(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 449 790**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **23.02.2009 E 09700010 (3)**

(97) Fecha y número de publicación de la concesión europea: **25.12.2013 EP 2163067**

(54) Título: **Sistemas y métodos para la gestión y la comunicación seguras en un grupo de trabajo**

(30) Prioridad:

22.02.2008 US 66699 P
28.01.2009 US 147961 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
21.03.2014

(73) Titular/es:

SECURITY FIRST CORP. (100.0%)
22362 Gilberto, Suite 130
Rancho Santa Margarita, CA 92688, US

(72) Inventor/es:

BONO, STEPHEN C.;
GREEN, MATTHEW D.;
LANDAU, GABRIEL D.;
ORSINI, RICK L.;
O'HARE, MARK S. y
DAVENPORT, ROGER

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Sistemas y métodos para la gestión y la comunicación seguras en un grupo de trabajo

Referencia cruzada a solicitudes relacionadas

Esta memoria reivindica los derechos de las Solicitudes de Patente Provisional de los Estados Unidos Nos. 61/066.699, titulada “Sistemas y métodos para la gestión segura de un grupo de trabajo” (“Systems and Methods for Secure Workgroup Management”), presentada el 22 de febrero de 2008, y 61/147.961, titulada “Gestión y distribución de claves de grupos de trabajo” (“Workgroup Key Management and Distribution”), presentada el 28 de enero de 2009.

Campo de la Invención

La presente invención se refiere, en general, a sistemas y métodos mejorados para asegurar datos en movimiento (es decir, datos que están siendo transferidos desde una posición a otra) dentro de un grupo de trabajo. Los sistemas y métodos que se describen en esta memoria pueden ser utilizados en combinación con otros sistemas y métodos descritos en la Patente de los EE.UU. 7.391.865, de propiedad en común con la presente, y en las Solicitudes de Patente de los EE.UU., de propiedad en común con la presente, Nos. 10/458.928, presentada el 11 de junio de 2003, 11/258.839, presentada el 25 de octubre de 2005, 11/602.667, presentada el 20 de noviembre de 2006, 11/983.355, presentada el 7 de noviembre de 2007, 11/999.575, presentada el 5 de diciembre de 2007, 12/209.703, presentada el 12 de septiembre de 2008, y 12/349.897, presentada el 7 de enero de 2009.

Antecedentes de la Invención

En la sociedad actual, las personas y las empresas llevan a cabo una cantidad cada vez mayor de actividades en sistemas informáticos y a través de ellos. Estos sistemas informáticos, incluyendo redes informáticas mantenidas en propiedad y no tenidas en propiedad, realizan con frecuencia el almacenamiento, archivo y transmisión de todo tipo de información delicada. Así, pues, existe una necesidad cada vez mayor de garantizar que los datos almacenados y transmitidos a través de estos sistemas no pueden ser leídos ni de otro modo comprometidos.

Una solución común para asegurar sistemas informáticos consiste en proporcionar la capacidad funcional de introducción de identificación y palabra de paso. Sin embargo, la gestión de las palabras de paso ha demostrado ser bastante costosa, con un alto porcentaje de llamadas de asistencia en el puesto referentes a problemas con las palabras de paso. Es más, las palabras de paso proporcionan una escasa seguridad por cuanto son, generalmente, almacenadas en un archivo susceptible de acceso indebido, a través, por ejemplo, de ataques usando la fuerza bruta.

Otra solución para asegurar sistemas informáticos consiste en proporcionar infraestructuras criptográficas. La criptografía se refiere, en general, a la protección de los datos al transformarlos, o cifrarlos, en un formato ilegible. Únicamente quienes poseen la(s) clave(s) de la encriptación o cifrado pueden descifrar los datos convirtiéndolos en un formato utilizable. La criptografía puede ser utilizada para identificar usuarios, por ejemplo, autentificación, con el fin de permitir el acceso a privilegios, por ejemplo, autorización, para crear certificados y firmas digitales, y funciones similares. Un sistema criptográfico popular es un sistema de clave pública que se sirve de dos claves, una clave pública conocida por todo el mundo y una clave privada conocida únicamente por la persona o la empresa propietaria de la misma. En general, los datos encriptados o cifrados con una de las claves son descifrados con la otra y ninguna de las claves puede ser recreada a partir de la otra.

Desgraciadamente, incluso los anteriores sistemas criptográficos de clave pública convencionales siguen basándose en gran medida en el usuario para su seguridad. Por ejemplo, los sistemas criptográficos facilitan la clave privada al usuario, por ejemplo, a través del navegador o explorador del usuario. Los usuarios sin conocimientos especializados almacenan entonces, por lo general, la clave privada en un dispositivo de accionamiento de disco duro accesible a otros a través de un sistema informático abierto, tal como, por ejemplo, la Internet. Por otra parte, los usuarios pueden escoger nombres inadecuados para los archivos que contienen su clave privada, tales como, por ejemplo, “clave”. El resultado de la anterior y de otras acciones es permitir que la clave o claves sean susceptibles de comprometerse o ponerse en peligro.

Las soluciones convencionales para el aseguramiento de los datos en movimiento no alcanzan tampoco a proporcionar un soporte de grupo de trabajo robusto y seguro. Por ejemplo, los miembros de un grupo de trabajo pueden desear comunicarse de forma segura (por ejemplo, de una manera privada y autentificada) con otros miembros del grupo de trabajo a través de uno o más canales seguros. Los protocolos seguros de comunicación de grupo de trabajo convencionales basados en claves de cifrado de grupo de trabajo previamente compartidas, en cifrado de difusión de clave pública, y en elementos similares, a menudo se vuelven inestables e inseguros debido a una gestión y distribución no seguras e ineficientes de la clave de grupo de trabajo compartida. Además de ello, estos protocolos de comunicación de grupo de trabajo seguros incluyen, generalmente, tan solo un soporte de revocación de cliente de grupo de trabajo limitado. Por ejemplo, los privilegios de comunicación de un miembro del grupo de trabajo cualquiera no pueden, por lo general, ser eficientemente revocados, por ejemplo, tras haberse puesto en peligro la identidad del miembro o la clave del grupo de trabajo compartida, o después de que el miembro

de grupo de trabajo ha abandonado un grupo de trabajo. Es más, con las soluciones convencionales, no hay, generalmente, modo alguno de renovar de una forma rápida y eficaz un mecanismo de seguridad de un grupo de trabajo, ya sea bajo petición, ya sea de forma periódica o automáticamente una vez que se han revocado los privilegios de comunicación de un miembro cualquiera del grupo de trabajo (o bien el miembro de grupo de trabajo ha abandonado el grupo de trabajo).

El documento US 2007/160.138 divulga una comunicación de grupo de trabajo segura en la que una clave del grupo de trabajo se convierte en un credencial compartido para los miembros del grupo de trabajo.

Compendio de la Invención

Basándose en lo anterior, existe la necesidad de proporcionar un esquema de seguridad de grupo de trabajo más robusto y seguro para uso con soluciones de datos en movimiento.

La presente invención se define por la materia objeto de las reivindicaciones independientes. Realizaciones preferidas se definen por las reivindicaciones dependientes.

Breve descripción de los dibujos

La presente invención se describe con mayor detalle en lo que sigue, en asociación con los dibujos que se acompañan, que se dan con la intención de ilustrar, y no limitar, la invención, y en los cuales:

La Figura 1 ilustra un diagrama de bloques de un sistema criptográfico de acuerdo con aspectos de una realización de la invención;

La Figura 2 ilustra un diagrama de bloques del motor de confianza de la Figura 1, de acuerdo con aspectos de una realización de la invención;

La Figura 3 ilustra un diagrama de bloques del motor de transacciones de la Figura 2, de acuerdo con aspectos de una realización de la invención;

La Figura 4 ilustra un diagrama de bloques del repositorio de la Figura 2, de acuerdo con aspectos de una realización de la invención;

La Figura 5 ilustra un diagrama de bloques del motor de autentificación de la Figura 2, de acuerdo con aspectos de una realización de la invención;

La Figura 6 ilustra un diagrama de bloques del motor criptográfico de la Figura 2, de acuerdo con aspectos de una realización de la invención;

La Figura 7 es un diagrama de bloques de un sistema de datos en movimiento ilustrativo, de acuerdo con una realización de la presente invención;

La Figura 8 es un diagrama de bloques de otro sistema de datos en movimiento ilustrativo, de acuerdo con una realización de la presente invención;

Las Figuras 9A y 9B son diagramas de flujo de procedimiento simplificados e ilustrativos para la generación de encabezamiento y la partición o división de datos para datos en movimiento, que pueden ser utilizados en cualquier combinación apropiada, con cualesquiera adiciones, borrados o modificaciones apropiados, de acuerdo con una realización de la presente invención;

La Figura 10 es un diagrama de bloques simplificado de un formato de compartimiento ilustrativo que puede ser utilizado en cualquier combinación adecuada, con cualesquiera adiciones, borrados o modificaciones apropiados, de acuerdo con una realización de la presente invención;

La Figura 11 es un protocolo simplificado que ilustra la secuencia de mensajes para la autentificación de un cliente dentro de un grupo de trabajo, de acuerdo con una realización de la presente invención;

La Figura 12 es un protocolo simplificado que ilustra la secuencia de mensajes para obtener tiques de servicio en un grupo de trabajo, de acuerdo con una realización de la presente invención;

La Figura 13 es un protocolo simplificado que ilustra la secuencia de mensajes para utilizar una clave de grupo de trabajo con el fin de asegurar datos en movimiento de acuerdo con una realización de la presente invención;

La Figura 14 es un protocolo simplificado que ilustra la secuencia de mensajes para la interacción de los espacios de Kernel y del usuario de acuerdo con una realización de la presente invención;

La Figura 15 es un diagrama de bloques simplificado del ajuste inicial de Autoridades de Grupos de Trabajo dentro de un dominio, de acuerdo con una realización de la presente invención;

La Figura 16 es un protocolo simplificado que ilustra la secuencia de conexión de dos clientes dentro de un grupo de trabajo, de acuerdo con una realización de la presente invención;

La Figura 17 es un diagrama de flujo de procedimiento ilustrativo para unirse a un grupo de trabajo, de acuerdo con una realización de la presente invención;

Las Figuras 18A, 18B y 18C son diagramas de flujo de procedimiento ilustrativos para iniciar una conexión entre dos clientes de grupo de trabajo, de acuerdo con una realización de la presente invención;

La Figura 19 es un diagrama de flujo de procedimiento ilustrativo para revocar privilegios de comunicación de un cliente dentro de un grupo de trabajo, de acuerdo con una realización de la presente invención; y

La Figura 20 es un diagrama de flujo de procedimiento ilustrativo para actualizar una clave de grupo de trabajo de acuerdo con una realización de la presente invención.

Descripción detallada

La presente invención proporciona un sistema criptográfico en el que uno o más servidores seguros, o un motor de confianza, almacenan claves criptográficas y datos de autentificación de usuario. Los usuarios pueden acceder a la capacidad funcional de los sistemas criptográficos convencionales a través de un acceso de red hacia el motor de confianza; sin embargo, el motor de confianza no facilita las claves reales ni otros datos de autentificación y, por tanto, las claves y los datos permanecen seguros. Este almacenamiento de las claves y los datos de autentificación centrado en el servidor proporciona una seguridad, portabilidad, disponibilidad e inmediatez de uso independientemente del usuario.

Debido a que los usuarios no pueden encomendarse al sistema criptográfico o confiar en este para que lleve a cabo la autentificación de usuarios y documentos así como otras funciones criptográficas, pueden incorporarse al sistema una amplia variedad de capacidades funcionales. Por ejemplo, el proveedor del motor de confianza puede asegurarse frente a un rechazo de un acuerdo, por ejemplo, autentificando los participantes en el acuerdo, firmando digitalmente el acuerdo en representación de los participantes o para ellos, y almacenando un registro del acuerdo firmado digitalmente por cada participante. Además de ello, el sistema criptográfico puede supervisar acuerdos y determinar la aplicación de diversos grados de autentificación basándose, por ejemplo, en el precio, el usuario, el vendedor, la ubicación geográfica, el lugar de uso o elementos similares.

A fin de facilitar una comprensión completa de la invención, lo que resta de la descripción detallada describe la invención con referencia a las figuras, en las que elementos similares se han designado con los mismos números en toda ella.

La Figura 1 ilustra un diagrama de bloques de un sistema criptográfico 100, de acuerdo con aspectos de una realización de la invención. Como se muestra en la Figura 1, el sistema criptográfico 100 incluye un sistema 105 de usuario, un motor de confianza 110, una autoridad de certificación 115 y un sistema 120 de vendedor, que se comunican a través de un enlace de comunicación 125.

De acuerdo con una realización de la invención, el sistema 105 de usuario comprende una computadora de propósito general convencional que tiene uno o más microprocesadores, tales como, por ejemplo, un procesador basado en Intel. Además, el sistema 105 de usuario incluye un sistema operativo apropiado, tal como, por ejemplo, un sistema operativo capaz de incluir gráficos o ventanas, tal como el Windows, Unix, Linux u otros similares. Como se ha mostrado en la Figura 1, el sistema 105 de usuario puede incluir un dispositivo biométrico 107. El dispositivo biométrico 107 puede, ventajosamente, captar un parámetro biométrico el usuario y transferir el parámetro biométrico captado al motor de confianza 110. De acuerdo con una realización de la invención, el dispositivo biométrico puede, ventajosamente, comprender un dispositivo que tiene atributos y características similares a las descritas en la Patente de los EE.UU. Nº 6.856.383, titulada "*GENERADOR DE IMAGEN DE UN OBJETO CON RELIEVE*" ("*RELIEF OBJECT IMAGE GENERATOR*"), en la Solicitud de Patente de los EE.UU. Nº 09/558.634, presentada el 26 de abril de 2000 y titulada "*DISPOSITIVO DE OBTENCIÓN DE IMÁGENES PARA UN OBJETO CON RELIEVE, Y SISTEMA Y MÉTODO PARA UTILIZAR EL DISPOSITIVO DE OBTENCIÓN DE IMÁGENES*" ("*IMAGING DEVICE FOR A RELIEF OBJECT AND SYSTEM AND METHOD OF USING THE IMAGE DEVICE*"), en la Patente de los EE.UU. Nº 6.631.201, titulada "*ADAPTADOR DE SENSOR PARA OBJETO CON RELIEVE*" ("*RELIEF OBJECT SENSOR ADAPTOR*"), y en la Solicitud de Patente de los EE.UU. Nº 09/477.943, presentada el 5 de enero de 2000 y titulada "*SENSOR DE IMAGEN ÓPTICA PLANA Y SISTEMA PARA GENERAR UNA IMAGEN ELECTRÓNICA DE UN OBJETO CON RELIEVE PARA LA LECTURA DE LA HUELLA DACTILAR*" ("*PLANAR OPTICAL IMAGE SENSOR AND SYSTEM FOR GENERATING AN ELECTRONIC IMAGE OF A RELIEF OBJECT FOR FINGERPRINT READING*"), todas las cuales son de la propiedad del presente Asignatario.

Además, el sistema 105 de usuario puede conectarse al enlace de comunicación 125 a través de un proveedor de servicios convencional, tal como, por ejemplo, un sistema de marcación manual, una línea de abonado digital (DSL – "digital subscriber line"), un módem, o modulador-desmodulador, por cable, una conexión por fibra o elementos similares. De acuerdo con otra realización, el sistema 105 de usuario se conecta con la red de comunicación 125 a través de capacidad de conexión de red, tal como, por ejemplo, una red de área local o extensa. De acuerdo con una realización, el sistema operativo incluye una pila de TCP / IP [Protocolo de Control de Transmisión / Protocolo de Internet –"Transmission Control Protocol / Internet Protocol"] que maneja todo el tráfico de mensajes entrante y saliente que pasa por el enlace de comunicación 125.

Si bien el sistema 105 de usuario se ha divulgado con referencia a las realizaciones anteriores, no se pretende que la invención esté limitada por estas. En lugar de ello, un profesional experto reconocerá, a partir de la descripción de esta memoria, un amplio número de realizaciones alternativas del sistema 105 de usuario, incluyendo casi cualquier dispositivo de computación que sea capaz de enviar o recibir información a, o desde, otro sistema informático. Por ejemplo, el sistema 105 de usuario puede incluir, si bien no está limitado por estos, una estación de trabajo informática, una televisión interactiva, un kiosco interactivo, un dispositivo de computación móvil personal, tal como un asistente digital, un teléfono móvil o celular, una computadora portátil o dispositivo similar, un dispositivo de comunicaciones inalámbricas, una tarjeta inteligente, un dispositivo informático encastrado o incorporado, o un dispositivo similar, que pueda interactuar con el enlace de comunicación 125. El tales sistemas alternativos, los

sistemas operativos diferirán de la misma manera y estarán adaptados para el dispositivo en cuestión. Sin embargo, de acuerdo con una realización, los sistemas operativos, ventajosamente, siguen proporcionando los protocolos de comunicaciones apropiados que se necesitan para establecer la comunicación con el enlace de comunicación 125.

La Figura 1 ilustra el motor de confianza 110. De acuerdo con una realización, el motor de confianza 110 comprende uno o más servidores seguros para acceder a información delicada y almacenarla, la cual puede consistir en cualquier tipo o forma de datos, tal como texto, audio, vídeo, datos de autentificación de usuario y claves criptográficas públicas o privadas, aunque sin estar limitada por estos. De acuerdo con una realización, los datos de autentificación incluyen datos diseñados para identificar de forma inequívoca a un usuario del sistema criptográfico 100. Por ejemplo, los datos de autentificación pueden incluir un número de identificación de usuario, uno o más parámetros biométricos y una serie de preguntas y respuestas generadas por el motor de confianza 110 o por el usuario, pero respondidas inicialmente por el usuario al incorporarse. Las anteriores cuestiones pueden incluir datos demográficos, tales como el lugar de nacimiento, la dirección, el día de cumpleaños o datos similares, datos personales, tales como el nombre de soltera de la madre, el helado favorito o datos similares, u otros datos concebidos para identificar inequívocamente al usuario. El motor de confianza 110 compara unos datos de autentificación del usuario, asociados con una transacción en curso, con los datos de autentificación proporcionados en un tiempo anterior, tal como, por ejemplo, durante la incorporación. El motor de confianza 110 puede requerir, ventajosamente, que el usuario produzca los autentificación en el momento de cada transacción, o bien, de forma ventajosa, el motor de confianza 110 puede permitir al usuario producir periódicamente datos de autentificación, tal como al comienzo de una cadena de transacciones o con la introducción de identificación en un sitio web de un vendedor particular.

De acuerdo con la realización en la que el usuario produce datos biométricos, el usuario proporciona una característica física, tal como una exploración o barrido facial, un barrido de la mano, un barrido de la oreja, un barrido del iris, un barrido de la retina, una configuración vascular, ADN, una huella dactilar, la escritura o el habla, aunque sin limitarse a estas, al dispositivo biométrico 107. El dispositivo biométrico produce, ventajosamente, una patrón electrónico, o biométrico, de la característica física. El patrón electrónico es transferido, a través del sistema 105 de usuario, al motor de confianza 110 para propósitos, ya sean de incorporación, ya sean de autentificación.

Una vez que el usuario ha producido los datos de autentificación apropiados y el motor de confianza 110 ha determinado una coincidencia positiva entre los datos de autentificación (datos de autentificación vigentes en ese momento) y los datos de autentificación proporcionados en el momento de la incorporación (datos de autentificación para incorporación), el motor de confianza 110 proporciona al usuario una capacidad funcional criptográfica completa. Por ejemplo, el usuario apropiadamente autentificado puede, ventajosamente, emplear el motor de confianza 110 para llevar a cabo el troceado o fragmentación, la firma digital, el cifrado y el descifrado (a los que se hace referencia, a menudo, conjuntamente como cifrado únicamente), la creación o la distribución de certificados digitales, y funciones similares. Sin embargo, las claves criptográficas privadas que se utilizan en las funciones criptográficas no estarán disponibles fuera del motor de confianza 110, por lo que se garantiza la integridad de las claves criptográficas.

De acuerdo con una realización, el motor de confianza 110 genera y almacena claves criptográficas. De acuerdo con una realización, existe al menos una clave criptográfica asociada con cada usuario. Es más, cuando las claves criptográficas incluyen tecnología de clave pública, cada clave privada asociada con un usuario es generada en el interior del motor de confianza 110, y no facilitada desde este. De esta forma, siempre y cuando el usuario tenga acceso al motor de confianza 110, el usuario o usuaria puede llevar a cabo funciones criptográficas utilizando su clave privada o pública. Semejante acceso a distancia o remoto permite, ventajosamente, a los usuarios seguir siendo completamente móviles y acceder a la capacidad funcional criptográfica a través de prácticamente cualquier conexión por Internet, tal como teléfonos celulares y vía satélite, kioscos, computadoras portátiles, habitaciones de hotel y medios similares.

De acuerdo con otra realización, el motor de confianza 110 lleva a efecto la capacidad funcional criptográfica utilizando un par de claves generadas para el motor de confianza 110. De acuerdo con esta realización, el motor de confianza 110 autentifica, en primer lugar, al usuario y, una vez que el usuario ha producido adecuadamente datos de autentificación que coinciden con los datos de autentificación para incorporación, el motor de confianza 110 se sirve de su propio par de claves criptográficas para llevar a cabo funciones criptográficas en representación del usuario autentificado.

Un profesional experto constatará, a partir de la descripción de esta memoria, que todas las claves criptográficas pueden, ventajosamente, incluir una o más claves de cifrado simétricas (por ejemplo, claves privadas) y claves de cifrado asimétricas (por ejemplo, pares de claves pública / privada). Además, un profesional experto constatará, a partir de la descripción proporcionada en esta memoria, que las anteriores claves pueden ser implementadas con un amplio número de algoritmos disponibles en tecnologías comerciales, tales como, por ejemplo, el RSA, el ELGAMAL, o algoritmos similares. Cuando se describe en la presente memoria un esquema criptográfico asimétrico, este esquema puede ser sustituido por un esquema simétrico, y viceversa.

La Figura 1 también ilustra la autoridad de certificación 115. De acuerdo con una realización, la autoridad de certificación 115 puede comprender, ventajosamente, una organización o empresa tercera de confianza que emita certificados digitales, tal como, por ejemplo, VeriSign, Baltimore, Entrust o una empresa similar. El motor de confianza 110 puede transmitir, ventajosamente, peticiones de certificados digitales a través de uno o más protocolos de certificado digital convencionales, tales como, por ejemplo, el PKCS10, a la autoridad de certificación 110. En respuesta, la autoridad de certificación 115 emitirá un certificado digital en uno o más de un cierto número de protocolos diferentes, tales como, por ejemplo, el PKCS7. De acuerdo con una realización de la invención, el motor de confianza 110 solicita certificados digitales de algunas, o todas, las autoridades de certificación 115 más importantes, de tal manera que el motor de confianza 110 tiene acceso a un certificado digital en correspondencia con el certificado estándar de cualquier parte que lo solicite.

De acuerdo con otra realización, el motor de confianza 110 lleva a cabo internamente emisiones de certificados. En esta realización, el motor de confianza 110 puede acceder a un sistema de certificación para generar certificados y/o puede generar internamente certificados cuando estos son solicitados, tal como, por ejemplo, en el momento de la generación de una clave o dentro de la norma de certificación solicitada en el momento de la petición. El motor de confianza 110 se describirá con mayor detalle más adelante.

La Figura 1 también ilustra el sistema 120 del vendedor. De acuerdo con una realización, el sistema 120 del vendedor comprende, ventajosamente, un servidor de web. Los servidores de web convencionales sirven, por lo general, contenidos a través de la Internet utilizando uno de entre diversos lenguajes de etiquetado o marcación por Internet o normas sobre formatos de documentos, tales como el Lenguaje de Marcación de Hipertexto (HTML –“Hyper-Text Markup Language”) o el Lenguaje de Marcación Extensible (XML –“Extensible Markup Language”). El servidor de web acepta peticiones procedentes de navegadores o exploradores como el Netscape y el Internet Explorer y, a continuación, remite los documentos electrónicos apropiados. Pueden utilizarse un cierto número de tecnologías del lado del servidor o del lado del cliente para aumentar la potencia del servidor de web más allá de su capacidad para suministrar documentos electrónicos normalizados. Por ejemplo, estas tecnologías incluyen guiones de Interfaz de Pasarela Común (CGI –“Common Gateway Interface”), seguridad de Capa de Enchufes Seguros (SSL –“Secure Sockets Layer”), y Páginas de Servidor Activo (ASPs –“Active Server Pages”). El sistema 120 del vendedor puede, ventajosamente, proporcionar contenido electrónico relativo a transacciones comerciales, personales, educativas y de otro tipo.

Si bien el sistema 120 del vendedor se ha divulgado con referencia a las anteriores realizaciones, no es la intención que la invención esté limitada por ellas. En lugar de eso, un profesional experto constatará, a partir de la descripción proporcionada en esta memoria, que el sistema 120 del vendedor puede, ventajosamente, comprender cualquiera de los dispositivos descritos con referencia al sistema 105 de usuario, o una combinación de los mismos.

La Figura 1 también ilustra el enlace de comunicación 125, que conecta el sistema 105 de usuario, el motor de confianza 110, la autoridad de certificación 115 y el sistema 120 del vendedor. De acuerdo con una realización, el enlace de comunicación 125 comprende, preferiblemente, la Internet. La Internet, tal y como se utiliza a todo lo largo de esta descripción, es una red global de computadoras. La estructura de la Internet, que es bien conocida por las personas con conocimientos ordinarios de la técnica, incluye una estructura troncal de red, con redes que se ramifican a partir de la estructura troncal. Estas ramas, a su vez, tienen redes que se ramifican desde ellas, y así sucesivamente. Unos dispositivos de encaminamiento, o *routers*, mueven los paquetes de información entre los niveles de la red y, a continuación, de una red a otra, hasta que el paquete llega a las inmediaciones de su destino. Desde el destino, el dispositivo anfitrión o principal de la red de destino dirige el paquete de información al terminal, o nodo, apropiado. En una realización ventajosa, los dispositivos centralizadores de encaminamiento de Internet comprenden servidores de sistema de nombre de dominio (DNS –“domain name systems”) que utilizan Protocolo de Control de Transmisión / Protocolo de Internet (TCP / IP –“Transmission Control Protocol / Internet Protocol”), como es bien conocido en la técnica. Los dispositivos centralizadores de encaminamiento se conectan a uno o más de otros dispositivos de encaminamiento a través de enlaces de comunicación de alta velocidad. Una parte popular de la Internet es la Red de Extensión Universal (“World Wide Web”). La Red de Extensión Universal contiene diferentes computadoras que almacenan documentos y capaces de presentar visualmente información de gráficos y de texto. Las computadoras que proporcionan información en la Red de Extensión Universal se denominan, por lo común, “sitios web” (“websites”). Un sitio web viene definido por una dirección de Internet que tiene una página electrónica asociada. La página electrónica puede identificarse por un Localizador de Recursos Uniformes (URL –“Uniform Resource Locator”). Generalmente, una página electrónica es un documento que organiza la presentación de texto, imágenes gráficas, audio, vídeo y así sucesivamente.

Si bien el enlace de comunicación 125 se describe en términos de su realización preferida, una persona con conocimientos ordinarios de la técnica constatará, a partir de la descripción proporcionada en esta memoria, que el enlace de comunicación 125 puede incluir un amplio abanico de enlaces de comunicaciones interactivos. Por ejemplo, el enlace de comunicación 125 puede incluir redes de televisión, redes de telefonía, sistemas de transmisión de datos inalámbricos, sistemas de cable de transmisión en ambos sentidos o bidireccional, redes informáticas privadas o públicas personalizadas, redes de kioscos interactivos, redes de cajeros automáticos, enlaces directos, redes vía satélite o celulares, todos ellos interactivos, y otros similares.

La Figura 2 ilustra un diagrama de bloques del motor de confianza 110 de la Figura 1, de acuerdo con aspectos de una realización de la invención. Como se ha mostrado en la Figura 2, el motor de confianza 110 incluye un motor de transacción 205, un depósito 210, un motor de autentificación 215 y un motor criptográfico 220. De acuerdo con una realización de la invención, el motor de confianza 110 también incluye un dispositivo de almacenamiento masivo 225. Como se ha mostrado adicionalmente en la Figura 2, el motor de transacción 205 se comunica con el depósito 210, con el motor de autentificación 215, con el motor criptográfico 220, así como con el dispositivo de almacenamiento masivo 225. Además, el depósito 210 se comunica con el motor de autentificación 215, con el motor criptográfico 220 y con el dispositivo de almacenamiento masivo 225. Por otra parte, el dispositivo de autentificación 215 está en comunicación con el motor criptográfico 220. De acuerdo con una realización de la invención, algunas de las anteriores comunicaciones, o todas ellas, pueden comprender, ventajosamente, la transmisión de documentos de XML a direcciones de IP que corresponden al dispositivo de recepción. Como se ha mencionado en lo anterior, los documentos de XML permiten, ventajosamente, a los diseñadores crear sus propias etiquetas de documento personalizadas, lo que hace posible la definición, transmisión, validación e interpretación de los datos entre aplicaciones y entre organizaciones. Además, algunas o todas las comunicaciones anteriores pueden incluir tecnologías de SSL convencionales.

De acuerdo con una realización, el motor de transacción 205 comprende un dispositivo de encaminamiento de datos, tal como un servidor de web convencional disponible en la Netscape, Microsoft, Apache u otros similares. Por ejemplo, el servidor de web puede, ventajosamente, recibir datos entrantes procedentes del enlace de comunicación 125. De acuerdo con una realización de la invención, los datos entrantes son dirigidos a un sistema de seguridad de terminal frontal para el motor de confianza 110. Por ejemplo, el sistema de seguridad de terminal frontal puede incluir, ventajosamente, un cortafuego, un sistema de detección de intrusión que busca perfiles de ataque conocidos, y/o un escáner o rastreador de virus. Una vez limpiado el sistema de seguridad de terminal frontal, los datos son recibidos por el motor de transacción 205 y encaminados a uno de entre el depósito 210, el motor de autentificación 215, el motor criptográfico 220 y el dispositivo de almacenamiento masivo 225. Además, el motor de transacción 205 supervisa los datos entrantes procedentes del motor de autentificación 215 y del motor criptográfico 220, y encamina los datos a sistemas particulares a través del enlace de comunicación 125. Por ejemplo, el motor de transacción 205 puede, ventajosamente, encaminar datos al sistema 105 de usuario, a la autoridad de certificación 115 o al sistema 120 del vendedor.

De acuerdo con una realización, los datos son encaminados utilizando técnicas de encaminamiento de HTTP convencionales, tal como, por ejemplo, empleando URLs o Indicadores de Recursos Uniformes (URIs –“Uniform Resource Indicators”). Los URIs son similares a los URLs, si bien los URIs, por lo común, indican la fuente de los archivos o acciones, tal como, por ejemplo, ejecutables, guiones y otros similares. Por lo tanto, de acuerdo con esa misma realización, el sistema 105 de usuario, la autoridad de certificación 115, el sistema 120 del vendedor y los componentes del motor de confianza 210 incluyen, ventajosamente, datos suficientes dentro de los URLs o URIs de comunicación para que el motor de transacción 205 encamine los datos apropiadamente a través del sistema criptográfico.

Si bien el encaminamiento de los datos se ha descrito con referencia a su realización preferida, un profesional experto concebirá un amplio número de soluciones o estrategias posibles para el encaminamiento de los datos. Por ejemplo, los paquetes de XML u otros paquetes de datos pueden, ventajosamente, ser desempaquetados y reconocidos por su formato, contenido o elementos similares, de tal manera que el motor de transacción 205 puede encaminar adecuadamente los datos a todo lo largo del motor de confianza 110. Es más, un profesional experto concebirá que el encaminamiento de los datos puede, ventajosamente, ser adaptado a los protocolos de transferencia de datos de conformidad con sistemas de red particulares, por ejemplo, cuando el enlace de comunicación 125 comprende una red local.

De acuerdo con aún otra realización de la invención, el motor de transacción 205 incluye tecnologías de encriptación o cifrado de SSL convencionales, de tal manera que los anteriores sistemas pueden autentificarse a sí mismos, y viceversa, con el motor de transacción 205, durante comunicaciones particulares. Como se utilizará a todo lo largo de esta descripción, la expresión “½ SSL” se refiere a comunicaciones en las que un servidor, pero no necesariamente el cliente, es autentificado en SSL, y la expresión “SSL COMPLETA” (“FULL SSL”) se refiere a las comunicaciones en las que el cliente y el servidor son autentificados en SSL. Cuando la descripción utiliza puntualmente el término “SSL”, la comunicación puede comprender ½ SSL o SSL COMPLETA.

Conforme el motor de transacción 205 encamina datos a los diversos componentes del sistema criptográfico 100, el motor de transacción 205 puede, ventajosamente, crear un proceso de revisión o auditoría. De acuerdo con una realización, el proceso de auditoría incluye un registro de al menos el tipo y el formato de los datos encaminados por el motor de transacción 205 a través del sistema criptográfico 100. Tal proceso de auditoría puede, ventajosamente, ser almacenado en el dispositivo de almacenamiento masivo 225.

La Figura 2 también ilustra el depósito 210. De acuerdo con una realización, el depósito 210 comprende una o más instalaciones de almacenamiento de datos, tales como, por ejemplo, un servidor de directorio, un servidor de base

de datos o un elemento similar. Como se ha mostrado en la Figura 2, el depósito 210 almacena claves criptográficas y datos de autentificación para incorporación. Las claves criptográficas pueden, ventajosamente, corresponder al motor de confianza 110 o a los usuarios del sistema criptográfico 100, tales como el usuario o el vendedor. Los datos de autentificación para incorporación pueden, ventajosamente, incluir datos diseñados para identificar de forma inequívoca a un usuario, tales como una ID [identificación] de usuario, palabras de paso, respuestas a preguntas, datos biométricos o datos similares. Estos datos de autentificación para incorporación pueden ser, ventajosamente, captados en el momento de la incorporación de un usuario o en otro momento alternativo ulterior. Por ejemplo, el motor de confianza 110 puede incluir una renovación o reemisión periódica, o de otro tipo, de datos de autentificación para incorporación.

De acuerdo con una realización, la comunicación desde el motor de transacción 205 hacia y desde el motor de autentificación 215 y el motor criptográfico 220, comprende una comunicación segura, tal como, por ejemplo, tecnología de SSL convencional. Además de ello, como se ha mencionado en lo anterior, los datos de las comunicaciones hacia y desde el depósito 210 pueden ser transferidos utilizando URLs, URIs, documentos en HTTP o en XML, de tal manera que cualquiera de los anteriores tiene, ventajosamente, peticiones de datos y formatos incorporados en su interior.

Como se ha mencionado anteriormente, el depósito 210 puede comprender, de forma ventajosa, una pluralidad de instalaciones de almacenamiento de datos seguras. En tal realización, las instalaciones de almacenamiento de datos seguras pueden haberse configurado de un modo tal, que un compromiso o puesta en riesgo de la seguridad en una instalación de almacenamiento de datos individual no comprometerá las claves criptográficas o los datos de autentificación almacenados en su interior. Por ejemplo, de acuerdo con esta realización, se opera matemáticamente sobre las claves criptográficas y los datos de autentificación con el fin de hacer aleatorios, estadística y sustancialmente, los datos almacenados en cada instalación de almacenamiento de datos. De acuerdo con una realización, la conversión a aleatorios de los datos de una instalación de almacenamiento de datos convierten los datos en indescifrables. De esta forma, la puesta en riesgo de una instalación de almacenamiento de datos individual produce únicamente un número transformado en aleatorio e indescifrable, y no compromete la seguridad de ninguna de las claves criptográficas ni los datos de autentificación en su conjunto.

La Figura 2 también ilustra el motor de confianza 110, que incluye el motor de autentificación 215. De acuerdo con una realización, el motor de autentificación 215 comprende un comparador de datos configurado para comparar los datos procedentes del motor de transacción 205 con datos procedentes del depósito 210. Por ejemplo, durante la autentificación, un usuario suministra datos de autentificación vigentes en ese momento al motor de confianza 110, de tal modo que el motor de transacción 205 recibe los datos de autentificación vigentes en ese momento. Como se ha mencionado en lo anterior, el motor de transacción 205 reconoce las peticiones de datos, preferiblemente en el URL o el URI, y encamina los datos de autentificación al motor de autentificación 215. Por otra parte, bajo petición, el depósito 210 remite datos de autentificación para incorporación correspondientes al usuario, al motor de autentificación 215. De este modo, el motor de autentificación 215 tiene tanto los datos de autentificación vigentes en ese momento como los datos de autentificación para incorporación, para su comparación.

De acuerdo con una realización, las comunicaciones hacia el motor de autentificación comprenden comunicaciones seguras tales como, por ejemplo, tecnología de SSL. De manera adicional, puede proporcionarse seguridad dentro de los componentes del motor de confianza 110, tal como, por ejemplo, el supercifrado utilizando tecnologías de clave pública. Por ejemplo, de acuerdo con una realización, el usuario cifra los datos de autentificación vigentes en ese momento con la clave pública del motor de autentificación 215. Además, el depósito 210 también cifra los datos de autentificación para incorporación con la clave pública del motor de autentificación 215. De esta manera, únicamente la clave privada del motor de autentificación puede ser utilizada para descifrar las transmisiones.

Como se ha mostrado en la Figura 2, el motor de confianza 110 también incluye el motor criptográfico 220. De acuerdo con una realización, el motor criptográfico comprende un módulo de gestión criptográfica, configurado para proporcionar, de forma ventajosa, funciones criptográficas convencionales tales como, por ejemplo, la capacidad funcional de infraestructura de clave pública (PKI –“public-key infrastructure”). Por ejemplo, el motor criptográfico 220 puede emitir, ventajosamente, claves públicas y privadas para los usuarios del sistema criptográfico 100. De esta manera, las claves criptográficas son generadas en el motor criptográfico 220 y remitidas al depósito 210 de un modo tal, que al menos las claves criptográficas privadas no están disponibles fuera del motor de confianza 110. De acuerdo con otra realización, el motor criptográfico 220 convierte en aleatorios y divide o fragmenta al menos los datos de clave criptográfica privada, por lo que se almacenan únicamente los datos divididos y convertidos en aleatorios. Similarmente a la división de los datos de autentificación para incorporación, el procedimiento de división garantiza que las claves almacenadas no están disponibles fuera del motor criptográfico 220. De acuerdo con otra realización, las funciones del motor criptográfico pueden ser combinadas con, y llevadas a cabo por, el motor de autentificación 215.

De acuerdo con una realización, las comunicaciones hacia y desde el motor criptográfico incluyen comunicaciones seguras, tales como por tecnología de SSL. Además de ello, pueden emplearse, ventajosamente, documentos en XML para transferir datos y/o realizar peticiones de la función criptográfica.

La Figura 2 también ilustra el motor de confianza 110 de manera que está provisto del dispositivo de almacenamiento masivo 225. Como se ha mencionado en lo anterior, el motor de transacción 205 conserva los datos correspondientes a un proceso de revisión o auditoría y almacena tales datos en el dispositivo de almacenamiento masivo 225. Similarmente, de acuerdo con una realización de la invención, el depósito 210 conserva los datos correspondientes a un proceso de revisión o auditoría y almacena tales datos en el dispositivo de almacenamiento masivo 225. Los datos del proceso de auditoría del depósito son similares a los del motor de transacción 205 por cuanto los datos del proceso de auditoría comprenden un registro de las peticiones recibidas por el depósito 210 y las respuestas del mismo. Además, el dispositivo de almacenamiento masivo 225 puede ser utilizado para almacenar certificados digitales que tienen la clave pública de un usuario contenida en su interior.

Si bien el motor de confianza 110 se ha divulgado con referencia a sus realizaciones preferidas y alternativas, no es la intención que la invención esté limitada por ellas. En lugar de ello, un profesional experto concebirá, por la descripción proporcionada en esta memoria, un amplio número de alternativas para el motor de confianza 110. Por ejemplo, el motor de confianza 110 puede, ventajosamente, llevar a cabo únicamente la autentificación, o, alternativamente, tan solo algunas de las funciones criptográficas, o todas ellas, tales como el cifrado y el descifrado de los datos. De acuerdo con tales realizaciones, uno de entre el motor de autentificación 215 y el motor criptográfico 220 puede ser, ventajosamente, suprimido, con lo que se crea un diseño más elemental para el motor de confianza 110. Además de ello, el motor criptográfico 220 puede también comunicarse con una autoridad de certificación de un modo tal, que la autoridad de certificación se dispone incorporada dentro del motor de confianza 110. De acuerdo con aún otra realización, el motor de confianza 110 puede, ventajosamente, llevar a cabo la autentificación y una o más funciones criptográficas, tales como, por ejemplo, la firma digital.

La Figura 3 ilustra un diagrama de bloques del motor de transacción 205 de la Figura 2, de acuerdo con aspectos de una realización de la invención. De acuerdo con esta realización, el motor de transacción 205 comprende un sistema operativo 305 que tiene una secuencia o hilo de gestión y un hilo de escucha. El sistema operativo 305 puede, ventajosamente, ser similar a los que se encuentran en servidores de alto volumen convencionales, tales como, por ejemplo, servidores de web disponibles en la Apache. El hilo de escucha supervisa la comunicación entrante procedente de uno de entre el enlace de comunicación 125, el motor de autentificación 215 y el motor criptográfico 220 para flujo de datos entrantes. El hilo de gestión reconoce estructuras de datos concretas del flujo de datos entrantes, tales como, por ejemplo, las anteriores estructuras de datos, con lo que se encaminan los datos entrantes a uno de entre el enlace de comunicación 125, el depósito 210, el motor de autentificación 215, el motor criptográfico 220 o el dispositivo de almacenamiento masivo 225. Como se ha mostrado en la Figura 3, los datos entrantes y salientes pueden ser, ventajosamente, asegurados por medio de, por ejemplo, tecnología de SSL.

La Figura 4 ilustra un diagrama de bloques del depósito 210 de la Figura 2, de acuerdo con aspectos de una realización de la invención. De acuerdo con esta realización, el depósito 210 comprende uno o más servidores de protocolo de acceso a directorio de peso ligero (LDAP –"lightweight directory access protocol"). Los servidores de directorio de LDAP se encuentran disponibles en una amplia variedad de fabricantes, tales como Netscape, ISO, Microsoft y otros. La Figura 4 también muestra que el servidor de directorio almacena, preferiblemente, datos 405 correspondientes a las claves criptográficas y datos 410 correspondientes a los datos de autentificación para incorporación. De acuerdo con una realización, el depósito 210 comprende una única estructura de memoria lógica que indexa datos de autentificación y datos de clave criptográfica a una ID de usuario única o exclusiva. La estructura de memoria lógica única incluye, preferiblemente, mecanismos para garantizar un elevado grado de confianza, o de seguridad, en los datos almacenados en su interior. Por ejemplo, la ubicación física del depósito 210 puede, ventajosamente, incluir un amplio número de medidas de seguridad convencionales, tales como un acceso limitado por parte de los empleados, sistemas de vigilancia modernos y medios similares. Además de, o en lugar de, las medidas de seguridad físicas, el sistema informático o servidor puede, ventajosamente, incluir soluciones de programación o software para proteger los datos almacenados. Por ejemplo, el depósito 210 puede, ventajosamente, crear y almacenar datos 415 correspondientes a un proceso de auditoría de las acciones emprendidas. Además, las comunicaciones entrantes y salientes pueden, ventajosamente, ser encriptadas o cifradas con cifrado de clave pública, combinado con tecnologías de SSL convencionales.

De acuerdo con otra realización, el depósito 210 puede incluir instalaciones de almacenamiento de datos diferenciadas y físicamente separadas. Por ejemplo, el depósito 210 puede incluir más de un dispositivo de almacenamiento físico (por ejemplo, un dispositivo de accionamiento de cinta, un dispositivo de accionamiento de disco duro, un dispositivo de accionamiento óptico, o cualquier combinación de los mismos), alojados en ubicaciones geográficamente separadas.

La Figura 5 ilustra un diagrama de bloques del motor de autentificación 215 de la Figura 2, de acuerdo con aspectos de una realización de la invención. Similarmente al motor de transacción 205 de la Figura 3, el motor de autentificación 215 comprende un sistema operativo 505 que tiene al menos un hilo de escucha y uno de gestión de una versión modificada de un servidor de web convencional, tal como, por ejemplo, servidores de web disponibles en la Apache. Como se ha mostrado en la Figura 5, el motor de autentificación 215 incluye el acceso a al menos una clave privada 510. La clave privada 510 puede, ventajosamente, ser utilizada, por ejemplo, para descifrar datos

procedentes del motor de transacción 205 o del depósito 210 que se habían cifrado con una clave pública correspondiente del motor de autentificación 215.

La Figura 5 también ilustra el motor de autentificación 215 de forma tal, que comprende un comparador 515, un módulo 520 de fragmentación o división de datos, así como un módulo 525 de ensamblaje de datos. De acuerdo con una realización de la invención, el comparador 515 incluye tecnología capaz de comparar patrones potencialmente complejos relacionados con los anteriores datos de autentificación biométricos. La tecnología puede incluir dispositivos físicos o hardware, programación o software, o soluciones combinadas para comparación de patrones, tales como, por ejemplo, las que representan patrones de huellas dactilares o patrones de voz. Además de ello, de acuerdo con una realización, el comparador 515 del motor de autentificación 215 puede, ventajosamente, comparar fragmentos convencionales de documentos con el fin de arrojar un resultado de la comparación. De acuerdo con una realización de la invención, el comparador 515 incluye la aplicación de la heurística 530 a la comparación. La heurística 530 puede, ventajosamente, tratar circunstancias que rodean un intento de autentificación, tales como, por ejemplo, la hora del día, la dirección de IP o máscara de subred, el perfil de adquisición o compra, la dirección de correo electrónico, el número de serie o ID del procesador, o elementos similares.

Es más, la naturaleza de las comparaciones de datos biométricos puede dar como resultado que se produzcan grados variables de confianza a partir de la coincidencia de datos de autentificación biométricos vigentes en ese momento con datos de la incorporación. Por ejemplo, a diferencia de una palabra de paso convencional que tan solo puede devolver una coincidencia positiva o negativa, puede determinarse que una huella dactilar es una coincidencia parcial, por ejemplo, una coincidencia al 90%, una coincidencia al 75% o una coincidencia al 10%, en lugar se ser simplemente correcta o incorrecta. Otros identificadores biométricos, tales como el análisis de impresión de voz o el reconocimiento del rostro, pueden compartir esta propiedad de autentificación probabilística, en lugar de una autentificación absoluta.

Cuando se trabaja con tal autentificación probabilística o, en otros casos, cuando una autentificación se considera menos que absolutamente fiable, es deseable aplicar la heurística 530 con el fin determinar si el nivel o grado de confianza de la autentificación proporcionada es lo suficientemente alto como para autentificar la transacción que está realizando.

Será, en ocasiones, el caso que la transacción en cuestión es una transacción de valor relativamente bajo, de tal manera que es aceptable que sea autentificada a un nivel o grado más bajo de confianza. Esto podría incluir una transacción que tuviera un valor en dólares bajo asociado con ella (por ejemplo, una compra de $10) o una transacción con un riesgo bajo (por ejemplo, la admisión a un sitio web reservado únicamente a sus miembros).

Y a la inversa, para autentificar otras transacciones, puede ser deseable requerir un alto grado de confianza en la autentificación antes de permitir que prosiga la transacción. Tales transacciones pueden incluir transacciones con un gran valor en dólares (por ejemplo, la firma de un contrato de suministro multimillonario en dólares), o transacciones con un elevado riesgo si se produce una autentificación incorrecta (por ejemplo, la introducción de identificación a distancia en una computadora gubernamental).

El uso de la heurística 530 en combinación con niveles de confianza y valores de transacción, puede emplearse de la forma que se describirá más adelante con el fin de permitir que el comparador proporcione un sistema de autentificación sensible al contexto y dinámico.

De acuerdo con otra realización de la invención, el comparador 515 puede, ventajosamente, hacer un seguimiento de los intentos de autentificación para una transacción particular. Por ejemplo, cuando una transacción no tiene éxito, el motor de confianza 110 puede solicitar al usuario o usuaria que reintroduzca sus datos de autentificación vigentes en ese momento. El comparador 515 del motor de autentificación 215 puede, ventajosamente, emplear un limitador de intentos 535 para limitar el número de intentos de autentificación, con lo que se prohíben los intentos forzados para suplantar los datos de autentificación de un usuario. De acuerdo con una realización, el limitador de intentos 535 comprende un módulo de software que supervisa las transacciones en busca de intentos de autentificación repetidos y, por ejemplo, que limita a tres los intentos de autentificación para una transacción dada. De esta forma, el limitador de intentos 535 limitará un intento automatizado de suplantar los datos de autentificación de una persona a, por ejemplo, solamente tres “tentativas”. Al producirse tres fallos, el limitador de intentos 535 puede, ventajosamente, denegar más intentos de autentificación. Tal denegación puede, ventajosamente, ser implementada a través de, por ejemplo, la devolución, por parte del comparador 515, de un resultado negativo con independencia de los datos de autentificación que en ese momento estén siendo transmitidos. Por otra parte, el motor de transacción 205 puede, ventajosamente, bloquear cualquier intento de autentificación adicional perteneciente a una transacción en la que ya han fallado anteriormente tres intentos.

El motor de autentificación 215 también incluye el módulo 520 de división de datos y el módulo 525 de ensamblaje de datos. El módulo 520 de división de datos comprende, ventajosamente, un software, hardware, o un módulo de combinación que tiene la capacidad de operar matemáticamente sobre varios datos con el fin de volver sustancialmente aleatorios (por ejemplo, hacer aleatorios o convertir en pseudoaleatorios) y dividir los datos en

porciones individuales (también denominadas compartimientos). En algunas realizaciones, para volver sustancialmente aleatorios los datos, el módulo 520 de división de datos puede generar números aleatorios o pseudoaleatorios. Los números aleatorios o pseudoaleatorios pueden ser, entonces, asociados con unidades (por ejemplo, un número cualquiera de bits, bytes o palabras, o bloques) de datos procedentes de un conjunto de datos. Los números aleatorios o pseudoaleatorios pueden ser también asociados con los compartimientos. El módulo 520 de división de datos puede determinar dentro de qué compartimiento se ha de almacenar cada unidad de datos procedente del conjunto de datos, basándose, al menos en parte, en la asociación de los números aleatorios o pseudoaleatorios con las unidades de datos y los compartimientos.

De acuerdo con una realización, los datos originales no son reproducibles a partir de una porción individual o compartimiento de usuario. El módulo 525 de ensamblaje de datos comprende, ventajosamente, un software, hardware, o un módulo de combinación configurado para operar matemáticamente sobre las anteriores porciones sustancialmente convertidas en aleatorias, de tal manera que la combinación de las mismas proporciona los datos descifrados originales. De acuerdo con una realización, el motor de autentificación 215 emplea el módulo 520 de división de datos para convertir en aleatorios y dividir en porciones datos de autentificación para incorporación, y emplea el módulo 525 de ensamblaje de datos para reensamblar las porciones hasta formar datos de autentificación para incorporación utilizables.

La Figura 6 ilustra un diagrama de bloques del motor criptográfico 220 del motor de confianza 200 de la Figura 2, de acuerdo con aspectos de una realización de la invención. Similarmente al motor de transacción 205 de la Figura 3, el motor criptográfico 220 comprende un sistema operativo 605 que tiene al menos un hilo de escucha y un hilo de gestión de una versión modificada de un servidor de web convencional, tal como, por ejemplo, servidores de web disponibles en la Apache. Como se ha mostrado en la Figura 6, el motor criptográfico 220 comprende un módulo 610 de división de datos y un módulo 620 de ensamblaje de datos que funcionan similarmente a los de la Figura 5. Sin embargo, de acuerdo con una realización, el módulo 610 de división de datos y el módulo 620 de ensamblaje de datos procesan o tratan datos de clave criptográfica, en contraposición a los anteriores datos de autentificación para incorporación. Sin embargo, un profesional experto concebirá, a partir de la descripción proporcionada en esta memoria, que el módulo 910 de división de datos y el módulo 620 de división de datos pueden ser combinados con los del motor de autentificación 215.

El motor criptográfico 220 también comprende un módulo de gestión criptográfica 625 configurado para llevar a cabo una, algunas o la totalidad de un amplio número de funciones criptográficas. De acuerdo con una realización, el módulo de gestión criptográfica 625 puede comprender módulos de software o programas, hardware, o ambos. De acuerdo con otra realización, el módulo de gestión criptográfica 625 puede llevar a cabo comparaciones de datos, análisis sintáctico de datos, división de datos, separación de datos, fragmentación de datos, cifrado o descifrado de datos, verificación o creación de firma digital, generación de certificado digital, almacenamiento, o peticiones, generación de clave criptográfica, o funciones similares. Además, un profesional experto concebirá, a partir de la descripción que se da en la presente memoria, que el módulo de gestión criptográfica 825 puede, ventajosamente, comprender una infraestructura de clave pública, tal como Pretty Good Privacy (PGP), un sistema de clave pública basado en el RSA, o bien un amplio número de sistemas de gestión de clave alternativos. Además de ello, el módulo de gestión criptográfica 625 puede llevar a cabo la encriptación o cifrado de clave pública, la encriptación o cifrado de clave simétrica, o ambas. Además de lo anterior, el módulo de gestión criptográfica 625 puede incluir uno o más programas o módulos informáticos, o ambos, a fin de implementar funciones de interoperatividad, u operatividad mutua, sin discontinuidades y transparentes.

Un profesional experto también concebirá, a partir de la descripción proporcionada en esta memoria, que la capacidad funcional criptográfica puede incluir un amplio número o variedad de funciones relativas, generalmente, a los sistemas de gestión de clave criptográfica.

El analizador sintáctico de datos seguro de la presente invención puede ser integrado en un sistema operativo de Kernel (por ejemplo, Linux, Unix o cualquier otro sistema operativo comercial o tenido en propiedad adecuado). Esta integración puede ser utilizada para proteger datos en el nivel del dispositivo, con lo que, por ejemplo, los datos que serían, normalmente, almacenados en uno o más dispositivos son separados en un cierto número de porciones por el analizador sintáctico de datos seguro que se encuentra integrado dentro del sistema operativo, y almacenados entre los uno o más dispositivos. Cuando se intenta acceder a los datos originales, el software apropiado, también integrado dentro del sistema operativo, puede recombinar las porciones de datos analizadas sintácticamente dentro de los datos originales de una manera que puede ser transparente para el usuario final.

El analizador sintáctico de datos seguro de la presente invención puede estar integrado dentro de un gestor de volumen o cualquier otro componente adecuado de un sistema de almacenamiento, a fin de proteger el almacenamiento de datos local y conectado a red a través de cualquiera de las plataformas a las que se da soporte, o a todas ellas. Por ejemplo, una vez integrado el analizador sintáctico de datos seguro, un sistema de almacenamiento puede hacer uso de la redundancia ofrecida por el analizador de datos seguro (o sea, lo que se utiliza para implementar la característica de necesitar un número menor que la totalidad de las porciones separadas de datos para reconstruir los datos originales) para proteger frente a la pérdida de datos. El analizador sintáctico de

datos seguro también permite que todos los datos inscritos en dispositivos de almacenamiento, ya sea utilizando redundancia o no, se encuentren en la forma de múltiples porciones que son generadas de acuerdo con el análisis sintáctico de la presente invención. Cuando se intenta acceder a los datos originales, el software apropiado, también integrado dentro del gestor de volumen u otro componente adecuado del sistema de almacenamiento, puede recombinar las porciones de datos analizadas sintácticamente dentro de los datos originales de un modo tal, que puede ser transparente para el usuario final.

En una solución apropiada, el analizador sintáctico de datos seguro de la presente invención puede ser integrado dentro de un controlador de RAID (ya sea como hardware, ya sea como software). Esto hace posible el almacenamiento de datos seguro en múltiples dispositivos de accionamiento al tiempo que se conserva la tolerancia a los fallos en caso de fallo del dispositivo de accionamiento.

El analizador sintáctico de datos seguro de la presente invención puede estar integrado dentro de una base de datos con el fin, por ejemplo, de proteger información en tablas delicada. Por ejemplo, en una solución apropiada, los datos asociados con celdas o casillas particulares de una tabla de base de datos (por ejemplo, casillas individuales, una o más columnas particulares, una o más filas particulares, cualquier combinación de las mismas, o bien una tabla de base de datos completa) pueden ser analizados sintácticamente y separados de acuerdo con la presente invención (por ejemplo, en el caso de que las diferentes porciones se almacenen en uno o más dispositivos de almacenamiento, en una o más posiciones, o en un único dispositivo de almacenamiento). El acceso para recombinar las porciones con el fin de ver los datos originales puede ser concedido por métodos de autentificación tradicionales (por ejemplo, la indagación sobre nombre de usuario y palabra de paso).

El analizador sintáctico seguro de la presente invención puede ser integrado en cualquier sistema adecuado que implique datos en movimiento (por ejemplo, la transferencia de datos desde una posición a otra). Tales sistemas incluyen, por ejemplo, servidores de archivos de red y sistemas de archivos, servidores de correo electrónico, servidores de web, difusiones de datos de reproducción según descarga, y comunicaciones inalámbricas (por ejemplo, WiFi). Con respecto al correo electrónico, en una solución apropiada, el analizador sintáctico seguro puede ser utilizado para analizar sintácticamente mensajes salientes (esto es, los que contienen texto, datos binarios, o ambos (por ejemplo, archivos anexados a un mensaje de correo electrónico)) y enviar las diferentes porciones de los datos sintácticamente analizados a lo largo de diferentes recorridos o caminos, con lo que se crean múltiples corrientes de datos. Si se pone en peligro cualquiera de estas corrientes de datos, el mensaje original sigue siendo seguro debido a que el sistema puede requerir que se combinen más de una de las porciones, de acuerdo con la presente invención, a fin de generar los datos originales. En otra solución apropiada, las diferentes porciones de datos pueden ser comunicadas a lo largo de un único camino de forma secuencial, de tal modo que, si se obtiene una sola porción, esta no puede ser suficiente para generar los datos originales. Las diferentes porciones llegan a la ubicación del destinatario deseado y pueden ser combinadas para generar los datos originales de acuerdo con la presente invención.

Las Figuras 7 y 8 son diagramas de bloques ilustrativos de tales sistemas de correo electrónico. La Figura 7 muestra un sistema remitente o emisor 700, que puede incluir cualquier hardware apropiado, tal como un terminal informático, una computadora personal, un dispositivo de mano (por ejemplo, una PDA [Asistente Personal Digital – “Personal Digital Assistant”], un dispositivo de Blackberry), un teléfono celular, una red informática, cualquier otro hardware apropiado, o bien cualquier combinación de los mismos. El sistema remitente 700 se utiliza para generar y/o almacenar un mensaje 704, el cual puede ser, por ejemplo, un paquete de red, un mensaje de correo electrónico, un archivo de datos binarios (por ejemplo, gráficos, voz, vídeo, etc.), o bien cualquier combinación de los anteriores. El mensaje 704 es analizado sintácticamente y dividido por el analizador sintáctico de datos seguro 702, de acuerdo con la presente invención. Las porciones de datos resultantes pueden ser comunicadas a través de uno o más recorridos de comunicaciones independientes 706, a través de las redes 708 (por ejemplo, la Internet, una Intranet, una LAN [Red de Área Local –“Local Area Network”], una red de tipo WiFi, Bluetooth, cualesquiera otros medios de comunicaciones por cable instalado o inalámbricas adecuados, o cualquier combinación de los mismos), a un sistema receptor o destinatario 710. Las porciones de datos pueden ser comunicadas paralelamente en el tiempo o de forma alternativa, de acuerdo con cualquier retardo temporal adecuado entre las comunicaciones de las diferentes porciones de datos. El sistema destinatario 710 puede consistir en cualquier hardware adecuado según se ha descrito anteriormente con respecto al sistema remitente 700. Las porciones de datos separadas que son transportadas a lo largo de los recorridos o caminos de comunicaciones 706, son recombinadas en el sistema destinatario 710 para generar el mensaje o los datos originales de acuerdo con la presente invención.

La Figura 8 muestra un sistema remitente 800, que puede incluir cualquier hardware adecuado, tal como un terminal informático, una computadora personal, un dispositivo de mano (por ejemplo, una PDA), un teléfono celular, una red informática, cualquier otro hardware adecuado, o bien cualquier combinación de los mismos. El sistema remitente 800 se utiliza para generar y/o almacenar un mensaje 804, el cual puede consistir, por ejemplo, en un paquete de red, un mensaje de correo electrónico, un archivo de datos binarios (por ejemplo, gráficos, voz, vídeo, etc.), o cualquier combinación de los anteriores. El mensaje 804 es analizado sintácticamente y dividido por un analizador sintáctico de datos seguro 802, de acuerdo con la presente invención. Las porciones de datos resultantes pueden ser comunicadas a través de caminos de comunicaciones individuales 806, por una red 808 (por ejemplo, la Internet,

una Intranet, una LAN, una red de tipo WiFi, Bluetooth, cualesquiera otros medios de comunicaciones adecuados, o bien cualquier combinación de los mismos), al sistema destinatario 810. Las porciones de datos pueden ser comunicadas en serie a través de un camino de comunicaciones 806, una con respecto a otra. El sistema destinatario 810 puede ser cualquier hardware apropiado según se ha descrito anteriormente con respecto al sistema remitente 800. Las porciones de datos independientes transportadas a lo largo del recorrido de comunicaciones 806 son recombinadas en el sistema destinatario con el fin de generar el mensaje o datos originales, de acuerdo con la presente invención.

Se comprenderá que la disposición de las Figuras 7 y 8 es meramente ilustrativa. Es posible utilizar cualquier otra disposición apropiada. Por ejemplo, en otra solución adecuada, las características de los sistemas de las Figuras 7 y 8 pueden combinarse, por lo que se utiliza la solución de múltiples caminos de la Figura 7, y en ella se utilizan uno o más de los caminos de comunicaciones 706 para transportar más de una porción de datos, como lo hace el camino de comunicaciones 806 en el contexto de la Figura 8.

El analizador sintáctico de datos seguro puede ser integrado en cualquier nivel apropiado de un sistema de datos en movimiento. Por ejemplo, en el contexto de un sistema de correo electrónico, el analizador sintáctico seguro puede estar integrado en el nivel de la interfaz de usuario (por ejemplo, dentro del Outlook de Microsoft®), en cuyo caso el usuario puede tener el control sobre el uso de las características del analizador sintáctico seguro cuando se utiliza el correo electrónico. Alternativamente, el analizador sintáctico seguro puede ser implementado dentro de un componente de terminal trasero, tal como en el servidor de intercambio, en cuyo caso los mensajes pueden ser automáticamente analizados sintácticamente, divididos y comunicados a lo largo de diferentes caminos de acuerdo con la presente invención, sin intervención alguna por parte del usuario. En algunas realizaciones, la integración puede ser transparente al usuario.

De forma similar, en el caso de difusiones para reproducción según descarga de datos (por ejemplo, de audio, vídeo), los datos salientes pueden ser analizados sintácticamente y separados en múltiples corrientes de datos, de tal modo que cada una de ellas contiene una porción de los datos analizados sintácticamente. Las múltiples corrientes pueden ser transmitidas a lo largo de uno o más caminos y recombinadas en la ubicación del destinatario, de acuerdo con la presente invención. Uno de los beneficios de esta solución es que evita la información de encabezamiento relativamente grande asociada con el cifrado tradicional de los datos, seguido de la transmisión de los datos cifrados a través de un único canal de comunicaciones. El analizador sintáctico seguro de la presente invención permite que los datos en movimiento sean enviados en múltiples corrientes paralelas de datos, lo que aumenta la velocidad y la eficiencia.

Se comprenderá que el analizador sintáctico de datos seguro puede ser integrado para la protección de, y la tolerancia ante los fallos de, cualquier tipo de datos en movimiento a través de cualquier medio de transporte, incluyendo, por ejemplo, cable instalado, inalámbrico o físico. Por ejemplo, las aplicaciones de protocolo de voz por Internet (VoIP –"voice over Internet protocol") pueden hacer uso del analizador sintáctico de datos seguro de la presente invención. El transporte de datos inalámbrico o por cable instalado desde, o hacia, cualesquiera dispositivos de asistente digital personal (PDA) adecuados, tales como Blackberries y SmartPhones (teléfonos inteligentes) puede ser asegurado utilizando el analizador sintáctico de datos seguro de la presente invención. Las comunicaciones que utilizan protocolos inalámbricos 802.11 para redes inalámbricas de igual a igual o entre pares y basadas en dispositivo centralizador, comunicaciones vía satélite, comunicaciones inalámbricas de punto a punto, comunicaciones de cliente / servidor por Internet, o cualesquiera otras comunicaciones apropiadas, pueden implicar las capacidades para datos en movimiento del analizador sintáctico de datos seguro, de acuerdo con la presente invención. Las comunicaciones de datos entre un dispositivo informático periférico (por ejemplo, una impresora, escáner, monitor o pantalla, teclado, dispositivo de encaminamiento de red, dispositivo de autentificación biométrica (por ejemplo, escáner para huellas dactilares), o cualquier otro dispositivo periférico adecuado) entre una computadora y un dispositivo informático periférico, entre un dispositivo informático periférico y cualquier otro dispositivo adecuado, o cualquier combinación de los mismos, puede hacer uso de las características de datos en movimiento de la presente invención.

Las características de datos en movimiento de la presente invención pueden también aplicarse al transporte físico de compartimientos seguros que utilice, por ejemplo, rutas, vehículos, métodos, cualquier otro transporte físico adecuado, o cualquier combinación de los mismos, todos ellos independientes. Por ejemplo, el transporte físico de los datos puede tener lugar sobre cintas digitales / magnéticas, discos flexibles, discos ópticos, fichas físicas, dispositivos de accionamiento de USB, dispositivos de accionamiento de disco duro extraíbles, dispositivos electrónicos consumibles con una memoria de tipo flash, o de acceso por impulsos (por ejemplo, IPODs de Apple u otros reproductores de MP3), memoria de tipo flash, cualquier otro medio adecuado que se utilice para transportar datos, o bien cualquier combinación de los mismos.

El analizador sintáctico de datos seguro de la presente invención puede proporcionar seguridad, con la capacidad de recuperarse de una situación de destrucción. De acuerdo con la presente invención, pueden necesitarse menos de la totalidad de las porciones de los datos separados generados por el analizador sintáctico de datos seguro, a fin de recuperar los datos originales. Esto es, aparte de las m porciones almacenadas, n puede ser el número mínimo de

estas m porciones que es necesario para recuperar los datos originales, siendo n <= m. Por ejemplo, si cada una de las cuatro porciones es almacenada en una posición física diferente con respecto a las otras tres porciones, entonces, si n = 2 en este ejemplo, dos de las posiciones pueden ponerse en peligro, con lo que los datos son destruidos o resultan inaccesibles, y los datos originales pueden aún ser recuperados de las porciones situadas en las otras dos posiciones. Puede utilizarse cualquier valor adecuado para n o m.

Además de ello, la característica n de m de la presente invención puede utilizarse para crear una "regla de dos hombres" en virtud de la cual, a fin de evitar poner la confianza en una única persona o cualquier otra entidad con acceso completo a lo que pueden ser datos delicados, puede ser necesario que dos o más entidades distintas, cada una de ellas con una porción de los datos separados analizados sintácticamente por el analizador sintáctico seguro de la presente invención, se pongan de acuerdo para juntar sus porciones con el fin de recuperar los datos originales.

El analizador sintáctico de datos seguro de la presente invención puede ser utilizado para proporcionar un grupo de entidades con una clave de amplitud de grupo que permite a los miembros del grupo acceder a información particular a la que se autoriza el acceso por ese grupo concreto. La clave de grupo puede ser una de las porciones de datos generadas por el analizador sintáctico seguro de acuerdo con la presente invención, que puede necesitarse para ser combinada con otra porción almacenada centralmente, por ejemplo, para recuperar la información buscada. Esta característica permite, por ejemplo, una colaboración segura entre un grupo. Puede aplicarse, por ejemplo, en redes de uso exclusivo o dedicadas, en redes privadas virtuales, en Intranets o en cualquier otra red adecuada.

Aplicaciones específicas de este uso del analizador sintáctico seguro incluyen, por ejemplo, el compartimiento de información de coalición en el que, por ejemplo, se proporciona a las fuerzas gubernamentales multinacionales coaligadas la capacidad de comunicarse datos operativos y delicados en otros sentidos, en un nivel de seguridad autorizado a cada país respectivo, a través de una única red o de una red doble (es decir, comparada con las muchas redes que implican procedimientos manuales relativamente sustanciales que se utilizan en la actualidad). Esta capacidad también es aplicable para empresas u otras organizaciones en las que la información que es necesario que conozcan una o más personas específicas (dentro de la organización o fuera de ella) puede ser comunicada a través de una única red, sin necesidad de preocuparse de que personas no autorizadas vean la información.

Otra aplicación específica incluye una jerarquía de seguridad de múltiples niveles para sistemas de gobierno. Es decir, el analizador sintáctico seguro de la presente invención puede proporcionar la capacidad de hacer funcionar un sistema gubernamental a diferentes niveles de información clasificada (por ejemplo, no clasificada, clasificada, secreta, de alto secreto) utilizando una única red. Si se desea, pueden utilizarse más redes (por ejemplo, una red independiente para alto secreto), pero la presente invención permite un número sustancialmente menor que en la disposición actual, en la que se utiliza una red independiente para cada nivel de clasificación.

Se comprenderá que es posible utilizar cualquier combinación de las aplicaciones anteriormente descritas del analizador sintáctico seguro de la presente invención. Por ejemplo, puede utilizarse la aplicación de clave de grupo conjuntamente con la aplicación de seguridad de datos en movimiento (esto es, por la que tan solo puede accederse a los datos que son comunicados por una red, por parte de un miembro del grupo respectivo, y en la que, mientras los datos se encuentran en movimiento, estos son divididos entre múltiples caminos (o enviados dentro de porciones secuenciales), de acuerdo con la presente invención).

El analizador sintáctico de datos seguro de la presente invención puede ser integrado dentro de cualquier aplicación de *middleware*, o mixta entre hardware y software, con el fin de permitir a las aplicaciones almacenar datos de forma segura en diferentes productos de base de datos o en diferentes dispositivos, sin tener que modificar las aplicaciones o la base de datos. *Middleware* es un término general para cualquier producto que permita comunicarse a dos programas ya existentes e independientes. Por ejemplo, en una solución apropiada, puede utilizarse *middleware* que tiene integrado el analizador sintáctico de datos seguro, para permitir que los programas escritos para una base de datos concreta se comuniquen con otras bases de datos sin una codificación personalizada.

El analizador sintáctico de datos seguro de la presente invención puede llevarse a la práctica de manera que tenga cualquier combinación de cualesquiera capacidades adecuadas, tales como las que se explican en esta memoria. En algunas realizaciones de la presente invención, por ejemplo, el analizador sintáctico de datos seguro puede ser implementado de modo que tenga tan solo ciertas capacidades, en tanto que otras capacidades pueden ser obtenidas mediante el uso de software o hardware externos, o de ambos, dispuestos a modo de interfaz, ya sea directa, ya sea indirectamente con el analizador sintáctico de datos seguro.

El analizador sintáctico de datos seguro de la presente invención puede, ventajosamente, ser utilizado en diversas aplicaciones y tecnologías. Por ejemplo, un sistema de correo electrónico, sistemas de RAID [conjunto ordenado redundante de discos independientes –"Reduntant Array of Independent Disks"], sistemas de difusión de vídeo, sistemas de bases de datos, sistemas de copia de seguridad de cinta, o cualquier otro sistema adecuado, pueden tener el analizador sintáctico de datos seguro integrado en cualquier nivel apropiado. Como se ha explicado

anteriormente, se comprenderá que el analizador sintáctico de datos seguro puede estar también integrado para la protección y la tolerancia ante fallos de cualquier tipo de datos en movimiento a través de cualquier medio de transporte, incluyendo, por ejemplo, medios de transporte por cable instalado, inalámbricos o físicos. Como ejemplo, las aplicaciones de protocolo de voz por Internet (VoIP –"voice over Internet protocol") pueden hacer uso del analizador sintáctico de datos seguro de la presente invención para resolver problemas relativos a ecos y retardos que se encuentran comúnmente en el VoIP. La necesidad de reintento de conexión a red para los paquetes inutilizados o "caídos" puede suprimirse utilizando tolerancia frente a fallos, lo que garantiza la entrega de los paquetes incluso con la pérdida de un número predeterminado de compartimientos. Los paquetes de datos (por ejemplo, los paquetes de red) pueden ser también eficazmente divididos y restituidos "sobre la marcha" con un retardo y almacenamiento intermedio mínimos, de lo que resulta una solución exhaustiva para los diversos tipos de datos en movimiento. El analizador sintáctico de datos seguro puede actuar sobre paquetes de datos de red, paquetes de voz de red, bloques de datos de sistemas de archivos, o cualquier otra unidad de información adecuada. Además de ser integrado en la aplicación de VoIP, el analizador sintáctico de datos seguro puede ser integrado con una aplicación de compartimiento de archivos (por ejemplo, una aplicación de compartimiento de archivos de igual a igual, o entre pares), una aplicación de difusión de vídeo, una aplicación de votación o sondeo electrónico (que puede poner en práctica un protocolo de votación electrónico y firmas ciegas, tal como el protocolo Sensus), una aplicación de correo electrónico, o cualquier otra aplicación de red que pueda requerir o desear una comunicación segura.

En algunas realizaciones, puede proporcionarse soporte para datos de red en movimiento por parte del analizador sintáctico de datos seguro de la presente invención, en dos fases diferenciadas –una fase de generación de encabezamiento y una fase de partición de datos. En las Figuras 9A y 9B se han mostrado, respectivamente, el procedimiento 900 de generación de encabezamiento simplificado y el procedimiento 910 de partición de datos simplificado. Uno de estos procedimientos, o ambos, pueden llevarse a cabo sobre paquetes de red, bloques de sistemas de archivos, o cualquier otra información apropiada.

En algunas realizaciones, el procedimiento 900 de generación de encabezamiento que se ha mostrado en la Figura 9A puede llevarse a cabo una vez al inicio de una corriente de paquetes de red. En la etapa 902, puede generarse una clave de cifrado de división aleatoria (o pseudoaleatoria), K. La clave de cifrado de división, K, puede entonces ser, opcionalmente, encriptada o cifrada (por ejemplo, utilizando la clave de grupo de trabajo anteriormente descrita) en la etapa 904 de envoltura de clave según la AES [Norma de Cifrado Avanzada –"Advanced Encryption Standard"]. Si bien puede utilizarse una envoltura de clave según la AES en algunas realizaciones, es posible utilizar, en otras realizaciones, cualquier algoritmo de cifrado de clave o de envoltura de clave adecuado. La etapa 904 de envoltura de clave de la AES puede operar sobre toda la clave de cifrado de división, K, o bien la clave de cifrado de división puede ser analizada sintácticamente y dividida en varios bloques (por ejemplo, bloques de 64 bits). La etapa 904 de envoltura de clave de AES puede, entonces, operar sobre bloques de la clave de cifrado de división, si se desea.

En la etapa 906, un algoritmo de compartimiento secreto (por ejemplo, de Shamir) puede ser utilizado para dividir la clave de cifrado de división, K, en compartimientos de clave. Cada compartimiento de clave puede, entonces, ser embebido o incorporado dentro de uno de los compartimientos de salida (por ejemplo, dentro de los encabezamientos de compartimiento). Por último, pueden anexarse al bloque de encabezamiento de cada compartimiento un bloque de integridad de compartimiento y (opcionalmente) una etiqueta de postautentificación (por ejemplo, de MAC). Cada bloque de compartimiento puede haberse diseñado de manera que quepa dentro de un único paquete de datos.

Una vez completada la generación de encabezamiento (por ejemplo, utilizando el procedimiento de generación de encabezamiento simplificado 900), el analizador sintáctico de datos seguro puede introducir la fase de partición de datos que se ha mostrado en la Figura 9B, utilizando el procedimiento de división de datos simplificado 910. Cada paquete de datos o bloque de datos entrante contenido en la corriente es cifrado utilizado la clave de cifrado de división, K, en la etapa 912. En la etapa 914, la información de integridad de compartimiento (por ejemplo, un fragmento H) puede ser computada en el texto cifrado resultante procedente de la etapa 912. Por ejemplo, puede computarse un fragmento SHA-256. En la etapa 916, el paquete de datos o bloque de datos puede ser entonces dividido en dos o más compartimientos de datos utilizando uno de los algoritmos de división de datos anteriormente descritos de acuerdo con la presente invención. En algunas realizaciones, el paquete de datos o bloque de datos puede ser dividido de un modo tal, que cada compartimiento de datos contiene una distribución sustancialmente aleatoria del paquete de datos o bloque de datos cifrado. La información de integridad (por ejemplo, el fragmento H) puede ser entonces anexada a cada compartimiento de datos. Una etiqueta de postautentificación opcional (por ejemplo, de MAC) puede también ser computada y anexada a cada compartimiento de datos, en algunas aplicaciones.

Cada compartimiento de datos puede incluir metadatos [datos relativos a otros datos], que pueden ser necesarios para permitir una correcta reconstrucción de los bloques de datos o paquetes de datos. Esta información puede ser incluida en el encabezamiento de compartimiento. Los metadatos pueden incluir información tal como compartimientos de clave criptográfica, identidades o identificadores de clave, términos ocasionales de

compartimiento, firmas / valores de MAC, así como bloques de integridad. A fin de maximizar la eficiencia de anchura de banda, los metadatos pueden ser almacenados en un formato binario compacto.

Por ejemplo, en algunas realizaciones, el encabezamiento de compartimiento puede incluir un segmento o fracción de encabezamiento despejada de texto, que no está cifrada y que pueda incluir elementos tales como el compartimiento de clave de Shamir, un término ocasional por cada sesión, un término ocasional por cada compartimiento, así como identificadores de clave (por ejemplo, un identificador de clave de grupo de trabajo y un identificador de clave de postautentificación). El encabezamiento de compartimiento puede también incluir una fracción de encabezamiento cifrada, la cual se cifra utilizando la clave de cifrado de división. Puede haberse incluido también en el encabezamiento una fracción de encabezamiento de integridad, que puede incluir comprobaciones de integridad para un número cualquiera de bloques previos (por ejemplo, los dos bloques previos). Pueden incluirse también en el encabezamiento de compartimiento, en otras realizaciones, cualesquiera otros valores o información adecuados.

Como se ha mostrado en el formato de compartimiento ilustrativo 1000 de la Figura 10, el bloque de encabezamiento 1002 puede estar asociado con dos o más bloques de entrada 1004. Cada bloque de encabezamiento, tal como el bloque de encabezamiento 1002, puede haberse diseñado para caber dentro de un único paquete de datos de red. En algunas realizaciones, una vez que el bloque de encabezamiento 1002 se ha transmitido desde una primera posición a una segunda posición, pueden ser entonces transmitidos los bloques de salida. Alternativamente, el bloque de encabezamiento 1002 y los bloques de salida 1004 pueden ser transmitidos al mismo tiempo, en paralelo. La transmisión puede producirse a través de uno o más caminos de comunicaciones similares o disímiles.

Cada bloque de salida puede incluir una porción de datos 1006 y una porción de integridad / autenticidad 1008. Como se ha descrito anteriormente, cada compartimiento de datos puede ser asegurado utilizando una porción de integridad de compartimiento que incluye información de integridad de compartimiento (por ejemplo, un fragmento SHA-256) de los datos cifrados, previamente divididos. A fin de verificar la integridad de los bloques de salida en el momento de la recuperación, el analizador sintáctico de datos seguro puede comparar los bloques de integridad de compartimiento de cada compartimiento y, seguidamente, invertir el algoritmo de división. El fragmento de los datos recuperados puede ser entonces verificado frente al fragmento de compartimiento.

Como se ha descrito anteriormente, el analizador sintáctico de datos seguro de la presente invención puede también ser utilizado para asegurar datos en movimiento (o datos que son comunicados desde un sistema o servicio a otro) dentro de un grupo de trabajo. En algunas realizaciones, un servidor centralizado se encarga de toda la gestión de usuario, servicios y grupos de trabajo para un único dominio (o a lo largo y ancho de múltiples dominios). El servidor centralizado puede incluir un único servidor o un agrupamiento de servidores (para tolerancia frente a defectos), y puede incluir un servidor de LDAP, tal como un servidor que hace funcionar el Microsoft® Server y el Active Directory.

Es posible proporcionar una autentificación de usuario sin interrupciones o discontinuidades dentro de un grupo de trabajo utilizando un protocolo de instancia / respuesta 110, tal y como se muestra en la Figura 11. Utilizando el protocolo 1100, el cliente 1102 del grupo de trabajo puede autentificarse a sí mismo frente al servidor de autentificación 1104. Puede concederse una autentificación de usuario sin discontinuidades a través de la verificación de un secreto compartido (por ejemplo, utilizando Autentificación Compendiada (“Digest Authentication”). Cuando un usuario introduce su identificación de entrada en el cliente 1102 del grupo de trabajo, una palabra de paso introducida por el usuario puede ser sometida a una función criptográfica que transforma el texto en ASCII [Código Estándar Norteamericano para Intercambio de Información –“American Standard Code for Information Exchange”] de la palabra de paso en una clave criptográfica. Esta clave basada en palabra de paso (designada como “PBK” [“password-based key”] en el ejemplo de la Figura 11) puede también ser almacenada en, o ser accesible por, el servidor de autentificación 1104.

Para ser autentificado, el cliente 1102 del grupo de trabajo puede identificarse a sí mismo ante el servidor de autentificación 1104 con el mensaje 1106. Por ejemplo, el mensaje 1106 puede incluir datos indicativos de la identidad del usuario, tales como, por ejemplo, el nombre del grupo de trabajo del usuario, el nombre de usuario para la identificación de entrada, la dirección de red, la dirección de MAC, o bien cualquier combinación de los anteriores. En respuesta al mensaje 1106, el servidor de autentificación 1104 puede enviar al cliente 1102 de grupo un valor de instancia en el mensaje 1108. El valor de instancia puede incluir un número cualquiera de bits o bytes que, una vez recibidos por el cliente 1102 del grupo de trabajo, pueden ser cifrados utilizando la clave basada en palabra de paso. El texto cifrado resultante (designado como “Y” en el ejemplo de la Figura 11) puede, a continuación, ser devuelto al servidor dentro de un mensaje 1110. El servidor de autentificación 1104 puede, seguidamente, llevar a cabo la misma encriptación o cifrado en el valor de instancia, utilizando la clave basada en palabra de paso almacenada para el cliente del grupo de trabajo, y verificar que su propio cifrado y el texto cifrado recibido coinciden. Si existe una coincidencia, entonces el usuario ha sido autentificado. En caso contrario, la petición de autentificación puede ser denegada.

La Figura 12 muestra un procedimiento ilustrativo 1200 para comunicarse con un servicio por la red. El procedimiento 1200 puede ser llevado a efecto utilizando un subsistema de Kerberos, el cual permite que dos clientes del grupo de trabajo (tales como los clientes 1202 y 1206) de una red demuestren su autenticidad el uno al otro mediante el uso de un servidor central al que se hace referencia en ocasiones como Centro de Distribución de Claves (KDC –"Key Distribution Center") 1204.

Una vez que ha sido autentificado (por ejemplo, utilizando un protocolo de instancia / respuesta según se ha mostrado por los mensajes 1208), puede darse a un usuario un Tique de Concesión de Tique (TGT –"Ticket Granting Ticket") dentro del mensaje 1210. Este tique puede servir como ficha que se ha de proporcionar al KDC 1204 siempre que el cliente 1202 intente comunicarse con otro usuario o servicio existente en la red (tal como un servidor de web, un servidor de correo electrónico o un cliente 1206). El TGT puede incluir, por ejemplo, un bloque de información que contiene el nombre o identidad del destinatario, un sello temporal y cualesquiera otra credenciales necesarias. El TGT puede, también, ser cifrado bajo la Clave Maestra del KDC, de tal manera que únicamente el KDC puede leer su contenido.

Cuando un usuario con un TGT desea comunicarse con un servicio de la red, puede hacer llegar el TGT al KDC y solicitar un Tique de Servicio (ST –"Service Ticket") válido. Por ejemplo, como se ha mostrado en la Figura 12, el cliente 1202 del grupo de trabajo ha solicitado un ST para el cliente 1206 a través del mensaje 1212. Si el TGT es válido, el KDC 1204 puede devolver al cliente 1202 dos STs por medio de un mensaje 1214, de tal manera que cada ST contiene los credenciales de las partes implicadas en la comunicación, un sello temporal y una clave de sesión (SK –"session key") única o exclusiva y nueva, destinada a ser utilizada como clave compartida temporal entre ambas partes para el cifrado. Uno de los STs puede ser cifrado bajo la clave basada en palabra de paso compartida entre el usuario y el KDC, y el otro ST puede ser cifrado bajo la clave basada en palabra de paso compartida entre el servicio o cliente con el que se está contactando (por ejemplo, el cliente 1206) y el KDC.

El ST cifrado para el cliente 1202 que realiza la petición puede ser de inmediato descifrado por el cliente 1202 y la SK sin cubrir. El cliente 1202 puede enviar, a continuación, el segundo ST y un mensaje cifrado bajo la SK al servicio o al cliente pretendido (por ejemplo, el cliente 1206) a través de un mensaje 1216. En una etapa final, el cliente o servicio (por ejemplo, el cliente 1206) puede descifrar, a continuación, el ST con su clave basada en palabra de paso, a fin de obtener el SK, y, subsiguientemente, descifrar el mensaje enviado por el cliente 1202. A través de este procedimiento, los clientes 1202 y 1206 comparten ahora el SK.

En la práctica, una o más de las etapas mostradas en el procedimiento 1200 pueden ser combinadas con otras etapas, llevarse a cabo en cualquier orden adecuado, realizarse en paralelo (por ejemplo, simultáneamente o de forma sustancialmente simultánea), o suprimirse.

La Figura 13 muestra un procedimiento ilustrativo 1300 para utilizar claves compartidas con el analizador sintáctico de datos seguro. El SK anteriormente descrito puede ser utilizado como una clave de grupo de trabajo (WK –"workgroup key") compartida, para dar soporte a la comunicación segura del grupo de trabajo utilizando el analizador sintáctico de datos seguro. En algunas realizaciones, la WK del analizador sintáctico de datos seguro puede ser utilizada para envolver claves de sesión generadas internamente, incluyendo la Clave de Sesión de Cifrado (ESK –"Encryption Session Key") y la clave de sesión de MAC (MK –"MAC session key"), tal como se ha descrito con mayor detalle en la Patente de los EE.UU. Nº 7.391.865 y en las Solicitudes de Patente de los EE.UU. 10/458.928, presentada el 11 de junio de 2003, 11/258.839, presentada el 25 de octubre de 2005, 11/602.667, presentada el 20 de noviembre de 2006, 11/983.355, presentada el 7 de noviembre de 2007, 11/999.575, presentada el 5 de diciembre de 2007, 12/209.703, presentada el 12 de septiembre de 2008, y 12/349.897, presentada el 7 de enero de 2009.

Una vez envueltos con la WK, los textos cifrados pueden ser compartidos de forma segura (por ejemplo, utilizando un esquema de compartimiento secreto, tal como el de Shamir) entre cada encabezamiento generado por el analizador sintáctico de datos seguro, de tal modo que se almacena con cada encabezamiento un único compartimiento de cada clave envuelta. La obtención de la ESK o de la MK puede ahora requerir la obtención de la WK y un quórum de compartimientos suficiente como para reconstruir los textos cifrados con la ESK y con la MK envueltas. En algunas realizaciones, la WK del analizador sintáctico de datos seguro puede ser utilizada para envolver una Clave de Sesión de Cifrado (ESK –"Encryption Session Key") internamente generada. Una vez envuelto con la WK, el texto cifrado puede envolverse de nuevo con una Clave de Cifrado de Clave (KEK –"Key Encrypting Key") que se acaba de generar. Ahora, la ESK ha sido doblemente envuelta y únicamente puede ser recuperada con el conocimiento tanto de la WK como de la KEK. La KEK puede ser compartida de forma segura entre cada encabezamiento generado por el analizador sintáctico de datos seguro, y la ESK doblemente envuelta puede ser almacenada dentro de cada encabezamiento. La obtención de la ESK puede requerir, ahora, la obtención de la WK y un quórum de compartimientos suficiente como para reconstruir la KEK. En una sesión de comunicación típica, dos usuarios o clientes de grupo de trabajo pueden obtener tiques cifrados únicamente para cada cliente individualmente, de tal modo que los tiques contienen el valor de la WK. El valor de la WK puede ser entonces importado o llevado al interior del dispositivo de almacenamiento de claves (KeyStore) para cada uno de los dos usuarios o clientes, y puede ser utilizado como una WK normal en el contexto de una sesión de comunicación de

analizador sintáctico de datos seguro.

Por ejemplo, el cliente 1302 puede importar o llevar una WK compartida al interior de su KeyStore y generar encabezamientos de analizador sintáctico de datos seguro, tal y como se ha descrito anteriormente en relación con las Figuras 9 y 10. Los encabezamientos de analizador sintáctico de datos seguro pueden incluir uno o más de entre la WK, la ID de clave de grupo de trabajo y el número de versión de WK (por ejemplo, la WK, la ID de clave y el número de sesión pueden ser enviados a los encabezamientos y compartidos con estos utilizando un esquema de compartimiento secreto, tal como el de Shamir, en algunas realizaciones). El cliente 1302 puede, a continuación, enviar estos encabezamientos al cliente 1304 por medio de unos mensajes 1306. El cliente 1304 puede reconstruir la WK, la ID de clave de grupo de trabajo y el número de versión de WK a partir de los encabezamientos recibidos, e importar el WK al interior de su dispositivo de almacenamiento de claves (KeyStore). Una vez que cada cliente ha almacenado la WK en su KeyStore respectivo, puede tener lugar entones una sesión de comunicaciones de analizador sintáctico de datos seguro (por ejemplo, que analice sintácticamente un conjunto de datos y que restituya el conjunto de datos) utilizando unos mensajes 1308 y 1310 de datos.

En la práctica, una o más etapas mostradas en el procedimiento 1300 pueden combinarse con otras etapas, llevarse a cabo en cualquier orden adecuado, realizarse en paralelo (por ejemplo, simultáneamente o de forma sustancialmente simultánea), o suprimirse.

Con el fin de que los anteriores mecanismos sean integrados con un dispositivo de accionamiento de red en el nivel de Kernel, en algunas realizaciones, se proporcionan modificaciones del servidor de autentificación para distribuir las claves de sesión. Pueden proporcionarse también modificaciones en la estación de trabajo, en algunas realizaciones, para solicitar TGTs y STs. El procedimiento 1400, tal y como se ha mostrado en la Figura 14, ilustra una secuencia de mensajes proporcionada a modo de ejemplo. Por ejemplo, la capacidad funcional de Kerberos y la comunicación con el KDC 1406 no pueden, por lo general, producirse en un espacio de Kernel 1404. En lugar de ello, el dispositivo de accionamiento de red puede llamar de vuelta al espacio 1402 de usuario para llevar a cabo los intercambios de clave de Kerberos, y hacer pasar, a continuación, de vuelta en sentido descendente cualesquiera datos que se utilicen por el dispositivo de accionamiento de red (o enviarlos al destino original). Por ejemplo, una vez que un cliente 1401 desea comunicarse con un cliente 1419, puede generarse un mensaje 1408 y suministrarse desde el espacio 1402 de usuario al dispositivo de accionamiento de red contenido en el espacio de Kernel 1404. El dispositivo de accionamiento de red puede determinar si existe ya o no una sesión del analizador sintáctico de datos seguro con la dirección de IP de destino deseada (u otro identificador de red), y, si es así, puede utilizar ese canal. Si no existe ninguna sesión, el dispositivo de accionamiento de red puede hacer pasar la dirección de IP (u otro identificador de red) en sentido ascendente hasta un servicio en el nivel del usuario, a fin de obtener STs utilizando un mensaje 1410.

El servicio puede entonces determinar si están guardados o no en memoria caché, en ese momento, los STs para la dirección de IP dada (u otro identificador de red), y, si no es así, el servicio en el nivel del usuario puede obtener los STs del KDC 1406 por medio de unos mensajes 1412. A continuación, el servicio en el nivel del usuario puede descifrar la WK embebida o incorporada en el ST para el cliente 1401, y hacer pasar la WK y el ST para el cliente 1419 de vuelta al dispositivo de accionamiento de red en el espacio de Kernel 1404, por medio de un mensaje 1414. El dispositivo de accionamiento de red puede, entonces, utilizar la WK para generar encabezamientos de analizador sintáctico de datos seguro y enviarlos, conjuntamente con el ST para el cliente 1419, al cliente 1419 por medio de unos mensajes 1416. Después de recibir los encabezamientos y el ST en el dispositivo de accionamiento de red dl cliente 1419, el ST puede hacerse pasar, entonces, en sentido ascendente, hasta su propio servicio en el nivel del usuario, por medio de un mensaje 1418. El servicio en el nivel del usuario puede descifrar el ST y extraer la WK, la cual se hace pasar, a continuación, de vuelta en sentido descendente al dispositivo de accionamiento de red, por medio de un mensaje 1420. El cliente 1419 puede entonces utilizar la WK para restituir los encabezamientos de analizador sintáctico de datos seguro que ha recibido y completar el canal.

En la práctica, pueden combinarse una o más de las etapas mostradas en el procedimiento 1400 con otras etapas, llevarse a cabo en cualquier orden adecuado, realizarse en paralelo (simultáneamente o de forma sustancialmente simultánea), o suprimirse.

La Figura 15 muestra una topología de red ilustrativa 1500. Una Autoridad de Certificación (CA –“Certificate Authority”) 1502 puede reclutar o incorporar cada Autoridad de Grupo de Trabajo (WA –“Workgroup Authority”) en la red o dominio. Si bien, en el ejemplo de la Figura 15, se han mostrado tres WAs (es decir, la WA 1504, la WA 1506 y la WA 1508), en implementaciones reales puede haber un número mayor o menor que tres WAs es una sola red o dominio. La CA 1502 puede reclutar o incorporar cada una de las WA 1504, WA 1506 y WA 1508 mediante la emisión con cada WA de un certificado de WA para su grupo de trabajo respectivo. Los certificados pueden ser firmados digitalmente por la CA 1502 para impedir su manipulación indebida.

Una vez reclutadas o incorporadas por la CA 1602, la WA 1504, la WA 1506 y la WA 1508 pueden empezar a incorporar clientes (por ejemplo, usuarios, máquinas y servicios) dentro de sus respectivos grupos de trabajo. Por ejemplo, en algunas realizaciones, la incorporación puede estar basada, al menos en parte, en semánticas de

pertenencia como miembro a Directorio Activo (u otro LDAP) preexistentes. A los clientes reclutados o incorporados se les pueden emitir certificados firmados por su respectiva WA, así como los certificados de la WA, de la CA, o ambos.

La Figura 16 muestra un montaje o disposición de conexión ilustrativa 1600. Un iniciador 1604 puede, en primer lugar, asegurarse de que está utilizando la última WK llevando a cabo una actualización de clave 1608 con una WA 1602. El iniciador 1604 puede proporcionar un término ocasional a la WA 1602 y demostrar que posee un certificado válido. La WA 1602 puede, entonces, proporcionar una WK cifrada y firmada que incluye el término ocasional del iniciador. En algunas realizaciones, el cifrado se lleva a cabo utilizando RSA PKCS #1 v2 con firmas de acuerdo con RSA-PSS o ECDSA. En otras realizaciones, se utiliza cifrado autentificado según AES-GCM bajo claves simétricas previamente compartidas.

El iniciador 1604 inicia, a continuación, una conexión con un destinatario 1606 utilizando la última WK, mediante un mensaje de petición 1610. Tras recibir la petición de conexión, el destinatario 1606 puede asegurar que tiene la última WK. Puede llevarse a cabo una actualización 1612 de clave de la misma manera cifrada, autentificada y resistente a contestaciones, que como se llevó a cabo por el iniciador 1604. Si el destinatario 1606 pertenece a más de un grupo de trabajo, el destinatario 1606 selecciona la WA apropiada basándose, al menos en parte, en la ID de clave de grupo de trabajo suministrada dentro del mensaje de petición 1610. Si el iniciador 1604 y el destinatario 1606 recuperan la misma WK de la WA 1602, entonces el destinatario 1606 puede enviar un mensaje de conexión con éxito 1614 al iniciador 1604.

Una o ambas de las etapas de actualización de clave mostradas en asociación con el montaje 1600 pueden llevarse a cabo, bien con la conexión inicial con otro cliente del grupo de trabajo, bien periódicamente una vez que se llega a un tiempo de aviso de refrescamiento de clave de grupo de trabajo, o bien periódicamente según cualquier otra programación temporal adecuada. En algunas realizaciones, como se describe con mayor detalle más adelante, las actualizaciones de clave se llevan a cabo automáticamente antes de que se establezca cada nueva sesión de comunicación. El control por parte del sistema o del usuario del aviso de TTL [tiempo de vida –"time to live"] y refrescamiento de la clave del grupo de trabajo puede proporcionar niveles o grados personalizados de susceptibilidad de renovación, o renovabilidad. Esto puede ser beneficioso, por ejemplo, después de que se han revocado los privilegios de comunicación de un cliente y se desea una capacidad de revocación inmediata.

La necesidad de listas de revocación de certificado (CRLs –"certificate revocation lists") puede también ser reducida o incluso eliminada en su totalidad utilizando esta solución. La pertenencia en calidad de miembro de un grupo de trabajo puede ser mantenida por el servidor de autentificación o de LDAP. En algunas realizaciones, se da también soporte a la revocación de WA utilizando el Protocolo de Estatus de Certificado En Línea (OCSP –"Online Certificate Status Protocol"). Por ejemplo, un respondedor de OSCP puede determinar el estatus de un certificado de WA sin comprobar la CRL publicada por la CA.

En la práctica, pueden combinarse una o más etapas mostradas en un montaje de conexión 1700 con otras etapas, llevarse a cabo en cualquier orden adecuado, realizarse en paralelo (por ejemplo, simultáneamente o de forma sustancialmente simultánea), o suprimirse.

Las Figuras 17-20 muestran procedimientos ilustrativos para dar soporte a la gestión y distribución de clave de grupo de trabajo segura de la presente invención. La Figura 17 muestra un procedimiento ilustrativo 1700 para unirse a un nuevo grupo de trabajo. En la etapa 1702, el cliente puede indicar su deseo de unirse a un grupo de trabajo. En la etapa 1704, la WA puede generar una clave secreta E_n para el cliente. En algunas realizaciones, E_n puede ser una clave para un lenguaje cifrado simétrico. En otras realizaciones, puede utilizarse un esquema de cifrado de clave pública que se sirve de un lenguaje cifrado asimétrico, y E_n puede ser una clave (por ejemplo, una clave privada) para un lenguaje cifrado asimétrico. Puede utilizarse, por ejemplo, las solución de cifrado de difusión con cobertura de subconjunto de Naor, Naor y Lotspeich, en lugar del esquema simétrico que se describe más adelante. El algoritmo de cifrado de clave pública puede ser construido encima de cualquier otro esquema de cifrado de clave pública seguro.

La generación de clave utilizando la solución de clave pública puede, en algunas realizaciones, ser llevada a cabo centralmente por la WA. Si M es el tamaño máximo del grupo de trabajo, entonces la WA puede generar $2M - 1$ pares de claves pública / privada distintos. Si existe un árbol binario de envergadura M, de manera que cada par de claves está asociado con un nodo interno del árbol, entonces, para cada dispositivo o cliente del grupo de trabajo, puede escogerse la hoja i-ésima del árbol y podrá proporcionarse al dispositivo o cliente i cada par de claves asociado con la hoja i-ésima hacia arriba, hasta la raíz del árbol. El tamaño total del dispositivo o del material de clave del cliente puede ser, entonces, igual a $\log M + 1$. Pueden utilizarse, en otras realizaciones, otras soluciones para la generación de claves utilizando un enfoque de clave pública o de clave secreta.

En la etapa 1706, la WA puede almacenar una o más de entre la identidad del cliente n, la clave secreta E_n del cliente, y una lista de IDs de clave de grupo de trabajo autorizada. En la etapa 1708, el cliente n puede almacenar su clave secreta localmente en un dispositivo de almacenamiento de claves. En la etapa 1710, el cliente n puede

también almacenar la ID de clave de grupo de trabajo (por ejemplo, un identificador de conocimiento público y/o de cadena) y ajustar el aviso de refrescamiento de clave de grupo de trabajo en 0 (es decir, inmediato) y la versión de clave en 0.

Un mismo cliente puede pertenecer a uno o más grupos de trabajo. Cada grupo de trabajo (y, por tanto, la WK vigente en ese momento para ese grupo de trabajo) puede estar asociado con un identificador de grupo de trabajo único o exclusivo. Los identificadores de grupo de trabajo exclusivos y las IDs de clave de grupo de trabajo asociadas pueden ayudar al cliente y a la WA a determinar a qué grupo de trabajo o grupos de trabajo pertenece en ese momento el cliente, así como a determinar qué clave de grupo de trabajo se ha de utilizar para establecer una sesión de comunicación con otro cliente que también pertenece a uno o más grupos de trabajo.

En la práctica, una o más de las etapas mostradas en el procedimiento 1700 pueden ser combinadas con otras etapas, llevarse a cabo en cualquier orden adecuado, realizarse en paralelo (por ejemplo, simultáneamente o de forma sustancialmente simultánea), o suprimirse.

Las Figuras 18A, 18B y 18C muestran un procedimiento ilustrativo 1800 para iniciar una conexión entre dos clientes. En la etapa 1802, el cliente 1 puede iniciar una sesión de comunicación con el cliente 2. Por ejemplo, el cliente 1 puede enviar su identidad (por ejemplo, dirección de red o nombre de usuario) al cliente 2 y solicitar una sesión de comunicación con el cliente 2. En la etapa 1804, el cliente 1 puede comprobar su tiempo de aviso de refrescamiento de clave de grupo de trabajo. En la etapa 1804, el cliente 1 puede también verificar que no ha expirado un valor cualquiera de tiempo de vida (TTL –"time to live") asociado con la WK del cliente 1. Por ejemplo, a fin de determinar si la WK del cliente 1 ha expirado, el cliente 1 puede comparar el valor de TTL asociado con la WK del cliente 1 con el tiempo u hora corriente o con el sello temporal de WK. El sello temporal de WK puede indicar cuándo se ha generado o se ha suministrado la WK al cliente 1. Si, en la etapa 1806, el tiempo de aviso de refrescamiento es mayor que el tiempo u hora corriente (o sello temporal de WK), el procedimiento ilustrativo 1800 puede proseguir por la Figura 18B. Si, en la etapa 1806, el tiempo de aviso de refrescamiento no es mayor que el tiempo u hora corriente (o sello temporal de WK), entonces, en la etapa 1808, el cliente 1 puede contactar con el cliente 2 con los encabezamientos generados del analizador sintáctico de datos seguro. Estos encabezamientos pueden incluir, por ejemplo, la WK y el número de la versión de la WK. En la etapa 1810, el cliente 2 puede leer la ID de clave de grupo de trabajo. Si, en la etapa 1812, la ID de clave de grupo de trabajo no es válida para este grupo de trabajo (a para un grupo de trabajo al que pertenece en ese momento el cliente 2), el cliente 2 puede informar del error a la aplicación llamante en la etapa 1814. En algunas realizaciones, la aplicación de llamada puede determinar la respuesta al error señalado. Si, en la etapa 1812, la ID de clave de grupo de trabajo es válida para este grupo de trabajo (o para un grupo de trabajo al que pertenece en ese momento el cliente 2), el procedimiento ilustrativo 1800 puede proseguir por la Figura 18C.

La Figura 18B continúa el procedimiento ilustrativo 1800 después de que se haya determinado, en la etapa 1806, que el tiempo de aviso de refrescamiento es mayor que el tiempo u hora corriente (o sello temporal de WK). En algunas realizaciones, esto puede indicar una WK caducada. Para que el cliente 1 continúe, en algunas realizaciones, este debe contactar con la WA y refrescar o renovar su WK. En la etapa 1816, el cliente 1 puede generar un término ocasional N_1. En la etapa 1816, el cliente 1 puede también enviar un mensaje a la WA. En algunas realizaciones, el mensaje puede ser formateado como sigue: {Cliente 1 ‖ E_1 {¿ACTUALIZADO? ‖ N_1 ‖ ID de clave de grupo de trabajo ‖ versión de clave de grupo de trabajo de cliente} }, donde Cliente 1 es la identidad del cliente 1, E_1 es una función criptográfica basada, al menos en parte, en la clave secreta del cliente 1, y ¿ACTUALIZADO? es el tipo de mensaje.

En la etapa 1818, la WA puede consultar el cliente 1 y acceder a la E_1, la clave secreta del cliente 1. Como se ha descrito anteriormente, la WA puede almacenar cada clave secreta del miembro del grupo de trabajo en un dispositivo de almacenamiento de claves, en un repositorio de claves, o en una base de datos. En la etapa 1818, la WA puede también descifrar el mensaje enviado por el cliente 1 en la etapa 1816. En la etapa 1820, la WA puede determinar si el cliente 1 está autorizado, validando que la ID de clave de grupo de trabajo recibida se ha autorizado para este cliente. La WA puede también hacer comprobaciones para verificar si existe una nueva versión de la WK, y calcular cuánto falta para que expire la WK (por ejemplo, puede computarse un valor de "tiempo de vida" o TTL para la WK). Si, en la etapa 1820, la WA determina que no se ha encontrado el cliente o no se ha autorizado para este grupo de trabajo, la WA puede enviar de vuelta un mensaje de no autorización en la etapa 1822. En caso contrario, en la etapa 1824, la WA puede enviar de vuelta un mensaje cifrado con la clave secreta del cliente 1. El mensaje puede estar, en algunas realizaciones, en el siguiente formato: E_1 {¿ACTUALIZADO? ‖ N_1 ‖ ID de clave de grupo de trabajo ‖ versión de clave de grupo de trabajo vigente en ese momento ‖ TTL}.

En la etapa 1826, el cliente 1 puede descifrar el mensaje y comparar su versión de WK con la versión de WK vigente en ese momento. Si la versión de WK del cliente 1 es anterior a la versión de WK vigente en ese momento, el cliente 1 puede actualizar su WK en la etapa 1830. En un procedimiento ilustrativo que un cliente puede utilizar para actualizar su WK se describe en relación con la Figura 20, más adelante. Si la versión de WK del cliente 1 no es anterior a la versión de WK vigente en ese momento (por ejemplo, es la versión vigente en ese momento), entonces el cliente 1 puede actualizar su aviso de refrescamiento de WK hasta el momento o tiempo corriente más el TTL

calculado por la WA en la etapa 1828.

Haciendo referencia, a continuación, a la Figura 18C, si una ID de clave de grupo de trabajo es válida para el grupo de trabajo concreto, el cliente 2 puede entonces determinar, en la etapa 1832, si el número de la versión de la WK del cliente 1 es menor que el número de la versión vigente en ese momento del cliente 2. Si es así, el cliente 2 puede informar de un error a la aplicación llamante en la etapa 1834. En algunas realizaciones, la aplicación llamante puede determinar la respuesta al erro señalado (por ejemplo, la aplicación llamante puede llevar a cabo automáticamente una actualización de clave para obtener una versión más reciente de la WK, y reintentar la conexión). Si, en la etapa 1832, el cliente 2 determina que el número de la versión de la WK del cliente 1 no es mayor que la versión del cliente 2, el cliente 2 puede entonces determinar, en la etapa 1836, si el tiempo corriente es mayor que el tiempo de aviso de refrescamiento de la WK. Si el tiempo corriente es mayor que el tiempo de aviso de refrescamiento, el cliente 2 puede contactar con la WA utilizando los tipos de mensajes ¿ACTUALIZADO? (anteriormente descrito) y/o PETICIÓN-CLAVE (que se describe en relación con la Figura 20, más adelante), a fin de verificar cuán reciente es la clave de grupo de trabajo vigente en ese momento, solicitar una nueva clave de grupo de trabajo, o ambas cosas. Ha de apreciarse que el tipo de mensaje ¿ACTUALIZADO? puede ser una optimización para comprobar que una clave de grupo de trabajo es reciente. No obstante, el tipo de mensaje PETICIÓN-CLAVE puede ser utilizado sin un tipo de mensaje ¿ACTUALIZADO? precedente con el fin de reducir la latencia o tiempo de retraso. En otras realizaciones, la WA puede obligar a los clientes a comprobar cuán recientes son las claves en cada intento de conexión, al ajustar el TTL en 0.

Una vez actualizada su clave en la etapa 1838 (o si el tiempo corriente no era mayor que el tiempo de aviso de refrescamiento en la etapa 1836), el cliente 2 puede entonces determinar, en la etapa 1840, si el número de la versión de la WK del cliente 1 no es igual al número de la versión ahora actualizada del cliente 2. Si los dos números de versión no son el mismo, el cliente 2 puede informar de un error a la aplicación llamante en la etapa 1842. Si la ID de clave de grupo de trabajo es válida y los números de versión son idénticos, el cliente 2 puede informar de un intento de conexión con éxito a la aplicación llamante en la etapa 1844.

En la práctica, una o más de las etapas mostradas en el procedimiento 1800 pueden ser combinadas con otras etapas, llevarse a cabo en cualquier orden adecuado, realizarse en paralelo (por ejemplo, simultáneamente o de forma sustancialmente simultánea), o suprimirse.

La Figura 19 muestra un procedimiento ilustrativo 1900 para revocar los privilegios de comunicación de un cliente de un grupo de trabajo. Como se ha descrito previamente, los protocolos de comunicación de grupo de trabajo seguros convencionales pueden requerir el uso de CRLs y pueden no dar soporte a la capacidad de revocación y renovación inmediatas del mecanismo de seguridad del grupo de trabajo. La presente invención, sin embargo, puede dar soporte al descubrimiento inmediato de clientes desautorizados o revocados mediante la renovación periódica (o en cada intento de conexión) del mecanismo de seguridad. Por ejemplo, para revocar o desautorizar a un cliente del grupo de trabajo, la WA puede empezar por enviar una nueva WK a todos los usuarios que no han sido revocados. Utilizando la WK versionada, las conexiones que hacen uso de una WK caducada pueden ser rechazadas, dependiendo de la política o criterios de seguridad en vigor en el cliente receptor.

Puede recibirse, en la etapa 1902, una petición de revocación de cliente de grupo de trabajo. Por ejemplo, uno o más usuarios pueden ser retirados de un grupo de trabajo (o sus privilegios de comunicación revocados). Como se ha descrito previamente, la pertenencia en calidad de miembro a un grupo de trabajo puede ser mantenida por un servidor de LDAP (por ejemplo, el Active Directory de Microsoft®), en algunas realizaciones. Ciertos usuarios (por ejemplo, administradores de grupos de trabajo) pueden estar autorizados para retirar a usuarios (o grupos de usuarios), máquinas (por ejemplo, computadoras e impresoras), o servicios (por ejemplo, servicios de web y servicios de impresión / archivo) específicos, o cualquier combinación de los mismos, de un grupo de trabajo utilizando una interfaz de administración de grupo de trabajo. En la etapa 1904, el servidor que gestiona la pertenencia en calidad de miembro al grupo de trabajo, puede determinar si la petición de revocación es válida. Las peticiones de revocación válidas pueden ser autentificadas (por ejemplo, firmadas) por un usuario u otra entidad autorizada (por ejemplo, una WA o CA) e indicar a un usuario, máquina o servicio válido del grupo de trabajo que se ha de revocar. Si la petición de revocación no es válida, puede devolverse un error a la aplicación llamante en la etapa 1906, y la petición de revocación es ignorada.

Si la petición de revocación es válida en la etapa 1904, sin embargo, la ID de clave de grupo de trabajo revocada puede ser eliminada de la lista del cliente del grupo de trabajo en la etapa 1908. Por ejemplo, la WA puede eliminar la ID de clave de grupo de trabajo del cliente de una tabla de IDs de clave de grupo de trabajo contenida en una base de datos relacional almacenada en la WA o en la CA. En la etapa 1910, la WA puede determinar si ha de dispararse o activarse una actualización de clave. En algunas realizaciones, en la etapa 1910, se dispara automáticamente una actualización de clave en respuesta a cada petición de revocación válida. En otras realizaciones, las actualizaciones de clave pueden ser desencadenadas únicamente después de un número predeterminado de peticiones de revocación válidas (según se haya definido por los criterios de seguridad del grupo de trabajo), después de un número predeterminado de clientes destacados en ese momento revocados, periódicamente después de un intervalo predeterminado de tiempo desde la última actualización de clave, bajo

demanda por parte de la WA o de un usuario autorizado, de forma automática una vez que uno o más usuarios han abandonado el grupo de trabajo, o en cualquier combinación de los tiempos anteriores. La activación o disparo de una actualización de clave puede, implícitamente, denegar el acceso a todos los usuarios revocados o desautorizados, debido a que los usuarios revocados pueden no tener acceso a la nueva WK. La comunicación que se sirve de WKs caducadas puede ser controlada, limitada o completamente prohibida por medio de la personalización de los números de versión de la WK, de los valores de TTL computados por la WA, y de los tiempos de aviso de refrescamiento de la WK.

Si no se dispara una actualización de clave en la etapa 1910, el procedimiento ilustrativo 1900 puede retornar a la etapa 1902 para esperar a otra petición de revocación. Si se dispara una actualización de clave en la etapa 1910, la WA puede incrementar su número de versión de WK vigente en ese momento y generar una nueva WK en la etapa 1912. A fin de generar una nueva WK, en algunas realizaciones, la WA puede evaluar el nombre del grupo de trabajo y el número de actualización vigente en ese momento utilizando su Clave de Generación de Clave Maestra (MKGK –"Master Key Generation Key"), a través de una Función de Deducción de Clave segura (KDF –"Key Derivation Function"). Pueden utilizarse, en otras realizaciones, otras soluciones para generar una nueva WK. La WK que se acaba de generar puede ser, seguidamente, encriptada o cifrada por la WA, y puede generarse, en la etapa 1914, un mensaje de actualización de clave firmado. En algunas realizaciones, el mensaje de actualización de clave generado en la etapa 1914 puede incluir algunos de los campos siguientes, o todos ellos: (1) Campo de Identificador y Certificado de WA, que puede incluir información identificativa de la WA que autoriza la actualización, incluyendo su certificado firmado por la CA; (2) Campo de Identificador de Grupo de Trabajo, que puede incluir un identificador exclusivo que especifica el nombre del grupo de trabajo al que se aplica esta actualización; (3) Campo de Identificador de Secuencia, que puede incluir un contador secuencial que indica el número de la actualización; (4) Campo de Periodo de Tiempo de Actualización, que puede incluir una indicación del periodo de tiempo durante el cual será válido el material de clave; (5) Campo de Carga Útil de Actualización, que puede incluir un texto cifrado que contiene el material de clave actualizado; (6) Campo de Datos Auxiliares, que puede incluir información adicional requerida por el cliente (por ejemplo, una política o criterios de clave y la ubicación en que pueden encontrarse actualizaciones adicionales); (7) Indicador de Regeneración de Clave, que, cuando se establece, puede dar instrucciones al cliente para que regenere su clave secreta y contacte con la WA para su nueva certificación; y (8) Campo de Firma, que puede incluir una firma digital computada a lo largo de los campos previos utilizando la clave de firma de la WA.

En el caso de que se utilice un esquema de clave pública, el mensaje de actualización de clave puede ser cifrado para todos los usuarios no revocados mediante la marcación de cada hoja del árbol binario anteriormente descrito en relación con la Figura 17, en función de si el dispositivo que se encuentra en esa posición ha sido revocado. A continuación, todos los nodos que son progenitores de (o que coexisten con) las hojas asociadas con los dispositivos no revocados, pueden ser identificados (pero *no* los revocados). Por ejemplo, la raíz del árbol completo es progenitora de la totalidad de las hojas; por lo tanto, este nodo es suficiente cuando no hay dispositivos revocados. A continuación, el mensaje puede ser cifrado bajo cada una de las claves asociadas con esos nodos. El resultado puede incluir una lista que identifica estos nodos, así como una lista de los textos cifrados producidos. Cuando se utiliza este esquema de encriptación o cifrado, cada usuario no revocado puede poseer al menos uno de los pares de claves que se han utilizado para cifrar el mensaje. Este puede identificar su par de claves, descifrar el texto cifrado apropiado, y suministrar como salida el mensaje.

Una vez que se ha generado el mensaje de actualización de clave, este puede hacerse público para todos los usuarios no revocados, por medio de un canal de confianza media (por ejemplo, un sitio web), en la etapa 1916. Puede también darse soporte a un funcionamiento desvinculado (o semivinculado). Cuando un cliente o dispositivo se prepara para desconectarse de la línea, la WA puede proveer de forma preliminar al cliente o al dispositivo de actualizaciones de clave para un número limitado de periodos de tiempo futuros. De manera adicional o alternativa, para los dispositivos con algún acceso a red, pueden expedirse mensajes de revocación de clave y de actualización de clave a una ubicación altamente disponible, por ejemplo, a un sitio web público asegurado según TLS.

En la práctica, una o más de las etapas mostradas en el procedimiento 1900 pueden ser combinadas con otras etapas, llevarse a cabo en cualquier orden adecuado, realizarse en paralelo (por ejemplo, simultáneamente o de forma sustancialmente simultánea), o suprimirse.

La Figura 20 muestra un procedimiento ilustrativo 2000 para solicitar una actualización de WK. En la etapa 2002, un cliente puede enviar a la WA un mensaje de petición de clave cifrado con la clave secreta del cliente (o clave privada, si se utiliza un esquema de cifrado asimétrico). Por ejemplo, en la etapa 2002, el cliente puede enviar un mensaje a la WA en el siguiente formato: {Cliente X ‖ E_X {PETICIÓN-CLAVE ‖ N_2 ‖ ID de clave de grupo de trabajo ‖ versión de clave solicitada} }, donde X es la identidad del cliente solicitante, E_X es la clave secreta del cliente X (o clave privada, en el caso de que se utilice un esquema de cifrado asimétrico), PETICIÓN-CLAVE representa el tipo de mensaje de petición de clave, y N_2 es un término ocasional generado por el cliente solicitante. En la etapa 2004, la WA puede recibir el menaje cifrado y consultar al cliente con el fin de obtener la clave de cifrado secreta E_X del cliente. En la etapa 2004, la WA puede también descifrar el mensaje de petición de clave y, en la etapa 2006, verificar que la ID de clave de grupo de trabajo es válida para este cliente. Si la ID de clave de grupo de trabajo no

es válida para este cliente, entonces, en la etapa 2008, la WA puede enviar de vuelta un mensaje de no autorización, y el procedimiento ilustrativo 2000 puede retornar a la etapa 2002. Si la ID de clave de grupo de trabajo es válida para este cliente, sin embargo, la WA puede acceder a la versión más reciente (es decir, la más actual) de la clave (esta puede ser más reciente que la versión solicitada). La WA puede entonces crear una repuesta al mensaje de petición de clave en la etapa 2012, y encriptar o cifrar la respuesta utilizando la clave secreta E_X del cliente. En algunas realizaciones, la respuesta de la WA al mensaje de petición de clave puede adoptar el siguiente formato: E_X {PETICIÓN-CLAVE ‖ N_2 ‖ ID de clave de grupo de trabajo ‖ versión de clave vigente en ese momento ‖ TTL ‖ clave}. Una vez recibida la respuesta desde la WA, el cliente puede actualizar su WK en la etapa 2014. Por último, en la etapa 2016, el cliente puede actualizar su tiempo de aviso de refrescamiento de WK en el tiempo u hora corriente más el valor de TTL recibido.

En la práctica, una o más de las etapas mostradas en el procedimiento 2000 pueden ser combinadas con otras etapas, llevarse a cabo en cualquier orden adecuado, realizarse en paralelo (por ejemplo, simultáneamente o de forma sustancialmente simultánea), o suprimirse.

Se han desarrollado diversos sistemas y protocolos de distribución de clave (por ejemplo, el protocolo de Kerberos) que dan soporte a la distribución de claves de una manera razonablemente eficiente. Sin embargo, estos sistemas y protocolos anteriores no logran satisfacer los requisitos de la distribución y gestión de claves de grupo de trabajo seguras para uso a la hora de asegurar datos en movimiento en combinación con el analizador sintáctico de datos seguro de la presente invención. Algunos de estos requisitos pueden incluir, por ejemplo: (1) Identificación No Disponible para Conexión –El sistema ha de dar soporte a la comunicación entre dos clientes cuando uno o ambos no disponen de la identidad completa del otro. Una consecuencia inmediata de este requisito puede ser excluir las claves de sesión entre pares; (2) Revocación –El sistema ha de ser capaz de revocar o desautorizar los privilegios de comunicación de cualquier cliente. El tiempo requerido para que se complete la revocación ha de ser configurable por el usuario. En algunas realizaciones, la revocación puede afectar únicamente a las nuevas conexiones, pero no a las ya existentes; (3) Chateador (o Conversador) de Red Parametrizado –Este sistema ha de dar soporte a una autoridad centralizada que puede validar y distribuir claves. Sin embargo, la comunicación con este servidor puede hacer posible que una clave distribuida sea utilizable o válida únicamente para un cierto periodo de tiempo configurable por el usuario o predeterminado; (4) Estado de Participante Mínimo –Los clientes pueden tan solo necesitar almacenar una pequeña cantidad de información para comunicarse. En particular, el estado almacenado por un cliente no debe incluir información entre pares. Todos los requisitos anteriores pueden ser satisfechos utilizando los sistemas y métodos que se han descrito en esta memoria.

En algunas realizaciones, pueden utilizarse las siguientes funciones de cliente para dar soporte a los procedimientos y sistemas de la presente invención en un cliente de grupo de trabajo. Las funciones que se describen en lo que sigue pueden ser implementas utilizando software, *firmware*, o software instalado de forma permanente en hardware, hardware (por ejemplo, sistemas incorporados), o cualquier combinación de los anteriores. Pueden indicarse los argumentos de la función proporcionados más adelante, a excepción de argumentos “ayudadores”, tales como el campo de longitud para un registro de almacenamiento intermedio. Asimismo, se mencionan tan solo algunos códigos de errores notables. En otras realizaciones, pueden utilizarse códigos de error, argumentos, o ambos, adicionales.

1. Función wa_inic – Esta función puede dar como resultado un tipo CódigoError, admitir Idcliente como entrada, y suministrar como salida un tipo ctx. Esta función puede ser utilizada para inicializar el servicio de distribución de clave en el lado del cliente. El ctx variable puede ser inicializado y mantener el estado en todas las claves que se están utilizando en ese momento, sus versiones y otra información específica de la clave. Esta función puede también establecer o ajustar un hilo de sucesos para el manejo de las comunicaciones asincrónicas. La Idcliente ha de ser el mismo identificador proporcionado a la WA.

2. Función wa_IdnuevaClave – Esta función puede dar como resultado un tipo CódigoError, admitir como entrada tipos ctx, IdClavewg, Direcciónwa y Claveprivada, y no tiene ninguna salida. Esta función puede ser utilizada para añadir una ID de clave de grupo de trabajo al contexto ctx para su gestión. Direcciónwa puede ser la dirección de red para la WA que es responsable de esta ID particular. Claveprivada puede ser utilizada para encriptar o cifrar la comunicación con la WA y debe ser la misma clave que la proporcionada a la WA.

3. Función wa_interrupción – Esta función puede dar como resultado un tipo CódigoError, admitir como entrada un tipo ctx, y no tiene ninguna salida. Esta función puede ser utilizada para interrumpir todos los estados gestionados por el servicio y deslocalizar la memoria para el contexto ctx. Esta función puede también cancelar cualesquiera peticiones pendientes (por ejemplo, tiques).

4. Función wa_Actualizarclave_asinc – Esta función puede dar como resultado un tipo CódigoError, admitir como entrada tipos ctx, IdClavewg y de llamada de contestación, y suministrar como salida un tipo Tique t. Esta función puede ser utilizada para comprobar que la clave de grupo de trabajo identificada por IdClavewg está actualizada. Puede no haber ninguna necesidad de especificar el número de versión en algunas realizaciones, debido a que el número de versión puede ser manejado internamente por el contexto de la gestión. Esta llamada puede ser

asincrónica y puede volver de inmediato. Cuando el bucle de sucesos recibe la respuesta del servidor, el bucle de sucesos puede apelar a la función de llamada de contestación. Puede entonces hacer llegar a esta función de llamada de contestación un código de error así como un código de estatus, si bien el código de estatus puede ser significativo en caso de que no haya ningún error. Si el cliente ya no está autorizado para comunicarse con este grupo de trabajo, la llamada de contestación puede recibir ERROR_AUTORIZACIÓN_GRUPODETRABAJO. Si no hay ningún error y la clave sigue siendo válida, puede recibir ESTATUS_CLAVE_CONFORME. En caso contrario, puede recibir ESTATUS_CLAVE_CADUCADA. Cuando esta función finaliza, el tique t puede servir como un identificador para el oyente de solicitud que está a la espera.

5. Función wa_Pedirclave_asinc – Esta función puede dar como resultado un tipo CódigoError, admitir como entrada tipos ctx, IdClavewg y de llamada de contestación, y dar como resultado un tipo Tique t. Esta función puede ser utilizada para refrescar el material de clave y dar una versión para este identificador de clave. Una apelación a esta función puede ser asincrónica y puede retornar de inmediato. Cuando el bucle de sucesos recibe la respuesta, el bucle de sucesos puede apelar a la función de llamada de contestación. Este puede hacer llegar a esta función de llamada de contestación un código de error que indica si la actualización de la clave ha sido satisfactoria o no. Si el cliente ya no está autorizado para comunicarse con este grupo de trabajo, la llamada de respuesta puede recibir ERROR_AUTORIZACIÓN_GRUPODETRABAJO. Cuando esta función termina, el tique t puede servir como un identificador para el oyente de solicitud que está a la espera.

6. Función wa_Validarclave_asinc – Esta función puede dar como resultado un tipo CódigoError, admitir como entradas ctx, IdClavewg, VersiónIDClavewg y llamada de contestación, y suministrar como salida un tipo Tique t. Esta función puede ser utilizada para validar una clave recibida desde otra parte. Esta función puede actualizar su propia clave (como para la wa_Pedirclave_asinc) como parte de su funcionamiento. Esta función puede también ser asincrónica y puede retornar de inmediato. Cuando el bucle de sucesos recibe la respuesta, el bucle de sucesos puede apelar a la función de llamada de contestación. Este puede hacer llegar a esta función de llamada de contestación un código de error que indica si la comprobación de clave ha tenido éxito, así como un código de estatus que indica la validez de la clave. Los tres códigos de estatus posibles pueden incluir, por ejemplo, ESTATUS_CLAVE_CONFORME, ESTATUS_CLAVE_CADUCADA y ESTATUS_CLAVE_NOVÁLIDA. Si la clave del grupo de trabajo no es la que se está gestionando en ese momento por el contexto ctx, esta función puede dar como resultado ERROR_CLAVE_DESCONOCIDA. Este código de error puede también hacerse llegar a la función de llamada de contestación como una optimización.

7. Función wa_Versiónactual – Esta función puede dar como resultado un tipo de CódigoError, admitir ctx e IdClavewg como entradas, y suministrar como salida una versión. Esta función puede ser utilizada para dar como resultado la versión vigente en ese momento, según es gestionada por el contexto ctx para la ID de clave de grupo de trabajo dada.

8. Función wa_siguienteRefrescamiento – Esta función puede dar como resultado un tipo CódigoError, admitir ctx e IdClavewg como entradas, y suministrar como salida tiempoRestante. Esta función puede ser utilizada para dar como resultado el número de segundos que restan antes de que la clave deba ser refrescada o renovada. Esta función puede dar como resultado 0 si ya ha expirado el siguiente tiempo de refrescamiento.

9. Función wa-estatus – Esta función puede dar como resultado un tipo, admitir tique t como entrada, y suministrar como salida el estatus del tipo. Esta función puede ser utilizada para proporcionar, por ejemplo, STATUS_COMPLETO o STATUS_ESPERANDO para el tique dado al estatus. Si el tique es desconocido, la función puede dar como resultado ERROR_TIQUE_DESCONOCIDO.

10. Función wa_tiempoEspera – Esta función puede dar como resultado un tipo CódigoError, admitir como entrada Tique t, y suministrar como salida segundos. Esta función puede ser utilizada para proporcionar el número de segundos que la petición ha estado pendiente, en segundos.

11. Función wa_cancelar – Esta función puede dar como resultado un tipo de CódigoError, admitir Tique t como entrada, y no tiene ninguna salida. Esta función puede ser utilizada para cancelar un petición pendiente.

Las funciones anteriores son meramente ilustrativas. Pueden definirse muchas otras funciones en un cliente de grupo de trabajo, para uso en la distribución y la gestión de claves de grupo de trabajo de acuerdo con la presente invención. Además, si bien se han descrito anteriormente algunas aplicaciones del analizador sintáctico de datos seguro y del módulo de gestión de grupos de trabajo, debe entenderse claramente que la presente invención puede ser integrada con cualquier aplicación de red con el fin de incrementar la seguridad, la tolerancia ante fallos, el anonimato o cualquier combinación apropiada de los anteriores.

Además, resultarán evidentes para el profesional experto otras combinaciones, adiciones, sustituciones y modificaciones a la vista de la divulgación proporcionada en la presente memoria. Por ejemplo, aunque muchos de los procedimientos ilustrados en las figuras se refieren a la criptografía de clave secreta y/o de clave simétrica de un cliente, un profesional experto constatará que un par de claves pública / privada puede, alternativamente, ser utilizado en un esquema criptográfico asimétrico correspondiente.

REIVINDICACIONES

1.- Un método para la comunicación segura comunicación en un grupo de trabajo, de tal modo que el método comprende:

recibir, en un primer cliente (1604) de grupo de trabajo, un mensaje encriptado o cifrado procedente de un servidor de claves de grupo de trabajo, de tal manera que el mensaje cifrado comprende una clave de grupo de trabajo, un número de versión de la clave de grupo de trabajo, y un valor de tiempo de vida, TTL, para la clave de grupo de trabajo; e
iniciar una sesión de comunicación con un segundo cliente (1606) de grupo de trabajo, de tal modo que iniciar la sesión de comunicación comprende:

determinar, en el primer cliente de grupo de trabajo, si la clave de grupo de trabajo ha expirado basándose, al menos en parte, en el valor de TTL para la clave de grupo de trabajo;
comprobar, en respuesta a la determinación de que la clave de grupo de trabajo ha expirado, la disponibilidad de una nueva clave de grupo de trabajo procedente del servidor de claves;
enviar al segundo cliente de grupo de trabajo, en respuesta a la determinación de que la clave de grupo de trabajo no ha expirado, una pluralidad de encabezamientos de compartimiento, de tal manera que los encabezamientos de compartimiento incluyen la clave de grupo de trabajo y el número de versión de la clave de grupo de trabajo; y
verificar, en el segundo cliente de grupo de trabajo, que la versión de la clave de grupo de trabajo del segundo cliente de grupo de trabajo coincide con la versión de la clave de grupo de trabajo del primer cliente de grupo de trabajo.

2.- El método de acuerdo con la reivindicación 1, que comprende adicionalmente generar la pluralidad de encabezamientos de compartimiento antes de enviar la pluralidad de encabezamientos de compartimiento, de tal manera que generar la pluralidad de encabezamientos de compartimiento comprende distribuir la clave de grupo de trabajo dentro de la pluralidad de encabezamientos de compartimiento utilizando un esquema de compartimiento secreto.

3.- El método de acuerdo con la reivindicación 1, en el cual el mensaje cifrado es cifrado utilizando un lenguaje cifrado simétrico que emplea la clave secreta del primer cliente de grupo de trabajo.

4.- El método de acuerdo con la reivindicación 1, en el cual el mensaje cifrado es cifrado utilizando un lenguaje cifrado asimétrico que emplea la clave pública del primer cliente de grupo de trabajo.

5.- El método de acuerdo con la reivindicación 1, en el cual los encabezamientos de compartimiento incluyen, adicionalmente, un identificador de grupo de trabajo, de tal manera que el método comprende, adicionalmente, verificar, en el segundo cliente de grupo de trabajo, que el identificador de grupo de trabajo es válido para un grupo de trabajo al que pertenece el segundo cliente de grupo de trabajo.

6.- El método de acuerdo con la reivindicación 1, que comprende adicionalmente:

recibir, en el primer cliente de grupo de trabajo, un mensaje de actualización de clave de grupo de trabajo, de tal manera que el mensaje de actualización de clave de grupo de trabajo incluye una nueva clave de grupo de trabajo, un nuevo número de versión de la clave de grupo de trabajo, y un nuevo valor de TTL para la nueva clave de grupo de trabajo; y
actualizar, en el primer cliente de grupo de trabajo, un aviso de refrescamiento o renovación de clave de grupo de trabajo, basándose, al menos en parte, en el nuevo valor de TTL.

7.- El método de acuerdo con la reivindicación 6, en el cual actualizar el aviso de refrescamiento de clave de grupo de trabajo comprende ajustar el aviso de refrescamiento de clave de grupo de trabajo en el tiempo u hora corriente más el nuevo valor de TTL.

8.- Un sistema para la comunicación segura en un grupo de trabajo, de tal modo que el sistema comprende:

un primer cliente (1604) de grupo de trabajo, configurado para:

recibir un mensaje encriptado o cifrado procedente de un servidor de claves de grupo de trabajo, de tal manera que el mensaje cifrado comprende una clave de grupo de trabajo, un número de versión de la clave de grupo de trabajo, y un valor de tiempo de vida, TTL, para la clave de grupo de trabajo; e
iniciar una sesión de comunicación con un segundo cliente (1606) de grupo de trabajo, de tal manera que el primer cliente de grupo de trabajo está configurado para:

determinar si la clave de grupo de trabajo ha expirado basándose, al menos en parte, en el valor de

TTL para la clave de grupo de trabajo;
comprobar, en respuesta a la determinación de que la clave de grupo de trabajo ha expirado, la disponibilidad de una nueva clave de grupo de trabajo procedente del servidor de claves;
enviar al segundo cliente de grupo de trabajo, en respuesta a la determinación de que la clave de grupo de trabajo no ha expirado, una pluralidad de encabezamientos de compartimiento, de tal manera que los encabezamientos de compartimiento incluyen la clave de grupo de trabajo y el número de versión de la clave de grupo de trabajo; y

un segundo cliente de grupo de trabajo, configurado para verificar que la versión de la clave de grupo de trabajo del segundo cliente de grupo de trabajo coincide con la versión de la clave de grupo de trabajo del primer cliente de grupo de trabajo.

9.- El sistema de acuerdo con la reivindicación 8, en el cual el primer cliente de grupo de trabajo está configurado para generar la pluralidad de encabezamientos de compartimiento al distribuir la clave de grupo de trabajo dentro de la pluralidad de encabezamientos de compartimiento utilizando un esquema de compartimiento secreto.

10.- El sistema de acuerdo con la reivindicación 8, en el cual el mensaje cifrado es cifrado utilizando un lenguaje cifrado simétrico que emplea la clave secreta del primer cliente de grupo de trabajo.

11.- El sistema de acuerdo con la reivindicación 8, en el cual el mensaje cifrado es cifrado utilizando un lenguaje cifrado asimétrico que emplea la clave pública del primer cliente de grupo de trabajo.

12.- El sistema de acuerdo con la reivindicación 8, en el cual los encabezamientos de compartimiento incluyen, adicionalmente, un identificador de grupo de trabajo, habiéndose configurado el segundo cliente de grupo de trabajo, adicionalmente, para verificar que el identificador de grupo de trabajo es válido para un grupo de trabajo al que pertenece el segundo cliente de grupo de trabajo.

13.- El sistema de acuerdo con la reivindicación 8, en el que el primer cliente de grupo de trabajo se ha configurado para:

recibir un mensaje de actualización de clave de grupo de trabajo, de tal manera que el mensaje de actualización de clave de grupo de trabajo incluye una nueva clave de grupo de trabajo, un nuevo número de versión de la clave de grupo de trabajo, y un nuevo valor de TTL para la nueva clave de grupo de trabajo; y
actualizar un aviso de refrescamiento o renovación de clave de grupo de trabajo, basándose, al menos en parte, en el nuevo valor de TTL.

14.- El sistema de acuerdo con la reivindicación 13, en el cual el primer cliente de grupo de trabajo se ha configurado para actualizar el aviso de refrescamiento de clave de grupo de trabajo ajustando el aviso de refrescamiento de clave de grupo de trabajo en el tiempo u hora corriente más el nuevo valor de TTL.

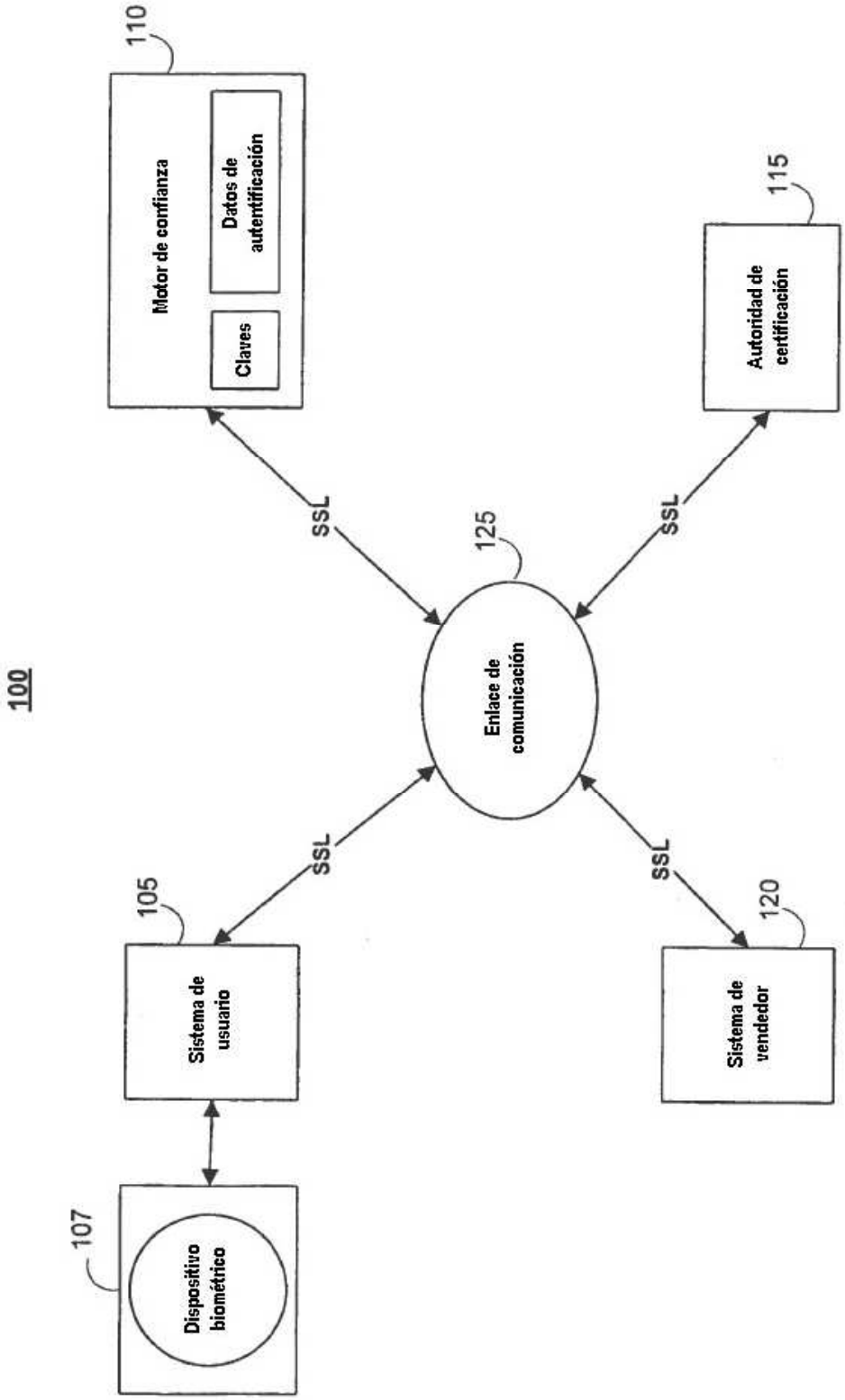
100
110
Motor de confianza
Datos de autentificación
Claves
115
Autoridad de certificación
125
Enlace de comunicación
SSL
SSL
SSL
SSL
105
Sistema de usuario
120
Sistema de vendedor
107
Dispositivo biométrico

FIG. 1

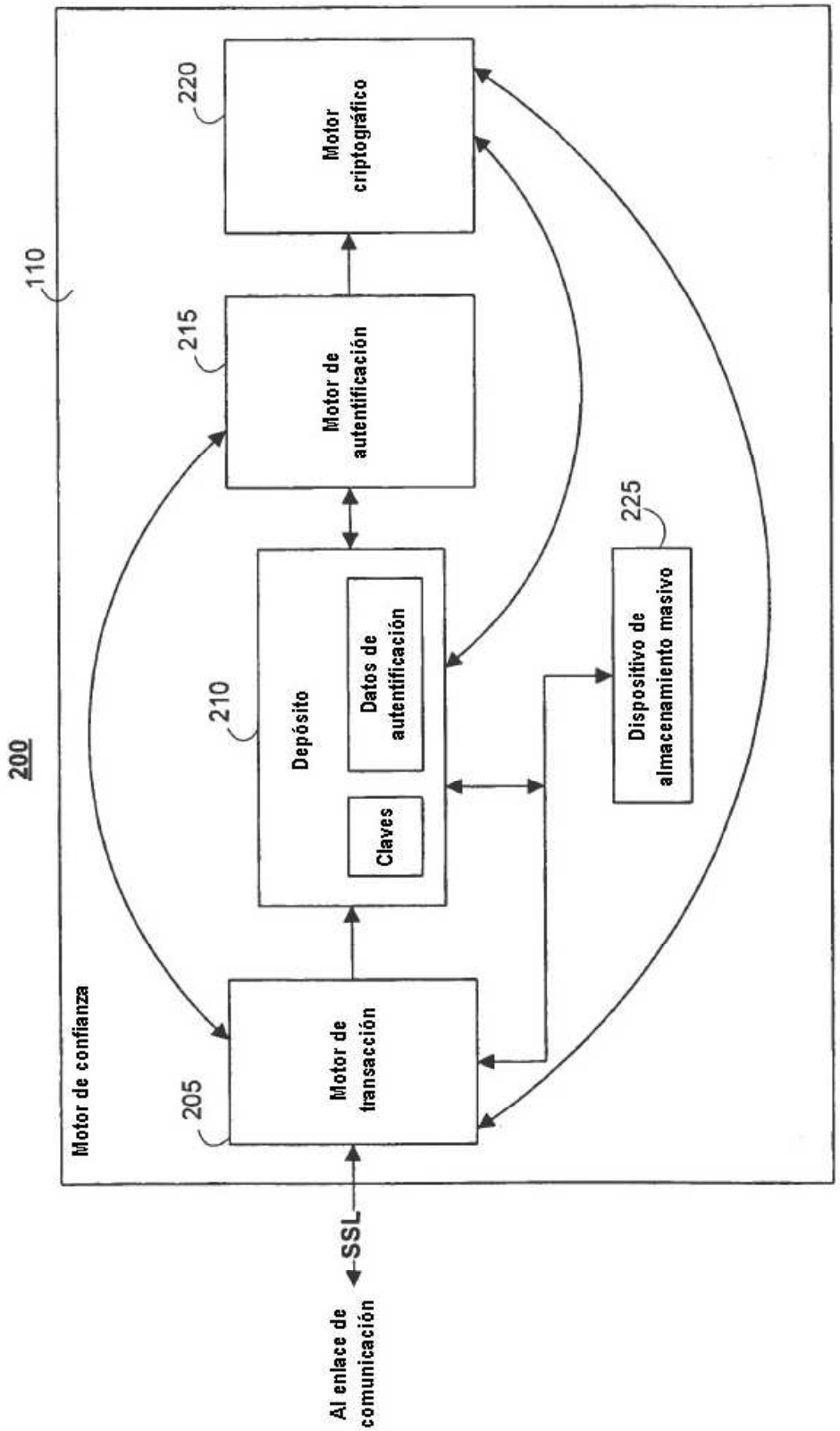
200
110
Motor de confianza
205
Motor de transacción
210
Depósito
Claves
Datos de autentificación
215
Motor de autentificación
220
Motor criptográfico
225
Dispositivo de almacenamiento masivo
SSL
Al enlace de comunicación

FIG. 2

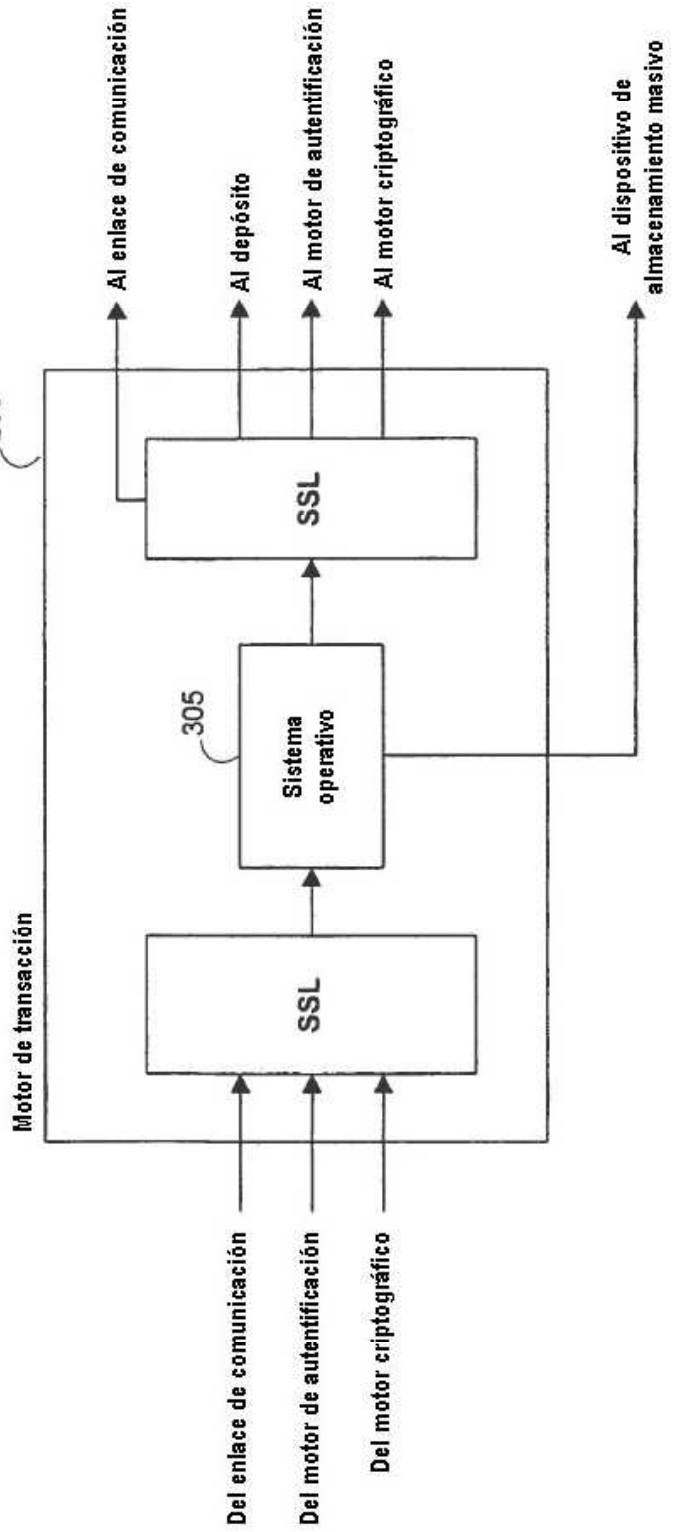
Al enlace de comunicación
Al depósito
Al motor de autentificación
Al motor criptográfico
Al dispositivo de almacenamiento masivo
205
SSL
305
Sistema operativo
SSL
Motor de transacción
Del enlace de comunicación
Del motor de autentificación
Del motor criptográfico

FIG. 3

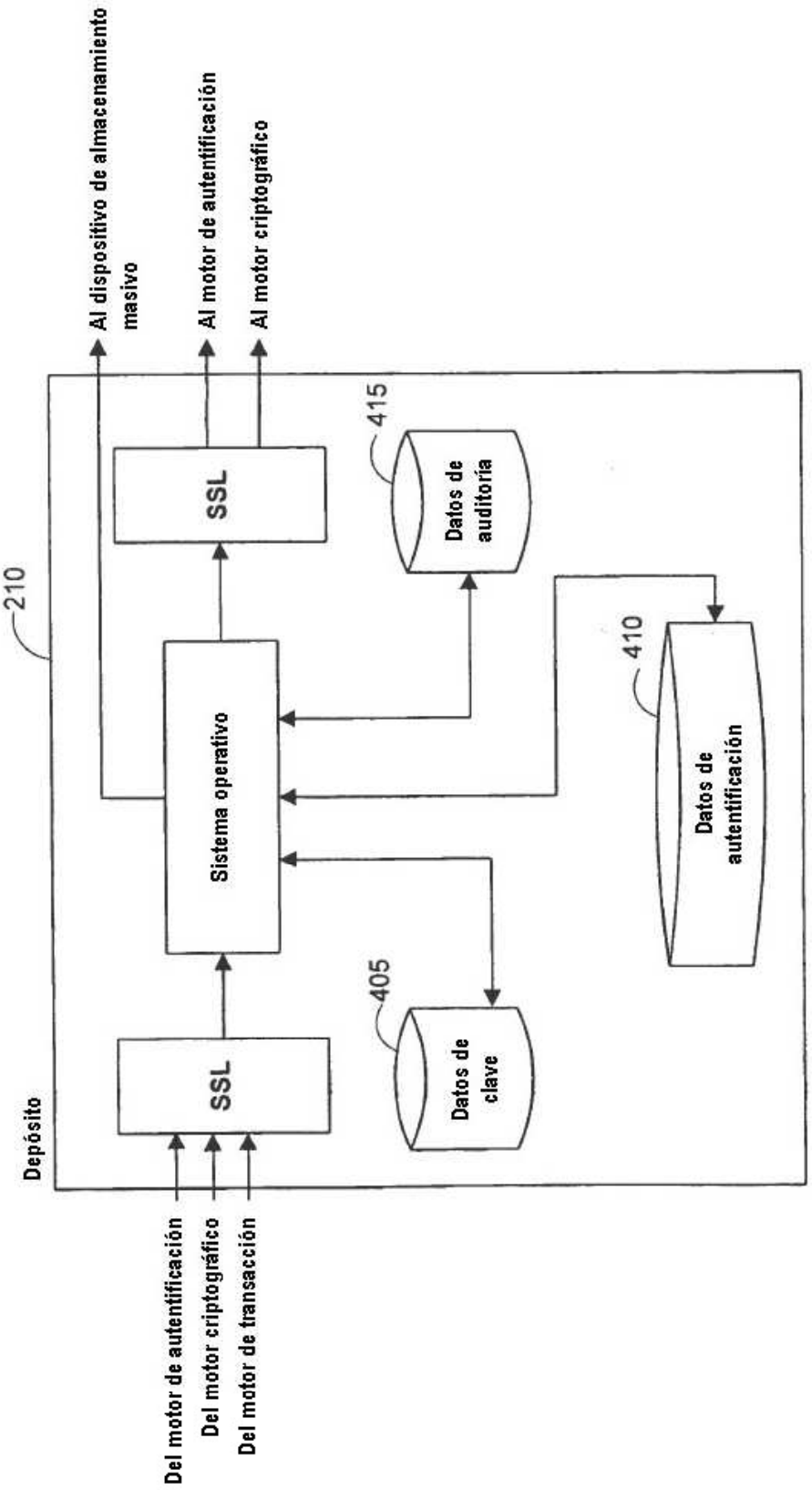
Al dispositivo de almacenamiento masivo
Al motor de autentificación
Al motor criptográfico
210
SSL
415
Datos de auditoría
Sistema operativo
410
Datos de autentificación
405
Datos de clave
SSL
Depósito
Del motor de autentificación
Del motor criptográfico
Del motor de transacción

FIG. 4

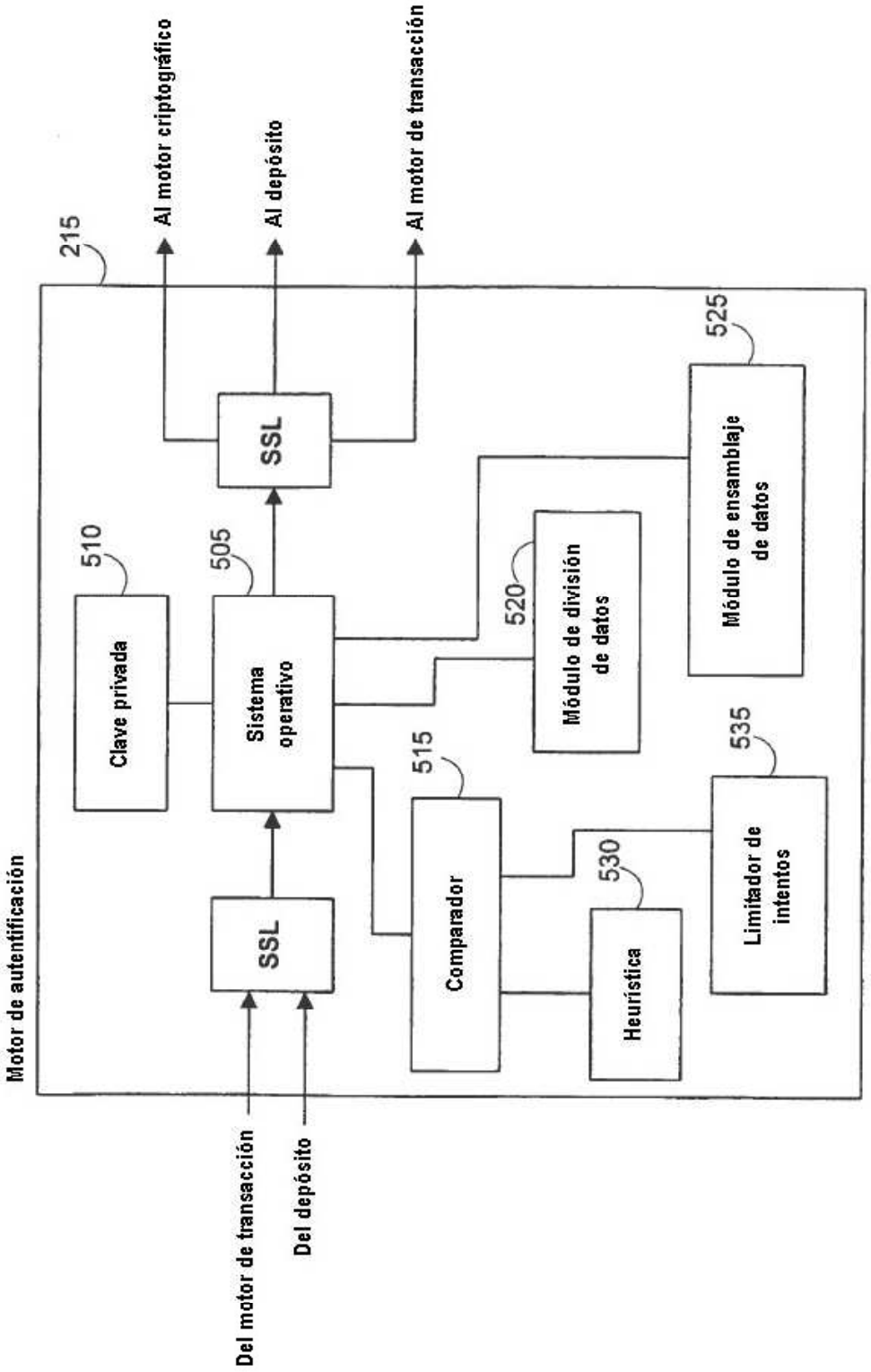
Motor de autentificación
215
Al motor criptográfico
Al depósito
Al motor de transacción
SSL
SSL
Clave privada
510
Sistema operativo
505
Módulo de división de datos
520
Módulo de ensamblaje de datos
525
Comparador
515
Heurística
530
Limitador de intentos
535
Del motor de transacción
Del depósito

FIG. 5

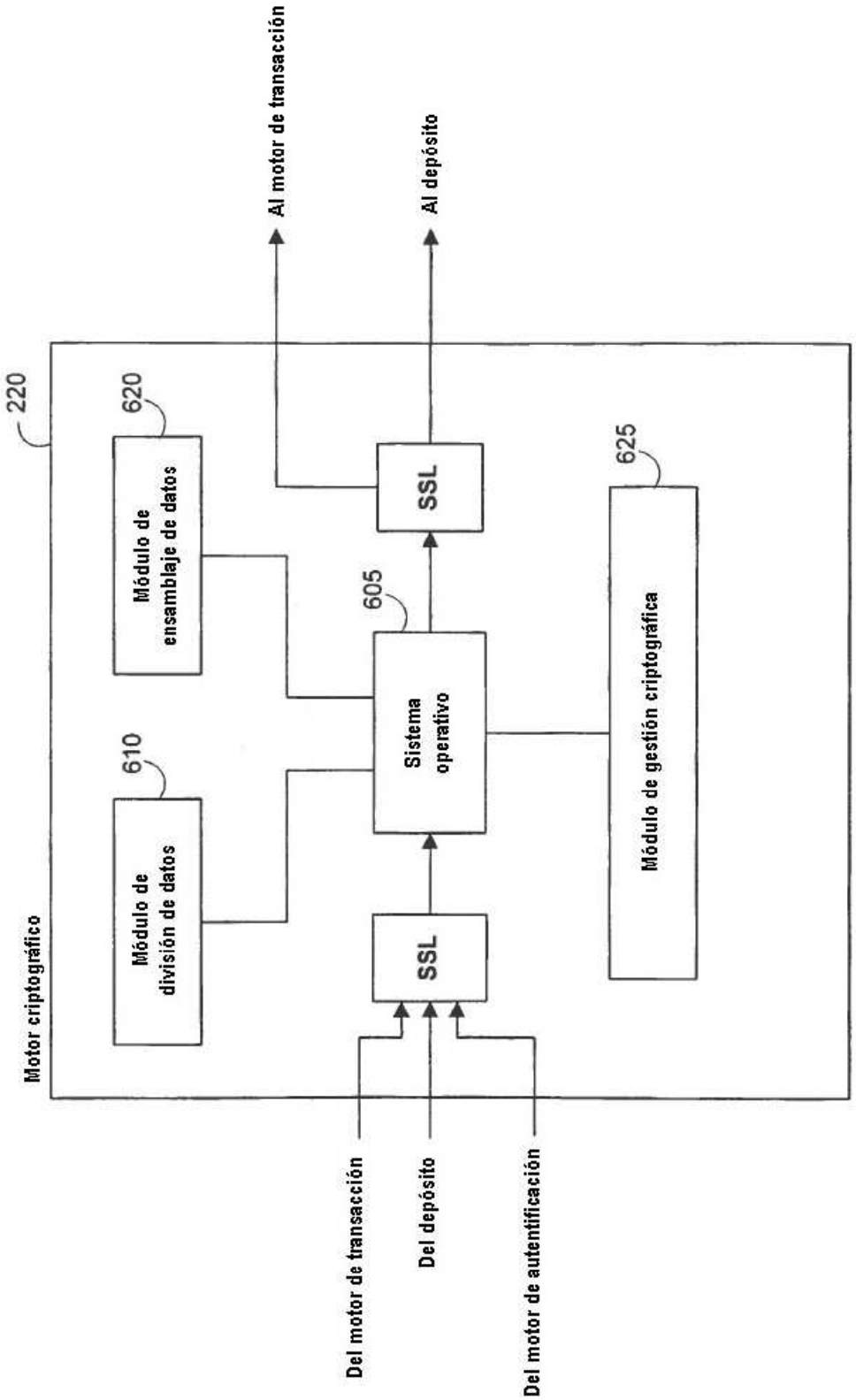
Al motor de transacción
Al depósito
220
620
Módulo de ensamblaje de datos
SSL
625
605
Sistema operativo
Módulo de gestión criptográfica
610
Módulo de división de datos
SSL
Motor criptográfico
Del motor de transacción
Del depósito
Del motor de autentificación

FIG. 6

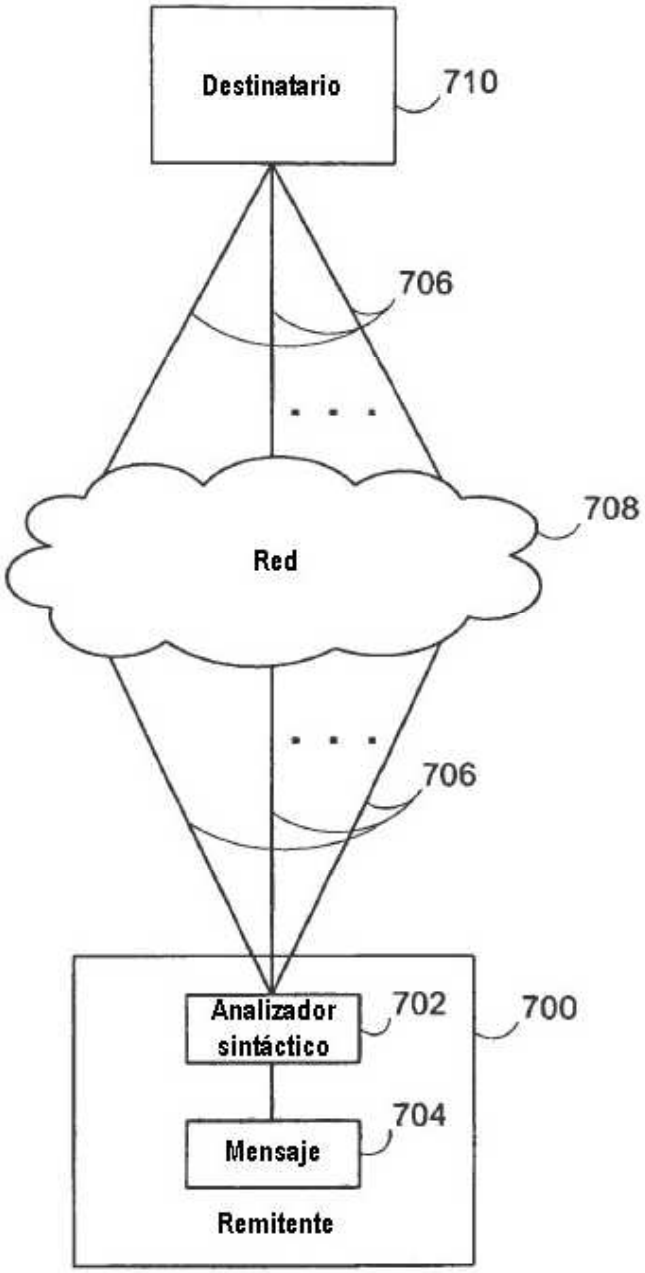
Destinatario
710
706
708
Red
706
Analizador sintáctico
702
700
704
Mensaje
Remitente

FIG. 7

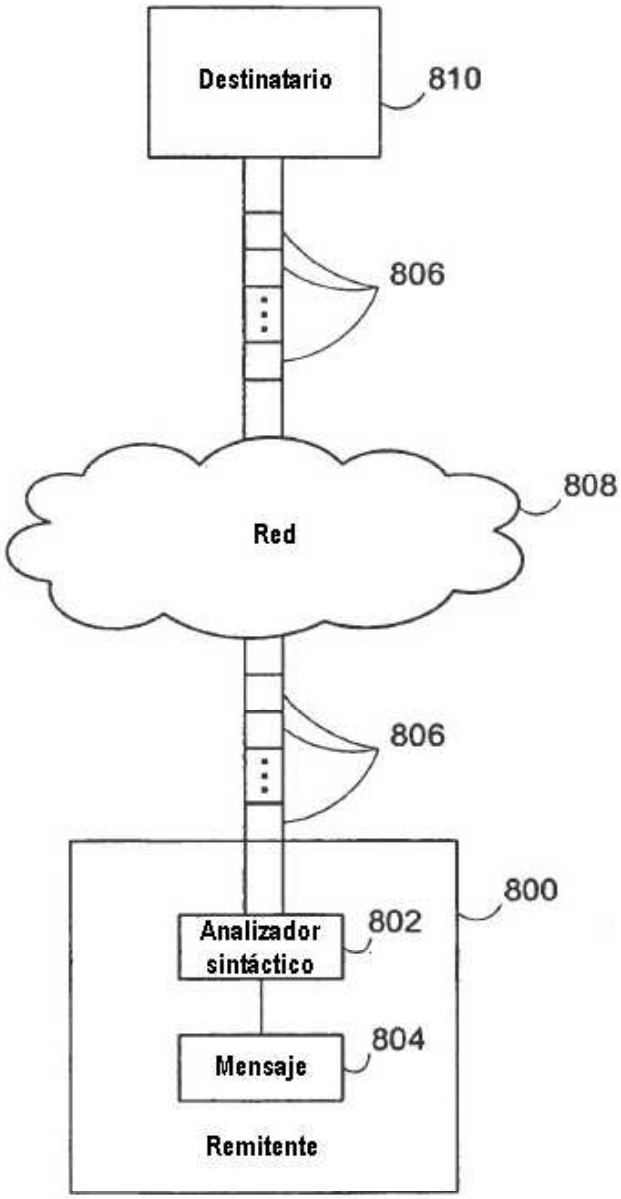
Destinatario
810
806
808
Red
806
800
Analizador sintáctico
802
Mensaje
804
Remitente

FIG. 8

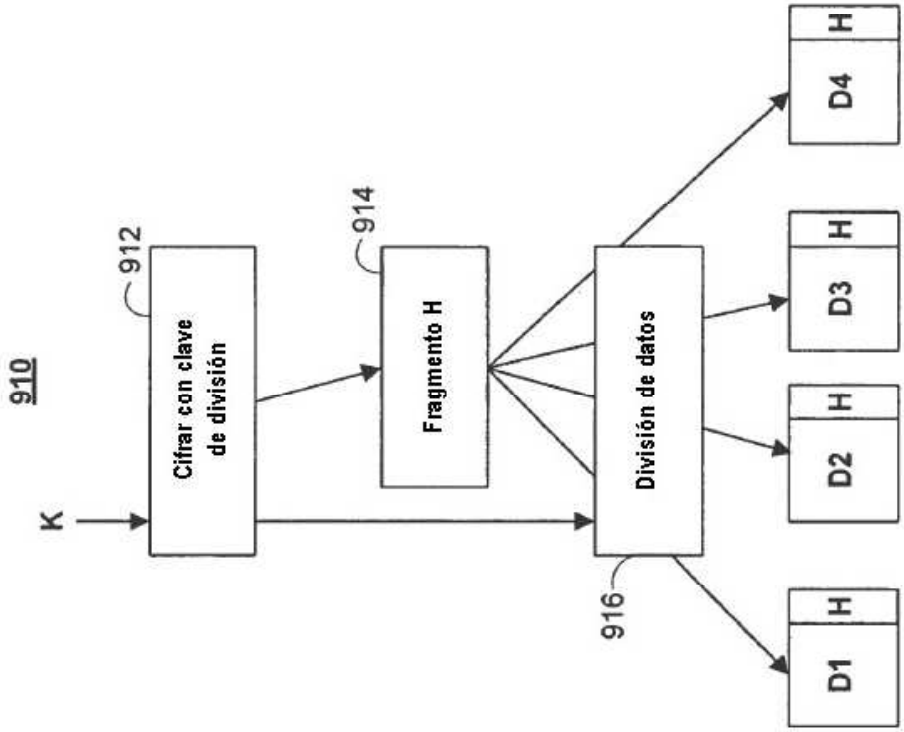
910
K
912
Cifrar con clave de división
914
Fragmento H
División de datos
916
D1
H
D2
H
D3
H
D4
H

FIG. 9B

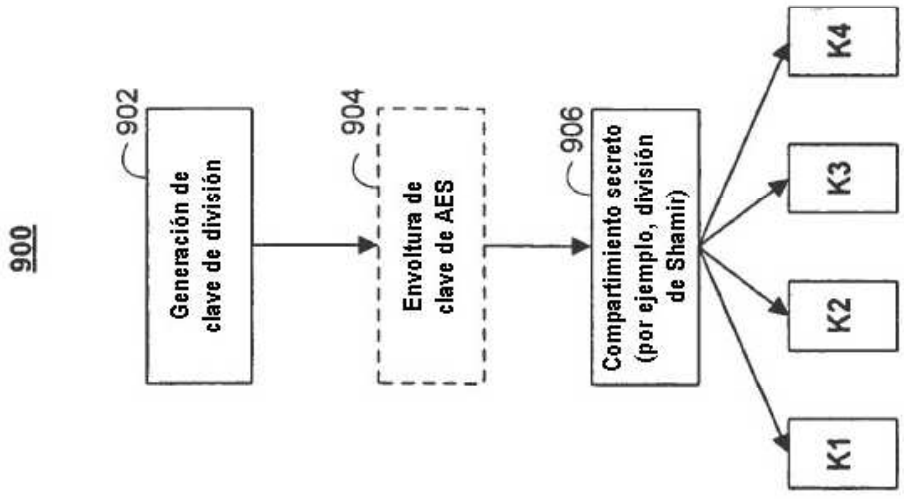
900
902
Generación de clave de división
904
Envoltura de clave de AES
906
Compartimiento secreto (por ejemplo, división de Shamir)
K1
K2
K3
K4

FIG. 9A

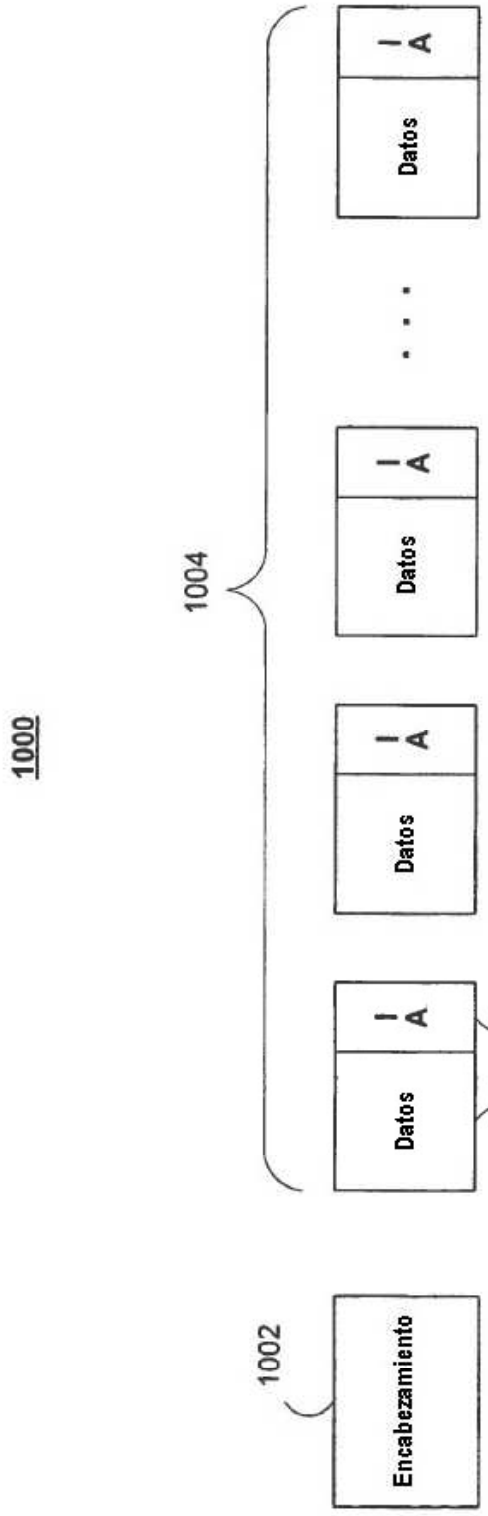

FIG. 10

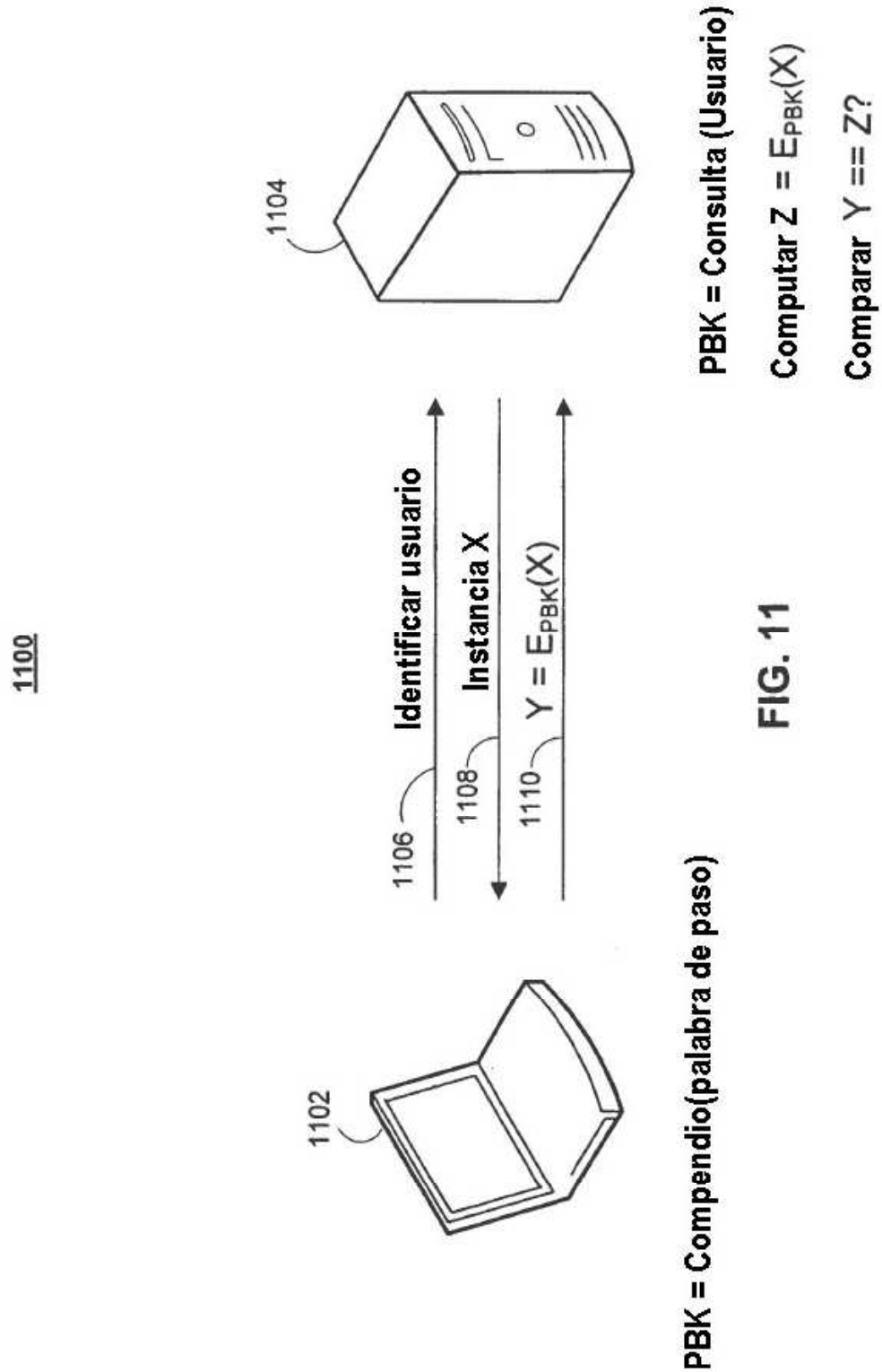
1100
1102
1104
1106
1108
1110
Identificar usuario
Instancia X
Y = EPBK(X)
PBK = Compendio(palabra de paso)
PBK = Consulta (Usuario)
Computar Z = EPBK(X)
Comparar Y == Z?

FIG. 11

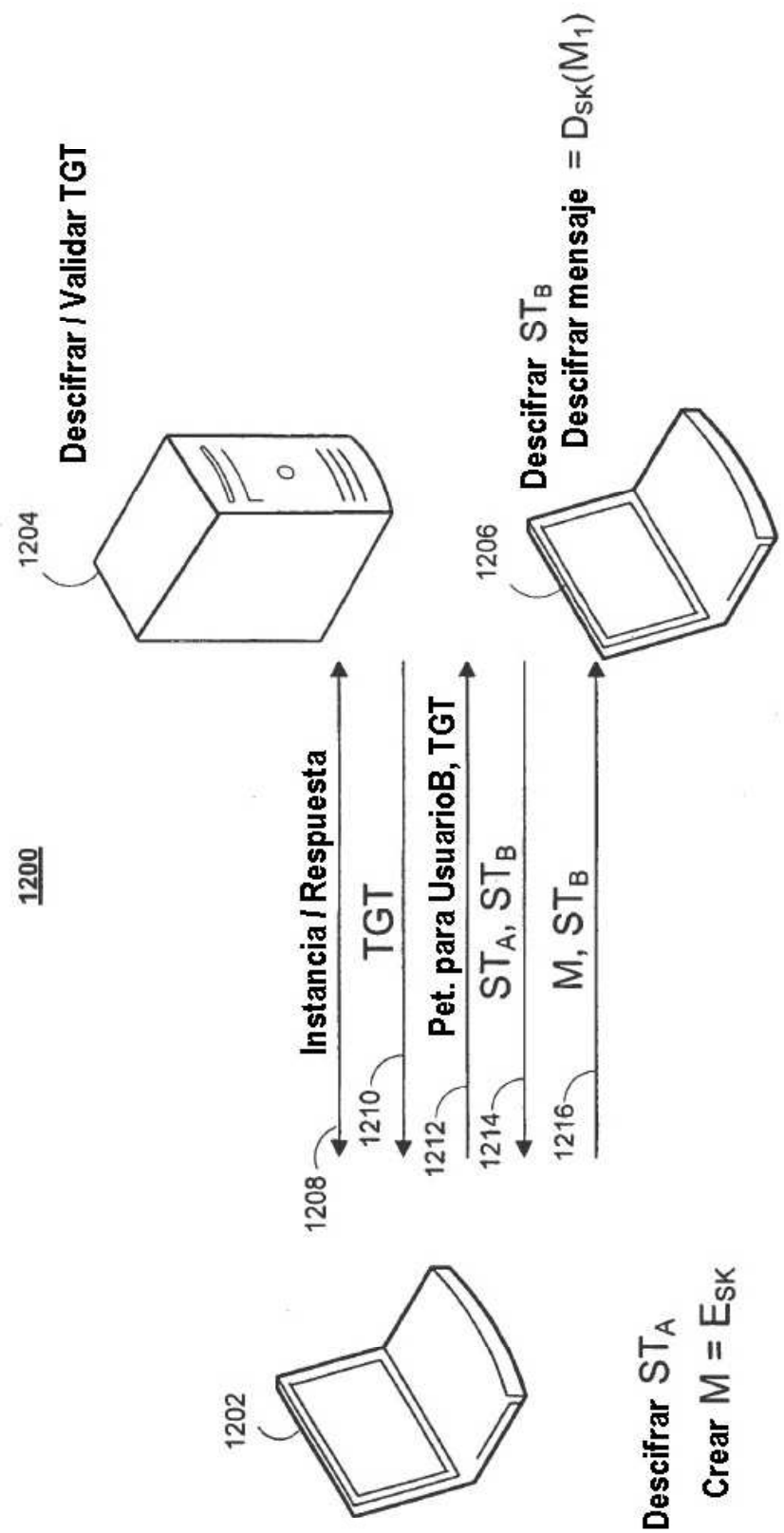
1200
1202
1204
1206
Descifrar / Validar TGT
Descifrar ST_B
Descifrar mensaje = D_SK(M_1)
Instancia / Respuesta
TGT
1208
1210
Pet. para UsuarioB, TGT
ST_A, ST_B
1212
1214
M, ST_B
1216
Descifrar ST_A
Crear M = E_SK

FIG. 12

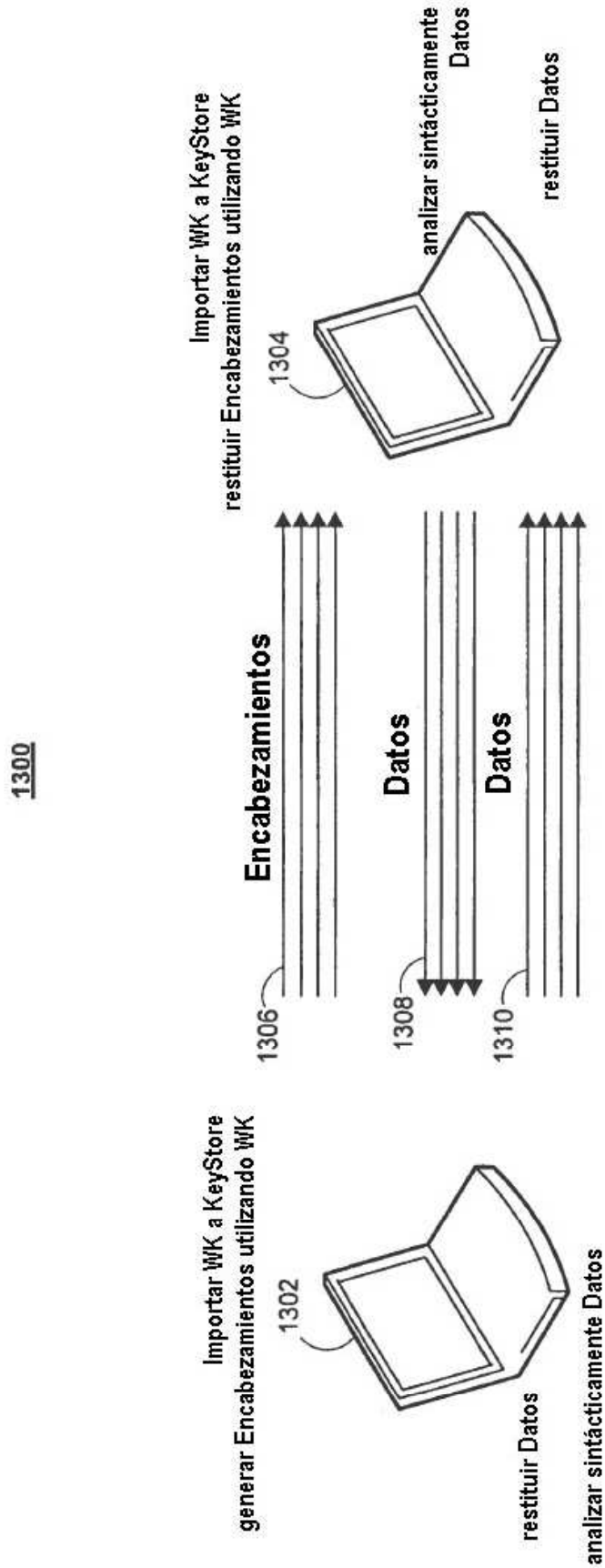
1300
Importar WK a KeyStore
generar Encabezamientos utilizando WK
1302
restituir Datos
analizar sintácticamente Datos
Encabezamientos
Datos
Datos
1306
1308
1310
Importar WK a KeyStore
restituir Encabezamientos utilizando WK
1304
analizar sintácticamente Datos
restituir Datos

FIG. 13

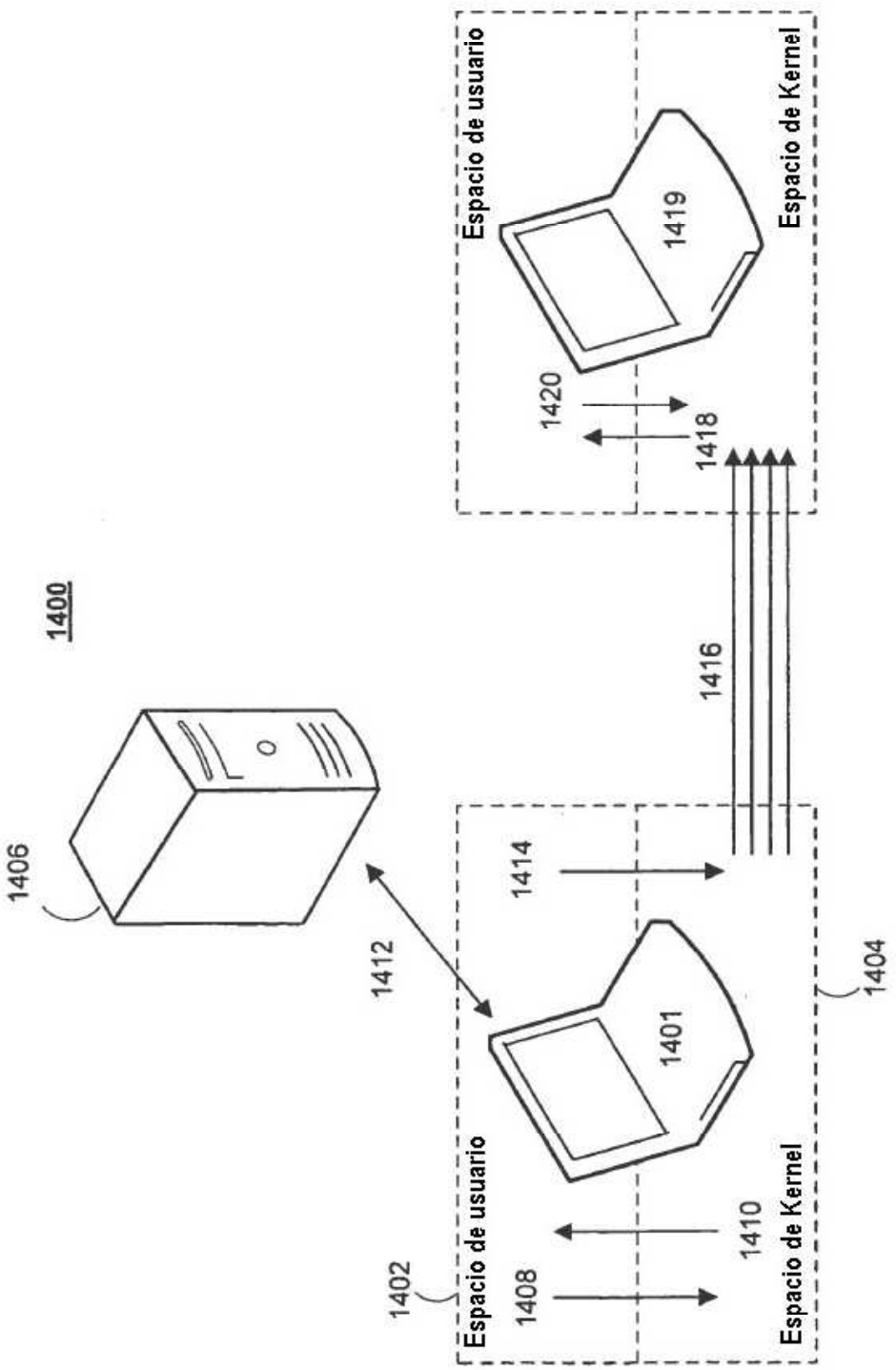
1400
1406
1412
1402
Espacio de usuario
1408
1410
Espacio de Kernel
1401
1404
1414
1416
Espacio de usuario
1420
1418
Espacio de Kernel
1419

FIG. 14

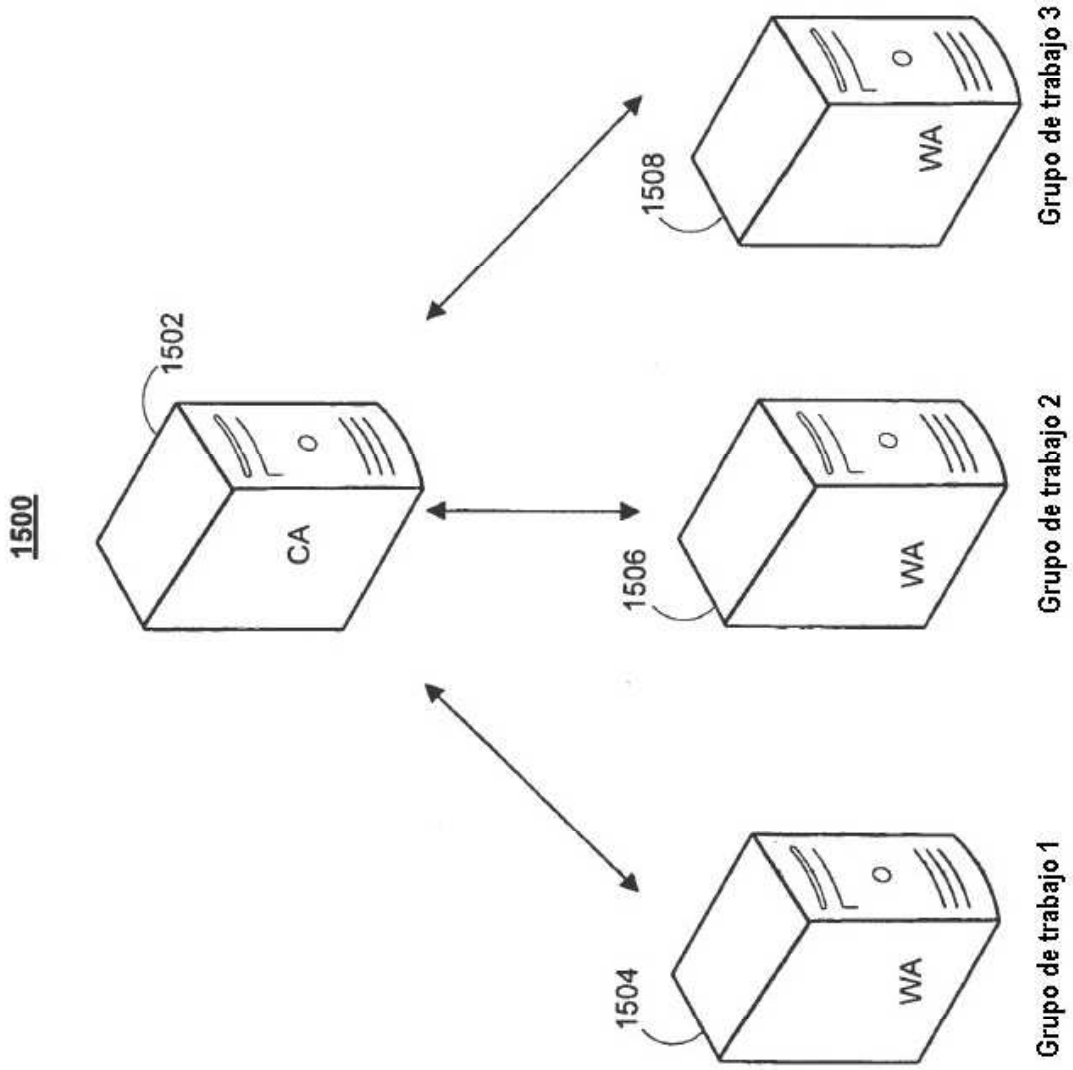
1500
1502
CA
1504
WA
Grupo de trabajo 1
1506
WA
Grupo de trabajo 2
1508
WA
Grupo de trabajo 3

FIG. 15

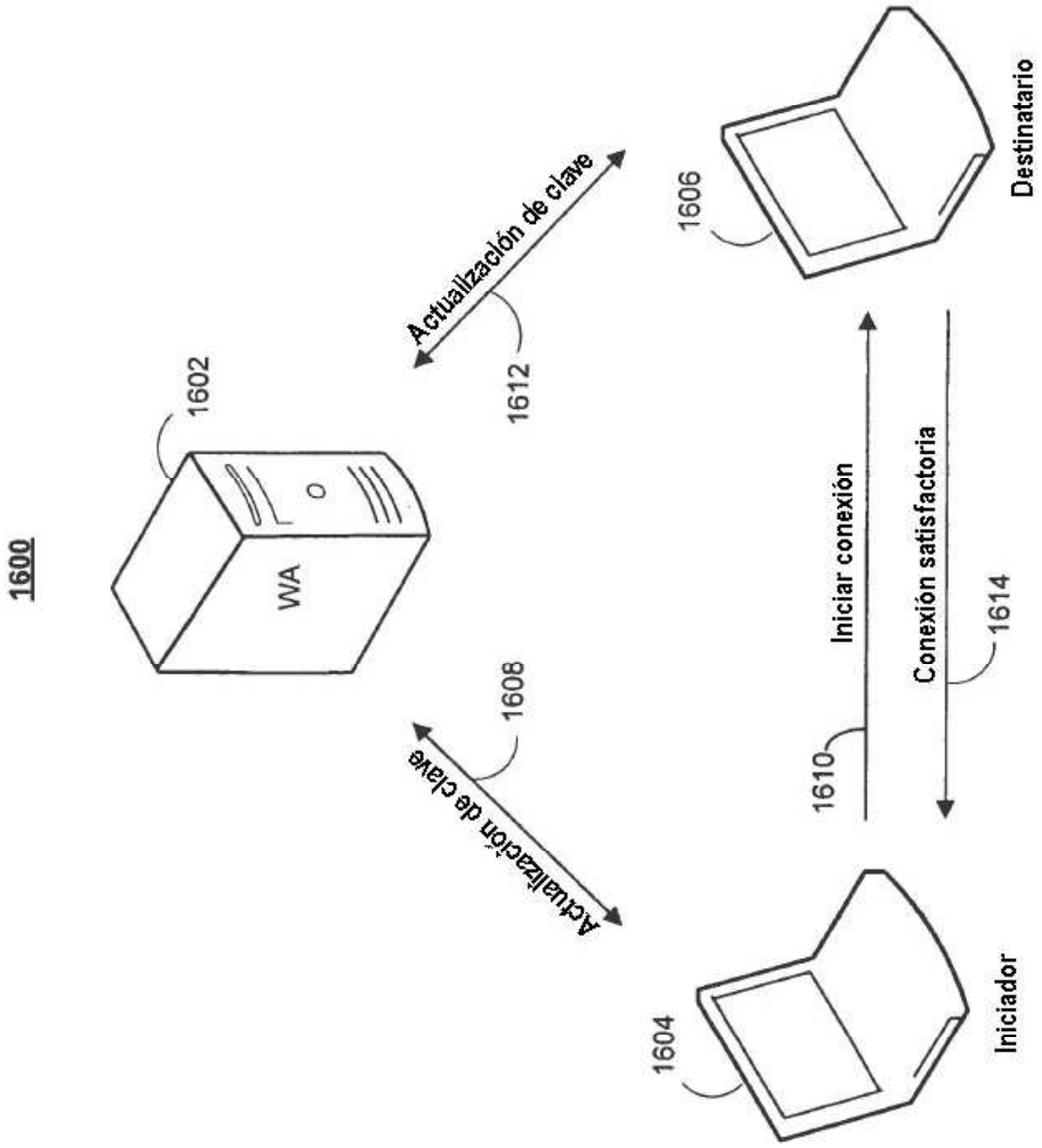
1600
1602
WA
1604
Iniciador
1606
Destinatario
Actualización de clave
1612
Actualización de clave
1608
Iniciar conexión
1610
Conexión satisfactoria
1614

FIG. 16


1700
1702
El cliente indica su deseo de unirse a un grupo de trabajo
1704
La WA genera la clave secreta para un lenguaje cifrado simétrico
1706
La WA almacena la clave secreta y una lista de IDs de clave de grupo de trabajo autorizada
1708
El cliente almacena la clave secreta
1710
El cliente almacena la ID de clave de grupo de trabajo y ajusta el aviso de refrescamiento de clave en 0 y la versión de clave en 0

FIG. 17

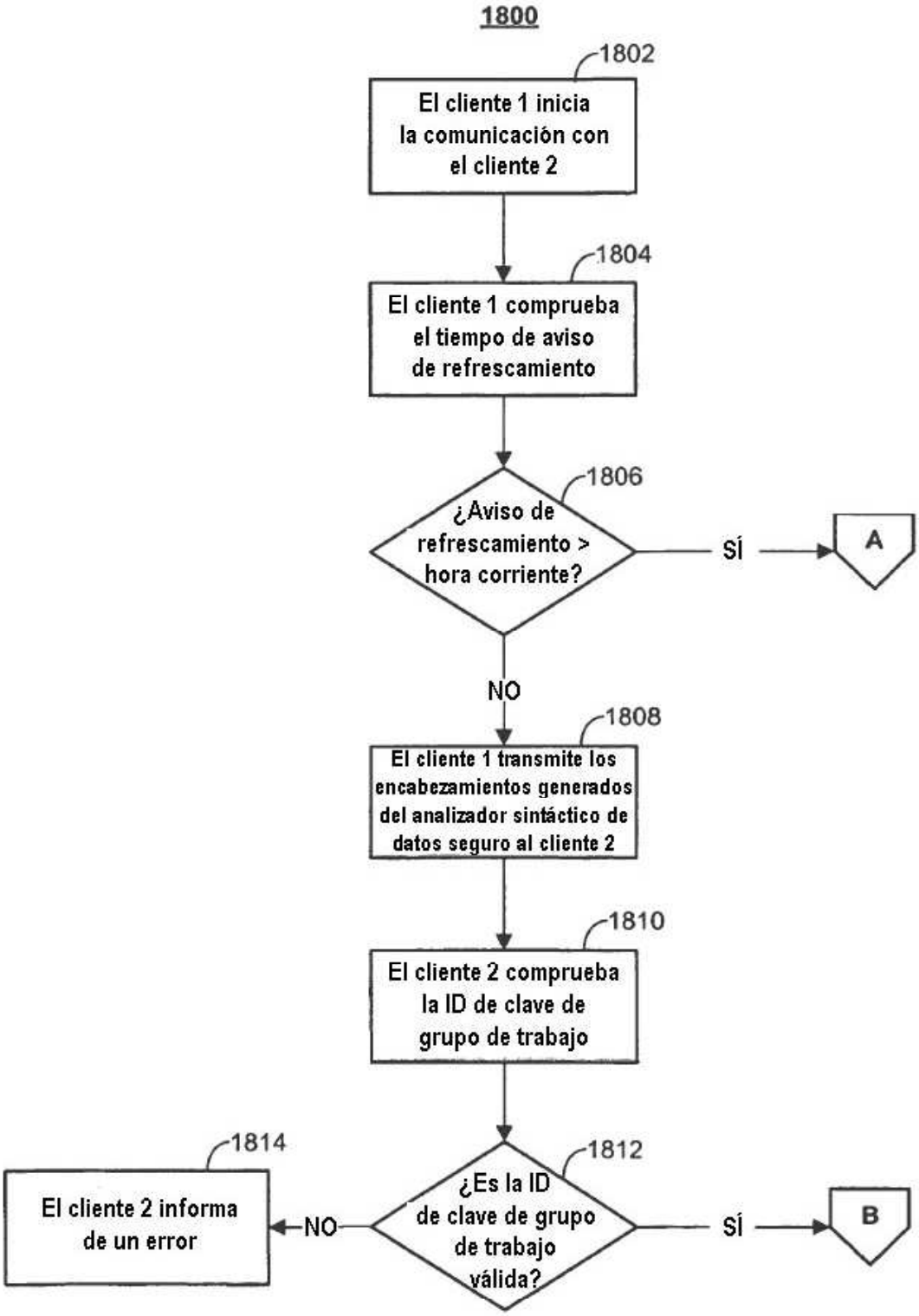
1800
1802
El cliente 1 inicia la comunicación con el cliente 2
1804
El cliente 1 comprueba el tiempo de aviso de refrescamiento
1806
¿Aviso de refrescamiento > hora corriente?
SÍ
A
NO
1808
El cliente 1 transmite los encabezamientos generados del analizador sintáctico de datos seguro al cliente 2
1810
El cliente 2 comprueba la ID de clave de grupo de trabajo
1812
¿Es la ID de clave de grupo de trabajo válida?
SÍ
B
NO
1814
El cliente 2 informa de un error

FIG. 18A

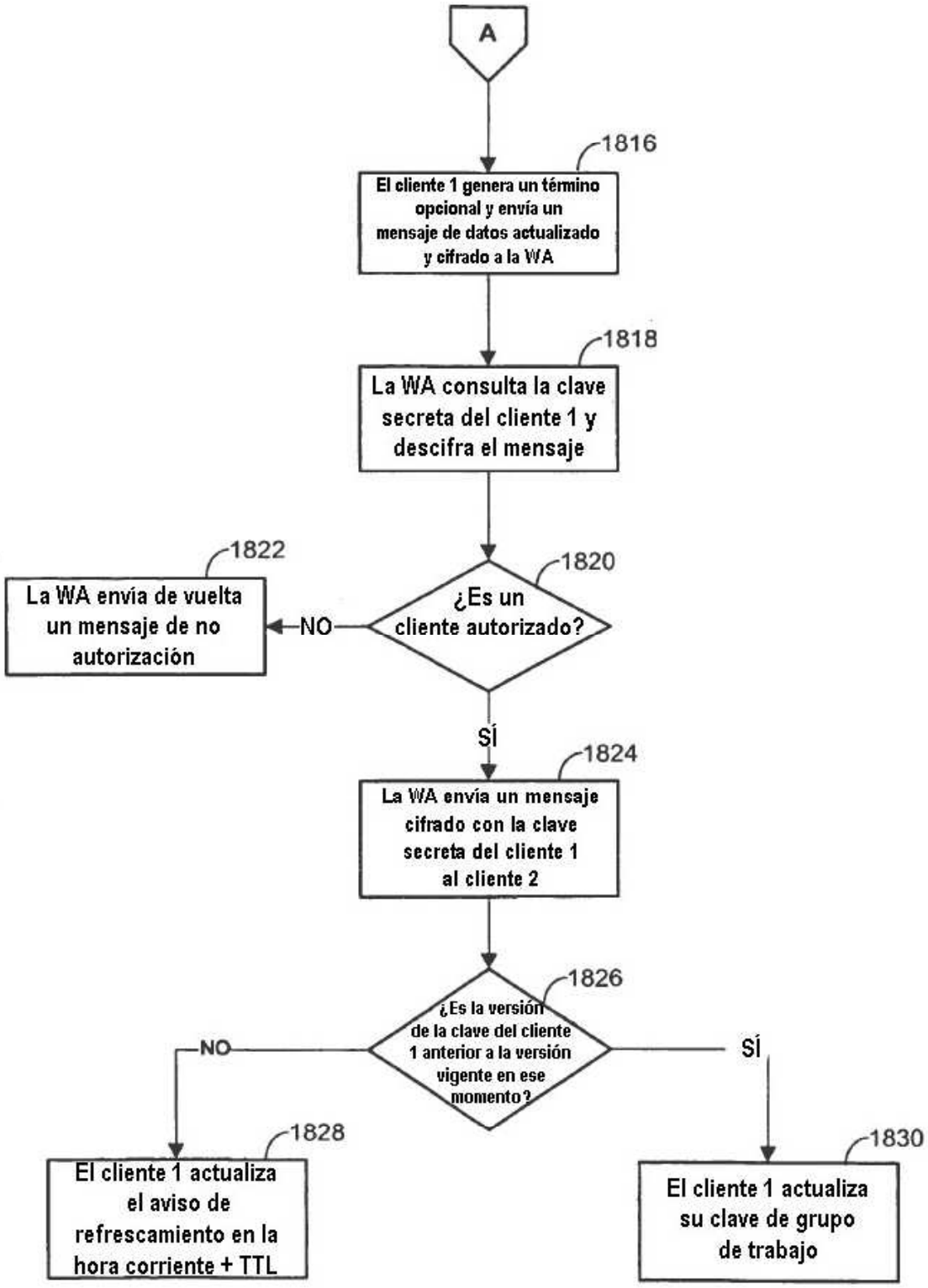
A
1816
El cliente 1 genera un término opcional y envía un mensaje de datos actualizado y cifrado a la WA
1818
La WA consulta la clave secreta del cliente 1 y descifra el mensaje
1820
¿Es un cliente autorizado?
NO
1822
La WA envía de vuelta un mensaje de no autorización
SÍ
1824
La WA envía un mensaje cifrado con la clave secreta del cliente 1 al cliente 2
1826
¿Es la versión de la clave del cliente 1 anterior a la versión vigente en ese momento?
NO
SÍ
1828
El cliente 1 actualiza el aviso de refrescamiento en la hora corriente + TTL
1830
El cliente 1 actualiza su clave de grupo de trabajo

FIG. 18B

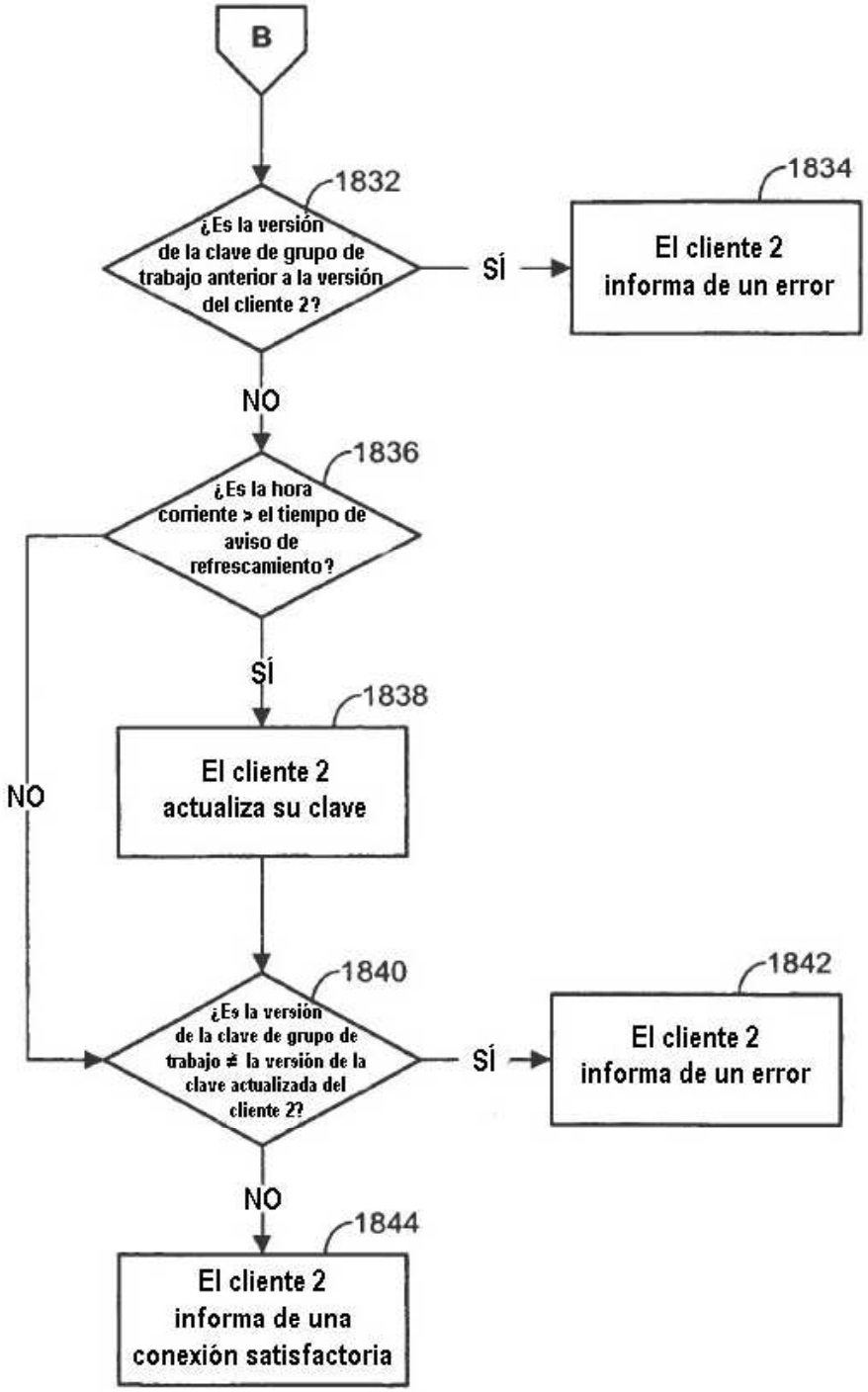
B
1832
¿Es la versión de la clave de grupo de trabajo anterior a la versión del cliente 2?
SÍ
1834
El cliente 2 informa de un error
NO
1836
¿Es la hora corriente > el tiempo de aviso de refrescamiento?
SÍ
1838
El cliente 2 actualiza su clave
NO
1840
¿Es la versión de la clave de grupo de trabajo ≠ la versión de la clave actualizada del cliente 2?
SÍ
1842
El cliente 2 informa de un error
NO
1844
El cliente 2 informa de una conexión satisfactoria

FIG. 18C

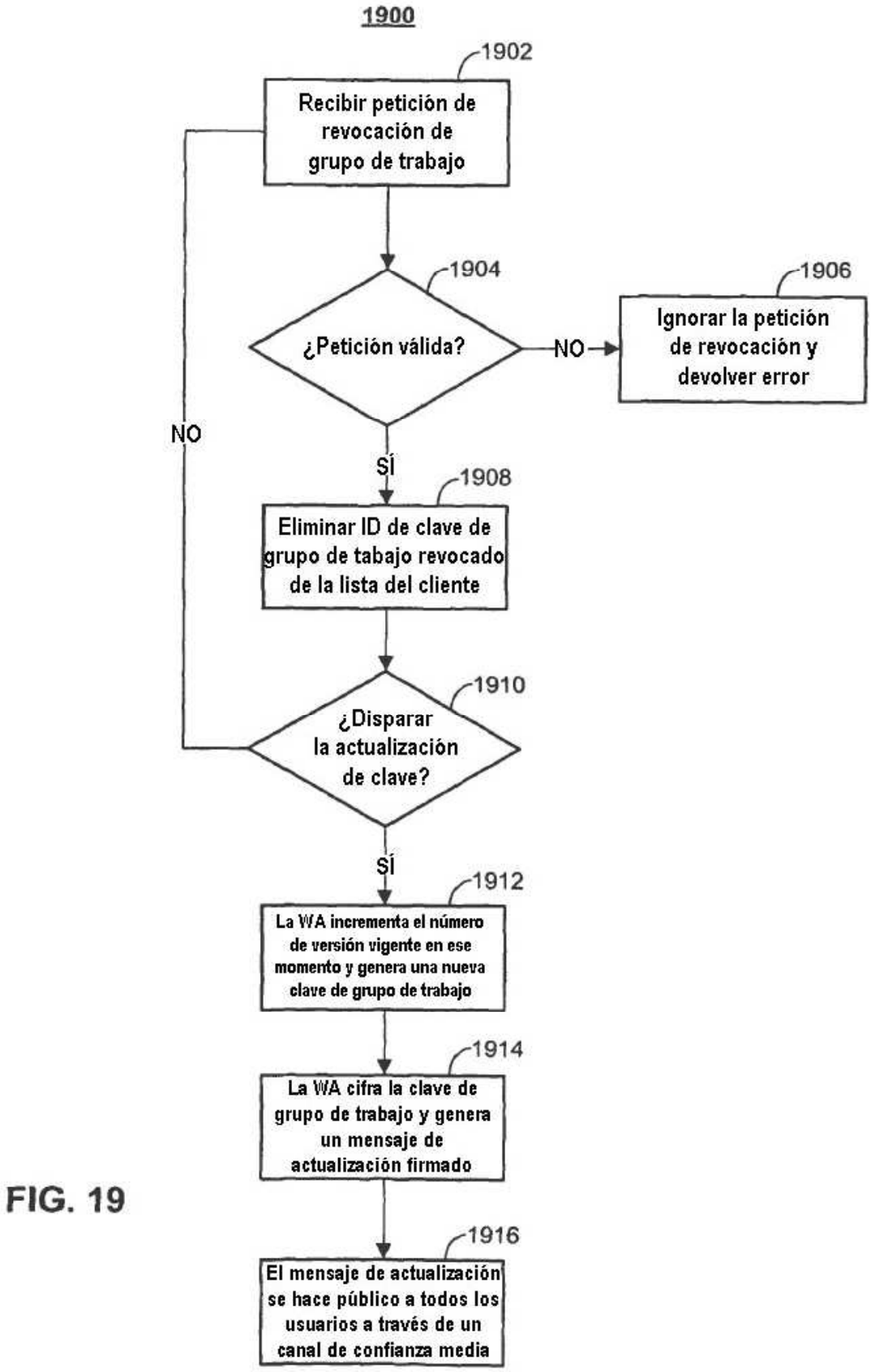
1900
1902
Recibir petición de revocación de grupo de trabajo
1904
¿Petición válida?
NO
1906
Ignorar la petición de revocación y devolver error
NO
SÍ
1908
Eliminar ID de clave de grupo de tabajo revocado de la lista del cliente
1910
¿Disparar la actualización de clave?
SÍ
1912
La WA incrementa el número de versión vigente en ese momento y genera una nueva clave de grupo de trabajo
1914
La WA cifra la clave de grupo de trabajo y genera un mensaje de actualización firmado
1916
El mensaje de actualización se hace público a todos los usuarios a través de un canal de confianza media

FIG. 19

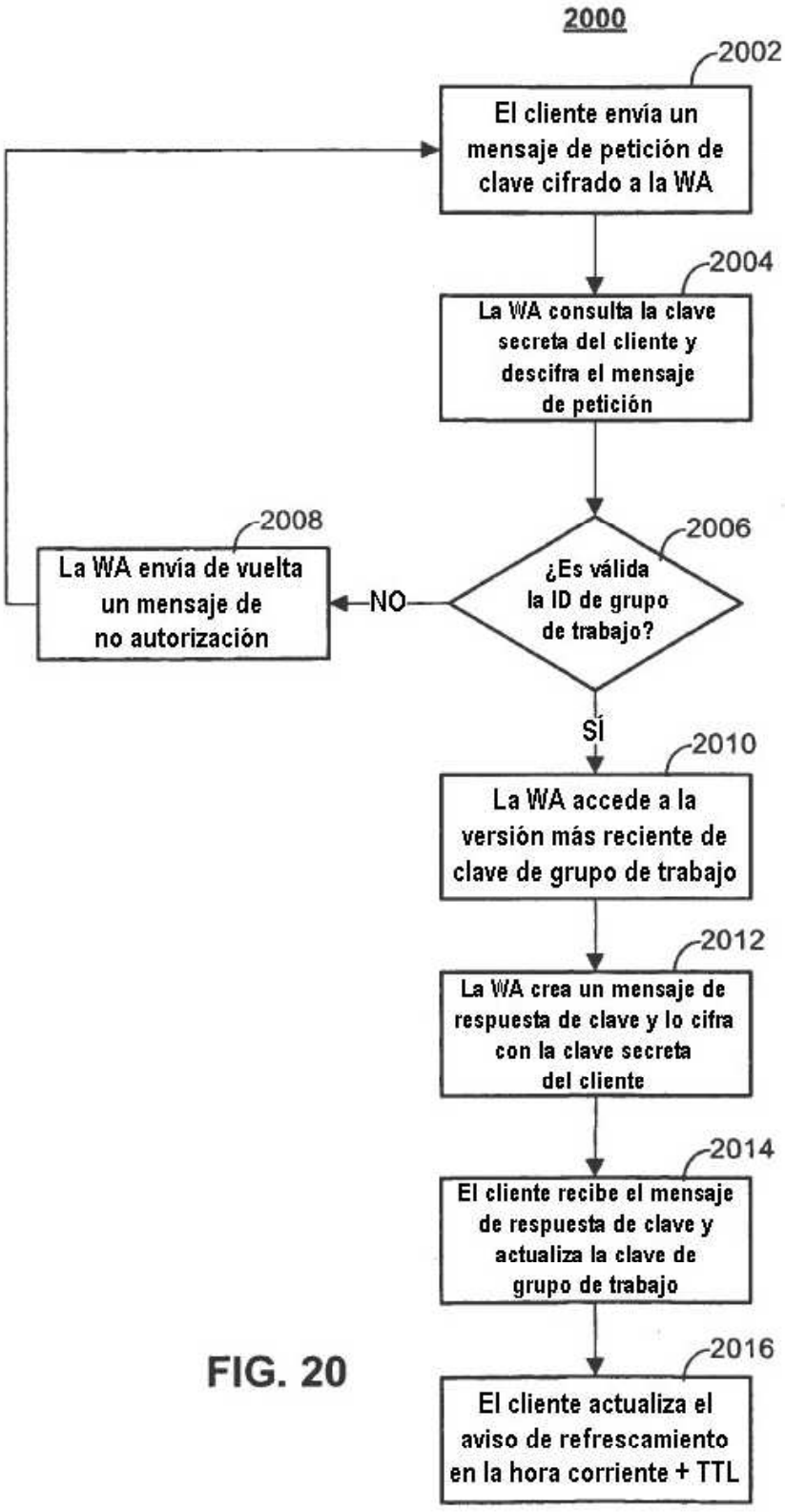
2000
2002
El cliente envía un mensaje de petición de clave cifrado a la WA
2004
La WA consulta la clave secreta del cliente y descifra el mensaje de petición
2006
¿Es válida la ID de grupo de trabajo?
NO
2008
La WA envía de vuelta un mensaje de no autorización
SÍ
2010
La WA accede a la versión más reciente de clave de grupo de trabajo
2012
La WA crea un mensaje de respuesta de clave y lo cifra con la clave secreta del cliente
2014
El cliente recibe el mensaje de respuesta de clave y actualiza la clave de grupo de trabajo
2016
El cliente actualiza el aviso de refrescamiento en la hora corriente + TTL

FIG. 20