorio de 128 bits, que tiene 2^{128} posibilidades (aproximadamente $3{,}48x10^{38}$) y, por lo tanto, extremadamente improbable que tenga conflictos o sea adivinado. En otro ejemplo, la clave globalmente única se genera de manera similar a un Identificador Globalmente Único (GUID).

En una realización, el módulo de generación de claves 308 también genera una clave de dispositivo. Una clave de dispositivo es una clave globalmente única. En una realización, la clave de dispositivo es extremadamente grande de modo que la clave de dispositivo sea virtualmente imposible de ser adivinada o descifrada. Por ejemplo, en una realización, la clave de dispositivo es un número aleatorio de 128 bits, que tiene 2^{128} posibilidades (aproximadamente $3{,}48x10^{38}$) y, por lo tanto, extremadamente improbable que tenga conflictos o sea adivinado. En otro ejemplo, la clave de dispositivo se genera similar a un Identificador Globalmente Único (GUID). En una realización, la clave de dispositivo se conoce solamente por el servidor NRM 101 asociado con la clave de dispositivo. Por ejemplo, en una realización, el módulo de generación de claves 308 del servidor NRM 101a genera una clave de dispositivo asociada con y conocida solamente por el servidor NRM 101a, y el módulo de generación de claves 308 del servidor NRM 101b genera una clave de dispositivo asociada con y conocida solamente por el servidor NRM 101b. En una realización, la clave de dispositivo se asocia con un servidor NRM 101, pero se conoce por al menos otro servidor NRM 101.

En una realización, la clave de dispositivo es dinámica. Por ejemplo, en algunas realizaciones, el módulo de generación de claves 308 genera una nueva clave de dispositivo cada vez que se pone en marcha el servidor NRM 101 o después de detectar un acceso (no) autorizado y de eliminar de la memoria no persistente todos los mensajes, claves, índices, etc. En una realización alternativa, la clave de dispositivo puede ser una clave estática y única asignada por el fabricante. Independientemente de si la clave de dispositivo es estática o dinámica, en algunas realizaciones, cada copia de un mensaje que puede existir en múltiples servidores NRM 101 (por ejemplo, para copia de seguridad) puede tener un índice hash y una clave de cifrado diferentes para cada copia del mismo mensaje en los diversos servidores NRM 101, debido a que cada servidor NRM 101 está asociado con una clave de dispositivo diferente.

En una realización, el módulo de generación de claves 308 pasa la clave globalmente única a uno o más del módulo de comprobación aleatoria de índice 312, el módulo de generación de claves de cifrado 314 y el módulo de almacenamiento de mensajes y generación de identificador 318. Por ejemplo, el módulo de generación de claves 308 se acopla comunicativamente a uno o más del módulo de comprobación aleatoria de índice 312, el módulo de generación de claves de cifrado 314 y el módulo de almacenamiento de mensajes y generación de identificador 318 para enviar la clave globalmente única a uno o más del módulo de comprobación aleatoria de índice 312, el módulo de generación de claves de cifrado 314 y el módulo de almacenamiento de mensajes y generación de identificador 318.

En una realización, el módulo de generación de claves 308 pasa la clave de dispositivo a uno o más del módulo de comprobación aleatoria de índice 312, el módulo de generación de claves de cifrado 314 y el módulo de

almacenamiento de mensajes y generación de identificador 318. Por ejemplo, el módulo de generación de claves 308 se acopla comunicativamente a uno o más del módulo de comprobación aleatoria de índice 312, el módulo de generación de claves de cifrado 314 y el módulo de almacenamiento de mensajes y generación de identificador 318 para enviar la clave de dispositivo a uno o más del módulo de comprobación aleatoria de índice 312, el módulo de generación de claves de cifrado 314 y el módulo de almacenamiento de mensajes y generación de identificador 318.

El módulo de generación de índices 310 opcional incluye código y rutinas para generar un índice globalmente único. En una realización, el módulo de generación de índices 310 es un conjunto de instrucciones ejecutables por el procesador 206. En otra realización, el módulo de generación de índices 310 se almacena en la memoria persistente 205 y es accesible y ejecutable por el procesador 206. En cualquier realización, el módulo de generación de índices 310 se adapta para cooperación y comunicación con el procesador 206, otros componentes del servidor NRM 101 y otros componentes del módulo de mensajería no retenida 220.

El módulo de generación de índices 310 opcional genera un índice globalmente único para cada mensaje. La generación de un índice globalmente único es opcional y el sistema de mensajes no retenidos 100 funciona y es seguro sin un índice globalmente único. No obstante, en una realización, la generación de un índice globalmente único puede aumentar la cantidad de esfuerzo necesario para localizar y descifrar un mensaje, añadiendo por ello seguridad adicional al sistema.

En una realización, el módulo de generación de índices 310 pasa el índice globalmente único al módulo de comprobación aleatoria de índice 312. Por ejemplo, el módulo de generación de índices 310 se acopla comunicativamente al módulo de comprobación aleatoria de índice 312 para enviar el índice globalmente único al módulo de comprobación aleatoria de índice 312.

El módulo de comprobación aleatoria de índice 312 opcional incluye código y rutinas para generar un índice hash. En una realización, el módulo de comprobación aleatoria de índice 312 es un conjunto de instrucciones ejecutables por el procesador 206. En otra realización, el módulo de comprobación aleatoria de índice 312 se almacena en la memoria 208 y es accesible y ejecutable por el procesador 206. En cualquier realización, el módulo de comprobación aleatoria de índice 312 se adapta para cooperación y comunicación con el procesador 206, otros componentes del servidor NRM 101 y otros componentes del módulo de mensajería no retenida 220.

El módulo de comprobación aleatoria de índice 312 genera un índice hash. En una realización, el módulo de comprobación aleatoria de índice 312 genera un índice hash en base a una clave globalmente única. Por ejemplo, en una realización, el módulo de comprobación aleatoria de índice 312 genera un índice hash mediante comprobación aleatoria de la clave globalmente única. En una realización, el módulo de comprobación aleatoria de índice 312 genera un índice hash en base a una clave globalmente única y una clave de dispositivo. Por ejemplo, en una realización, el módulo de comprobación aleatoria de índice 312 genera un índice hash mediante comprobación aleatoria de la clave globalmente única como la sal y la clave de dispositivo.

En una realización, el módulo de comprobación aleatoria de índice 312 genera un índice hash en base a la clave globalmente única recibida desde el módulo de generación de claves 308 y el índice globalmente único recibido desde el módulo de generación de índices 310. Por ejemplo, en una realización, el módulo de comprobación aleatoria de índice 312 genera un índice hash mediante comprobación aleatoria de la clave globalmente única como la sal y el índice globalmente único. Por ejemplo, en otra realización, el módulo de comprobación aleatoria de índice 312 genera un índice hash mediante comprobación aleatoria de la clave globalmente única como la sal en combinación con el índice globalmente único y la clave de dispositivo.

En una realización, el módulo de comprobación aleatoria de índice 312 pasa el índice hash al módulo de almacenamiento de mensajes y generación de identificador 318. Por ejemplo, el módulo de comprobación aleatoria de índice 312 se acopla comunicativamente al módulo de almacenamiento de mensajes y generación de identificador 318 para enviar el índice hash al módulo de almacenamiento de mensajes y generación de identificador 318.

El módulo de generación de claves de cifrado 314 incluye código y rutinas para generar una clave de cifrado. En una realización, el módulo de generación de claves de cifrado 314 es un conjunto de instrucciones ejecutables por el procesador 206. En otra realización, el módulo de generación de claves de cifrado 314 se almacena en la memoria persistente 205 y es accesible y ejecutable por el procesador 206. En cualquier realización, el módulo de generación de claves de cifrado 314 se adapta para cooperación y comunicación con el procesador 206, otros componentes del servidor NRM 101 y otros componentes del módulo de mensajería no retenida 220.

El módulo de generación de claves de cifrado 314 genera una clave de cifrado. En algunas realizaciones, el módulo de generación de claves de cifrado 314 genera una clave de cifrado para un mensaje en base a la clave globalmente única asociada con ese mensaje. Por lo tanto, en algunas realizaciones, la clave de cifrado es única para cada mensaje.

En una realización, el módulo de generación de claves de cifrado 314 genera una clave de cifrado en base a la clave globalmente única. Por ejemplo, en una realización, el módulo de generación de claves de cifrado 314 genera una clave de cifrado usando la clave globalmente única. En una realización, el módulo de generación de claves de

cifrado 314 genera una clave de cifrado en base a la clave globalmente única y la clave de dispositivo. Por ejemplo, en una realización, el módulo de generación de claves de cifrado 314 genera una clave de cifrado combinando la clave globalmente única y la clave de dispositivo, o usando la clave de dispositivo como la clave de cifrado y la clave globalmente única como el vector de inicialización para el cifrado.

En algunas realizaciones, que incluyen tanto el módulo de comprobación aleatoria de índice 312 como el módulo de generación de claves de cifrado 314, el módulo de generación de claves de cifrado 314 genera una clave de cifrado usando un proceso diferente al que usa el módulo de comprobación aleatoria de índice 312 para generar el índice hash. Por ejemplo, en una realización, el módulo de generación de claves de cifrado 314 genera la clave de cifrado usando la clave globalmente única en combinación con la clave de dispositivo y el módulo de comprobación aleatoria de índice 312 genera un índice hash mediante comprobación aleatoria de la clave globalmente única como la sal combinada con el índice globalmente único y la clave de dispositivo.

En una realización, el módulo de generación de claves de cifrado 314 pasa la clave de cifrado al módulo de cifrado de mensajes 316. Por ejemplo, el módulo de generación de claves de cifrado 314 se acopla comunicativamente al módulo de cifrado de mensajes 316 para enviar la clave de cifrado al módulo de cifrado de mensajes 316.

El módulo de cifrado de mensajes 316 opcional incluye código y rutinas para cifrar un mensaje. En una realización, el módulo de cifrado de mensajes 316 es un conjunto de instrucciones ejecutables por el procesador 206. En otra realización, el módulo de cifrado de mensajes 316 se almacena en la memoria persistente 205 y es accesible y ejecutable por el procesador 206. En cualquier realización, el módulo de cifrado de mensajes 316 está adaptado para cooperación y comunicación con el procesador 206, otros componentes del servidor NRM 101 y otros componentes del módulo de mensajería no retenida 220.

El módulo de cifrado de mensajes 316 cifra opcionalmente el mensaje recibido por el módulo receptor de mensajes 304. En una realización, el módulo de cifrado 316 cifra el mensaje recibido por el módulo receptor de mensajes 304 usando la clave de cifrado generada por, y recibida desde, el módulo de generación de claves de cifrado 314. En otra realización, el módulo de cifrado 316 cifra el mensaje usando una clave de cifrado diferente. En una realización, el mensaje no cifrado se borra de la memoria no persistente 207 en respuesta al cifrado. Por ejemplo, en una realización, el mensaje no cifrado se elimina por el módulo de eliminación 324 en respuesta al cifrado. En una realización, el módulo de cifrado 316 descifra un mensaje recuperado por el módulo de recuperación de mensajes 322.

En una realización, el módulo de cifrado de mensajes 316 pasa el mensaje cifrado al módulo de almacenamiento de mensajes y generación de identificador 318 para su almacenamiento en la memoria no persistente. Por ejemplo, el módulo de cifrado de mensajes 316 se acopla comunicativamente al módulo de almacenamiento de mensajes y generación de identificador 318 para enviar el mensaje cifrado al módulo de almacenamiento de mensajes y generación de identificador 318.

El módulo de almacenamiento de mensajes y generación de identificador 318 incluye código y rutinas para almacenar un mensaje, generar un identificador y enviar el identificador a un destinatario. En una realización, el módulo de almacenamiento de mensajes y generación de identificador 318 es un conjunto de instrucciones ejecutables por el procesador 206. En otra realización, el módulo de almacenamiento de mensajes y generación de identificador 318 se almacena en la memoria persistente 205 y es accesible y ejecutable por el procesador 206. En cualquier realización, el módulo de almacenamiento de mensajes y generación de identificador 318 se adapta para cooperación y comunicación con el procesador 206, otros componentes del servidor NRM 101 y otros componentes del módulo de mensajería no retenida 220.

El módulo de almacenamiento de mensajes y generación de identificador 318 almacena el mensaje. En una realización, el módulo de almacenamiento de mensajes y generación de identificador 318 en la memoria no persistente 207 de un servidor NRM 101. En una realización, el módulo de almacenamiento de mensajes y generación de identificador 318 recibe el índice hash generado por el módulo de comprobación aleatoria de índice 312 y almacena el mensaje usando el índice hash como un identificador para almacenar y recuperar el mensaje. Tal realización proporciona beneficiosamente un índice ofuscado para almacenar el mensaje. En una realización, el mensaje almacenado por el módulo de almacenamiento de mensajes y generación de identificador 318 es una versión cifrada del mensaje.

El módulo de almacenamiento de mensajes y generación de identificador 318 genera un identificador de mensaje. El identificador de mensaje es un identificador único que tiene un número enorme de valores potenciales, de modo que es virtualmente imposible adivinar o iterar un paso para descubrir un identificador válido, especialmente dado que un mensaje no se retiene indefinidamente en el sistema 100. El identificador de mensaje se asocia únicamente con un mensaje almacenado en la memoria no persistente 207 de al menos un servidor NRM 101. En una realización, el identificador de mensaje es un URL para el sistema de mensajería no retenida 100.

En realizaciones donde una clave globalmente única se generó por el módulo de generación de claves 308 y se usó por el módulo de comprobación aleatoria de índice 312 para generar un índice hash y/o por el módulo de generación de claves de cifrado 314 para generar una clave de cifrado, el identificador de mensaje incluye la clave globalmente

única. Por ejemplo, el módulo de almacenamiento de mensajes y generación de identificador 318 genera un URL que contiene la clave globalmente única.

En realizaciones donde un índice globalmente único se generó por el módulo de generación de índices 310 y se usó por el módulo de comprobación aleatoria de índice 321 para generar un índice hash, el identificador de mensaje incluye el índice globalmente único. Por ejemplo, el módulo de almacenamiento de mensajes y generación de identificador 318 genera un URL que contiene la clave globalmente única y opcionalmente un índice globalmente único. En una realización, el URL no es un URL de HTTP indeterminado. En una realización, el URL es un URL de HTTPS indeterminado, que puede proporcionar beneficiosamente mayor seguridad que un URL de HTTP. Se reconocerá que un URL es meramente un ejemplo de un identificador de mensaje y existen otros identificadores de mensaje.

El módulo de almacenamiento de mensajes y generación de identificador 318 envía el identificador de mensaje al destinatario. En una realización, el mensaje no se envía usando un servidor de terceros 190 (por ejemplo, los de servicios de mensajes tradicionales tales como correo electrónico, que retiene copias del mensaje). En su lugar, el módulo de almacenamiento de mensajes y generación de identificador 318 envía el identificador de mensaje usando un servidor de terceros. Por ejemplo, el módulo de almacenamiento de mensajes y generación de identificador 318 envía el identificador de mensaje a través de un servicio de correo electrónico estándar alojado por un servidor de terceros 190. En una realización, el módulo de almacenamiento de mensajes y generación de identificador 318 usa un servicio de pasarela, por ejemplo, un servicio de pasarela de correo electrónico para evitar problemas con los filtros de correo no deseado y/o para balancear la carga de red.

En algunas realizaciones, en respuesta al envío del identificador, la información se elimina de la memoria no persistente del servidor o servidores NRM 101. En algunas realizaciones, la información eliminada del servidor o servidores NRM 101 asegura que el servidor o servidores NRM no tengan toda la información para identificar, localizar y descifrar el mensaje de manera independiente. Tales realizaciones pueden evitar beneficiosamente que se acceda a un mensaje por alguien distinto del destinatario. Ejemplos de información que se puede eliminar incluyen una o más de la clave globalmente única, el índice globalmente único, el índice hash, la clave de cifrado y el identificador de mensaje. Por ejemplo, en una realización, la clave globalmente única, el índice globalmente único, el índice hash, la clave de cifrado y el identificador de mensaje se eliminan del servidor o servidores NRM 101. En algunas realizaciones, la información eliminada del servidor o servidores NRM 101 y el identificador de mensajería aseguran que ni el servidor o servidores NRM 101 ni el destinatario del identificador de mensajería tengan toda la información para identificar, localizar y descifrar el mensaje de manera independiente. Por ejemplo, el identificador incluye la clave globalmente única, pero no la clave de dispositivo y el servidor NRM 101 no tiene la clave globalmente única, pero tiene la clave de dispositivo.

La información eliminada después de que se envíe el identificador depende de la realización y de qué información existe. Por ejemplo, un índice globalmente único no se elimina cuando no se generó uno (por ejemplo, el módulo de mensajería no retenida 220 no incluía el módulo de generación de índices 310 opcional). En una realización, la información se elimina por el módulo de eliminación 324 tratado a continuación.

En algunas realizaciones, la identidad del remitente puede no ser compartida con el destinatario. Por ejemplo, el correo electrónico que incluye el identificador de mensaje no identifica el usuario remitente, pero el mensaje cuando se recupera y se presenta puede identificar o no al remitente dependiendo de la realización. En otro ejemplo, el mensaje recuperado por el módulo de recuperación de mensajes 322 y presentado al usuario destinatario no identifica al usuario remitente. En una realización, si el usuario remitente se identifica con el destinatario y/o en qué punto se determina en base a una preferencia de usuario del remitente y/o un ajuste del administrador (por ejemplo, un administrador asociado con una organización para la cual es empleado el remitente). En una realización, si el usuario remitente no se identifica, el remitente identificado es el servidor NRM 101 que contiene el URL para el mensaje. En una realización, si el usuario remitente no se identifica, el sistema en su lugar identifica una cuenta para una organización con la que está asociado el remitente o una cuenta para el público en general. En una realización, un mensaje se envía sin información de identificación de usuario (es decir, no solamente no se identifica el remitente al destinatario, sino que no hay información de identificación de remitente asociada con el mensaje y almacenada en el sistema 100). En algunas realizaciones, un administrador puede controlar si y en qué grado los usuarios son capaces de enviar mensajes de manera anónima usando el sistema 100. Por ejemplo, en una realización, un administrador de la Corporación A puede establecer controles de manera que un usuario individual (por ejemplo, Bob de contabilidad) o grupo de usuarios (por ejemplo, el departamento de contabilidad) no pueda enviar mensajes de manera anónima.

En una realización, el módulo de almacenamiento de mensajes y generación de identificador 318 pasa el identificador de mensaje a un servidor de terceros 190. Por ejemplo, el módulo de almacenamiento de mensajes y generación de identificador 318 se acopla comunicativamente al servidor de terceros 190 para enviar el identificador de mensaje al destinatario a través del servidor de terceros 190.

El módulo de copia de seguridad de mensajes 320 opcional incluye código y rutinas para proporcionar redundancia. En una realización, el módulo de copia de seguridad de mensajes 320 es un conjunto de instrucciones ejecutables por el procesador 206. En otra realización, el módulo de copia de seguridad de mensajes 320 se almacena en la

memoria persistente 205 y es accesible y ejecutable por el procesador 206. En cualquier realización, el módulo de copia de seguridad de mensajes 320 se adapta para cooperación y comunicación con el procesador 206, otros componentes del servidor NRM 101 y otros componentes del módulo de mensajería no retenida 220.

En algunas realizaciones, la configuración del servidor NRM 101 hace más probable que un mensaje se pierda permanentemente antes de la entrega que en un sistema de mensajería tradicional (por ejemplo, correo electrónico). Por ejemplo, en algunas realizaciones, el servidor NRM 101 carece de almacenamiento persistente y escribible y los mensajes se almacenan en memoria no persistente; por lo tanto, una interrupción en la alimentación del servidor NRM 101 (por ejemplo, corte de energía o desastre natural) puede eliminar los mensajes no entregados en ese servidor NRM 101. En otro ejemplo, en algunas realizaciones, el servidor NRM 101 se configura para eliminar activamente toda la memoria si el servidor NRM 101 se registra con el fin de mejorar la seguridad. Bajo tales circunstancias, los mensajes no entregados también se perderían de manera permanente.

En una realización, el módulo de copia de seguridad de mensajes 320 proporciona redundancia enviando información de copia de seguridad a al menos un servidor NRM 101 adicional. Tal realización aumenta beneficiosamente las oportunidades de que el mensaje sea entregable incluso si se elimina una memoria del servidor NRM. En una realización, la información de copia de seguridad incluye el mensaje recibido desde el cliente de mensajería del remitente 120. Por ejemplo, el módulo receptor de mensajes 304 del servidor NRM 101a recibe un mensaje y el módulo de copia de seguridad de mensajes 320 reenvía automáticamente una copia del mensaje recibido al servidor NRM 101b donde el módulo receptor de mensajes 304 del servidor NRM 101b recibe la copia.

En algunas realizaciones, cuando una clave globalmente única asociada con un mensaje recibido se genera por el módulo de generación de claves 308, esa clave globalmente única es información de copia de seguridad y se envía por el módulo de copia de seguridad 320 a al menos otro servidor NMR 101. Por ejemplo, en una realización, el módulo receptor de mensajes 304 del servidor NMR 101a recibe un mensaje, el módulo de generación de claves 308 genera una clave globalmente única para ese mensaje y el módulo de copia de seguridad de mensajes 320 reenvía automáticamente una copia del mensaje recibido y la clave globalmente única al servidor NRM 101b.

En alguna realización, cuando un índice globalmente único asociado con un mensaje recibido se genera por el módulo de generación de índices 310 y se asocia con un mensaje recibido, ese índice globalmente único es información de copia de seguridad y se envía por el módulo de copia de seguridad 320 a al menos otro servidor NRM 101. Por ejemplo, en una realización, el módulo receptor de mensajes 304 del servidor NRM 101a recibe un mensaje, el módulo de generación de claves 308 genera una clave globalmente única para ese mensaje, el módulo de generación de índices 310 genera un índice globalmente único para el mensaje y el módulo de copia de seguridad de mensajes 320 reenvía automáticamente una copia del mensaje recibido, la clave globalmente única y el índice globalmente único al servidor NRM 101b.

En algunas realizaciones, cualquier índice hash o clave de cifrado generada para el al menos otro servidor NRM 101 (por ejemplo, el servidor NRM 101b) será diferente del índice hash o de la clave de cifrado para el servidor NRM 101 que recibió originalmente el mensaje (por ejemplo, el servidor NRM 101a) independientemente de si la misma clave globalmente única y/o índice globalmente único se reenvía y usa, debido a que cada servidor NRM 101 se asocia con una clave de dispositivo diferente.

A diferencia de los sistemas de mensajería tradicionales, tales como correo electrónico, cualquier mensaje redundante, al que también se hace referencia ocasionalmente en la presente memoria como “copias de seguridad”, “copias” o similares se eliminan del sistema de mensajería no retenida 101 cuando, dependiendo de la realización, el mensaje se recupera por el módulo de recuperación de mensajes 322, el mensaje se entrega para su presentación al destinatario o expira la vida útil del mensaje.

En una realización, el módulo de copia de seguridad de mensajes 320 pasa información de copia de seguridad a al menos otro servidor NRM 101. Por ejemplo, el módulo de copia de seguridad de mensajes 320 se acopla comunicativamente a al menos otro servidor NRM 101 para enviar la información de copia de seguridad a al menos otro servidor NRM 101.

El módulo de recuperación de mensajes 322 incluye código y rutinas para recuperar un mensaje. En una realización, el módulo de recuperación de mensajes 322 es un conjunto de instrucciones ejecutables por el procesador 206. En otra realización, el módulo de recuperación de mensajes 322 se almacena en la memoria persistente 205 y es accesible y ejecutable por el procesador 206. En cualquier realización, el módulo de recuperación de mensajes 322 se adapta para cooperación y comunicación con el procesador 206, otros componentes del servidor NRM 101 y otros componentes del módulo de mensajería no retenida 220.

El módulo de recuperación de mensajes 322 recupera un mensaje usando el identificador. En una realización, el módulo de recuperación de mensajes 322 recupera un mensaje usando el identificador en respuesta a la selección del identificador. Por ejemplo, supongamos que el identificador de mensaje es un URL de HTTPS que se envió al destinatario a través de correo electrónico. En una realización, el destinatario recibe el correo electrónico, abre el correo electrónico y selecciona el URL de HTTPS, el módulo de recuperación de mensajes 322 recibe el URL de HTTPS en respuesta a la selección y recupera el mensaje asociado y envía ese mensaje para su presentación al

usuario (por ejemplo, en un cliente de mensajería 120 o una ventana del navegador web (no mostrada)). En una realización, el módulo de recuperación de mensajes 322 recupera un mensaje usando el identificador en respuesta a la selección del identificador y la verificación del destinatario como se describe a continuación con referencia al módulo de verificación de destinatario 326.

Dado que muchos módulos del módulo de mensajería no retenida 220 son opcionales, existen muchas combinaciones de módulos y, por lo tanto, realizaciones. Los pasos que el módulo de recuperación de mensajes 322 da para recuperar un mensaje varían dependiendo de la realización y qué, en su caso, módulos opcionales (por ejemplo, 308, 310, 312, 314, 316, 326 y 328) se incluyen en el módulo de mensajería no retenida 200. Por ejemplo, supongamos que el módulo de mensajería no retenida 220 incluye un módulo de comprobación aleatoria de índice 312; en una realización, el módulo de recuperación de mensajes 322 recupera un mensaje usando una clave globalmente única incluida en el identificador de mensaje para obtener el índice hash para recuperar el mensaje de la memoria no persistente. En otro ejemplo, supongamos que el módulo de mensajería no retenida 220 incluye un módulo de cifrado 316; en una realización, el módulo de recuperación de mensajes 322 recupera una versión cifrada del mensaje y debe obtener una versión descifrada antes de enviar el mensaje para su presentación al usuario. En otro ejemplo más, supongamos que el módulo de mensajería no retenida 220 incluye un módulo de verificación de destinatario 326; en una realización, el módulo de recuperación de mensajes 322 recupera el mensaje en respuesta al módulo de verificación de destinatario 326 que determina que el usuario que seleccionó el identificador es uno o más de un humano y el destinatario deseado.

En una realización, el módulo de recuperación de mensajes 322 recupera un mensaje usando el identificador en combinación con una clave de dispositivo. Por ejemplo, en una realización, el módulo de recuperación de mensajes 322 pasa la clave globalmente única (y, dependiendo de la realización, el índice globalmente único) desde el URL al módulo de comprobación aleatoria de índice 312 que recupera la clave de dispositivo asociada con el servidor NRM 101 y genera el índice hash que se usó para almacenar el mensaje. El módulo de recuperación de mensajes 322 recupera el mensaje usando el índice hash como identificador.

Dependiendo de la realización, el mensaje que recupera el módulo de recuperación de mensajes 322 está cifrado y necesita ser descifrado. En una realización, el módulo de recuperación de mensajes 322 pasa la clave globalmente única al módulo de generación de claves de cifrado 314 que recupera la clave de dispositivo asociada con el servidor NRM 101 y genera la clave de cifrado usada para descifrar el mensaje. En una realización, el módulo de recuperación de mensajes 322 descifra el mensaje en sí mismo. Por ejemplo, el módulo de recuperación de mensajes 322 recibe la clave de cifrado del módulo de clave de cifrado 314 y descifra el mensaje. En otra realización, el módulo de cifrado de mensajes 316 recibe la clave de cifrado y descifra el mensaje.

El módulo de recuperación de mensajes 322 envía el mensaje para su presentación al usuario en base al identificador. Por simplicidad y claridad, ocasionalmente se hace referencia a un usuario 125 que presenta un mensaje enviado usando y recuperado del sistema de mensajería no retenida como “destinatario”. Por ejemplo, supongamos que el identificador de mensaje es un URL; en una realización, el módulo de recuperación de mensajes 322 envía el mensaje a la localización asociada con el URL para su presentación al usuario. En una realización, cuando el mensaje se presenta al destinatario, el mensaje tiene un formato visual similar al de un correo electrónico. Por ejemplo, el mensaje se presenta a través del cliente de mensajería 120 o del navegador web con una línea de asunto, un cuerpo del mensaje y archivos adjuntos.

En una realización, el módulo de recuperación de mensajes 322 pasa información incluida en el identificador de mensaje (por ejemplo, una clave globalmente única) recibida en respuesta a la selección del identificador de mensaje por el usuario destinatario a uno o más de los otros módulos (por ejemplo, 312, 314, 316) del módulo de mensajería no retenida 220 con el fin de recuperar el mensaje y enviar el mensaje para su presentación. Por ejemplo, el módulo de recuperación de mensajes 322 se acopla comunicativamente al módulo de comprobación aleatoria de índice 312 para pasar la clave globalmente única recibida al módulo de comprobación aleatoria de índice 312 con el fin de obtener el identificador para recuperar el mensaje (es decir, el índice hash).

En una realización, el módulo de recuperación de mensajes 322 pasa un mensaje para su presentación a un usuario destinatario. Por ejemplo, el módulo de recuperación de mensajes 322 se acopla comunicativamente al cliente de mensajería 120, o al navegador web, del dispositivo cliente 115 del destinatario para enviar el mensaje al cliente de mensajería 120, o al navegador web, del dispositivo cliente 115 del destinatario. En una realización, el módulo de recuperación de mensajes 322 pasa una indicación de que el mensaje se ha recuperado al módulo de eliminación 324. Por ejemplo, el módulo de recuperación de mensajes 322 se acopla comunicativamente al módulo de eliminación 324 para enviar la indicación de que se ha recuperado el mensaje al módulo de eliminación 324.

El módulo de eliminación 324 incluye código y rutinas para eliminar mensajes de un servidor NRM 101. En una realización, el módulo de eliminación 324 es un conjunto de instrucciones ejecutables por el procesador 206. En otra realización, el módulo de eliminación 324 se almacena en la memoria persistente 205 y es accesible y ejecutable por el procesador 206. En cualquier realización, el módulo de eliminación 324 se adapta para cooperación y comunicación con el procesador 206, otros componentes del servidor NRM 101 y otros componentes del módulo de mensajería no retenida 220.

El módulo de eliminación 324 elimina los mensajes de un servidor NRM 101. En una realización, el módulo de eliminación 324 elimina un mensaje de un servidor de NRM 101 en respuesta a la recuperación del mensaje. Por ejemplo, supongamos que el módulo de eliminación 324 recibe una indicación desde el módulo de recuperación de mensajes 322 de que el mensaje se ha recuperado para su entrega o el módulo de eliminación 324 en sí mismo detecta que el módulo de recuperación de mensajes 322 detecta la recuperación del mensaje para su entrega; en una realización, el módulo de eliminación 324 elimina el mensaje del servidor o servidores NRM 101 que almacenan ese mensaje.

En una realización, el módulo de eliminación 324 elimina un mensaje de un servidor NRM 101 en respuesta a la entrega del mensaje. Por ejemplo, supongamos que el módulo de eliminación 324 recibe una indicación desde el cliente de mensajería de mensajes 120, o desde el navegador web, de que se ha recibido el mensaje; en una realización, el módulo de eliminación 324 elimina el mensaje del servidor o servidores NRM 101 que almacenan ese mensaje. En una realización, eliminar el mensaje incluye eliminar la información del remitente y del receptor en respuesta a la recuperación o entrega. En otras palabras, en una realización, el sistema de mensajería no retenida 100 no retiene ninguna información del remitente o del receptor, incluyendo registros de quién envió a quién un mensaje.

En una realización, el módulo de eliminación 324 elimina un mensaje de un servidor NRM 101 en respuesta a la expiración de un período de tiempo asociado con el mensaje. Se hace referencia ocasionalmente en la presente memoria a la expiración de un período de tiempo asociado con el mensaje como el “mensaje que excede su vida útil” o similar. En una realización, el período de tiempo, al que se hace referencia ocasionalmente en la presente memoria como “vida útil” de un mensaje, se define por el usuario. Por ejemplo, supongamos que el usuario especifica un período de tiempo usando el cliente de mensajería 120, y el período de tiempo se almacena en el dispositivo cliente 115 (por ejemplo, como preferencia de un usuario) y se envía con cada mensaje saliente enviado usando ese cliente de mensajería 120; en una realización, el módulo de eliminación 324 recibe el período de tiempo definido por el usuario y establece un temporizador en consecuencia. Cuando expira el temporizador (es decir, el período de tiempo definido por el usuario ha pasado), el módulo de eliminación 324 elimina el mensaje del servidor o servidores NRM 101 suponiendo que el mensaje no se haya eliminado aún (por ejemplo, el mensaje se recuperó y se eliminó del servidor o servidores NRM 101 en respuesta a la recuperación y antes de la expiración del temporizador). Dependiendo de la realización, el usuario puede definir un período de tiempo para cada mensaje individual o definir un período de tiempo a ser usado para todos los mensajes salientes a menos que se redefina. Las realizaciones que proporcionan la eliminación de mensajes después de un tiempo definido por el usuario permiten beneficiosamente que un usuario asegure de que un mensaje no esté disponible en el servidor o servidores NRM 101 cuando el usuario ya no quiere que el mensaje esté disponible.

En una realización, el período de tiempo se define por el sistema. En una realización, el período de tiempo definido por el sistema incluye un valor por defecto usado cuando no se ha establecido un período de tiempo definido por el usuario. Por ejemplo, no define una vida útil del mensaje; en una realización, el módulo de eliminación 324 establece un temporizador por defecto que se define por el sistema. Cuando expira el temporizador por defecto, el módulo de eliminación 324 elimina el mensaje del servidor o servidores NRM 101 suponiendo que el mensaje no se haya eliminado ya.

En una realización, el período de tiempo definido por el sistema define una vida útil máxima del mensaje. Por ejemplo, en una realización, el módulo de eliminación 324 establece un temporizador que se define por el sistema, y cuando expira el temporizador definido por el sistema, el módulo de eliminación 324 elimina el mensaje del servidor o servidores NRM 101 suponiendo que el mensaje no se ha eliminado ya e independientemente de si ha expirado el temporizador definido por el usuario. Las realizaciones que proporcionan la eliminación de mensajes después de un período de tiempo máximo definido por el sistema reducen beneficiosamente los costes de ejecución del sistema NRMS 100. Por ejemplo, la memoria no persistente 207 es a menudo más costosa por byte de capacidad que el almacenamiento persistente; por lo tanto, es deseable una tasa de rotación de memoria más alta, debido a que eliminar mensajes que no se hayan recuperado después de un cierto período de tiempo de modo que la memoria no persistente 207 se pueda usar por otros mensajes puede evitar el coste de añadir servidores NRM 101 adicionales y/o memoria no persistente 207 para acomodar mensajes que pueden no ser recuperados nunca. Las realizaciones que proporcionan la eliminación de mensajes después de un período de tiempo máximo definido por el sistema también pueden proporcionar seguridad adicional al sistema NRMS 100 limitando la cantidad de tiempo que un pirata informático u otra entidad malvada podría acceder potencialmente al mensaje en ruta desde el remitente al destinatario.

Un período de tiempo, independientemente de si el período de tiempo se define por el usuario o se define por el sistema, se puede medir a partir de uno de una pluralidad de eventos. Ejemplos de eventos incluyen, pero no se limitan a, la recepción del mensaje, el envío del identificador asociado con el mensaje al destinatario, recuperación del mensaje y entrega del mensaje. Las realizaciones en las que el período de tiempo se mide a partir de la recuperación o entrega del mensaje pueden permitir potencialmente a un destinatario otra oportunidad de recibir el mensaje a condición de que ocurra un error durante la recuperación o entrega del mensaje.

En una realización, el módulo de eliminación 324 elimina un mensaje de un servidor NRM 101 en respuesta a recibir una solicitud de retratación desde el remitente. En una realización, la solicitud de retractación incluye el identificador

de mensaje del mensaje que el remitente desea eliminar y el módulo de eliminación 324 identifica y elimina el mensaje asociado con ese identificador del servidor o servidores NRM 101 que almacenan el mensaje. En una realización, un remitente puede solicitar retractar un mensaje antes de una recuperación del destinatario del mensaje y el módulo de eliminación 324 elimina ese mensaje en respuesta a la solicitud de retractación. Por ejemplo, supongamos que un remitente envía un mensaje por error y solicita retractar ese mensaje; en una realización, el módulo de eliminación 324 recibe la solicitud de retractación, identifica el mensaje pertinente, determina que el mensaje no se ha recuperado por el módulo de recuperación de mensajes 322 y elimina el mensaje del servidor o servidores NRM 101 que almacenan el mensaje, haciendo por ello que el mensaje ya no esté disponible.

En una realización, un remitente puede solicitar retractar un mensaje incluso después de que el mensaje se reciba y entregue a un destinatario. Por ejemplo, supongamos que el mensaje se recupera antes de la expiración de la vida útil del mensaje pero no se elimina inmediatamente por el módulo de eliminación 324 en respuesta a la recuperación; en una realización, el módulo de eliminación 324 puede recibir una solicitud de retractación desde el remitente en el tiempo entre la recuperación del mensaje y la expiración de la vida útil del mensaje y eliminar el mensaje con anticipación (es decir, en respuesta a la solicitud de retractación y antes de la expiración del periodo de tiempo definido por la vida útil).

En una realización, el módulo de eliminación 324 elimina otra información de un servidor NRM 101 además de los mensajes. Ejemplos de otra información incluyen, pero no se limitan a, una o más de la clave y el índice globalmente únicos y el identificador de mensaje, la clave de cifrado, el mensaje no cifrado, el remitente y el destinatario. Por ejemplo, en una realización, en respuesta al envío del identificador de mensaje asociado con un mensaje, el módulo de eliminación 324 elimina la clave globalmente única y el identificador de mensaje asociado con ese mensaje del servidor NRM 101 asegurando que el servidor NRM carece de la información necesaria para identificar y localizar el mensaje de manera independiente.

En una realización, el módulo de eliminación 324 elimina todo de la memoria en respuesta a la detección de un acceso no autorizado del servidor NRM 101. Por ejemplo, supongamos que el servidor NRM 101 detecta un número predeterminado de intentos fallidos de inicio de sesión usando el nombre de usuario de un administrador del sistema; en una realización, el servidor NRM 101 elimina todo de la memoria. En una realización, el módulo de eliminación 324 elimina todo de la memoria en respuesta a la detección de un acceso del servidor NRM 101, independientemente de si el acceso está autorizado o no autorizado. Por ejemplo, supongamos que el servidor NRM 101 detecta un inicio de sesión del administrador del sistema con éxito; en una realización, el servidor NRM 101 elimina todo de la memoria en respuesta a la detección del inicio de sesión.

La eliminación impide el acceso a los datos eliminados. La eliminación que realiza el módulo de eliminación 324 puede variar dependiendo de la realización. Ejemplos de eliminación incluyen, pero no se limitan a, eliminar identificadores (por ejemplo, punteros) de los datos eliminados, sobrescribir los datos eliminados con datos nuevos (por ejemplo, un nuevo mensaje o escribir con ceros) o cualquier otro método de borrado de datos de la memoria, lo que permite que la memoria se reutilice.

El módulo de verificación de destinatario 326 incluye código y rutinas para verificar a un usuario destinatario antes de recuperar y presentar el mensaje al usuario destinatario. En una realización, el módulo de verificación de destinatario 326 es un conjunto de instrucciones ejecutables por el procesador 206. En otra realización, el módulo de verificación de destinatario 326 se almacena en la memoria no persistente 205 y es accesible y ejecutable por el procesador 206. En cualquier realización, el módulo de verificación de destinatario 326 se adapta para cooperación y comunicación con el procesador 206, otros componentes del servidor NRM 101 y otros componentes del módulo de mensajería no retenida 220.

El módulo de verificación de destinatario 326 verifica un usuario destinatario antes de recuperar y presentar el mensaje al usuario destinatario. En una realización, la verificación de destinatario verifica que el usuario destinatario (es decir, el usuario que seleccionó el identificador de mensaje) es uno o más de un humano y el destinatario deseado. Tal verificación de destinatario puede proporcionar beneficiosamente seguridad adicional al sistema de mensajería no retenida 100 reduciendo además la posibilidad de acceso no autorizado a un mensaje enviado a través del sistema de mensajería no retenida 100.

En una realización, el módulo de verificación de destinatario 326 verifica que un destinatario es humano. En una realización, el módulo de verificación de destinatario 326 verifica que el destinatario es humano (más que, por ejemplo, un robot, rastreador, ordenador u otro lector automatizado, no humano) usando una prueba Turing Pública Completamente Automatizada para diferenciar Ordenadores de Humanos (CAPTCHA). En algunas realizaciones, la CAPTCHA puede ser auditiva, visual o una combinación. Por ejemplo, en una realización, el módulo de verificación de destinatario 326 presenta una CAPTCHA visual en forma de un desafío legible en pantalla y solamente por humanos al destinatario en respuesta a la selección de un identificador de mensaje. En otro ejemplo, el módulo de verificación de destinatario 326 presenta una auditoría CAPTCHA en forma de un desafío de audio inteligible solamente por humanos al destinatario en respuesta a la selección de un identificador de mensaje. El módulo de verificación de destinatario 326 recibe una respuesta del destinatario al desafío CAPTCHA presentado, y determina si la respuesta coincide con el desafío. En una realización, el módulo de recuperación de mensajes 322 recupera el mensaje en base, al menos en parte, en si el módulo de verificación de destinatario 326 determina que la respuesta

coincida con el desafío. En una realización, el módulo de recuperación de mensajes 322 no recupera el mensaje cuando el módulo de verificación de destinatario 326 determina que la respuesta no coincide con el desafío.

En una realización, el módulo de verificación de destinatario 326 determina si verificar que un destinatario es humano en base a la preferencia de un remitente. Por ejemplo, un remitente puede establecer una preferencia para verificar la humanidad del destinatario para todos los mensajes o para mensajes a un destinatario particular o grupo de destinatarios, y el módulo de verificación de destinatario 326, en respuesta a la selección del identificador de mensaje, determina si el mensaje está marcado para verificación de destinatario en base a la preferencia del usuario y presenta (o no presenta) un desafío en consecuencia. En una realización, el módulo de verificación de destinatario 326 determina si verificar que un destinatario es humano automáticamente y sin intervención del usuario. Por ejemplo, el módulo de verificación de destinatario 326 determina desafiar al destinatario, cuando la selección del identificador se recibe desde una localización no familiar (por ejemplo, una dirección IP o dispositivo no usado previamente por o asociado con el destinatario).

En una realización, el módulo de verificación de destinatario 326 verifica que un destinatario es el destinatario deseado. En una realización, el módulo de verificación de destinatario 326 verifica que el destinatario es el destinatario deseado usando información de verificación. La verificación puede ser algo que el usuario es (por ejemplo, un biométrico), algo que el usuario tiene (por ejemplo, una clave electrónica) o algo que el usuario conoce (por ejemplo, un PIN o una contraseña). Por claridad y comodidad, la descripción a continuación se centra fundamentalmente en una contraseña (por ejemplo, una cadena numérica o alfanumérica), pero se debería reconocer que la descripción en la presente memoria se extiende a otra información de verificación.

En una realización, el módulo de verificación de destinatario 326 recibe una selección del identificador de mensaje, determina si verificar la identidad del usuario. En respuesta a la determinación de verificar la identidad del usuario, el módulo de verificación de destinatario 326 solicita y recibe información de verificación (por ejemplo, una contraseña) del destinatario y determina si la información recibida (por ejemplo, la contraseña introducida) coincide con la información de verificación almacenada (por ejemplo, una contraseña asociada con el mensaje o el destinatario). En una realización, el módulo de recuperación de mensajes 322 recupera el mensaje en base, al menos en parte, a si el módulo de verificación de destinatario 326 determina que la información de verificación recibida coincide con la información de verificación almacenada. En una realización, el módulo de recuperación de mensajes 322 no recupera el mensaje cuando el módulo de verificación de destinatario 326 determine que la información de verificación recibida no coincide con la información de verificación almacenada.

En una realización, la información de verificación es específica del mensaje, es decir, específica a un mensaje individual o grupo de mensajes. Por ejemplo, una contraseña diferente se puede asociar con cada mensaje individual tras la creación del mensaje (por ejemplo, cuando el módulo receptor de mensajes 304 reciba el mensaje). En una realización, la información de verificación es especifica del destinatario, es decir, específica a un destinatario individual o grupo de destinatarios. Por ejemplo, un destinatario (por ejemplo, el Usuario 125b) se asocia con una primera contraseña, que el destinatario (es decir, el Usuario 125b) proporciona con el fin de acceder a un mensaje desde un remitente (por ejemplo, el Usuario 125a), y una segunda contraseña, que el destinatario (es decir, el Usuario 125b) proporciona con el fin de acceder a un mensaje desde otro remitente (por ejemplo, el Usuario 125n). Dependiendo de la realización, la información de verificación se puede almacenar de manera diferente. Por ejemplo, en una realización, la información de verificación específica de mensaje se puede asociar con ese mensaje específico y almacenar en asociación con el mensaje en la memoria no persistente 207, y la información de verificación específica de destinatario, en una realización, se almacena en el almacén de datos 130 similar a las credenciales de un remitente.

Dependiendo de la realización, la información de verificación se puede generar automáticamente o definir por el remitente. Por ejemplo, en algunas realizaciones, el módulo de verificación de destinatario 326 recibe una contraseña desde el remitente y asocia la contraseña recibida con un mensaje, destinatario o grupo de destinatarios dependiendo de la realización. En otro ejemplo, en algunas realizaciones, el módulo de verificación de destinatario 326 genera automáticamente (por ejemplo, aleatoriamente) una contraseña y asocia la contraseña generada con un mensaje, destinatario o grupo de destinatarios dependiendo de la realización.

En una realización, el módulo de verificación de destinatario 326 envía la información de verificación al destinatario usando un servicio de mensajería tradicional (por ejemplo, correo electrónico, mensaje instantáneo, publicación de red social, publicación de microblog, mensaje SMS, etc.). En una realización, el módulo de verificación de destinatario 326 envía la información de verificación al destinatario usando el mismo servicio de mensajería tradicional que se usa para enviar el identificador de mensaje. Por ejemplo, supongamos que el identificador de mensaje se envió al destinatario a través de correo electrónico; en una realización, el módulo de verificación de destinatario 326 envía una contraseña generada aleatoriamente para ese mensaje en un correo electrónico separado.

En una realización, el módulo de verificación de destinatario 326 envía la información de verificación al destinatario usando un servicio de mensajería tradicional diferente que se usa para enviar el identificador de mensaje. Por ejemplo, supongamos que el identificador de mensaje se envió al destinatario a través de correo electrónico; en una realización, el módulo de verificación de destinatario 326 envía una contraseña generada aleatoriamente para ese

mensaje en un mensaje de texto SMS. Tal comunicación fuera de banda de la verificación puede proporcionar beneficiosamente seguridad adicional en la medida que es mayor el número de cuentas o dispositivos a los que un destinatario no autorizado o no deseado necesitaría tener acceso con el fin de recuperar el mensaje.

En algunas realizaciones, el módulo de verificación de destinatario 326 puede proporcionar una insinuación asociada con la información de verificación. Por ejemplo, supongamos que la información de verificación es una contraseña definida por el remitente, específica del mensaje, en una realización, el módulo de verificación de destinatario 326 sugiere al usuario una insinuación (por ejemplo, proporciona un campo de texto en el cual el remitente puede escribir una insinuación o pregunta de seguridad), que se proporciona por el destinatario de modo que el destinatario pueda determinar y proporcionar la información de verificación correcta y acceder con éxito al mensaje. En otro ejemplo, supongamos que la información de verificación sea una contraseña específica del destinatario, en una realización, el módulo de verificación de destinatario 326 proporciona una insinuación (por ejemplo, proporciona una pregunta de seguridad tal como "¿Cuál era el nombre de tu primera mascota?") de modo que el destinatario deseado pueda determinar y proporcionar la información de verificación correcta y acceder con éxito al mensaje.

En una realización, el módulo de verificación de destinatario 326 proporciona una insinuación que se envía con el identificador de mensaje. Por ejemplo, un destinatario recibe un correo electrónico tanto con un URL (es decir, identificador de mensaje) como con "¿Cuál era el apodo del primer año de Tom?" (es decir, una insinuación). En otro ejemplo, una publicación de red social en el perfil del remitente puede incluir tanto un URL (es decir, un identificador de mensaje) como "Mi color favorito" (es decir, una insinuación). Las realizaciones en las que se proporciona una insinuación con el identificador de mensaje puede añadir beneficiosamente verificación de destinatario a un mensaje sin necesitar comunicar por separado la información de verificación. Por ejemplo, proporcionar insinuaciones de contraseña con el identificador de mensaje permite que tales realizaciones utilicen verificación sin usar un mensaje fuera de banda (por ejemplo, en persona o un sistema de comunicación electrónica diferente) o fuera del mensaje (por ejemplo, enviando un segundo correo electrónico separado).

Se debería observar que, aunque la realización tratada en la presente memoria tiene dos módulos – el módulo de verificación de destinatario 326 que se trata fundamentalmente con respecto a la verificación de destinatario y el módulo de autenticación 240 se trata fundamentalmente con respecto a autenticar un remitente, en algunas realizaciones, se puede usar un único módulo para autenticar/verificar tanto a remitentes como a destinatarios.

En una realización, el módulo de verificación de destinatario 326 pasa el identificador de mensaje seleccionado o una aprobación para recuperar el mensaje asociado con el módulo de recuperación de mensajes 322. Por ejemplo, el módulo de verificación de destinatario 326 se acopla comunicativamente con el módulo de recuperación de mensajes 322 para enviar el identificador de mensaje seleccionado o la aprobación para recuperar el mensaje asociado al módulo de recuperación de mensajes 322. En otra realización, el módulo de verificación de destinatario 326 pasa el identificador de mensaje o la aprobación para recuperar el mensaje asociado con el módulo de recuperación de mensajes 322. Por ejemplo, el módulo de verificación de destinatario 326 se acopla comunicativamente con el módulo de recuperación de mensajes 322 para enviar el identificador de mensaje o la aprobación para recuperar el mensaje asociado al módulo de recuperación de mensajes 322.

El módulo de registro y notificación 328 incluye código y rutinas para uno o más de generar registros de eventos y notificar a los usuarios eventos asociados con el sistema de mensajería no retenida 100. En una realización, el módulo de registro y notificación 328 es un conjunto de instrucciones ejecutables por el procesador 206. En otra realización, el módulo de registro y notificación 328 se almacena en la memoria persistente 205 y es accesible y ejecutable por el procesador 206. En cualquier realización, el módulo de registro y notificación 328 se adapta para cooperación y comunicación con el procesador 206, otros componentes del servidor NRM 101 y otros componentes del módulo de mensajería no retenida 220.

En una realización, el módulo de registro y notificación 328 genera registros del uno o más eventos asociados con el sistema de mensajería no retenida 100. Ejemplos de eventos incluyen, pero no se limitan a, la recepción del sistema de mensajería no retenida de un mensaje a ser enviado usando el sistema de mensajería no retenida 100, la selección del identificador de mensaje por un destinatario (es decir, solicitud de recuperación del mensaje), la entrega con éxito del mensaje a un destinatario (es decir, un mensaje completo recuperado y entregado al dispositivo del destinatario), el acceso de un archivo adjunto asociado con el mensaje, etc.

En una realización, el módulo de registro y notificación 328 genera un registro de la recepción del sistema de mensajería no retenida de un mensaje a ser enviado usando el sistema de mensajería no retenida 100. Por ejemplo, el módulo de registro y notificación 328 genera un registro cuando el módulo receptor de mensajes 304 recibe un mensaje. En una realización, el módulo de registro y notificación 328 genera un registro en forma de una entrada de registro. Por ejemplo, el módulo de registro y notificación 328 genera una entrada de registro que incluye uno o más del remitente, el destinatario, la localización del remitente y el tiempo de recepción del mensaje a ser enviado. En una realización el módulo de registro y notificación 328 genera un registro en forma de un mensaje tradicional. Por ejemplo, el módulo de registro y notificación 328 genera y envía una copia de correo electrónico del mensaje a una dirección de correo electrónico asociada con el remitente (por ejemplo, el correo electrónico personal o corporativo del usuario), de modo que la bandeja de entrada de correo electrónico del remitente tenga un registro de los mensajes enviados por ese usuario a través del sistema de mensajería no retenida 100. En otro ejemplo, el módulo

de registro y notificación 328 genera y envía un mensaje de correo electrónico que describe el mensaje enviado usando el sistema de mensajes no retenidos 100 (por ejemplo, un correo electrónico describe el remitente, destinatario, contenido, etc., pero no incluye realmente el contenido del mensaje enviado usando el sistema 100).

En una realización, el módulo de registro y notificación 328 genera un registro de selección del identificador de mensaje por un destinatario (es decir, solicitud de recuperación del mensaje). Por ejemplo, en una realización, el módulo de registro y notificación 328 genera un registro que incluye el destinatario, el tiempo y la localización de la selección. En una realización, un usuario puede solicitar tal registro (por ejemplo, seleccionando el identificador de mensaje o proporcionar de otro modo el identificador de mensaje) y recibir el registro para ese mensaje desde el módulo de registro y notificación 328. Tal realización, puede permitir beneficiosamente que el usuario verifique si el destinatario solicitó el mensaje.

En una realización, el módulo de registro y notificación 328 genera un registro de entrega con éxito del mensaje a un destinatario (es decir, un mensaje completo recuperado y entregado al dispositivo del destinatario). Por ejemplo, en una realización, el módulo de registro y notificación 328 genera un registro que incluye el destinatario, el tiempo y la localización del destinatario tras la entrega con éxito del mensaje. En una realización, un usuario puede solicitar tal registro (es decir, seleccionando el identificador de mensaje o proporcionando de otro modo el identificador de mensaje) y recibir el registro para ese mensaje desde el módulo de registro y notificación 328. Tal realización, puede permitir beneficiosamente que el usuario verifique si el destinatario recibió con éxito el mensaje.

En una realización, el módulo de registro y notificación 328 genera un registro para la vista de un archivo adjunto asociado con el mensaje. Por ejemplo, en una realización, el módulo de registro y notificación 328 recibe un identificador de archivo adjunto en respuesta a una apertura del destinatario (o vista de otro modo) de un archivo adjunto y genera un registro que incluye el destinatario, el identificador de archivo adjunto, el archivo adjunto de tiempo que se solicitó para su vista (es decir, abrió) y la localización del destinatario. En una realización, un usuario puede solicitar tal registro (por ejemplo, seleccionando el identificador de mensaje o proporcionando de otro modo el identificador de mensaje) y recibir el registro para ese mensaje del módulo de registro y notificación 328. Tal realización, puede permitir beneficiosamente que el usuario verifique si el destinatario vio un archivo adjunto.

En una realización, el remitente controla si el módulo de registro y notificación 328 genera un registro para un evento. Por ejemplo, en una realización, el remitente puede seleccionar preferencias de manera que una copia de correo electrónico de mensajes enviados usando el sistema de mensajería no retenida se envíe a la cuenta de correo electrónico personal del usuario. En otra realización, un administrador controla si el módulo de registro y notificación 328 genera un registro para un evento. Por ejemplo, un administrador de empresa puede controlar si una copia de mensajes enviados usando el sistema de mensajería no retenida 100 se envía a ese correo electrónico corporativo de empleado u otra cuenta de correo electrónico corporativo para archivar/mantener/auditar registros. En algunas realizaciones, los ajustes del administrador desbancan a los de un remitente. Por ejemplo, en una realización, un administrador puede establecer controles de manera que una copia de correo electrónico de un mensaje enviado usando el sistema de mensajería no retenida 100 se envía a una cuenta de correo electrónico corporativo (por ejemplo, asociada con el grupo de usuarios del remitente) y el remitente no puede anular ese ajuste o evitar de otro modo que la copia del correo electrónico sea enviada.

En una realización, el módulo de registro y notificación 328 notifica a un usuario uno o más eventos asociados con el sistema de mensajería no retenida 100. Por ejemplo, el módulo de registro y notificación 328 envía un mensaje de correo electrónico u otro tradicional (por ejemplo, un mensaje de texto SMS) a un remitente del mensaje en respuesta al módulo de recuperación de mensajes 322 que recibe una selección del identificador de mensaje para ese mensaje. En una realización, el remitente puede controlar si un evento desencadena una notificación y qué sistema de mensajes tradicional se usa para enviar la notificación para ese tipo de evento. En una realización, un administrador puede controlar si un evento desencadena una notificación y qué sistema de mensajes tradicional se usa para enviar la notificación para ese tipo de evento.

Como se ha mencionado previamente, aunque muchos de los ejemplos en la presente memoria hacen referencia fundamentalmente a correo electrónico (por ejemplo, discutir un cliente de correo electrónico, enviar un identificador a través de un correo electrónico, etc.), se debería reconocer que la descripción en la presente memoria se aplica a otros sistemas de mensajería. Por ejemplo, en una realización, un remitente (por ejemplo, el Usuario A 125a) que usa un cliente de mensajería 120 puede esbozar una publicación de red social (por ejemplo, una publicación de Facebook) y el módulo de almacenamiento de mensajes y generación de identificador 318 publica el identificador de mensaje (por ejemplo, un URL) asociado con esa publicación de red social bajo la cuenta de red social del remitente (por ejemplo, en el “muro” del Usuario A). En algunas realizaciones, el identificador de mensaje publicado se puede acompañar por una descripción de texto o la descripción de texto puede servir como un enlace de hipertexto. Cuando un usuario (que puede ser el remitente u otro usuario tal como un amigo del remitente) visita el sitio de red social del remitente, se presenta al usuario la publicación con el identificador de mensaje (es decir, un URL) y puede seleccionar el identificador de mensaje (es decir, el usuario es un destinatario) y el módulo de recuperación de mensajes 322 recupera la publicación de red social. Por lo tanto, el mensaje de red social (es decir, el contenido) ya no es accesible después de que se elimine del sistema de mensajes no retenidos 100 e, incluso si la red social retiene el identificador de mensaje publicado indefinidamente, el contenido yo no está almacenado ni está accesible indefinidamente. En algunas realizaciones, el módulo de verificación de destinatario 326 coopera con los ajustes de

privacidad de la red social (es decir, proporciona información de verificación a un conjunto de usuarios con permiso del sistema de red social para ver las publicaciones de red social del remitente) o complementa los ajustes de privacidad (por ejemplo, el destinatario que se demuestra que es humano, con permiso de la red social para ver el muro de la red social del remitente y recibida una contraseña específica de mensaje para la publicación se puede presentar la publicación).

En una realización, existen diferentes casos del módulo de mensajería no retenida 220 y cada caso realiza mensajería no retenida para un tipo diferente de servicio de mensajería (por ejemplo, un módulo de mensajería no retenida 220 para correo electrónico, un módulo de mensajería no retenida 220 para redes sociales, etc.). En otra realización, existen diferentes casos del módulo de mensajería no retenida 220 y cada uno puede acomodar un proveedor diferente dentro de un tipo de servicio de mensajería, por ejemplo, dentro de una red social puede haber módulos de mensajería no retenida 220 separados personalizados para cada uno de Google+, LinkedIn, Twitter, Facebook, etc. En otra realización más, existe un único caso del módulo de mensajería no retenida 220 y cada uno puede acomodar servicios de mensajería heterogéneos, por ejemplo, cuando recibe el mensaje el módulo de mensajería no retenida 220 puede determinar (por ejemplo, en base al cliente de mensajería 120) si enviar el identificador de mensaje como un correo electrónico o como una publicación de red social y, si es esta última, en qué red social publicar el identificador de mensaje.

Procesos de ejemplo

Las Figuras 4, 5 y 6A-B representan diversos métodos 400, 500, 600 realizados por el sistema descrito anteriormente en referencia a las Figuras 1-3.

La Figura 4 es un diagrama de flujo que ilustra un método 400 para mensajería electrónica no retenida según una realización. En el bloque 402, el módulo receptor de mensajes 304 del módulo de mensajería no retenida 220 recibe un mensaje del cliente de mensajería de un remitente 120. En el bloque 410, el módulo de cifrado de mensajes 316 cifra opcionalmente el mensaje recibido en el bloque 402. En el bloque 412, el módulo de almacenamiento de mensajes y generación de identificador 318 almacena el mensaje en la memoria no persistente 207. En el bloque 414, el módulo de almacenamiento de mensajes y generación de identificador 318 genera y envía un identificador de mensaje asociado con el mensaje almacenado en el paso 412. En el bloque 418, el módulo de recuperación de mensajes 322 recibe una selección del identificador de mensaje. En respuesta a recibir la selección del identificador de mensaje en el bloque 418, el módulo de recuperación de mensajes 322, en el bloque 420, recupera el mensaje, descifra el mensaje si se cifró en el bloque 410, y envía el mensaje para su presentación. En el bloque 422, el módulo de eliminación 324 elimina el mensaje de la memoria no persistente 207.

La Figura 5 es un diagrama de flujo que ilustra un método 500 para mensajería electrónica no retenida según otra realización. En el bloque 502, el módulo receptor de mensajes 304 del módulo de mensajería no retenida 220 recibe un mensaje del cliente de mensajería 120 del remitente. En el bloque 504, el módulo de generación de claves 308 genera una clave globalmente única. En el bloque 506, el módulo de generación de índices 310 genera opcionalmente un índice globalmente único. En el bloque 508, el módulo de comprobación aleatoria de índice 312 genera un índice hash en base, al menos en parte, a la clave globalmente única generada en el bloque 504 y el índice globalmente único si se generó en el bloque 506. En el bloque 510, el módulo de cifrado de mensajes 316 cifra el mensaje usando una clave de cifrado en base, al menos en parte, a la clave globalmente única generada en el bloque 504. En el bloque 512, el módulo de almacenamiento de mensajes y generación de identificador 318 almacena el mensaje cifrado en memoria no persistente según el índice hash generado en el bloque 508. En el bloque 514, el módulo de almacenamiento de mensajes y generación de identificadores 318 genera y envía un identificador de mensaje que incluye la clave globalmente única generada en el bloque 504. Cuando se genera un índice globalmente único en el bloque 506 y se usa para generar el índice hash en el bloque 508, el identificador de mensaje generado en el bloque 514 también incluye ese índice globalmente único. En el bloque 516, la información (por ejemplo, la clave globalmente única generada en el bloque 504, el índice globalmente único generado opcionalmente en el bloque 506, el índice hash generado en el bloque 508 y el identificador de mensaje generado en el bloque 514) se elimina de la memoria no persistente 207 por el módulo de eliminación 324. En el bloque 518, el módulo de recuperación de mensajes 322 recibe la selección del identificador de mensaje enviado en el bloque 514. En respuesta a la recepción de la selección del identificador de mensaje, en el bloque 518, el módulo de recuperación de mensajes 322 recupera, en el bloque 520, el mensaje y envía el mensaje para su presentación. En el bloque 522, el módulo de eliminación 324 elimina el mensaje de la memoria no persistente 207.

Las Figuras 6A y 6B son diagramas de flujo que ilustran un método 600 para mensajería electrónica no retenida según otra realización más.

En el bloque 602, el módulo receptor de mensajes 304 del módulo de mensajería no retenida 220 recibe un mensaje del cliente de mensajería del remitente 120. En el bloque 604, el módulo de solicitud de autenticación 306 solicita y recibe la autenticación del remitente desde un servidor de autorización 107. En el bloque 606, en respuesta a la autenticación en el bloque 604, el módulo de mensajería no retenida 220 recupera las preferencias del remitente, incluyendo una preferencia de la vida útil del mensaje y la preferencia de identificación del remitente. En el bloque 608, el módulo de generación de claves 308 genera una clave globalmente única. En el bloque 610, el módulo de generación de índices 310 genera opcionalmente un índice globalmente único. En el bloque 612, el módulo de

comprobación aleatoria de índice 312 genera un índice hash en base, al menos en parte, a la clave globalmente única generada en el bloque 608 y el índice globalmente único si se generó en el bloque 610. En el bloque 614, el módulo de cifrado de mensajes 316 cifra el mensaje usando una clave de cifrado en base, al menos en parte, a la clave globalmente única generada en el bloque 608. En el bloque 616, el módulo de almacenamiento de mensajes y generación de identificador 318 almacena el mensaje cifrado en memoria no persistente según el índice hash. En el bloque 618, el módulo de eliminación 324 establece un temporizador asociado con el mensaje. En el bloque 620, el módulo de almacenamiento de mensajes y generación de identificador 318 genera y envía un identificador de mensaje que incluye la clave globalmente única generada en el bloque 608. Cuando se genera un índice globalmente único en el bloque 610 y se usa para generar el índice hash en el bloque 612, el identificador de mensaje generado en el bloque 620 también incluye ese índice globalmente único.

Con referencia ahora a la Figura 6B, en el bloque 622, la información (por ejemplo, la clave globalmente única generada en el bloque 608, el índice globalmente único generado opcionalmente en el bloque 610, el índice hash generado en el bloque 612, la clave de cifrado usada en el bloque 614 y el identificador de mensaje generado en el bloque 620) se elimina de la memoria no persistente 207 por el módulo de eliminación 324.

En el bloque 624, el módulo de recuperación de mensajes 322 determina si se ha recibido una selección del identificador de mensaje. Si el módulo de recuperación de mensajes 322 determina que se ha recibido una selección del identificador de mensaje (624-Sí), el método 600 continúa en el bloque 629 o en el bloque 630 dependiendo de la realización. Cuando no se realiza la verificación de destinatario, para el mensaje asociado con el identificador seleccionado o de manera general, se salta o se omite el bloque 629 y el método 600 continúa en el bloque 630. Cuando se realiza la verificación de destinatario, para el mensaje asociado con el identificador seleccionado o de manera general, el método 600 continúa en el bloque 629. En el bloque 629, el módulo de verificación de destinatario 326 verifica el destinatario y en respuesta a una verificación con éxito del destinatario el método 600 continúa en el bloque 630. En el bloque 630, el módulo de recuperación de mensajes 322 recupera el mensaje y envía el mensaje para su presentación al usuario. El módulo de eliminación 324 elimina, en el bloque 632, el mensaje de la memoria no persistente 207, y el método 600 termina.

Si el módulo de recuperación de mensajes 322 determina que no se ha recibido una selección del identificador de mensaje (624-No), el método 600 continúa en el bloque 626. En el bloque 626, el módulo de eliminación 324 determina si se ha cumplido o excedido la vida útil del mensaje definida por el usuario. Si el módulo de eliminación 324 determina que se ha cumplido o excedido la vida útil del mensaje definida por el usuario (626-Sí), el método 600 continúa en el bloque 632. Si el módulo de eliminación 324 determina que no se ha cumplido o excedido la vida útil del mensaje definida por el usuario (626-No), el método 600 continúa en el bloque 628.

En el bloque 628, el módulo de eliminación 324 determina si se ha cumplido o excedido la vida útil del mensaje definida por el sistema. Si el módulo de eliminación 324 determina que se ha cumplido o excedido la vida útil del mensaje definida por el sistema (628-Sí), el método 600 continúa en el bloque 632. Si el módulo de eliminación 324 determina que no se ha cumplido o excedido la vida útil del mensaje definida por el sistema (628-No), el método 600 continúa en el bloque 624. En el bloque 632, el módulo de eliminación 324 elimina el mensaje de la memoria no persistente 207, y el método 600 termina.

La Figura 7 es un diagrama de flujo que ilustra un método 629 para verificar un destinatario según una realización. En el bloque 702, el módulo de verificación de destinatario 326 del módulo de mensajería no retenida 220 recibe un identificador de mensaje seleccionado. En el bloque 704, el módulo de verificación de destinatario 326 determina que el mensaje asociado con el identificador de mensaje seleccionado en el bloque 702 requiere verificación de destinatario. En el bloque 706, el módulo de verificación de destinatario 326 verifica la humanidad del destinatario. En el bloque 708, el módulo de verificación de destinatario 326 verifica la identidad del destinatario como el destinatario deseado (por ejemplo, usando información de verificación). Se debería observar que el método 629 verifica tanto la humanidad como la identidad del destinatario como el receptor deseado; no obstante, existen otras realizaciones que verifican solamente la humanidad o solamente que el destinatario es el destinatario deseado.

La Figura 8 es un diagrama de flujo que ilustra un método 800 para generar un registro y una notificación de un evento según una realización. En el bloque 802, el módulo de registro y notificación 328 del módulo de mensajería no retenida 220 detecta un evento en el sistema de mensajería no retenida 100. En el bloque 804, el módulo de registro y notificación 328 determina que el evento detectado desencadena la generación de un registro de ese evento detectado. En el bloque 806, el módulo de registro y notificación 328 genera un registro del evento detectado. En el bloque 808, el módulo de registro y notificación 328 determina que el evento detectado desencadena una notificación del evento detectado. En el bloque 810, el módulo de registro y notificación 328 determina un tipo de notificación (por ejemplo, correo electrónico, SMS, etc.). En el bloque 812, el módulo de registro y notificación 328 genera y formatea la notificación. En el bloque 814, el módulo de registro y notificación 328 envía la notificación. Se debería observar que aunque el método 800 describe un evento que desencadena tanto un registro como una notificación, en algunas realizaciones, algunos eventos pueden desencadenar o bien una generación de un registro o bien una notificación al usuario, pero no ambos. Se debería observar también que aunque el método 800 describe un evento que desencadena tanto un registro como una notificación, en algunas realizaciones, el módulo de registro y notificación 328 puede no proporcionar una de la funcionalidad de grabación y la funcionalidad de notificación.

En las realizaciones, se describe un sistema y un método para mensajería no retenida. En una realización, el sistema incluye un módulo receptor de mensajes, un módulo de almacenamiento de mensajes y generación de identificador, un módulo de recuperación de mensajes y un módulo de eliminación. El módulo receptor de mensajes recibe un mensaje. El módulo de generación de mensajes y generación de identificador almacena el mensaje en una memoria no transitoria y no persistente, la memoria no persistente de uno o más dispositivos informáticos, genera un identificador de mensaje y envía el identificador de mensaje al dispositivo destinatario. El módulo de recuperación de mensajes recibe una selección del identificador de mensaje desde el dispositivo destinatario, recupera el mensaje de la memoria no transitoria y no persistente, y envía el mensaje al dispositivo para su presentación. El módulo de eliminación elimina el mensaje del uno o más dispositivos en respuesta al envío del mensaje al dispositivo destinatario para su presentación.

La descripción anterior de las realizaciones se ha presentado con propósitos de ilustración y de descripción. Muchas modificaciones y variaciones son posibles a la luz de la enseñanza anterior. Del mismo modo, la denominación y división particular de los módulos, rutinas, rasgos, atributos, metodologías y otros aspectos no son obligatorios o significativos, y los mecanismos que implementan una realización o sus rasgos pueden tener diferentes nombres, divisiones y/o formatos. Además, como será evidente, los módulos, rutinas, rasgos, atributos, metodologías y otros aspectos de las realizaciones se pueden implementar como software, hardware, microprogramas o cualquier combinación de los tres. También, siempre que un componente, un ejemplo del cual es un módulo, se implemente como software, el componente se puede implementar como un programa autónomo, como parte de un programa más grande, como una pluralidad de programas separados, como una biblioteca vinculada estática o dinámicamente, como un módulo cargable del núcleo, como un controlador de dispositivo, y/o de todas y cada una de otras formas conocidas ahora o en el futuro. Además, las realizaciones no se limitan de ninguna forma a la implementación en ningún lenguaje de programación específico, o para cualquier sistema operativo o entorno específico.

REIVINDICACIONES

1. Un método (600) que comprende:

recibir, usando uno o más dispositivos informáticos, un mensaje (602);

generar, usando el uno o más dispositivos informáticos, una clave globalmente única (608);

generar, usando el uno o más dispositivos informáticos, un índice hash en base, al menos en parte, a la clave globalmente única (612);

almacenar, usando el uno o más dispositivos informáticos, el mensaje en una memoria no transitoria y no persistente, del uno o más dispositivos informáticos usando el índice hash (616);

establecer, usando el uno o más dispositivos informáticos, un temporizador usado para determinar si se ha excedido una vida útil asociada con el mensaje y si se ha de eliminar del uno o más dispositivos informáticos (618);

generar, usando el uno o más dispositivos informáticos, un identificador de mensaje, el identificador de mensaje en base, al menos en parte, a la clave globalmente única (620);

enviar, usando el uno o más dispositivos informáticos, el identificador de mensaje a un dispositivo destinatario (620);

eliminar, usando el uno o más dispositivos informáticos, la clave globalmente única, el índice hash y el identificador de mensaje del uno o más dispositivos informáticos en respuesta al envío del identificador de mensaje al dispositivo destinatario (622);

recibir, usando el uno o más dispositivos informáticos, una selección del identificador de mensaje desde el dispositivo destinatario y la clave globalmente única (624);

recibir, usando el uno o más dispositivos informáticos, una respuesta a un desafío;

verificar, usando el uno o más dispositivos informáticos, que un usuario del dispositivo destinatario es humano en base a la respuesta al desafío (706);

recuperar, usando el uno o más dispositivos informáticos, el mensaje de la memoria no transitoria y no persistente (630), en donde el mensaje se recupera de la memoria no transitoria y no persistente en base a que el usuario se verifique como humano;

enviar el mensaje al dispositivo destinatario para su presentación (630); y

eliminar, usando el uno o más dispositivos informáticos, el mensaje del uno o más dispositivos posterior a enviar el mensaje al dispositivo destinatario para su presentación (632).

2. El método (600) de la reivindicación 1 que comprende además:

recibir, usando el uno o más dispositivos informáticos, información de verificación desde el dispositivo destinatario;

verificar, usando el uno o más dispositivos informáticos, que un usuario del dispositivo destinatario es un destinatario deseado (708); y

en donde el mensaje se recupera de la memoria no transitoria y no persistente en base a que el usuario se verifica como destinatario deseado.

3. El método (600) de la reivindicación 2 que comprende además:

enviar una insinuación de información de verificación correcta con el identificador del mensaje.

4. El método (600) de la reivindicación 2 que comprende además:

enviar el identificador de mensaje y la información de verificación por separado; y/o

en donde uno o más del identificador de mensaje y el mensaje se envían de manera anónima; y/o

en donde el identificador de mensaje se envía a un dispositivo destinatario como uno o más de un correo electrónico a un usuario destinatario, un mensaje de texto al número de teléfono de un usuario destinatario y una publicación asociada con el sitio de red social de un usuario remitente.

5. El método (800) de una de las reivindicaciones anteriores que comprende además:

detectar, usando el uno o más dispositivos informáticos, un evento (802);

determinar, usando el uno o más dispositivos informáticos, si el evento detectado desencadena una o más de una generación de un registro del evento y una notificación del evento a un usuario (804, 808); y

generar, usando el uno o más dispositivos informáticos, uno o más del registro del evento y la notificación del evento en base a la determinación (806, 812).

6. El método (600) de una de las reivindicaciones anteriores que comprende además:

recibir, usando el uno o más dispositivos informáticos, una solicitud de retractación que incluye el identificador de mensaje del mensaje a ser retractado;

identificar, usando el uno o más dispositivos informáticos, el mensaje en una memoria no transitoria y no persistente del uno o más dispositivos informáticos en base al identificador de mensaje; y

eliminar, usando el uno o más dispositivos informáticos, el mensaje del uno o más dispositivos en respuesta a recibir la solicitud de retractación, en donde el mensaje ya no está disponible para su recuperación y envío al dispositivo destinatario en respuesta a recibir la solicitud de retractación.

7. Un sistema que comprende:

un procesador de hardware (206); y

una memoria (205, 208), la memoria (205, 208) que almacena instrucciones que, cuando se ejecutan por el procesador de hardware (206), hacen que el sistema:

reciba un mensaje;

genere una clave globalmente única;

genere un índice hash en base, al menos en parte, a la clave globalmente única;

almacene el mensaje en una memoria no transitoria y no persistente (207) usando el índice hash;

establezca un temporizador usado para determinar si se ha excedido una vida útil asociada con el mensaje y si se ha de eliminar de la memoria no transitoria y no persistente (207);

genere un identificador de mensaje, el identificador de mensaje en base, al menos en parte, a la clave globalmente única;

envíe el identificador de mensaje a un dispositivo destinatario;

elimine la clave globalmente única, el índice hash y el identificador de mensaje en respuesta al envío del identificador de mensaje al dispositivo destinatario;

reciba una selección del identificador de mensaje desde el dispositivo destinatario y la clave globalmente única;

reciba una respuesta a un desafío y verifique que un usuario del dispositivo destinatario sea humano en base a la respuesta al desafío;

recupere el mensaje de la memoria no transitoria y no persistente (207), en donde el mensaje se recupera de la memoria no transitoria y no persistente (207) en base a que el usuario se verifique como humano;

envíe el mensaje al dispositivo destinatario para su presentación; y

elimine el mensaje de la memoria no transitoria y no persistente (207) posterior al envío del mensaje al dispositivo destinatario para su presentación.

8. El sistema de la reivindicación 7 que comprende además instrucciones que hacen que el sistema:

reciba información de verificación desde el dispositivo destinatario y verifique que un usuario del dispositivo destinatario es un destinatario deseado; y

en donde el mensaje se recupera de la memoria no transitoria y no persistente (207) en base a que el usuario se verifica como un destinatario deseado.

9. El sistema de una de las reivindicaciones 7 a 8 en donde el identificador de mensaje y la insinuación de información de verificación correcta se envían juntos; y/o

en donde uno o más del identificador de mensaje y el mensaje se envían de manera anónima; y/o

en donde el identificador de mensaje se envía a un dispositivo destinatario como uno o más de un correo electrónico al correo electrónico de un usuario destinatario, un mensaje de texto al número de teléfono de un usuario destinatario y una publicación en el sitio de red social de un usuario remitente.

10. El sistema de la reivindicación 8 o 9 en donde el identificador de mensaje y la información de verificación se envían por separado.

11. El sistema de una de las reivindicaciones 7 a 8 que comprende además instrucciones que hacen que el sistema:

detecte un evento, determine si el evento detectado desencadena una o más de una generación de un registro del evento y una notificación del evento a un usuario, y genere uno o más del registro del evento y la notificación del evento en base a la determinación.

12. Un medio de almacenamiento no transitorio que incluye instrucciones que, cuando se ejecutan por un dispositivo informático, hacen que el dispositivo informático:

reciba un mensaje;

genere una clave globalmente única;

genere un índice hash en base, al menos en parte, a la clave globalmente única;

almacene el mensaje en una memoria no transitoria y no persistente del dispositivo informático usando el índice hash;

establezca un temporizador usado para determinar si se ha excedido una vida útil asociada con el mensaje y si se ha de eliminar del uno o más dispositivos informáticos;

genere un identificador de mensaje, el identificador de mensaje en base, al menos en parte, a la clave globalmente única;

envíe el identificador de mensaje a un dispositivo destinatario;

elimine la clave globalmente única, el índice hash y el identificador de mensaje del uno o más dispositivos informáticos en respuesta al envío del identificador de mensaje al dispositivo destinatario;

reciba una selección del identificador de mensaje desde el dispositivo destinatario y la clave globalmente única;

reciba una respuesta a un desafío y verifique que un usuario del dispositivo destinatario sea humano en base a la respuesta al desafío;

recupere el mensaje de la memoria no transitoria y no persistente, en donde el mensaje se recupera de la memoria no transitoria y no persistente en base a que el usuario se verifique como humano;

envíe el mensaje al dispositivo destinatario para su presentación; y

elimine el mensaje del uno o más dispositivos en respuesta al envío del mensaje al dispositivo destinatario para su presentación.

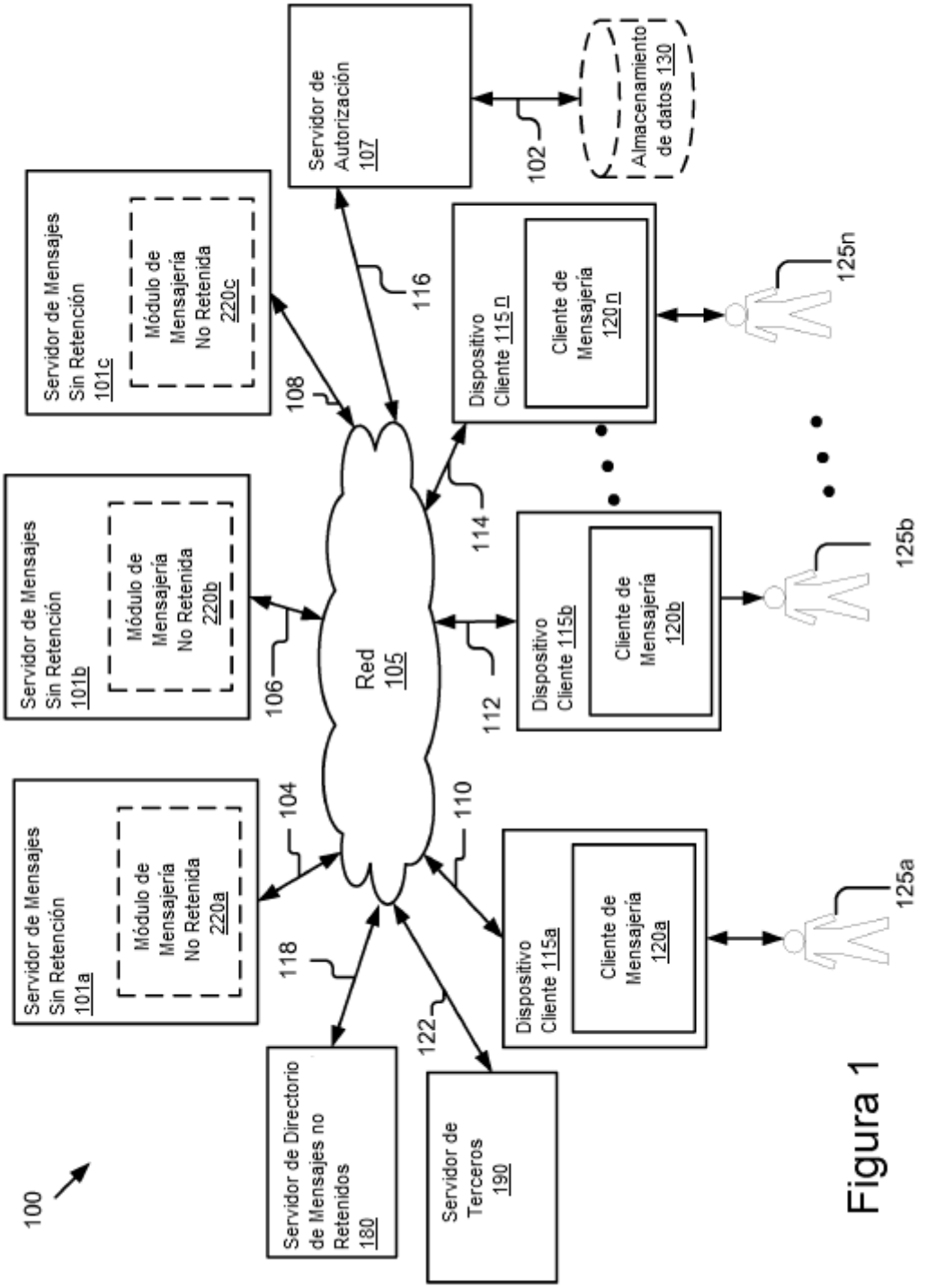
100
Servidor de Mensajes Sin Retención 101a
Módulo de Mensajería No Retenida 220a
Servidor de Mensajes Sin Retención 101b
Módulo de Mensajería No Retenida 220b
Servidor de Mensajes Sin Retención 101c
Módulo de Mensajería No Retenida 220c
Servidor de Autorización 107
Almacenamiento de datos 130
Servidor de Directorio de Mensajes no Retenidos 180
Servidor de Terceros 190
Red 105
Dispositivo Cliente 115a
Cliente de Mensajería 120a
Dispositivo Cliente 115b
Cliente de Mensajería 120b
Dispositivo Cliente 115 n
Cliente de Mensajería 120 n
102
104
106
108
110
112
114
116
118
122
125a
125b
125n

Figura 1

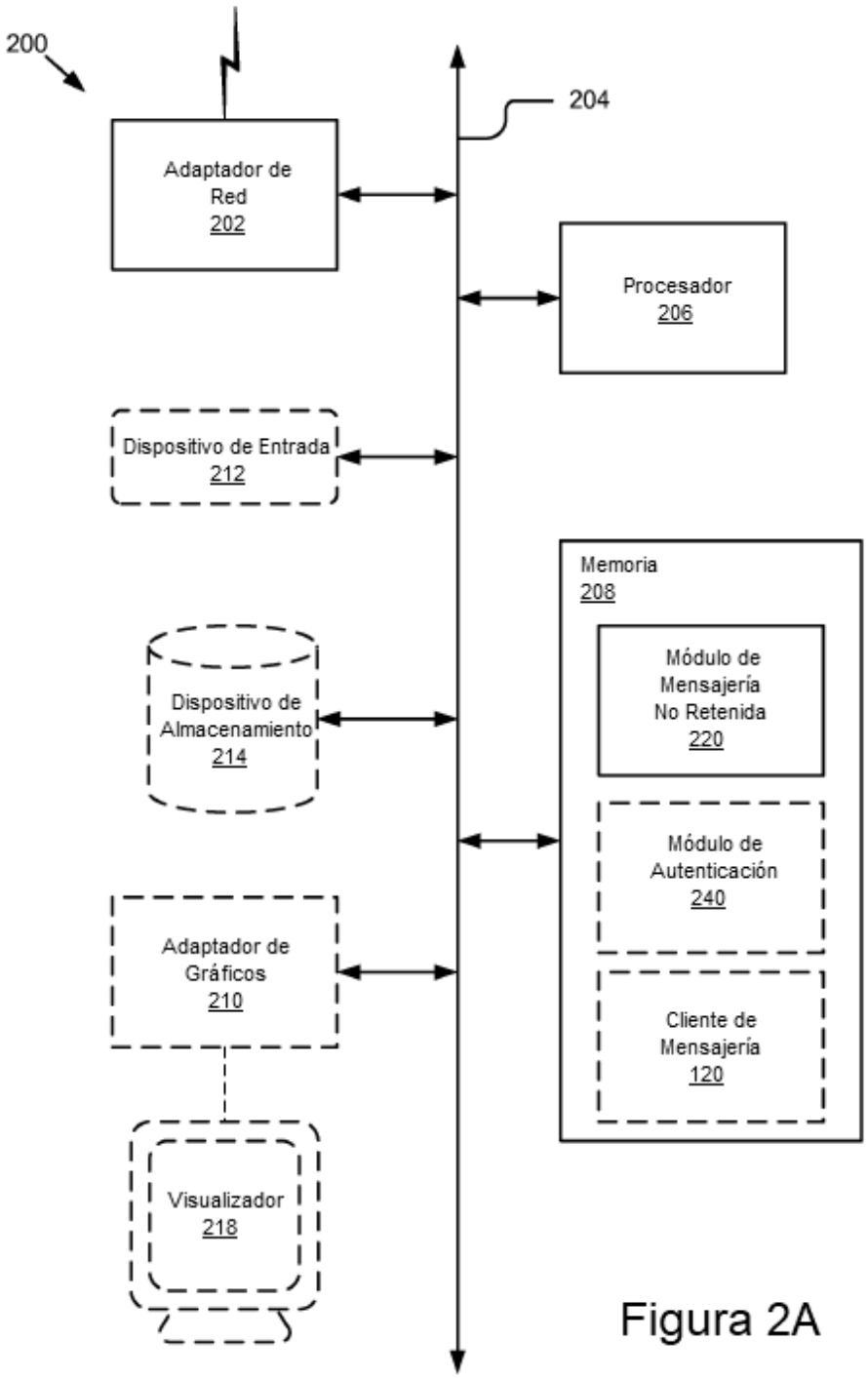
200
204
Adaptador de Red 202
Procesador 206
Dispositivo de Entrada 212
Memoria 208
Módulo de Mensajería No Retenida 220
Dispositivo de Almacenamiento 214
Módulo de Autenticación 240
Adaptador de Gráficos 210
Cliente de Mensajería 120
Visualizador 218

Figura 2A

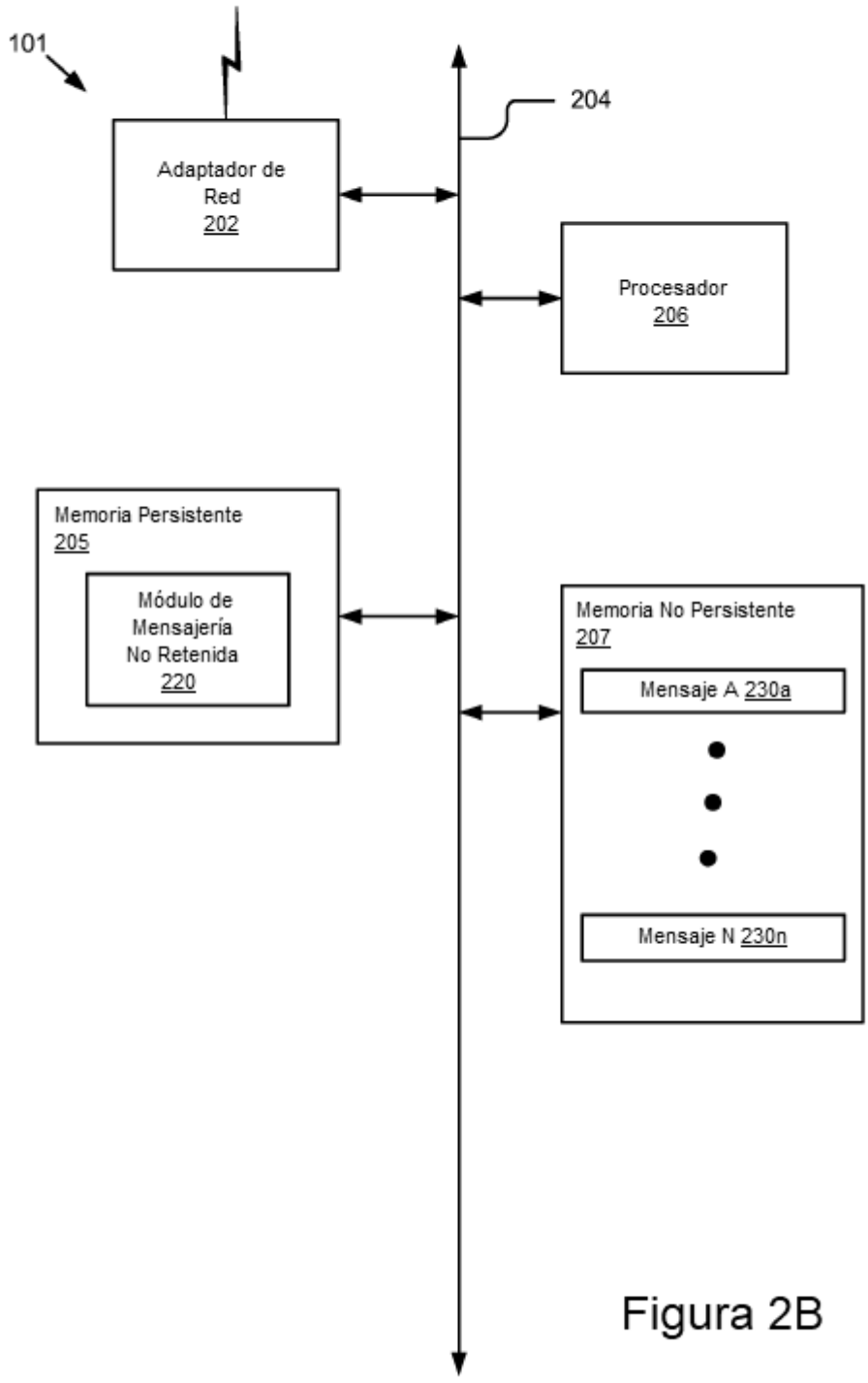
101
204
Adaptador de Red 202
Procesador 206
Memoria Persistente 205
Módulo de Mensajería No Retenida 220
Memoria No Persistente 207
Mensaje A 230a
Mensaje N 230n

Figura 2B

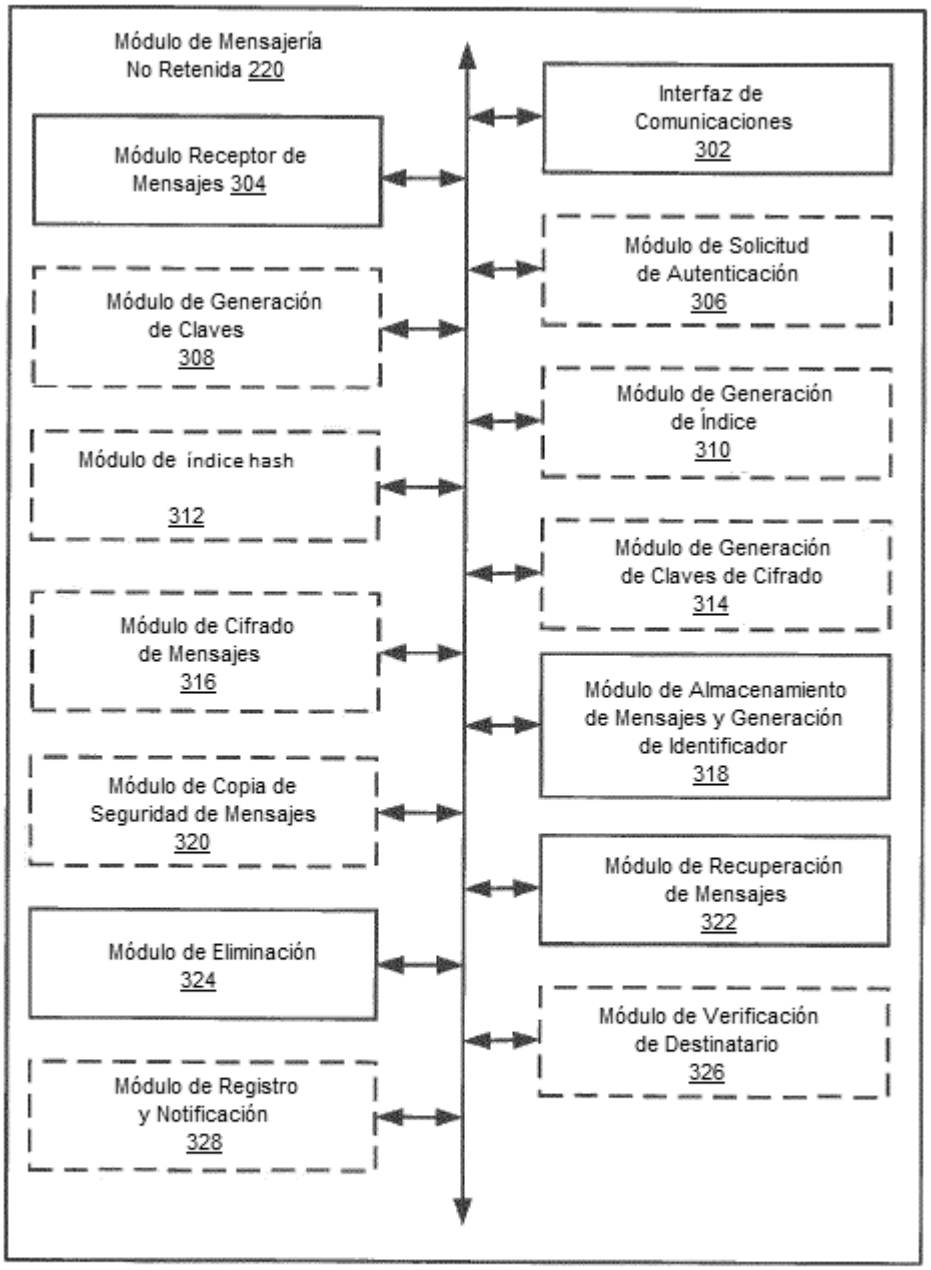
Módulo de Mensajería No Retenida 220
Módulo Receptor de Mensajes 304
Módulo de Generación de Claves 308
Módulo de índice hash 312
Módulo de Cifrado de Mensajes 316
Módulo de Copia de Seguridad de Mensajes 320
Módulo de Eliminación 324
Módulo de Registro y Notificación 328
Interfaz de Comunicaciones 302
Módulo de Solicitud de Autenticación 306
Módulo de Generación de Índice 310
Módulo de Generación de Claves de Cifrado 314
Módulo de Almacenamiento de Mensajes y Generación de Identificador 318
Módulo de Recuperación de Mensajes 322
Módulo de Verificación de Destinatario 326

Figura 3

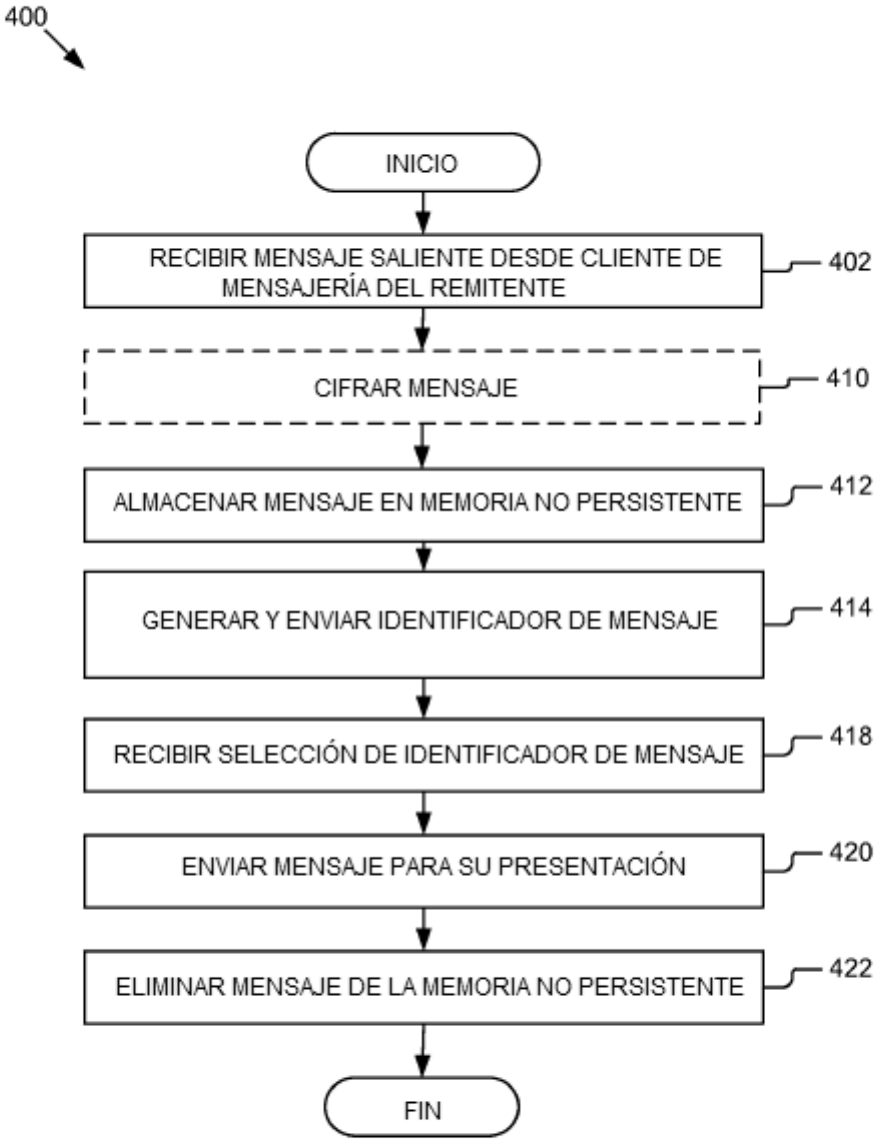
400
INICIO
RECIBIR MENSAJE SALIENTE DESDE CLIENTE DE MENSAJERÍA DEL REMITENTE
402
CIFRAR MENSAJE
410
ALMACENAR MENSAJE EN MEMORIA NO PERSISTENTE
412
GENERAR Y ENVIAR IDENTIFICADOR DE MENSAJE
414
RECIBIR SELECCIÓN DE IDENTIFICADOR DE MENSAJE
418
ENVIAR MENSAJE PARA SU PRESENTACIÓN
420
ELIMINAR MENSAJE DE LA MEMORIA NO PERSISTENTE
422
FIN

Figura 4

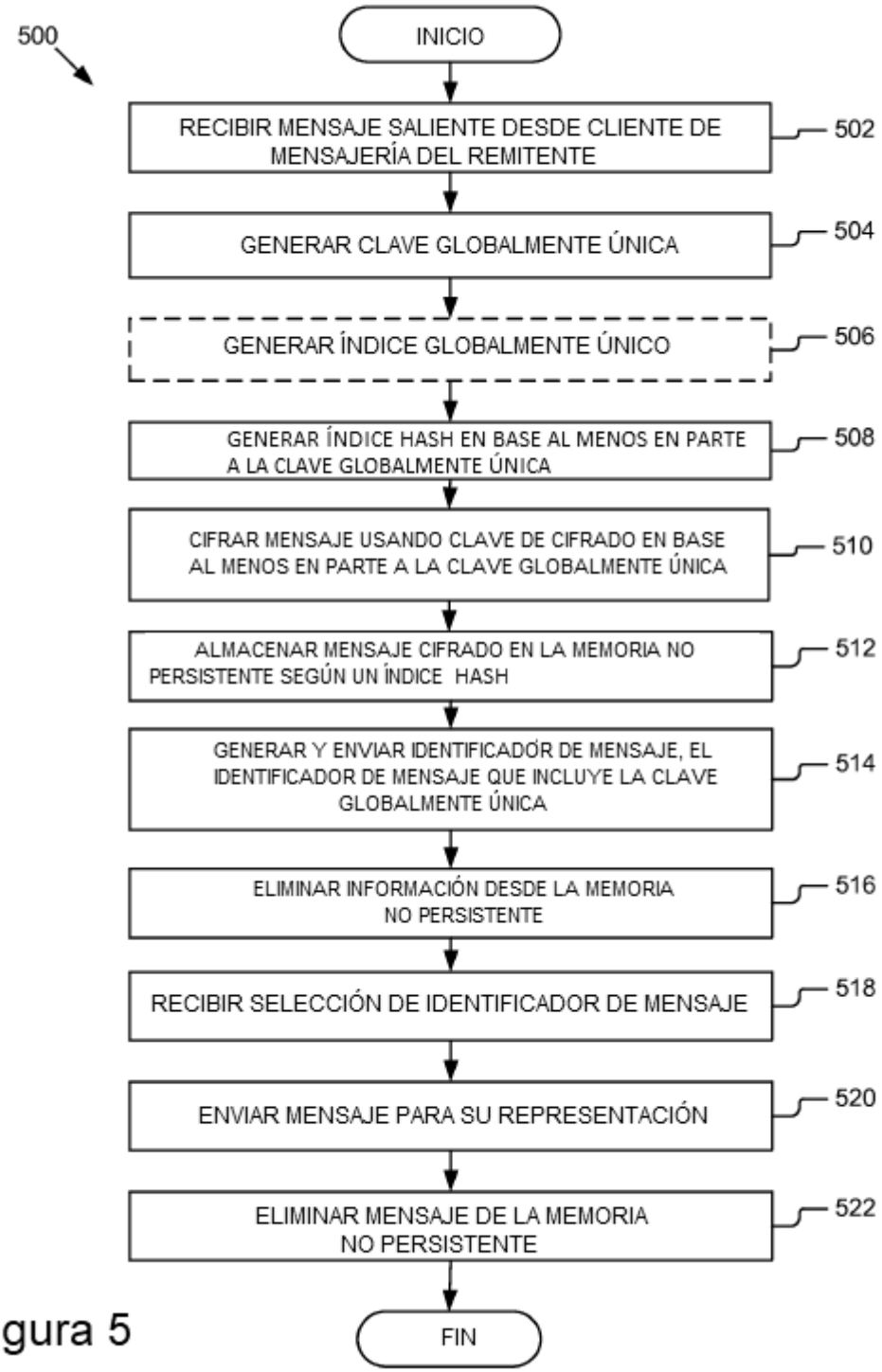
500
INICIO
RECIBIR MENSAJE SALIENTE DESDE CLIENTE DE MENSAJERÍA DEL REMITENTE
502
GENERAR CLAVE GLOBALMENTE ÚNICA
504
GENERAR ÍNDICE GLOBALMENTE ÚNICO
506
GENERAR ÍNDICE HASH EN BASE AL MENOS EN PARTE A LA CLAVE GLOBALMENTE ÚNICA
508
CIFRAR MENSAJE USANDO CLAVE DE CIFRADO EN BASE AL MENOS EN PARTE A LA CLAVE GLOBALMENTE ÚNICA
510
ALMACENAR MENSAJE CIFRADO EN LA MEMORIA NO PERSISTENTE SEGÚN UN ÍNDICE HASH
512
GENERAR Y ENVIAR IDENTIFICADOR DE MENSAJE, EL IDENTIFICADOR DE MENSAJE QUE INCLUYE LA CLAVE GLOBALMENTE ÚNICA
514
ELIMINAR INFORMACIÓN DESDE LA MEMORIA NO PERSISTENTE
516
RECIBIR SELECCIÓN DE IDENTIFICADOR DE MENSAJE
518
ENVIAR MENSAJE PARA SU REPRESENTACIÓN
520
ELIMINAR MENSAJE DE LA MEMORIA NO PERSISTENTE
522
FIN

Figura 5

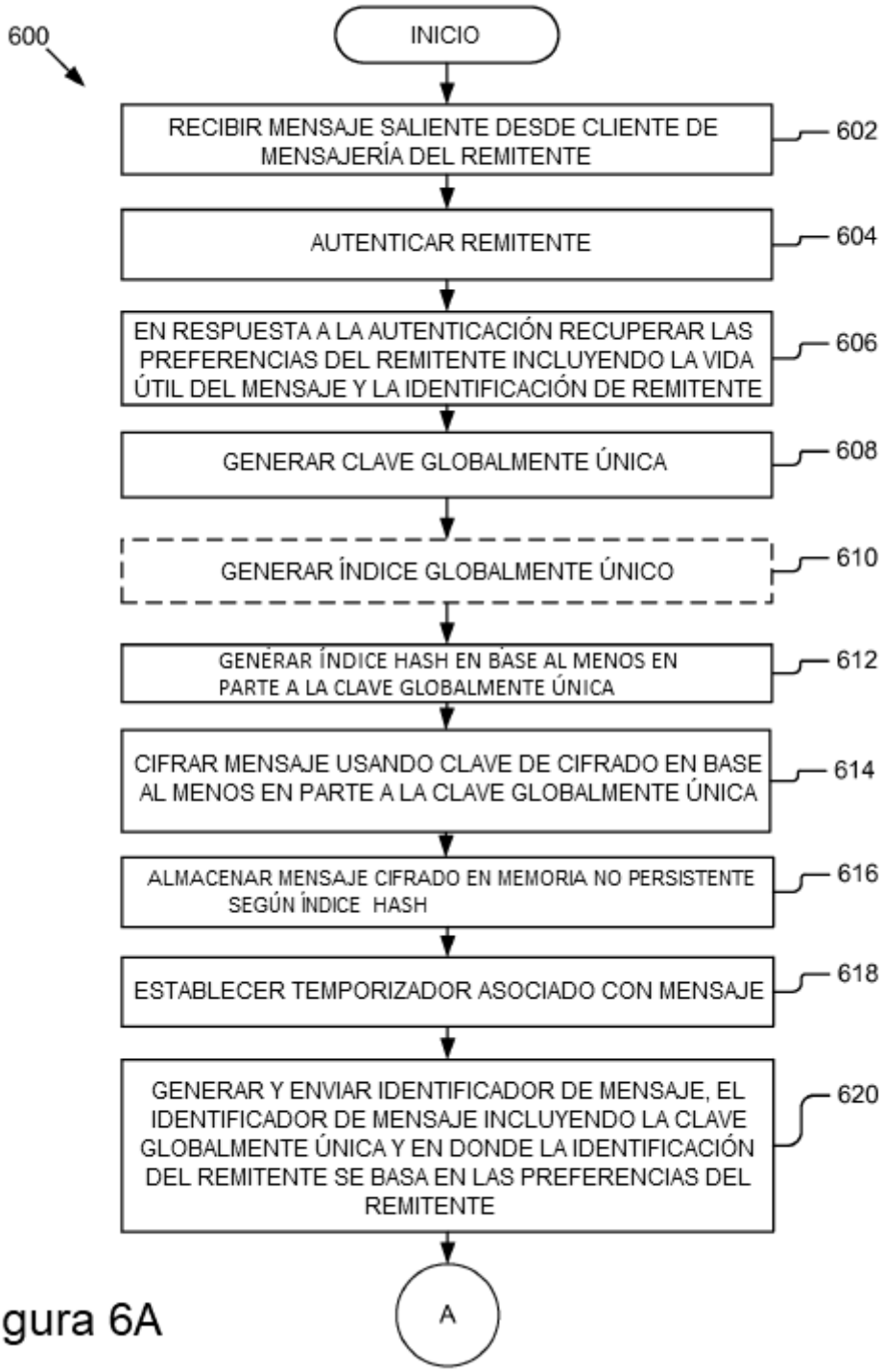
600
INICIO
RECIBIR MENSAJE SALIENTE DESDE CLIENTE DE MENSAJERÍA DEL REMITENTE
602
AUTENTICAR REMITENTE
604
EN RESPUESTA A LA AUTENTICACIÓN RECUPERAR LAS PREFERENCIAS DEL REMITENTE INCLUYENDO LA VIDA ÚTIL DEL MENSAJE Y LA IDENTIFICACIÓN DE REMITENTE
606
GENERAR CLAVE GLOBALMENTE ÚNICA
608
GENERAR ÍNDICE GLOBALMENTE ÚNICO
610
GENERAR ÍNDICE HASH EN BASE AL MENOS EN PARTE A LA CLAVE GLOBALMENTE ÚNICA
612
CIFRAR MENSAJE USANDO CLAVE DE CIFRADO EN BASE AL MENOS EN PARTE A LA CLAVE GLOBALMENTE ÚNICA
614
ALMACENAR MENSAJE CIFRADO EN MEMORIA NO PERSISTENTE SEGÚN ÍNDICE HASH
616
ESTABLECER TEMPORIZADOR ASOCIADO CON MENSAJE
618
GENERAR Y ENVIAR IDENTIFICADOR DE MENSAJE, EL IDENTIFICADOR DE MENSAJE INCLUYENDO LA CLAVE GLOBALMENTE ÚNICA Y EN DONDE LA IDENTIFICACIÓN DEL REMITENTE SE BASA EN LAS PREFERENCIAS DEL REMITENTE
620
A

Figura 6A

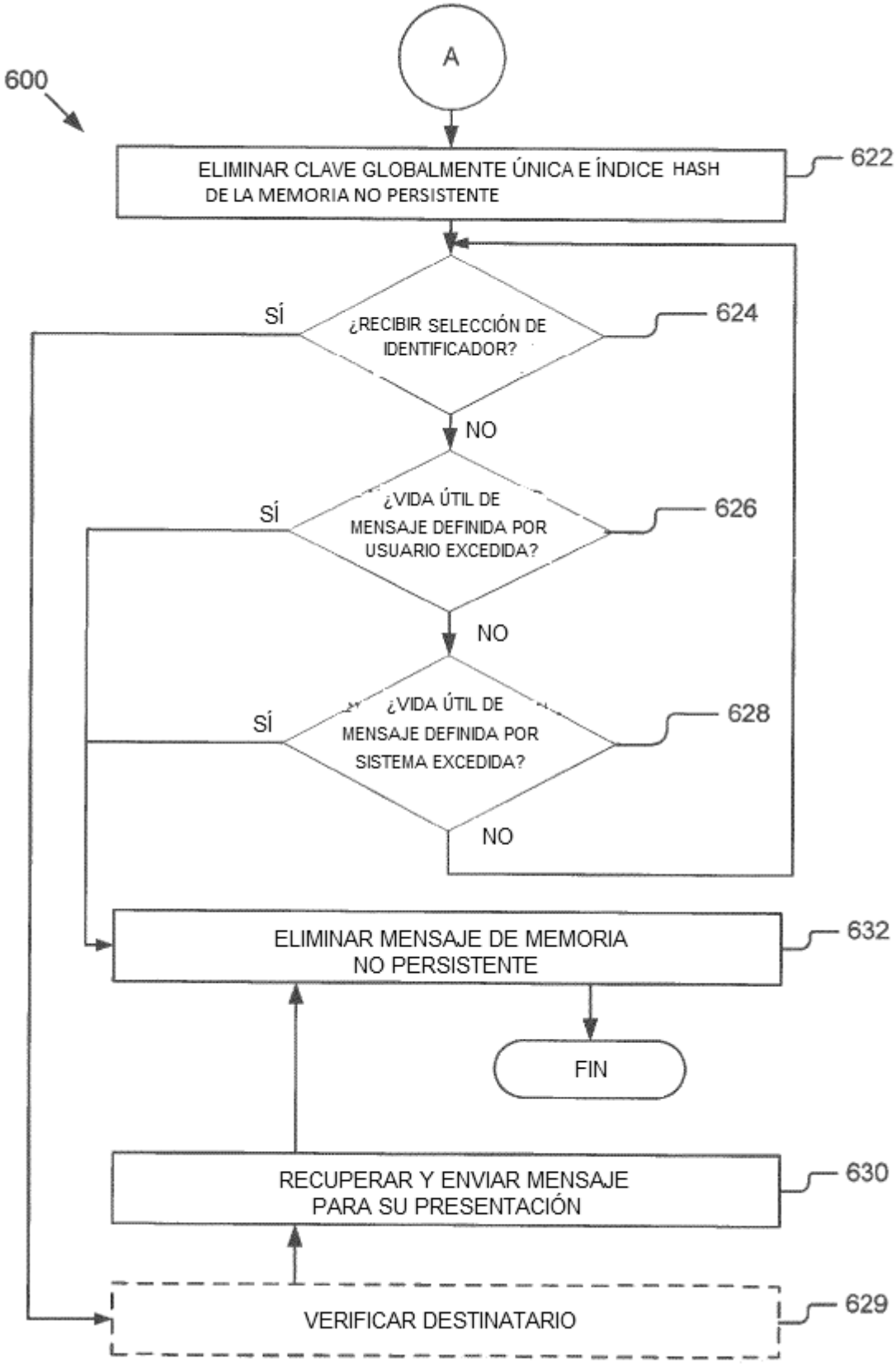
600
A
ELIMINAR CLAVE GLOBALMENTE ÚNICA E ÍNDICE HASH DE LA MEMORIA NO PERSISTENTE
622
¿RECIBIR SELECCIÓN DE IDENTIFICADOR?
624
SÍ
NO
¿VIDA ÚTIL DE MENSAJE DEFINIDA POR USUARIO EXCEDIDA?
626
SÍ
NO
¿VIDA ÚTIL DE MENSAJE DEFINIDA POR SISTEMA EXCEDIDA?
628
SÍ
NO
ELIMINAR MENSAJE DE MEMORIA NO PERSISTENTE
632
FIN
RECUPERAR Y ENVIAR MENSAJE PARA SU PRESENTACIÓN
630
VERIFICAR DESTINATARIO
629

Figura 6B

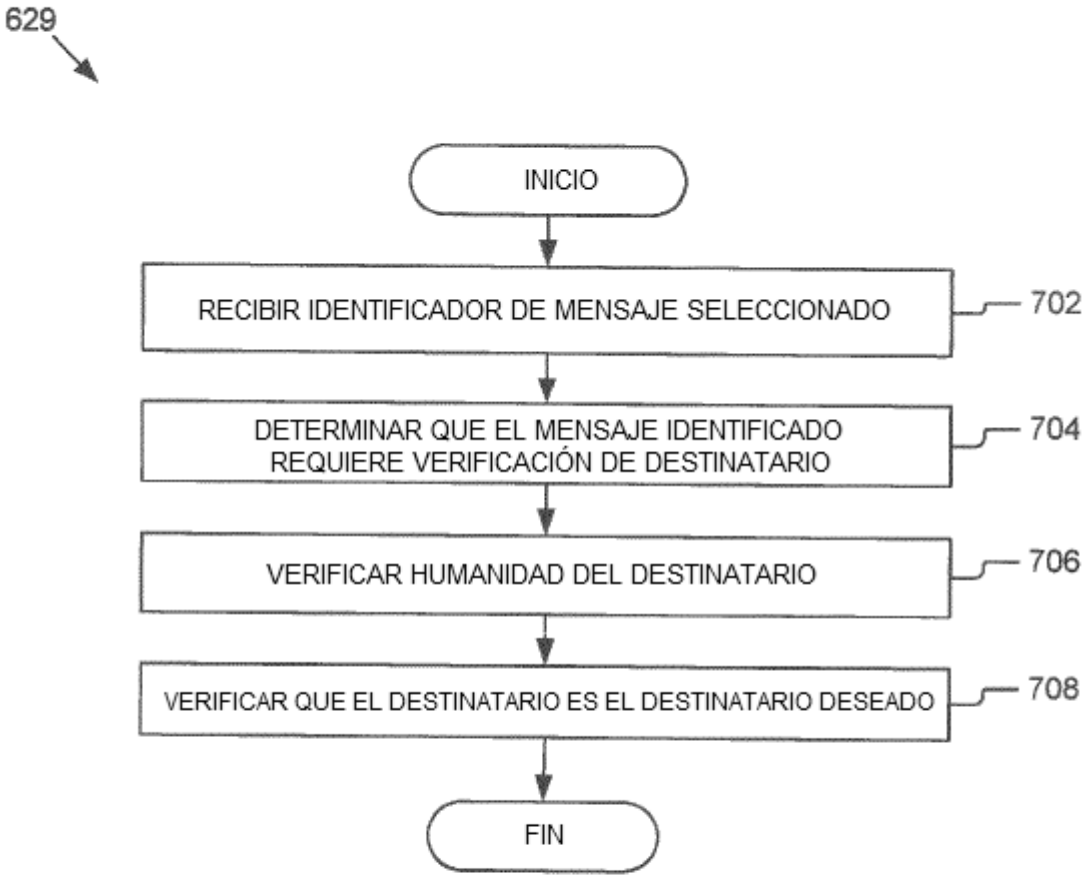
629
INICIO
RECIBIR IDENTIFICADOR DE MENSAJE SELECCIONADO
702
DETERMINAR QUE EL MENSAJE IDENTIFICADO REQUIERE VERIFICACIÓN DE DESTINATARIO
704
VERIFICAR HUMANIDAD DEL DESTINATARIO
706
VERIFICAR QUE EL DESTINATARIO ES EL DESTINATARIO DESEADO
708
FIN

Figura 7

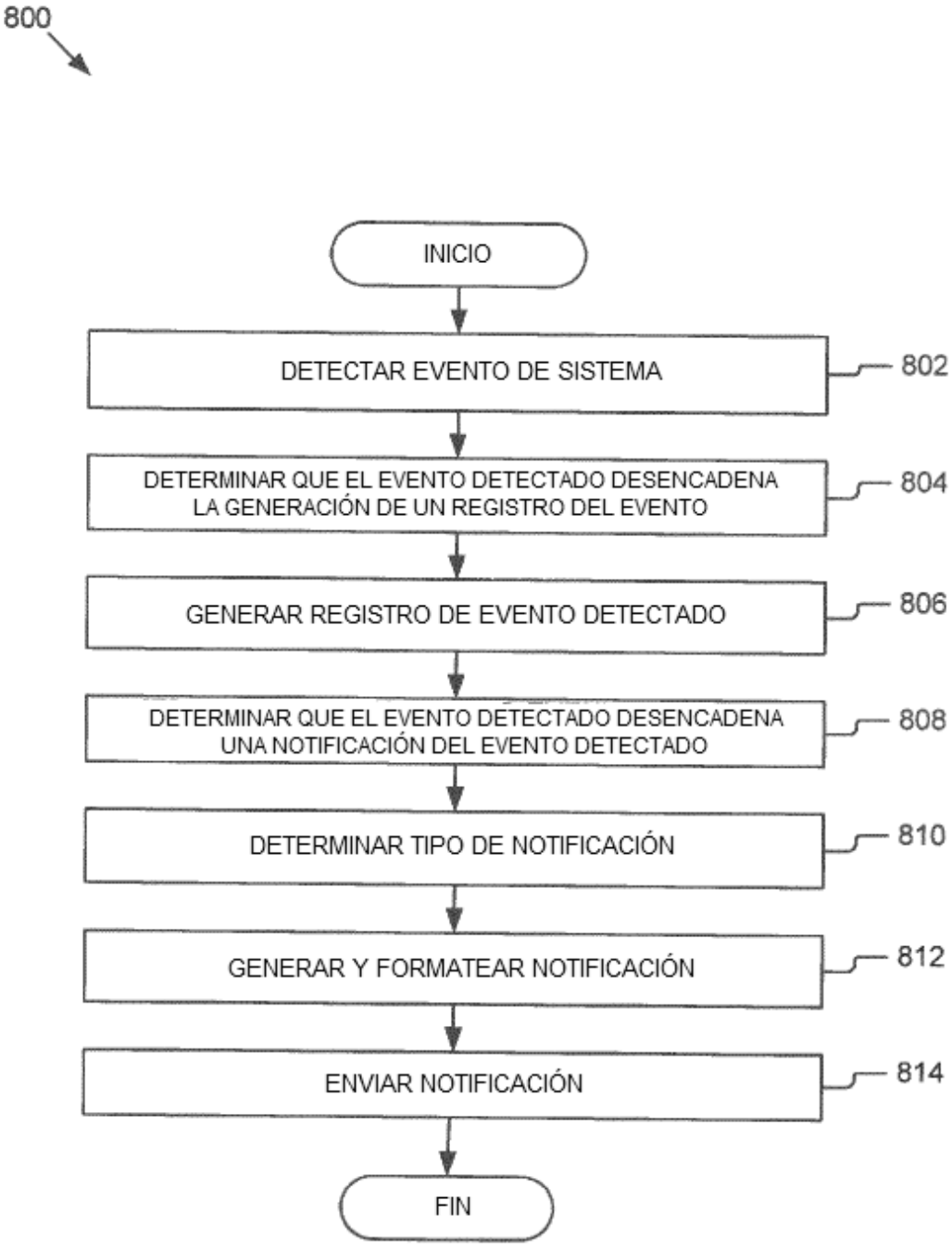
800
INICIO
DETECTAR EVENTO DE SISTEMA
802
DETERMINAR QUE EL EVENTO DETECTADO DESENCADENA LA GENERACIÓN DE UN REGISTRO DEL EVENTO
804
GENERAR REGISTRO DE EVENTO DETECTADO
806
DETERMINAR QUE EL EVENTO DETECTADO DESENCADENA UNA NOTIFICACIÓN DEL EVENTO DETECTADO
808
DETERMINAR TIPO DE NOTIFICACIÓN
810
GENERAR Y FORMATEAR NOTIFICACIÓN
812
ENVIAR NOTIFICACIÓN
814
FIN

Figura 8