(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 620 962**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 12/22 (2006.01)
H04L 12/46 (2006.01)
H04L 9/32 (2006.01)
H04L 9/08 (2006.01)
H04L 9/00 (2006.01)
G06F 21/60 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **24.11.2010 PCT/US2010/058087**

(87) Fecha y número de publicación internacional: **09.06.2011 WO2011068738**

(96) Fecha de presentación y número de la solicitud europea: **24.11.2010 E 10818134 (8)**

(97) Fecha y número de publicación de la concesión europea: **16.11.2016 EP 2504973**

(54) Título: **Sistemas y procedimientos para asegurar datos en movimiento**

(30) Prioridad:

25.11.2009 US 264464 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
30.06.2017

(73) Titular/es:

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

(72) Inventor/es:

O'HARE, MARK S.;
ORSINI, RICK, L.;
BONO, STEPHEN, C.;
NIELSON, SETH, JAMES y
LANDAU, GABRIEL, D.

(74) Agente/Representante:

PONS ARIÑO, Ángel

DESCRIPCIÓN

Sistemas y procedimientos para asegurar datos en movimiento.

Campo de la invención

La presente invención se refiere, en general, a sistemas y procedimientos para asegurar comunicaciones distribuyendo confianza entre autoridades de certificación. Los sistemas y procedimientos descritos en este documento pueden usarse conjuntamente con otros sistemas y procedimientos descritos en la patente de EE.UU. de propiedad común nº 7.391.865 y las solicitudes de patente de EE.UU. de propiedad común n^{os} 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, 12/148.365, presentada el 18 de abril de 2008, 12/209.703, presentada el 12 de septiembre de 2008, 12/349.897, presentada el 7 de enero de 2009, 12/391.025, presentada el 23 de febrero de 2009.

Antecedentes de la invención

En la sociedad actual, los individuos y las empresas llevan a cabo una cantidad de actividades cada vez mayor en sistemas informáticos y por medio de ellos. Estos sistemas informáticos, incluyendo redes informáticas en propiedad y no en propiedad, a menudo están almacenando, archivando y transmitiendo todo tipo de información sensible. Así, existe una necesidad cada vez mayor de asegurar que los datos almacenados y transmitidos por estos sistemas no puedan ser leídos o verse comprometidos de otro modo.

Una solución es asegurar los datos usando claves de una autoridad de certificación. Las autoridades de certificación pueden ser administradas por organizaciones o compañías de terceros de confianza como, por ejemplo, VeriSign, Baltimore, Entrust o similares. El certificado digital certifica la propiedad de una clave pública por el sujeto designado del certificado. Esto permite que otros confíen en firmas o afirmaciones realizadas por la clave privada que corresponde a la clave pública que está certificada. Las solicitudes de un certificado digital pueden realizarse a través de protocolos de certificación digital como, por ejemplo, PKCS10. En respuesta a una solicitud, la autoridad de certificación expedirá un certificado en varios protocolos diferentes como, por ejemplo, PKCS7. Pueden intercambiarse mensajes entre dispositivos basándose en los certificados expedidos.

Si la autoridad de certificación se ve comprometida, entonces la seguridad del sistema puede perderse para cada usuario para el cual la autoridad de certificación está certificando un enlace entre una clave pública y una identidad. Por ejemplo, un atacante puede comprometer a una autoridad de certificación induciendo a esa autoridad de certificación a expedir un certificado que reivindica falsamente representar a una entidad. El atacante tendría la clave privada asociada con el certificado de la autoridad de certificación. El atacante podría entonces usar este certificado para enviar mensajes firmados digitalmente a un usuario y engañar al usuario haciéndole creer que el mensaje procedía de la entidad de confianza. El usuario puede responder a los mensajes firmados digitalmente, los cuales el atacante puede descifrar usando la clave privada. Por consiguiente, la confianza que el usuario puso en la autoridad de certificación puede verse comprometida.

El documento WO02/062032A2 está dirigido a asegurar la transmisión de datos por una red usando intermediarios de confianza para retransmitir las comunicaciones entre las partes.

El documento US2010/242038del 23 de septiembre de 2010 (23-09-2010), describe un procedimiento donde puede generarse y usarse una clave criptográfica para cifrar datos de usuario para crear una porción de texto cifrado. Puede crearse un conjunto de n cuotas de clave aplicando un algoritmo de compartición de secreto a la clave criptográfica.

Resumen de la invención

Basándose en lo anterior, existe una necesidad de proporcionar un servicio de apoderado seguro que incluya un sistema que asegure las comunicaciones distribuyendo confianza entre un conjunto de autoridades de certificación.

De acuerdo con un primer aspecto, se proporciona un procedimiento de acuerdo con la reivindicación 1.

Este aspecto puede proporcionar un sistema de acuerdo con la reivindicación 9.

Por consiguiente, se proporciona una estrategia para distribuir confianza entre un conjunto de autoridades de certificación. Un analizador sintáctico de datos seguros puede estar integrado con cualquier tecnología de cifrado adecuada. Se entenderá que en algunas realizaciones el servicio de apoderado seguro puede implementarse integrando un analizador sintáctico de datos seguros con el protocolo de seguridad de la capa de transporte ("TLS"), con el protocolo de capa de zócalo segura (SSL), con SSL y TLS completa, o implementando el analizador sintáctico de datos seguros sin el uso de SSL y/o TLS completa. Además, se entenderá que en algunas realizaciones el servicio de apoderado seguro puede implementarse conjuntamente con cualquier protocolo adecuado que haga uso de autoridades de certificación para asegurar la confidencialidad, integridad y autenticidad de los mensajes intercambiados.

Tal analizador sintáctico de datos seguros puede usarse para distribuir confianza en un conjunto de autoridades de certificación durante la negociación inicial (por ejemplo, la fase de establecimiento de clave) de una conexión entre dispositivos. Las autoridades de certificación pueden ser únicas porque los certificados expedidos por cada una tienen diferentes pares de claves pública y privada. Esto ofrece la garantía de que si algunas (pero menos que un *quorum*) de las autoridades de certificación se han visto comprometidas, la conexión todavía puede establecerse y pueden intercambiarse mensajes sin alterar la confidencialidad o integridad de la comunicación.

El cálculo de claves de cifrado compartidas puede formar parte de una fase de establecimiento de clave de las comunicaciones seguras entre dispositivos. Puede generarse información secreta y pueden obtenerse claves públicas de autoridades de certificación únicas. La información secreta puede ser dispersada en cualquier número de cuotas de información secreta. Cada cuota de información secreta puede ser cifrada basándose en una clave pública de un certificado asociado con una autoridad diferente de las autoridades de certificación únicas. Opcionalmente, cada una de las cuotas de información secreta puede ser cifrada basándose en una envoltura de clave. La envoltura de clave puede estar basada en una clave de grupo de trabajo. En algunas realizaciones, las cuotas pueden ser recombinadas y los datos pueden ser transmitidos basándose en las cuotas recombinadas.

En algunas realizaciones puede generarse un conjunto de números aleatorios. Puede calcularse una primera clave de cifrado compartida basándose en el conjunto de números aleatorios y la información secreta original. Puede calcularse una segunda clave de cifrado compartida basándose en el conjunto de números aleatorios y las cuotas recombinadas. Los datos pueden ser transmitidos basándose en la primera y la segunda claves de cifrado compartidas. En algunas realizaciones pueden compararse la primera y la segunda claves de cifrado compartidas. Puede realizarse una determinación en cuanto a si transmitir los datos basándose en esta comparación y los datos pueden ser transmitidos basándose en esta determinación.

Breve descripción de los dibujos

La presente invención se describe en más detalle más adelante en relación con los dibujos adjuntos que pretenden 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 transacción de la figura 2 de acuerdo con aspectos de una realización de la invención;
la figura 4 ilustra un diagrama de bloques del depósito 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 autenticación 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 ilustra un diagrama de bloques de un sistema de depósito de acuerdo con aspectos de otra realización de la invención;
la figura 8 ilustra un diagrama de flujo de un proceso de división de datos de acuerdo con aspectos de una realización de la invención;
la figura 9, panel A, ilustra un flujo de datos de un proceso de inscripción de acuerdo con aspectos de una realización de la invención;
la figura 9, panel B, ilustra un diagrama de flujo de un proceso de interoperabilidad de acuerdo con aspectos de una realización de la invención;

la figura 10 ilustra un flujo de datos de un proceso de autenticación de acuerdo con aspectos de una realización de la invención;
la figura 11 ilustra un flujo de datos de un proceso de firma de acuerdo con aspectos de una realización de la invención;
la figura 12 ilustra un flujo de datos y un proceso de cifrado/descifrado de acuerdo con aspectos y otra realización más de la invención;
la figura 13 ilustra un diagrama de bloques simplificado de un sistema de motor de confianza de acuerdo con aspectos de otra realización de la invención;
la figura 14 ilustra un diagrama de bloques simplificado de un sistema de motor de confianza de acuerdo con aspectos de otra realización de la invención;
la figura 15 ilustra un diagrama de bloques del módulo de redundancia de la figura 14 de acuerdo con aspectos de una realización de la invención;
la figura 16 ilustra un proceso para evaluar autenticaciones de acuerdo con un aspecto de la invención;
la figura 17 ilustra un proceso para asignar un valor a una autenticación de acuerdo con un aspecto como se muestra en la figura 16 de la invención;
la figura 18 ilustra un proceso para realizar arbitraje de confianza en un aspecto de la invención como se muestra en la figura 17; y
la figura 19 ilustra una transacción de muestra entre un usuario y un vendedor de acuerdo con aspectos de una realización de la invención donde un contacto basado en web inicial conduce a un contrato de ventas firmado por ambas partes.
La figura 20 ilustra un sistema de usuario de muestra con un módulo proveedor de servicio criptográfico que proporciona funciones de seguridad a un sistema de usuario.
La figura 21 ilustra un proceso para analizar sintácticamente, dividir y/o separar datos con cifrado y almacenamiento de la clave maestra de cifrado con los datos.
La figura 22 ilustra un proceso para analizar sintácticamente, dividir y/o separar datos con cifrado y almacenar la clave maestra de cifrado por separado de los datos.
La figura 23 ilustra el proceso de clave intermedia para analizar sintácticamente, dividir y/o separar datos con cifrado y almacenamiento de la clave maestra de cifrado con los datos.
La figura 24 ilustra el proceso de clave intermedia para analizar sintácticamente, dividir y/o separa datos con cifrado y almacenar la clave maestra de cifrado por separado de los datos.
La figura 25 ilustra la utilización de los procedimientos y sistemas criptográficos de la presente invención con un grupo de trabajo pequeño.
La figura 26 es un diagrama de bloques de un sistema de seguridad de testigo físico ilustrativo que emplea el analizador sintáctico de datos seguros de acuerdo con una realización de la presente invención.
La figura 27 es un diagrama de bloques de una disposición ilustrativa en la cual el analizador sintáctico de datos seguros está integrado en un sistema de acuerdo con una realización de la presente invención.
La figura 28 es un diagrama de bloques de un sistema de datos en movimiento ilustrativo de acuerdo con una realización de la presente invención.
La figura 29 es un diagrama de bloques de otro sistema de datos en movimiento ilustrativo de acuerdo con una realización de la presente invención.
Las figuras 30-32 son diagramas de bloques de un sistema ilustrativo que tiene el analizador sintáctico de datos seguros integrado de acuerdo con una realización de la presente invención.
La figura 33 es un diagrama de flujo de proceso de un proceso ilustrativo para analizar sintácticamente y dividir datos de acuerdo con una realización de la presente invención.
La figura 34 es un diagrama de flujo de proceso de un proceso ilustrativo para restaurar porciones de datos en datos originales de acuerdo con una realización de la presente invención.
La figura 35 es un diagrama de flujo de proceso de un proceso ilustrativo para dividir datos a nivel de bit de acuerdo con una realización de la presente invención.
La figura 36 es un diagrama de flujo de proceso de etapas y características ilustrativas de acuerdo con una realización de la presente invención.
La figura 37 es un diagrama de flujo de proceso de etapas y características ilustrativas de acuerdo con una realización de la presente invención.
La figura 38 es un diagrama de bloques simplificado del almacenamiento de componentes de clave y datos dentro de cuotas de acuerdo con una realización de la presente invención.
La figura 39 es un diagrama de bloques simplificado del almacenamiento de componentes de clave y datos dentro de cuotas usando una clave de grupo de trabajo de acuerdo con una realización de la presente invención.
Las figuras 40A y 40B son diagramas de flujo de proceso simplificados e ilustrativos para generación de encabezamiento y división de datos para datos en movimiento de acuerdo con una realización de la presente invención.

La figura 41 es un diagrama de bloques simplificado de un formato de cuota ilustrativo de acuerdo con una realización de la presente invención.
La figura 42 es una jerarquía de autoridades de certificación simplificada e ilustrativa de acuerdo con una realización de la presente invención.
Las figuras 43-47, 48A y 48B son diagramas de flujo de proceso de etapas y características ilustrativas para un servicio de apoderado seguro de acuerdo con una realización de la presente invención.
La figura 48C es un diagrama de bloques simplificado de un servicio de apoderado seguro que distribuye confianza entre un conjunto de autoridades de certificación en la estructura de canales de comunicación de acuerdo con una realización de la presente invención.
Las figuras 49 y 50 son diagramas de flujo de proceso de etapas y características ilustradas para un servicio de apoderado seguro que distribuye confianza entre un conjunto de autoridades de certificación en la estructura de canales de comunicación de acuerdo con una realización de la presente invención.

Descripción detallada de la invención

Un aspecto de la presente invención es proporcionar un sistema criptográfico donde uno o más servidores seguros o motor de confianza, almacene claves criptográficas y datos de autenticación de usuario. Los usuarios acceden a la funcionalidad de sistemas criptográficos convencionales a través de acceso de red al motor de confianza, sin embargo, el motor de confianza no da a conocer claves reales ni otros datos de autenticación y, por lo tanto, las claves y los datos siguen siendo seguros. Esta almacenamiento centrado en el servidor de claves y datos de autenticación proporciona seguridad independiente del usuario, portabilidad, disponibilidad, sencillez árida.

Como los usuarios pueden fiarse de o confiar en el sistema criptográfico para realizar la autenticación de usuarios y documentos y otras funciones criptográficas, puede incorporarse dentro del sistema una amplia variedad de funcionalidad. Por ejemplo, el proveedor de motor de confianza puede garantizar que no se produzca rechazo de acuerdo, por ejemplo, autenticando los participantes en el acuerdo, firmando digitalmente el acuerdo en nombre de o por los participantes y almacenando un registro del acuerdo firmado digitalmente por cada participante. Además, el sistema criptográfico puede monitorizar los acuerdos y tomar la determinación de aplicar grados variables de autenticación, basándose, por ejemplo, en el precio, el usuario, el vendedor, la ubicación geográfica, el lugar de uso o similares.

Para facilitar una comprensión completa de la invención, el resto de la descripción detallada describe la invención con referencia a las figuras, donde a lo largo de todas ellas se hace referencia a elementos iguales con números iguales.

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 de usuario (105), un motor de confianza (110), una autoridad de certificación (115) y un sistema de vendedor (120) que se comunican a través de un enlace de comunicación (125).

De acuerdo con una realización de la invención, el sistema de usuario (105) comprende un ordenador de propósito general convencional que tiene uno o más microprocesadores como, por ejemplo, un procesador Intel. Por otra parte, el sistema de usuario (105) incluye un sistema operativo apropiado como, por ejemplo, un sistema operativo capaz de incluir gráficos o ventanas tal como Windows, Unix, Linux o similares. Como se muestra en la figura 1, el sistema de usuario (105) puede incluir un dispositivo biométrico (107). El dispositivo biométrico (107) puede captar ventajosamente una biometría del usuario y transferir la biometría captada al motor de confianza (110). De acuerdo con una realización de la invención, el dispositivo biométrico puede comprender ventajosamente un dispositivo que tiene atributos y características similares a las descritas en la solicitud de patente de EE.UU. nº 08/926.277, presentada el 5 de septiembre de 1997, titulada *"RELIEF OBJECT IMAGE GENERATOR"*, la solicitud de patente de EE.UU. nº 09/558.634, presentada el 26 de abril de 2000, titulada *"IMAGING DEVICE FOR A RELIEF OBJECT AND SYSTEM AND METHOD OF USING THE IMAGE DEVICE"*, la solicitud de patente de EE.UU. nº 09/435.011, presentada el 5 de noviembre de 1999, titulada *"RELIEF OBJECT SENSOR ADAPTOR"*, y la solicitud de patente de EE.UU. nº 09/477.943, presentada el 5 de enero de 2000, titulada *"PLANAR OPTICAL IMAGE SENSOR AND SYSTEM FOR GENERATING AN ELECTRONIC IMAGE OF A RELIEF OBJECT FOR FINGERPRINT READING"*, todas las cuales son propiedad del presente cesionario, y todas las cuales se incorporan por la presente por referencia en este documento.

Además, el sistema de usuario (105) puede conectarse al enlace de comunicación (125) a través de un proveedor de servicios convencionales como, por ejemplo, un sistema de marcación manual, una línea de abonado digital

(DSL), un módem de cable, una conexión por fibra o similares. De acuerdo con otra realización, el sistema de usuario (105) se conecta al enlace de comunicación (125) a través de conectividad de red como, por ejemplo, una red de área local o de área amplia. De acuerdo con una realización, el sistema operativo incluye una pila TCP/IP que se encarga de todo el tráfico de mensajes entrantes y salientes que pasa por el enlace de comunicación (125).

Aunque el sistema de usuario (105) se describe con referencia a las realizaciones anteriores, la invención no pretende estar limitada por las mismas. Más bien, un experto en la materia reconocerá, a partir de la descripción de este documento, un gran número de realizaciones alternativas del sistema de usuario (105), incluyendo casi cualquier dispositivo informático capaz de enviar o recibir información de otro sistema informático. Por ejemplo, el sistema de usuario (105) puede incluir, pero no está limitado a, una estación de trabajo informática, una televisión interactiva, un quiosco interactivo, un dispositivo informático móvil personal, tal como un asistente digital, un teléfono móvil, un ordenador portátil o similares, equipo personal de conexión en red, tal como un encaminador doméstico, un dispositivo de almacenamiento en red ("NAS"), un punto de acceso personal o similares, o un dispositivo de comunicaciones inalámbricas, una tarjeta inteligente, un dispositivo informático integrado o similares, que pueda interactuar con el enlace de comunicación (125). En tales sistemas alternativos, los sistemas operativos probablemente diferirán y estarán adaptados para el dispositivo particular. Sin embargo, de acuerdo con una realización, los sistemas operativos siguen proporcionando ventajosamente los protocolos de comunicaciones apropiados necesarios para establecer 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 sensible y almacenarla, la cual puede ser cualquier tipo o forma de datos, tales como, pero no limitados a texto, audio, vídeo, datos de autenticación de usuario y claves criptográficas públicas y privadas. De acuerdo con una realización, los datos de autenticación incluyen datos diseñados para identificar de manera única un usuario del sistema criptográfico (100). Por ejemplo, los datos de autenticación pueden incluir un número de identificación de usuario, una o más biometrías y una serie de preguntas y respuestas generadas por el motor de confianza (110) o el usuario, pero contestadas inicialmente por el usuario en la inscripción. Las preguntas anteriores pueden incluir datos demográficos tales como el lugar de nacimiento, la dirección, el aniversario o similares, datos personales, tales como el nombre de soltera de la madre, el helado favorito o similares, u otros datos diseñados para identificar de manera única al usuario. El motor de confianza (110) compara los datos de autenticación de un usuario asociados con una transacción actual con los datos de autenticación proporcionados en un momento anterior como, por ejemplo, durante la inscripción. El motor de confianza (110) puede requerir ventajosamente que el usuario produzca los datos de autenticación en el momento de cada transacción, o el motor de confianza (110) puede permitir ventajosamente que el usuario produzca periódicamente datos de autenticación, tales como al comienzo de una cadena de transacciones o el registro en un sitio web de un vendedor particular.

De acuerdo con la realización donde el usuario produce datos biométricos, el usuario proporciona una característica física, tal como, pero no limitada a, un escaneo facial, un escaneo de la mano, un escaneo de la oreja, un escaneo del iris, un escaneo de la retina, un patrón vascular, ADN, una huella dactilar, escritura o voz, al dispositivo biométrico (107). El dispositivo biométrico produce ventajosamente un patrón electrónico o biométrico de la característica física. El patrón electrónico es transferido a través del sistema de usuario (105) al motor de confianza (110) con fines de inscripción o autenticación.

Una vez que el usuario produce los datos de autenticación apropiados y el motor de confianza (110) determina una coincidencia positiva entre los datos de autenticación (datos de autenticación actuales) y los datos de autenticación proporcionados en el momento de la inscripción (datos de autenticación de inscripción), el motor de confianza (110) proporciona al usuario una funcionalidad criptográfica completa. Por ejemplo, el usuario autenticado correctamente emplea ventajosamente el motor de confianza (110) para realizar troceo, firma digital, cifrado y descrifrado (a menudo denominados conjuntamente solo como cifrado), creación o distribución de certificados digitales y similares. Sin embargo, las claves criptográficas privadas usadas en las funciones criptográficas no estarán disponibles fuera del motor de confianza (110), garantizando así la integridad de las claves criptográficas.

De acuerdo con una realización, el motor de confianza (110) genera y almacena claves criptográficas. De acuerdo con otra realización, al menos una clave criptográfica está asociada con cada usuario. Por otra parte, cuando las claves criptográficas incluyen tecnología de clave pública, cada clave privada asociada con un usuario es generada dentro del motor de confianza (110) y no se da a conocer desde el mismo. Así, siempre y cuando el usuario tenga acceso al motor de confianza (110), el usuario puede realizar funciones criptográficas usando su clave pública o privada. Tal acceso remoto permite ventajosamente que los usuarios sigan siendo completamente móviles y accedan a la funcionalidad criptográfica a través de prácticamente cualquier conexión de internet, tal como teléfonos

celulares y vía satélite, quioscos, ordenadores portátiles, habitaciones de hotel y similares.

De acuerdo con otra realización, el motor de confianza (110) realiza la funcionalidad criptográfica usando un par de claves generadas para el motor de confianza (110). De acuerdo con esta realización, el motor de confianza (110) en primer lugar autentica el usuario, y después de que el usuario ha producido correctamente datos de autenticación que coinciden con los datos de autenticación de inscripción, el motor de confianza (110) usa su propio par de claves criptográficas para realizar funciones criptográficas en representación del usuario autenticado.

Un experto en la materia reconocerá, a partir de la descripción de este documento, que las claves criptográficas pueden incluir ventajosamente algunas de claves simétricas, claves públicas y claves privadas o todas. Además, un experto en la materia reconocerá, a partir de la descripción de este documento, que las claves anteriores pueden implementarse con un gran número de algoritmos proporcionados por tecnologías comerciales como, por ejemplo, RSA, ELGAMAL o similares.

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 compañía de terceros de confianza que expide certificados digitales como, por ejemplo, VeriSign, Baltimore, Entrust o similares. El motor de confianza (110) puede transmitir ventajosamente solicitudes de certificados digitales a través de uno o más protocolos de certificación digital convencionales como, por ejemplo, PKCS10, a la autoridad de certificación (115). En respuesta, la autoridad de certificación (115) expedirá un certificado digital en uno o más de varios protocolos diferentes como, por ejemplo, PKCS7. De acuerdo con una realización de la invención, el motor de confianza (110) solicita certificados digitales de varias o todas las autoridades de certificación importantes (115), de modo que el motor de confianza (110) tiene acceso a un certificado digital que corresponde al estándar de certificación de cualquier parte solicitante.

De acuerdo con otra realización, el motor de confianza (110) realiza internamente expediciones 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 son solicitados como, por ejemplo, en el momento de la generación de clave o en el estándar de certificación solicitado en el momento de la solicitud. El motor de confianza (110) se describirá en mayor detalle más adelante.

La figura 1 también ilustra el sistema de vendedor (120). De acuerdo con una realización, el sistema de vendedor (120) comprende ventajosamente un servidor web. Los servidores web típicos generalmente sirven contenido por internet usando uno de entre varios lenguajes de marcaje de internet o estándares de formato de documento, tales como el lenguaje de marcaje de hipertexto (HTML) o el lenguaje de marcaje extensible (XML). El servidor web acepta solicitudes procedentes de navegadores como Netscape e internet Explorer y luego devuelve los documentos electrónicos apropiados. Pueden usarse varias tecnologías del lado del servidor o del lado del cliente para aumentar la potencia del servidor web más allá de su capacidad de distribuir documentos electrónicos estándar. Por ejemplo, estas tecnologías incluyen guiones de interfaz de pasarela común (CGI), seguridad de SSL y páginas de servidor activo (ASP). El sistema de vendedor (120) puede proporcionar ventajosamente contenido electrónico relacionado con transacciones comerciales, personales, educativas u otras transacciones.

Aunque el sistema de vendedor (120) se describe con referencia a las realizaciones anteriores, la invención no pretende estar limitada por las mismas. Más bien, un experto en la materia reconocerá, a partir de la descripción de este documento, que el sistema de vendedor (120) puede comprender ventajosamente cualquiera de los dispositivos descritos con referencia al sistema de usuario (105) o combinaciones de los mismos.

La figura 1 también ilustra el enlace de comunicación (125) que conecta el sistema de usuario (105), el motor de confianza (110), la autoridad de certificación (115) y el sistema de vendedor (120). De acuerdo con una realización, el enlace de comunicación (125) comprende preferentemente internet. Internet, tal como se usa a lo largo de toda esta descripción es una red global de ordenadores. La estructura de internet, que es bien conocida por cualquier experto en la materia, incluye una red principal con redes que se ramifican de la principal. Estas ramas, a su vez, tienen redes que se ramifican desde ellas, y así sucesivamente. Los encaminadores mueven paquetes de información entre niveles de la red, y luego de red a red, hasta que el paquete llega a las inmediaciones de su destino. Desde el destino, el anfitrión de la red de destino dirige el paquete de información al terminal o nodo, apropiado. En una realización ventajosa, los nodos centralizados de encaminamiento de internet comprenden servidores del sistema de nombres de dominio (DNS) que usan el protocolo de control de transmisión/protocolo internet (TCP/IP) como es bien conocido en la técnica. Los nodos centralizados de encaminamiento se conectan a uno o más de otros nodos centralizados de encaminamiento por medio de enlaces de comunicación de alta

velocidad.

Una parte popular de internet es la World Wide Web. La World Wide Web contiene diferentes ordenadores que almacenan documentos capaces de mostrar información gráfica y de texto. Los ordenadores que proporcionan información en la World Wide Web se denominan típicamente “sitios web”. Un sitio web está definido por una dirección de internet que tiene una página electrónica asociada. La página electrónica puede identificarse por un localizador uniforme de recursos (URL). Generalmente, una página electrónica es un documento que organiza la presentación de texto, imágenes gráficas, audio, vídeo, etcétera.

Aunque el enlace de comunicación (125) se describe en cuanto a su realización preferente, cualquier experto en la materia reconocerá, a partir de la descripción de este documento, que el enlace de comunicación (125) puede incluir una amplia variedad de enlaces de comunicaciones interactivos. Por ejemplo, el enlace de comunicación (125) puede incluir redes de televisiones interactivas, redes telefónicas, sistemas de transmisión inalámbrica de datos, sistemas de cable bidireccionales, redes informáticas privadas o públicas personalizadas, redes de quioscos interactivos, redes de cajeros automáticos, enlaces directos, redes vía satélite o celulares y 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 muestra en la figura 2, el motor de confianza (110) incluye un motor de transacción (205), un depósito (210), un motor de autenticación (215) y un motor criptográfico (220). De acuerdo con una realización de la invención, el motor de confianza (110) también incluye una memoria de almacenamiento masivo (225). Como se muestra además en la figura 2, el motor de transacción (205) se comunica con el depósito (210), el motor de autenticación (215) y el motor criptográfico (220) junto con la memoria de almacenamiento masivo (225). Además, el depósito (210) se comunica con el motor de autenticación (215), el motor criptográfico (220) y la memoria de almacenamiento masivo (225). Por otra parte, el motor de autenticación (215) se comunica con el motor criptográfico (220). De acuerdo con una realización de la invención, algunas o todas las comunicaciones anteriores pueden comprender ventajosamente la transmisión de documentos XML a direcciones IP que corresponden al dispositivo receptor. Como se mencionó en lo anterior, los documentos XML permiten ventajosamente que los diseñadores creen sus propias etiquetas de documento personalizadas, lo que permite la definición, transmisión, validación e interpretación de datos entre aplicaciones y entre organizaciones. Por otra parte, algunas o todas las comunicaciones anteriores pueden incluir tecnologías SSL convencionales.

De acuerdo con una realización, el motor de transacción (205) comprende un dispositivo de encaminamiento de datos, tal como un servidor web convencional proporcionado por Netscape, Microsoft, Apache o similares. Por ejemplo, el servidor web puede recibir ventajosamente datos de entrada procedentes del enlace de comunicación (125). De acuerdo con una realización de la invención, los datos de entrada son direccionados a un sistema de seguridad de extremo frontal para el motor de confianza (110). Por ejemplo, el sistema de seguridad de extremo frontal puede incluir ventajosamente un cortafuego, un sistema de detección de intrusión que busca perfiles de ataque conocidos y/o un escáner de virus. Después de despejar el sistema de seguridad de extremo frontal, los datos son recibidos por el motor de transacción (205) y encaminados a uno de entre el depósito (210), el motor de autenticación (215), el motor criptográfico (220) y la memoria de almacenamiento masivo (225). Además, el motor de transacción (205) monitoriza los datos de entrada procedentes del motor de autenticación (215) y el 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 encaminar ventajosamente los datos al sistema de usuario (105), al autoridad de certificación (115) o al sistema de vendedor (120).

De acuerdo con una realización, los datos son encaminados usando técnicas de encaminamiento HTTP convencionales como, por ejemplo, empleando URL o identificadores uniformes de recursos (URI). Los URI son similares a los URL, sin embargo, los URI indican típicamente la fuente de los archivos o acciones como, por ejemplo, ejecutables, guiones y similares. Por lo tanto, de acuerdo con una realización, el sistema de usuario (105), la autoridad de certificación (115), el sistema de vendedor (120) y los componentes del motor de confianza (210), incluyen ventajosamente datos suficientes dentro de los URL o URI de comunicación para que el motor de transacción (205) encamine correctamente los datos por todo el sistema criptográfico.

Aunque el encaminamiento de datos se describe con referencia a su realización preferente, un experto en la materia reconocerá un gran número de posibles soluciones o estrategias de encaminamiento de datos. Por ejemplo, los paquetes XML u otros paquetes de datos pueden, ventajosamente, ser desempaquetados y reconocidos por su formato, contenido o similares, de modo que el motor de transacción (205) puede encaminar correctamente los datos por todo el motor de confianza (110). Por otra parte, un experto en la materia reconocerá que el encaminamiento de datos puede, ventajosamente, ser adaptado a los protocolos de transferencia de datos de conformidad con sistemas

de redes particulares como, 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 cifrado SSL convencionales, de modo que los sistemas anteriores pueden autenticarse a sí mismos, y viceversa, con el motor de transacción (205), durante comunicaciones particulares. Como se usará a lo largo de toda esta descripción, el término "½ SSL" se refiere a comunicaciones en las que un servidor, pero no necesariamente el cliente, es autenticado por SSL, y el término "SSL COMPLETA" se refiere a comunicaciones en las que el cliente y el servidor son autenticados por SSL. Cuando la presente descripción usa el término "SSL", la comunicación puede comprender ½ SSL o SSL COMPLETA.

Como el motor de transacción (205) encamina datos a los diversos componentes del sistema criptográfico (100), el motor de transacción (205) puede crear ventajosamente un registro de auditoría. De acuerdo con una realización, el registro de auditoría incluye un registro de al menos el tipo y formato de los datos encaminados por el motor de transacción (205) por todo el sistema criptográfico (100). Tales datos de auditoría pueden ser almacenados ventajosamente en la memoria 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 como, por ejemplo, un servidor de directorio, un servidor de base de datos o similares. Como se muestra en la figura 2, el depósito (210) almacena claves criptográficas y datos de autenticación de inscripción. Las claves criptográficas pueden corresponder ventajosamente al motor de confianza (110) o a usuarios del sistema criptográfico (100) tales como el usuario o el vendedor. Los datos de autenticación de inscripción pueden incluir ventajosamente datos diseñados para identificar de manera única a un usuario tales como ID de usuario, contraseñas, respuestas a preguntas, datos biométricos o similares. Estos datos de autenticación de inscripción pueden ser adquiridos ventajosamente en el momento de la inscripción de un usuario u otro momento posterior alternativo. Por ejemplo, el motor de confianza (110) puede incluir la renovación o reexpedición periódica u otra renovación o reexpedición de datos de autenticación de inscripción.

De acuerdo con una realización, la comunicación desde el motor de transacción (205) hacia y desde el motor de autenticación (215) y el motor criptográfico (220) comprende comunicación segura como, por ejemplo, tecnología SSL convencional. Además, como se mencionó en lo anterior, los datos de las comunicaciones hacia y desde el depósito (210) pueden ser transferidos usando URL, URI, HTTP o documentos XML, teniendo cualquiera de los anteriores, ventajosamente, solicitudes de datos y formatos integrados en los mismos.

Como se menciona anteriormente, el depósito (210) puede comprender ventajosamente una pluralidad de instalaciones de almacenamiento de datos seguros. En una realización tal, las instalaciones de almacenamiento de datos seguros pueden estar configuradas de modo que un compromiso de la seguridad en una instalación de almacenamiento de datos individual no comprometerá las claves criptográficas o los datos de autenticación almacenados en la misma. Por ejemplo, de acuerdo con esta realización, se opera matemáticamente sobre las claves criptográficas y los datos de autenticación para aleatorizar estadística y sustancialmente los datos almacenados en cada instalación de almacenamiento de datos. De acuerdo con una realización, la aleatorización de los datos de una instalación de almacenamiento de datos individual hace que esos datos resulten indescifrables. Así, el compromiso de una instalación almacenamiento de datos individual solo produce un número impredecible aleatorizado y no compromete la seguridad de ninguna clave criptográfica o los datos de autenticación en su conjunto.

La figura 2 también ilustra el motor de confianza (110) que incluye el motor de autenticación (215). De acuerdo con una realización, el motor de autenticación (215) comprende un comparador de datos configurado para comparar datos procedentes del motor de transacción (205) con datos procedentes del depósito (210). Por ejemplo, durante la autenticación, un usuario suministra datos de autenticación actuales al motor de confianza (110) de modo que el motor de transacción (205) recibe los datos de autenticación actuales. Como se menciona en lo anterior, el motor de transacción (205) reconoce las solicitudes de datos, preferentemente en el URL o el URI, y encamina los datos de autenticación al motor de autenticación (215). Por otra parte, en el momento de la solicitud, el depósito (210) reenvía los datos de autenticación de inscripción que corresponden al usuario al motor de autenticación (215). Así, el motor de autenticación (215) tiene tanto los datos de autenticación actuales como los datos de autenticación de inscripción para su comparación.

De acuerdo con una realización, las comunicaciones hacia el motor de autenticación comprenden comunicaciones seguras como, por ejemplo, tecnología SSL. Además, puede proporcionarse seguridad dentro de los componentes del motor de confianza (110) como, por ejemplo, supercifrado usando tecnologías de clave pública. Por ejemplo, de

acuerdo con una realización, el usuario cifra los datos de autenticación actuales con la clave pública del motor de autenticación (215). Además, el depósito (210) también cifra los datos de autenticación de inscripción con la clave pública del motor de autenticación (215). De este modo, solo puede usarse la clave privada del motor de autenticación para descifrar las transmisiones.

Como se muestra 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 tratamiento criptográfico, configurado para proporcionar ventajosamente funciones criptográficas convencionales como, por ejemplo, funcionalidad de infraestructura de clave pública (PKI). Por ejemplo, el motor criptográfico (220) puede expedir 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 reenviadas al depósito (210) de modo 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) aleatoriza y divide al menos los datos de clave criptográfica privada, almacenando de ese modo solo los datos divididos aleatorizados. De manera similar a la división de los datos de autenticación de inscripción, el proceso 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 realizadas por, el motor de autenticación (215).

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

La figura 2 también ilustra el motor de confianza (110) que tiene la memoria de almacenamiento masivo (225). Como se menciona en lo anterior, el motor de transacción (205) guarda datos que corresponden a un registro de auditoría y almacena tales datos en el dispositivo de memoria de almacenamiento masivo (225). De manera similar, de aucerdo con una realización de la invención, el depósito (210) guarda los datos que corresponden a un registro de auditoría y almacena tales datos en el dispositivo de almacenamiento masivo (225). Los datos de registro de auditoría del depósito son similares a los del motor de transacción (205) porque los datos de registro de auditoría comprenden un registro de las solicitudes recibidas por el depósito (210) y la respuesta del mismo. Además, la memoria de almacenamiento masivo (225) puede usarse para almacenar certificados digitales que tienen la clave pública de un usuario contenida en los mismos.

Aunque el motor de confianza (110) se describe con referencia a sus realizaciones preferentes y alternativas, la invención no pretende estar limitada por las mismas. Más bien, un experto en la materia reconocerá en la descripción de este documento un gran número de alternativas para el motor de confianza (110). Por ejemplo, el motor de confianza (110) puede realizar ventajosamente solo la autenticación o, alternativamente, solo algunas o todas las funciones criptográficas, tales como el cifrado y el descifrado de datos. De acuerdo con tales realizaciones, uno de entre el motor de autenticación (215) y el motor criptográfico (220) puede ser suprimido ventajosamente, creando de ese modo un diseño más sencillo para el motor de confianza (110). Además, el motor criptográfico (220) también puede comunicarse con una autoridad de certificación de modo que la autoridad de certificación esté incorporada dentro del motor de confianza (110). De acuerdo con otra realización, el motor de confianza (110) puede realizar ventajosamente la autenticación y una o más funciones criptográficas como, por ejemplo, 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 un hilo de tratamiento y un hilo de escucha. El sistema operativo (305) puede ser ventajosamente similar a los encontrados en servidores de gran volumen convencionales como, por ejemplo, servidores web proporcionados por Apache. El hilo de escucha monitoriza la comunicación entrante procedente de uno de entre el enlace del comunicación (125), el motor de autenticación (215) y el motor criptográfico (220) para el flujo de datos de entrada. El hilo de tratamiento reconoce estructuras de datos particulares del flujo de datos de entrada como, por ejemplo, las estructuras de datos anteriores, encaminando de ese modo los datos de entrada a uno de entre enlace de comunicación (125), el depósito (210), el motor de autenticación (215), el motor criptográfico (220) o la memoria de almacenamiento masivo (225). Como se muestra en la figura 3, los datos de entrada y de salida pueden ser asegurados ventajosamente, por ejemplo, mediante tecnología 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 ligero de acceso a directorios (LDAP). Los servidores de directorio LDAP son proporcionados por una amplia variedad de fabricantes tales como Netscape, ISO y otros. La figura 4 también muestra que el servidor de

directorio preferentemente almacena datos (405) que corresponden a las claves criptográficas y datos (410) que corresponden a los datos de autenticación de inscripción. De acuerdo con una realización, el depósito (210) comprende una estructura de memoria lógica individual que indexa datos de autenticación y datos de clave criptográfica a una ID de usuario única. La estructura de memoria lógica individual incluye preferentemente mecanismos para asegurar un alto grado de confianza, o seguridad, en los datos almacenados en la misma. Por ejemplo, la ubicación física del depósito (210) puede incluir ventajosamente un gran número de medidas de seguridad convencionales tales como acceso limitado por parte de los empleados, sistemas de vigilancia modernos y similares. Además de, o en lugar de, las medidas de seguridad físicas, el sistema informático o servidor puede incluir ventajosamente soluciones por software para proteger los datos almacenados. Por ejemplo, el depósito (210) puede crear y almacenar ventajosamente datos (415) que corresponden a un registro de auditoría de acciones emprendidas. Además, las comunicaciones entrantes y salientes pueden ser cifradas ventajosamente con cifrado de clave pública junto con tecnologías SSL convencionales.

Según otra realización, el depósito (210) puede comprender instalaciones de almacenamiento de datos distintas y separadas físicamente como se describe con más detalle con referencia a la figura 7.

La figura 5 ilustra un diagrama de bloques del motor de autenticación (215) de la figura 2 de acuerdo con aspectos de una realización de la invención. De manera similar al motor de transacción (205) de la figura 3, el motor de autenticación (215) comprende un sistema operativo (505) que tiene al menos un hilo de escucha y uno de tratamiento de una versión modificada de un servidor web convencional como, por ejemplo, los servidores web proporcionados por Apache. Como se muestra en la figura 5, el motor de autenticación (215) incluye acceso a al menos una clave privada (510). La clave privada (510) puede usarse ventajosamente, por ejemplo, para descifrar datos procedentes del motor de transacción (205) o del depósito (210), los cuales fueron cifrados con una clave pública correspondiente del motor de autenticación (215).

La figura 5 también ilustra el motor de autenticación (215) que comprende un comparador (515), un módulo de división de datos (520) y un módulo de ensamblaje de datos (525). De acuerdo con la realización anterior de la invención, el comparador (515) incluye tecnología capaz de comparar patrones potencialmente complejos relacionados con los datos de autenticación biométrica anteriores. La tecnología puede incluir hardware, software o soluciones combinadas para comparaciones de patrones como, por ejemplo, las que representan patrones de huellas dactilares o patrones de voz. Además, de acuerdo con una realización, el comparador (515) del motor de autenticación (215) puede comparar ventajosamente troceos convencionales de documentos con el fin de dar un resultado de 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 encargarse ventajosamente de las circunstancias que rodean un intento de autenticación como, por ejemplo, la hora del día, la dirección IP o la máscara de subred, el perfil de adquisición, la dirección de correo electrónico, el número de serie o la ID del procesador o similares.

Por otra parte, la naturaleza de las comparaciones de datos biométricos puede dar como resultado que se produzcan grados variables de confidencia a partir de la coincidencia de los datos de autenticación biométrica actuales con los datos de inscripción. Por ejemplo, a diferencia de una contraseña tradicional que solo puede devolver una coincidencia positiva o negativa, puede determinarse que una huella dactilar es una coincidencia parcial, por ejemplo un 90 % de coincidencia, un 75 % de coincidencia o un 10 % de coincidencia, más que ser simplemente correcta o incorrecta. Otros identificadores biométricos tales como el análisis de impresión de voz o el reconocimiento facial pueden compartir esta propiedad de autenticación probabilística, más que autenticación absoluta.

Cuando se trabaja con tal autenticación probabilística o en otros casos en los que una autenticación se considera menos que absolutamente fiable, es deseable aplicar la heurística (530) para determinar si el nivel de confidencia en la autenticación proporcionada es suficientemente alto como para autenticar la transacción que se está efectuando.

En ocasiones se dará el caso en que la transacción en cuestión es una transacción de valor relativamente bajo donde es aceptable que sea autenticada a un nivel de confidencia más bajo. Esto podría incluir una transacción que tuviera un bajo valor monetario asociado a la misma (por ejemplo, una adquisición de 10 $) o una transacción con riesgo bajo (por ejemplo, la admisión en un sitio web solo para miembros).

A la inversa, para autenticar otras transacciones, puede ser deseable requerir un alto grado de confidencia en la autenticación antes de permitir que la transacción continúe. Tales transacciones pueden incluir transacciones de gran valor monetario (por ejemplo, la firma de un contrato de suministro de muchos millones de dólares) o una transacción con un alto riesgo si se produce una autenticación incorrecta (por ejemplo, el registro a distancia en un

ordenador gubernamental).

El uso de la heurística (530) en combinación con niveles de confidencia y valores de transacciones puede usarse como se describirá más adelante para permitir que el comparador proporcione un sistema de autenticación dinámico sensible al contexto.

De acuerdo con otra realización de la invención, el comparador (515) puede, ventajosamente, hacer un seguimiento de los intentos de autenticación para una transacción particular. Por ejemplo, cuando una transacción falla, el motor de confianza (110) puede solicitar al usuario que vuelva a introducir sus datos de autenticación actuales. El comparador (515) del motor de autenticación (215) puede emplear ventajosamente un limitador de intentos (535) para limitar el número de intentos de autenticación, prohibiendo de ese modo intentos por fuerza bruta de hacerse pasar por los datos de autenticación de un usuario. De acuerdo con una realización, el limitador de intentos (535) comprende un módulo de software que monitoriza las transacciones para repetir intentos de autenticación y, por ejemplo, limita a tres los intentos de autenticación para una transacción dada. Así, el limitador de intentos (535) limitará un intento automatizado de hacerse pasar por los datos de autenticación de un individuo a, por ejemplo, simplemente tres “oportunidades”. Tras tres fallos, el limitador de intentos (535) puede denegar ventajosamente intentos de autenticación adicionales. Tal denegación puede implementarse ventajosamente mediante, por ejemplo, el comparador (515) que devuelve un resultado negativo independientemente de los datos de autenticación actuales que son transmitidos. Por otra parte, el motor de transacción (205) puede bloquear ventajosamente cualquier intento de autenticación adicional perteneciente a una transacción en la cual han fallado previamente tres intentos.

El motor de autenticación (215) también incluye el módulo de división de datos (520) y el módulo de ensamblaje de datos (525). El módulo de división de datos (520) comprende ventajosamente un módulo de software, hardware, o combinado que tiene la capacidad de operar matemáticamente sobre diversos datos para aleatorizar sustancialmente y dividir los datos en porciones. De acuerdo con una realización, los datos originales no pueden ser recreados a partir de una porción individual. El módulo de ensamblaje de datos (525) comprende ventajosamente un módulo de software, hardware o combinado configurado para operar matemáticamente sobre las porciones sustancialmente aleatorizadas anteriores, de modo que la combinación de las mismas proporciona los datos descifrados originales. De acuerdo con una realización, el motor de autenticación (215) emplea el módulo de división de datos (520) para aleatorizar y dividir datos de autenticación de inscripción en porciones y emplea el módulo de ensamblaje de datos (525) para volver a ensamblar las porciones en datos de autenticación de inscripción 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. De manera similar 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 uno de tratamiento de una versión modificada de un servidor web convencional como, por ejemplo, los servidores web proporcionados por Apache. Como se muestra en la figura 6, el motor criptográfico (220) comprende un módulo de división de datos (610) y un módulo de ensamblaje de datos (620) que funcionan de manera similar a los de la figura 5. Sin embargo, de acuerdo con una realización, el módulo de división de datos (610) y el módulo de ensamblaje de datos (620) procesan datos de clave criptográfica, a diferencia de los datos de autenticación de inscripción anteriores. Aunque un experto en la materia reconocerá a partir de la descripción de este documento que el módulo de división de datos (910) y el módulo de división de datos (620) pueden ser combinados con los del motor de autenticación (215).

El motor criptográfico (220) también comprende un módulo de tratamiento criptográfico (625) configurado para realizar una, algunas o todas de un gran número de funciones criptográficas. De acuerdo con una realización, el módulo de tratamiento criptográfico (625) puede comprender módulos o programas de software, hardware o ambos. De acuerdo con otra realización, el módulo de tratamiento criptográfico (625) puede realizar comparaciones de datos, análisis sintáctico de datos, división de datos, separación de datos, troceo de datos, cifrado y descifrado de datos, verificación o creación de firma digital, generación de certificados digitales, almacenamiento o solicitudes, generación de claves criptográficas o similares. Por otra parte, un experto en la materia reconocerá a partir de la descripción de este documento que el módulo de tratamiento criptográfico (825) puede comprender ventajosamente un infraestructura de clave pública, tal como Pretty Good Privacy (PGP), un sistema de clave pública basado en RSA o un gran número de sistemas de gestión de claves alternativos. Además, el módulo de tratamiento criptográfico (625) puede realizar cifrado de clave pública, cifrado de clave simétrica o ambos. Además de lo anterior, el módulo de tratamiento criptográfico (625) puede incluir uno o más programas o módulos informáticos, hardware o ambos para implementar funciones de interoperabilidad transparentes e ininterrumpidas.

Un experto en la materia también reconocerá, a partir de la descripción de este documento, que la funcionalidad criptográfica puede incluir un gran número o diversidad de funciones relacionadas generalmente con sistemas de gestión de claves criptográficas.

La figura 7 ilustra un diagrama de bloques simplificado de un sistema de depósito (700) de acuerdo con aspectos de una realización de la invención. Como se muestra en la figura 7, el sistema de depósito (700) comprende ventajosamente múltiples instalaciones de almacenamiento de datos, por ejemplo, las instalaciones de almacenamiento de datos (D1), (D2), (D3) y (D4). Sin embargo, se entiende fácilmente por parte de cualquier experto en la materia que el sistema de depósito puede tener solo una instalación de almacenamiento de datos. De acuerdo con una realización de la invención, cada una de las instalaciones de almacenamiento de datos (D1) a (D4) puede comprender ventajosamente algunos o todos los elementos descritos con referencia al depósito (210) de la figura 4. De manera similar al depósito (210), las instalaciones de almacenamiento de datos (D1) a (D4) se comunican con el motor de transacción (205), el motor de autenticación (215) y el motor criptográfico (220), preferentemente a través de SSL convencional. Transfiriendo los enlaces de comunicación, por ejemplo, documentos XML. Las comunicaciones procedentes del motor de transacción (205) pueden incluir ventajosamente solicitudes de datos, donde la solicitud es difundida ventajosamente a la dirección IP de cada instalación de almacenamiento de datos (D1) a (D4). Por otra parte, el motor de transacción (205) puede difundir solicitudes a instalaciones de almacenamiento particulares basándose en un gran número de criterios como, por ejemplo, tiempo de respuesta, cargas del servidor, calendarios de mantenimiento o similares.

En respuesta a las solicitudes de datos procedentes del motor de transacción (205), el sistema de depósito (700) reenvía ventajosamente los datos almacenados al motor de autenticación (215) y el motor criptográfico (220). Los módulos de ensamblaje de datos respectivos reciben los datos reenviados y ensamblan los datos en formatos utilizables. Por otra parte, las comunicaciones del motor de autenticación (215) y el motor criptográfico (220) a las instalaciones de almacenamiento de datos (D1) a (D4) pueden incluir la transmisión de datos sensibles que han de ser almacenados. Por ejemplo, de acuerdo con una realización, el motor de autenticación (215) y el motor criptográfico (220) pueden emplear ventajosamente sus módulos de división de datos respectivos para dividir los datos sensibles en porciones indescifrables y luego transmitir una o más porciones indescifrables de los datos sensibles a una instalación de almacenamiento de datos particular.

De acuerdo con una realización, cada instalación de almacenamiento de datos, (D1) a (D4), comprende un sistema de almacenamiento separado e independiente como, por ejemplo, un servidor de directorio. De acuerdo con otra realización de la invención, el sistema de depósito (700) comprende múltiples sistemas de almacenamiento de datos independientes separados geográficamente. Distribuyendo los datos sensibles en instalaciones de almacenamiento distintas e independientes (D1) a (D4), de las cuales algunas o todos pueden estar ventajosamente separadas geográficamente, el sistema de depósito (700) proporciona redundancia junto con medidas de seguridad adicionales. Por ejemplo, de acuerdo con una realización, solo los datos procedentes de dos de las múltiples instalaciones de almacenamiento de datos, (D1) a (D4), son necesarios para descifrar y volver a ensamblar los datos sensibles. Así, hasta dos de las cuatro instalaciones de almacenamiento de datos (D1) a (D4) pueden estar inoperativas debido a mantenimiento, fallo del sistema, fallo de alimentación o similares, sin afectar a la funcionalidad del motor de confianza (110). Además, debido a que, de acuerdo en una realización, los datos almacenados en cada instalación de almacenamiento de datos son aleatorizados e indescifrables, el compromiso de cualquier instalación de almacenamiento de datos individual no compromete necesariamente los datos sensibles. Por otra parte, en la realización que tiene separación geográfica de las instalaciones de almacenamiento de datos, un compromiso de múltiples instalaciones remotas geográficamente se vuelve cada vez más difícil. De hecho, incluso a un empleado incontrolable le supondrá un gran desafío subvertir las múltiples instalaciones de almacenamiento de datos remotas geográficamente independientes necesarias.

Aunque el sistema de depósito (700) se describe con referencia a sus realizaciones preferentes y alternativas, la invención no pretende estar limitada por las mismas. Más bien, un experto en la materia reconocerá a partir de la descripción de este documento un gran número de alternativas para el sistema de depósito (700). Por ejemplo, el sistema de depósito (700) puede comprender una, dos o más instalaciones de almacenamiento de datos. Además, puede operarse matemáticamente sobre los datos sensibles de modo que sean necesarias porciones procedentes de dos o más instalaciones de almacenamiento de datos para volver a ensamblar y descifrar los datos sensibles.

Como se menciona en lo anterior, el motor de autenticación (215) y el motor criptográfico (220) incluyen cada uno un módulo de división de datos (520) y (610), respectivamente, para dividir cualquier tipo o forma de datos sensibles como, por ejemplo, texto, audio, vídeo, los datos de autenticación y los datos de clave criptográfica. La figura 8 ilustra un diagrama de flujo de un proceso de división de datos (800) realizado por el módulo de división de datos de

acuerdo con aspectos de una realización de la invención. Como se muestra en la figura 8, el proceso de división de datos (800) comienza en la etapa (805) cuando los datos sensibles “S” son recibidos por el módulo de división de datos del motor de autenticación (215) o el motor criptográfico (220). Preferentemente, en la etapa (810), el módulo de división de datos genera entonces un número, valor o cadena o conjunto de bits sustancialmente aleatorio, “A”. Por ejemplo, el número aleatorio A puede ser generado en un gran número de técnicas convencionales variables disponibles para cualquier experto en la materia, para producir números aleatorios de alta calidad adecuados para uso en aplicaciones criptográficas. Además, de acuerdo con una realización, el número aleatorio A comprende una longitud de bits que puede ser cualquier longitud adecuada, tal como más corta, más larga o igual que la longitud de bits de los datos sensibles, S.

Además, en la etapa (820), el proceso de división de datos (800) genera otro número estadísticamente aleatorio “C”. De acuerdo con la realización preferente de la invención, la generación de los números estadísticamente aleatorios A y C puede hacerse ventajosamente en paralelo. El módulo de división de datos combina entonces los números A y C con los datos sensibles S de modo que se generan nuevos números “B” y “D”. Por ejemplo, el número B puede comprender la combinación binaria de A XOR S y el número D puede comprender la combinación binaria de C XOR S. La función XOR o la función “OR exclusiva” es bien conocida por cualquier experto en la materia. Las combinaciones anteriores se producen preferentemente en las etapas (825) y (830), respectivamente, y, de acuerdo con una realización, las combinaciones anteriores también se producen en paralelo. El proceso de división de datos (800) pasa entonces a la etapa (835) donde los números aleatorios A y C y los números B y D son emparejados de modo que ninguna de las parejas contienen suficientes datos, por sí mismas, para reorganizar y descifrar los datos sensibles originales S. Por ejemplo, los números pueden ser emparejados de la siguiente manera: AC, AD, BC y BD. De acuerdo con una realización, cada una de las parejas anteriores es distribuida a uno de los depósitos (D1) a (D4) de la figura 7. De acuerdo con otra realización, cada una de las parejas anteriores es distribuida aleatoriamente a uno de los depósitos (D1) a (D4). Por ejemplo, durante un primer proceso de división de datos (800), la pareja AC puede ser enviada al depósito (D2) mediante, por ejemplo, una selección aleatoria de direcciones IP de (D2). Después, durante un segundo proceso de división de datos (800), la pareja AC puede ser enviada al depósito (D4) mediante, por ejemplo, una selección aleatoria de direcciones IP de (D4). Además, todas las parejas pueden ser almacenadas en un depósito y pueden ser almacenadas en ubicaciones separadas en dicho depósito.

Basándose en lo anterior, el proceso de división de datos (800) pone ventajosamente porciones de los datos sensibles en cada una de las cuatro instalaciones de almacenamiento de datos (D1) a (D4), de modo que ninguna instalación de almacenamiento de datos individual (D1) a (D4) incluye suficientes datos cifrados para recrear los datos sensibles originales S. Como se menciona en lo anterior, tal aleatorización de los datos en porciones cifradas inutilizables individualmente aumenta la seguridad y proporciona una confianza mantenida en los datos incluso si una de las instalaciones de almacenamiento de datos, (D1) a (D4), se vea comprometida.

Aunque el proceso de división de datos (800) se describe con referencia a su realización preferente, la invención no pretende estar limitada por la misma. Más bien, un experto en la materia reconocerá a partir de la descripción de este documento un gran número de alternativas para el proceso de división de datos (800). Por ejemplo, el proceso de división de datos puede dividir ventajosamente los datos en dos números, por ejemplo, un número A y un número B aleatorios y distribuir aleatoriamente A y B por dos instalaciones de almacenamiento de datos. Por otra parte, el proceso de división de datos (800) puede dividir ventajosamente los datos entre un gran número de instalaciones de almacenamiento de datos mediante la generación de números aleatorios adicionales. Los datos pueden ser divididos en cualquier unidad de tamaño deseado, seleccionado, predeterminado o asignado aleatoriamente, incluyendo, pero no limitada a, un bit, bits, *bytes*, *kilobytes*, *megabytes*, o mayor o cualquier combinación o secuencia de tamaños. Además, variar los tamaños de las unidades de datos que resultan del proceso de división puede hacer que los datos resulten más difíciles de restaurar a una forma utilizable, aumentando de ese modo la seguridad de los datos sensibles. Resulta inmediatamente evidente para cualquier experto en la materia que los tamaños de unidad de datos divididos pueden ser una amplia variedad de tamaños de unidad de datos o patrones de tamaños o combinaciones de tamaños. Por ejemplo, los tamaños de unidad de datos pueden seleccionarse o predeterminarse para que sean todos del mismo tamaño, un conjunto fijo de tamaños diferentes o combinaciones de tamaños o tamaños generados aleatoriamente. De manera similar, las unidades de datos pueden ser distribuidas en una o más cuotas de acuerdo con un tamaño de unidad de datos fijo o predeterminado, un patrón o combinación de tamaños de unidad de datos o un tamaño o tamaños de unidad de datos generados aleatoriamente por cuota.

Como se menciona en lo anterior, con el fin de recrear los datos sensibles S, las porciones de datos tienen que ser desaleatorizadas y reorganizadas. Este proceso puede producirse ventajosamente en los módulos de ensamblaje de datos, (525) y (620), del motor de autenticación (215) y el motor criptográfico (220), respectivamente. El módulo de ensamblaje de datos, por ejemplo, el módulo de ensamblaje de datos (525), recibe porciones de datos procedentes

de las instalaciones de almacenamiento de datos (D1) a (D4), y vuelve a ensamblar los datos en forma utilizable. Por ejemplo, de acuerdo con una realización donde el módulo de división de datos (520) empleaba el proceso de división de datos (800) de la figura 8, el módulo de ensamblaje de datos (525) usa porciones de datos procedentes de al menos dos de las instalaciones de almacenamiento de datos (D1) a (D4) para recrear los datos sensibles S. Por ejemplo, las parejas de AC, AD, BC y BD fueron distribuidas de modo que dos cualesquiera proporcionan uno de A y B, o C y D. Obsérvese que S = A XOR B o S = C XOR D indica que cuando el módulo de ensamblaje de datos recibe uno de A y B, o C y D, el módulo de ensamblaje de datos (525) puede volver a ensamblar ventajosamente los datos sensibles S. Así, el módulo de ensamblaje de datos (525) puede ensamblar los datos sensibles S, cuando, por ejemplo, recibe porciones de datos procedentes de al menos las dos primeras de las instalaciones de almacenamiento de datos (D1) a (D4) para responder a una solicitud de ensamblaje por parte del motor de confianza (110).

Basándose en los procesos de división y ensamblaje de datos anteriores, los datos sensibles S salen en formato utilizable solo en un área limitada del motor de confianza (110). Por ejemplo, cuando los datos sensibles S incluyen datos de autenticación de inscripción, solo se dispone de datos de autenticación de inscripción utilizables, no aleatorizados, en el motor de autenticación (215). Asimismo, cuando los datos sensibles S incluyen datos de clave criptográfica, solo se dispone de datos de clave criptográfica privada utilizables, no aleatorizados, en el motor criptográfico (220).

Aunque los procesos de división y ensamblaje de datos se describen con referencia a sus realizaciones preferentes, la invención no pretende estar limitada por las mismas. Más bien, un experto en la materia reconocerá a partir de la descripción de este documento un gran número de alternativas para dividir y volver a ensamblar los datos sensibles S. Por ejemplo, puede usarse cifrado de clave pública para asegurar más los datos en las instalaciones de almacenamiento de datos (D1) a (D4). Además, resulta inmediatamente evidente para cualquier experto en la materia que el módulo de división de datos descrito en este documento también es una realización separada y distinta de la presente invención que puede incorporarse en, combinarse con o hacerse parte de otro modo de cualquier sistema informático, paquete de software, base de datos o combinaciones de los mismos existentes u otras realizaciones de la presente invención, tal como el motor de confianza, el motor de autenticación, y el motor de transacción expuestos y descritos en este documento.

La figura 9A ilustra un flujo de datos de un proceso de inscripción (900) de acuerdo con aspectos de una realización de la invención. Como se muestra en la figura 9A, el proceso de inscripción (900) comienza en la etapa (905) cuando un usuario desea inscribirse con el motor de confianza (110) del sistema criptográfico (100). De acuerdo con esta realización, el sistema de usuario (105) incluye ventajosamente una miniaplicación del lado del cliente, tal como una basada en Java, que interroga al usuario para que introduzca datos de inscripción, tal como datos demográficos y datos de autenticación de inscripción. De acuerdo con una realización, los datos de autenticación de inscripción incluyen ID de usuario, contraseña(s), biometría(s) o similares. De acuerdo con una realización, durante el proceso de indagación, la miniaplicación del lado del cliente se comunica preferentemente con el motor de confianza (110) para asegurar que una ID de usuario escogida es única. Cuando la ID de usuario no es única, el motor de confianza (110) puede sugerir ventajosamente una ID de usuario única. La miniaplicación del lado del cliente recopila los datos de inscripción y transmite los datos de inscripción, por ejemplo, a través de un documento XML, al motor de confianza (110) y, en particular, al motor de transacción (205). De acuerdo con una realización, la transmisión es codificada con la clave pública del motor de autenticación (215).

De acuerdo con una realización, el usuario realiza una sola inscripción durante la etapa (905), del proceso de inscripción (900). Por ejemplo, el usuario se inscribe a sí mismo como una persona particular, tal como Joe User. Cuando Joe User desea inscribirse como Joe User, director ejecutivo de Mega Corp, entonces, de acuerdo con esta realización, Joe User se inscribe una segunda vez, recibe una segunda ID de usuario única y el motor de confianza (110) no asocia las dos identidades. De acuerdo con otra realización de la invención, el proceso de inscripción (900) proporciona múltiples identidades de usuario para una sola ID de usuario. Así, en el ejemplo anterior, el motor de confianza (110) asociará ventajosamente las dos identidades de Joe User. Como se entenderá por parte de un experto en la materia a partir de la descripción de este documento, un usuario puede tener muchas identidades, por ejemplo, Joe User el cabeza de familia, Joe User el miembro de las Fundaciones Benéficas y similares. Aun cuando el usuario puede tener múltiples identidades, de acuerdo con esta realización, el motor de confianza (110) almacena preferentemente solo un conjunto de datos de inscripción. Por otra parte, los usuarios pueden añadir, editar/actualizar o borrar ventajosamente identidades cuando se necesiten.

Aunque el proceso de inscripción (900) se describe con referencia a su realización preferente, la invención no pretende estar limitada por las mismas. Más bien, un experto en la materia reconocerá a partir de la descripción de

este documento un gran número de alternativas para recopilación de datos de inscripción y, en particular, datos de autenticación de inscripción. Por ejemplo, la miniaplicación puede ser una miniaplicación basada en modelo de objeto común (COM) o similares.

Por otra parte, el proceso de inscripción puede incluir una inscripción graduada. Por ejemplo, a un nivel de inscripción más bajo, el usuario puede inscribirse por el enlace de comunicación (125) sin producir documentación en cuanto a su identidad. De acuerdo con un mayor nivel de inscripción, el usuario se inscribe usando un tercero de confianza, tal como un notario digital. Por ejemplo, y el usuario puede aparecer en persona en el tercero de confianza, producir credenciales tales como un certificado de nacimiento, permiso de conducción, ID militar o similares, y el tercero de confianza puede incluir ventajosamente, por ejemplo, su firma digital en la presentación de inscripción. El tercero de confianza puede incluir un notario real, un organismo gubernamental tal como la Dirección General de Correos o el Departamento de Vehículos a Motor, una persona de recursos humanos en una gran compañía que inscribe un empleado o similares. Un experto en la materia entenderá, a partir de la descripción de este documento, que puede producirse un gran número de niveles variables de inscripción durante el proceso de inscripción (900).

Después de recibir los datos de autenticación de inscripción, en la etapa (915), el motor de transacción (205), usando tecnología SSL completa convencional reenvía los datos de autenticación de inscripción al motor de autenticación (215). En la etapa (920), el motor de autenticación (215) descifra los datos de autenticación de inscripción usando la clave privada del motor de autenticación (215). Además, el motor de autenticación (215) emplea el módulo de división de datos para operar matemáticamente sobre los datos de autenticación de inscripción para dividir los datos en al menos dos números aleatorizados indescifrables independientemente. Como se menciona en lo anterior, al menos dos números pueden comprender un número aleatorio estadísticamente y un número XORed binario. En la etapa (925), el motor de autenticación (215) reenvía cada porción de los números aleatorizados a una de las instalaciones de almacenamiento de datos (D1) a (D4). Como se menciona en lo anterior, el motor de autenticación (215) también puede aleatorizar ventajosamente qué porciones son transferidas a qué depósitos.

A menudo durante el proceso de inscripción (900), el usuario también deseará tener un certificado digital expedido de modo que pueda recibir documentos cifrados procedentes otros fuera del sistema criptográfico (100). Como se menciona en lo anterior, la autoridad de certificación (115) generalmente expide certificados digitales de acuerdo con uno o más de varios estándares convencionales. Generalmente, el certificado digital incluye una clave pública del usuario o el sistema que es conocida por todos.

Ya sea que el usuario solicita un certificado digital en la inscripción o en otro momento, la solicitud es transferida a través del motor de confianza (110) al motor de autenticación (215). De acuerdo con una realización, la solicitud incluye un documento XML que tiene, por ejemplo, el nombre propio del usuario. De acuerdo con la etapa (935), el motor de autenticación (215) transfiere la solicitud al motor criptográfico (220) que ordena al motor criptográfico (220) que genere una clave o un par de claves criptográficas.

En el momento de la solicitud, en la etapa (935), el motor criptográfico (220) genera al menos una clave criptográfica. De acuerdo con una realización, el módulo de tratamiento criptográfico (625) genera un par de claves, donde una clave se usa como clave privada y una se usa como clave pública. El motor criptográfico (220) almacena la clave privada y, de acuerdo con una realización, una copia de la clave pública. En la etapa (945), el motor criptográfico (220) transmite una solicitud de un certificado digital al motor de transacción (205). De acuerdo con una realización, la solicitud incluye ventajosamente una solicitud estandarizada tal como PKCS10 insertada, por ejemplo, en un documento XML. La solicitud de un certificado digital puede corresponder ventajosamente a una o más autoridades de certificación y el uno o más formatos estándar que las autoridades de certificación requieren.

En la etapa (950), el motor de transacción (205) reenvía esta solicitud a la autoridad de certificación (115) quien, en la etapa (955), devuelve un certificado digital. El certificado digital de retorno puede estar ventajosamente en un formato estandarizado tal como PKCS7 o en un formato en propiedad de una o más de las autoridades de certificación (115). En la etapa (960), el certificado digital es recibido por el motor de transacción (205), y una copia es reenviada al usuario y una copia es almacenada con el motor de confianza (110). El motor de confianza (110) almacena una copia del certificado de modo que el motor de confianza (110) no tendrá que depender de la disponibilidad de la autoridad de certificación (115). Por ejemplo, cuando el usuario desea enviar un certificado digital o un tercero solicita el certificado digital del usuario, la solicitud del certificado digital es enviada típicamente a la autoridad de certificación (115). Sin embargo, si la autoridad de certificación (115) está llevando a cabo mantenimiento o ha sido víctima de un fallo o un compromiso de seguridad, el certificado digital puede no estar

disponible.

En cualquier momento después de expedir las claves criptográficas, el motor criptográfico (220) puede emplear ventajosamente el proceso de división de datos (800) descrito anteriormente de modo que las claves criptográficas son divididas en números aleatorizados indescifrables independientemente. De manera similar a los datos de autenticación, en la etapa (965) el motor criptográfico (220) transfiere los números aleatorizados a las instalaciones de almacenamiento de datos (D1) a (D4).

Un experto en la materia reconocerá a partir de la descripción de este documento que el usuario puede solicitar un certificado digital en cualquier momento después de la inscripción. Por otra parte, las comunicaciones entre sistemas pueden incluir ventajosamente SSL completa o tecnologías de cifrado de clave pública. Por otra parte, el proceso de inscripción puede expedir múltiples certificados digitales procedentes de múltiples autoridades de certificación, incluyendo una o más autoridades de certificación en propiedad internas o externas al motor de confianza (110).

Como se describe en las etapas (935) a (960), una realización de la invención incluye la solicitud de un certificado que es almacenada finalmente en el motor de confianza (110). Debido a que, de acuerdo con una realización, el módulo de tratamiento criptográfico (625) expide las claves usadas por el motor de confianza (110), cada certificado corresponde a una clave privada. Por lo tanto, el motor de confianza (110) puede proporcionar ventajosamente interoperabilidad mediante la monitorización de los certificados poseídos por, o asociados con, un usuario. Por ejemplo, cuando el motor criptográfico (220) recibe una solicitud de una función criptográfica, el módulo de tratamiento criptográfico (625) puede investigar los certificados poseídos por el usuario solicitante para determinar si el usuario posee una clave privada que coincida con los atributos de la solicitud. Cuando existe tal certificado, el módulo de tratamiento criptográfico (625) puede usar el certificado o las claves públicas o privadas asociadas con el mismo, para realizar la función solicitada. Cuando no existe tal certificado, el módulo de tratamiento criptográfico (625) puede realizar de manera ventajosa y transparente varias acciones para intentar remediar la falta de una clave apropiada. Por ejemplo, la figura 9B ilustra un diagrama de flujo de un proceso de interoperabilidad (970), que de acuerdo con aspectos de una realización de la invención, describe las etapas anteriores para asegurar que el módulo de tratamiento criptográfico (625) realiza funciones criptográficas usando claves apropiadas.

Como se muestra en la figura 9B, el proceso de interoperabilidad (970) comienza con la etapa (972) donde el módulo de tratamiento criptográfico (925) determina el tipo de certificado deseado. De acuerdo con una realización de la invención, el tipo de certificado puede estar especificado ventajosamente en la solicitud de funciones criptográficas u otros datos proporcionados por el solicitante. De acuerdo con otra realización, el tipo de certificado puede establecerse mediante el formato de datos de la solicitud. Por ejemplo, el módulo de tratamiento criptográfico (925) puede reconocer ventajosamente que la solicitud corresponde a un tipo particular.

De acuerdo con una realización, el tipo de certificado puede incluir uno o más estándares de algoritmo, por ejemplo, RSA, ELGAMAL o similares. Además, el tipo de certificado puede incluir uno o más tipos de clave, tales como claves simétricas, claves públicas, claves de cifrado fuerte tales como claves de 256 bits, claves menos seguras o similares. Por otra parte, el tipo de certificado puede incluir actualizaciones o sustituciones de uno o más de los estándares de algoritmo o claves anteriores, uno o más formatos de mensaje o de datos, uno o más esquemas de encapsulación o codificación de datos, tales como Base 32 o Base 64. El tipo de certificado también puede incluir la compatibilidad con una o más aplicaciones o interfaces criptográficas de terceros, uno o más protocolos de comunicación, o uno o más estándares o protocolos de certificación. Un experto en la materia reconocerá a partir de la descripción de este documento que pueden existir otras diferencias en los tipos de certificados y las traducciones a y de esas diferencias pueden implementarse como se describe en este documento.

Una vez que el módulo de tratamiento criptográfico (625) determina el tipo de certificado, el proceso de interoperabilidad (970) pasa a la etapa (974) y determina si el usuario posee un certificado que coincida con el tipo determinado en la etapa (974). Cuando el usuario posee un certificado coincidente, por ejemplo, el motor de confianza (110) tiene acceso al certificado coincidente a través de, por ejemplo, antes del almacenamiento del mismo, el módulo de tratamiento criptográfico (825) sabe que una clave privada coincidente también está almacenada dentro del motor de confianza (110). Por ejemplo, la clave privada coincidente puede ser almacenada dentro del depósito (210) o el sistema de depósito (700). El módulo de tratamiento criptográfico (625) puede solicitar ventajosamente que la clave privada coincidente sea ensamblada, por ejemplo, desde el depósito (210) y después en la etapa (976), usar la clave privada coincidente para realizar acciones o funciones criptográficas. Por ejemplo, como se menciona en lo anterior, el módulo de tratamiento criptográfico (625) puede realizar ventajosamente troceo, comparaciones de troceo, cifrado o descifrado de datos, verificación o creación de firma digital o similares.

Cuando el usuario no posee un certificado coincidente, el proceso de interoperabilidad (970) pasa a la etapa (978) donde el módulo de tratamiento criptográfico (625) determina si el usuario posee un certificado con certificación cruzada. De acuerdo con una realización, la certificación cruzada entre autoridades de certificación se produce cuando una primera autoridad de certificación determina confiar en los certificados procedentes de una segunda autoridad de certificación. En otras palabras, la primera autoridad de certificación determina que los certificados procedentes de la segunda autoridad de certificación cumplen ciertos estándares de calidad, y por lo tanto, pueden ser “certificados” como equivalentes a los propios certificados de la primera autoridad de certificación. La certificación cruzada se vuelve más compleja cuando las autoridades de certificación expiden, por ejemplo, certificados que tienen niveles de confianza. Por ejemplo, la primera autoridad de certificación puede proporcionar tres niveles de confianza para un certificado particular, habitualmente basándose en el grado de fiabilidad en el proceso de inscripción, mientras que la segunda autoridad de certificación puede proporcionar siete niveles de confianza. La certificación cruzada puede seguir ventajosamente qué niveles y qué certificados procedentes de la segunda autoridad de certificación pueden ser sustituidos por qué niveles y qué certificados procedentes de la primera. Cuando la certificación cruzada precedente se efectúa oficial y públicamente entre dos autoridades de certificación, la correspondencia de certificados y niveles entre sí a menudo se denomina “concatenación”.

De acuerdo con otra realización de la invención, el módulo de tratamiento criptográfico (625) puede desarrollar ventajosamente certificaciones cruzadas fuera de las acordadas por las autoridades de certificación. Por ejemplo, el módulo de tratamiento criptográfico (625) puede acceder a una declaración de prácticas de certificación (CPS) de una primera autoridad de certificación u otra declaración de política publicada y usando, por ejemplo, los testigos de certificación requeridos por niveles de confianza particulares, hacer coincidir los certificados de la primera autoridad de certificación con los de otra autoridad de certificación.

Cuando, en la etapa (978), el módulo de tratamiento criptográfico (625) determina que los usuarios poseen un certificado con certificación cruzada, el proceso de interoperabilidad (970) pasa a la etapa (976), y realiza la acción o función criptográfica usando la clave pública con certificación cruzada, la clave privada o ambas. Alternativamente, cuando el módulo de tratamiento criptográfico (625) determina que el usuario no posee un certificado con certificación cruzada, el proceso de interoperabilidad (970) pasa a la etapa (980), donde el módulo de tratamiento criptográfico (625) selecciona una autoridad de certificación que expide el tipo de certificado solicitado o un certificado con certificación cruzada al mismo. En la etapa (982), el módulo de tratamiento criptográfico (625) determina si los datos de autenticación de inscripción de usuario, analizados en lo anterior, cumplen los requisitos de autenticación de la autoridad de certificación escogida. Por ejemplo, si el usuario inscrito por una red, por ejemplo, contestando preguntas demográficas y otras preguntas, los datos de autenticación proporcionados pueden establecer un nivel de confianza más bajo que un usuario que proporciona datos biométricos y que aparece ante un tercero como, por ejemplo, un notario. De acuerdo con una realización, los requisitos de autenticación anteriores pueden ser proporcionados ventajosamente en las CPS de la autoridad de certificación escogida.

Cuando el usuario ha proporcionado al motor de confianza (110) datos de autenticación de inscripción que cumplen los requisitos de la autoridad de certificación escogida, el proceso de interoperabilidad (970) pasa a la etapa (984), donde el módulo de tratamiento criptográfico (825) adquiere el certificado de la autoridad de certificación escogida. De acuerdo con una realización, el módulo de tratamiento criptográfico (625) adquiere el certificado siguiendo las etapas (945) a (960) del proceso de inscripción (900). Por ejemplo, el módulo de tratamiento criptográfico (625) puede emplear ventajosamente una o más claves públicas procedentes de uno o más de los pares de claves ya disponibles para el motor criptográfico (220) para solicitar el certificado de la autoridad de certificación. De acuerdo con otra realización, el módulo de tratamiento criptográfico (625) puede generar ventajosamente uno o más pares de claves nuevos y usar las claves públicas que corresponden a los mismos, para solicitar el certificado de la autoridad de certificación.

De acuerdo con otra realización, el motor de confianza (110) puede incluir ventajosamente uno o más módulos expedidores de certificados capaces de expedir uno o más tipos de certificado. De acuerdo con esta realización, el módulo expedidor de certificados puede proporcionar el certificado precedente. Cuando el módulo de tratamiento criptográfico (625) adquiere el certificado, el proceso de interoperabilidad (970) pasa a la etapa (976), y realiza la acción o función criptográfica usando la clave pública, la clave privada o ambas, que corresponden al certificado adquirido.

Cuando el usuario, en la etapa (982), no ha proporcionado al motor de confianza (110) datos de autenticación de inscripción que cumplan los requisitos de la autoridad de certificación escogida, el módulo de tratamiento criptográfico (625) determina, en la etapa (986), si existen otras autoridades de certificación que tengan requisitos de autenticación diferentes. Por ejemplo, el módulo de tratamiento criptográfico (625) puede buscar autoridades de

certificación que tengan requisitos de autenticación más bajos, pero aun así expidan los certificados escogidos o certificaciones cruzadas de los mismos.

Cuando existe la autoridad de certificación precedente que tiene requisitos más bajos, el proceso de interoperabilidad (970) pasa a la etapa (980) y escoge esa autoridad de certificación. Alternativamente, cuando no existe tal autoridad de certificación, en la etapa (988), el motor de confianza (110) puede solicitar testigos de autenticación adicionales del usuario. Por ejemplo, el motor de confianza (110) puede solicitar nuevos datos de autenticación de inscripción que comprendan, por ejemplo, datos biométricos. También, el motor de confianza (110) puede solicitar que el usuario aparezca ante un tercero de confianza y proporcione credenciales de autenticación apropiadas como, por ejemplo, apareciendo ante un notario con un permiso de conducción, una tarjeta de la seguridad social, una tarjeta bancaria, un certificado de nacimiento, una ID militar o similares. Cuando el motor de confianza (110) recibe datos de autenticación actualizados, el proceso de interoperabilidad (970) pasa a la etapa (984) y adquiere el certificado escogido precedente.

Mediante el proceso de interoperabilidad precedente (970), el módulo de tratamiento criptográfico (625) proporciona ventajosamente traducciones y conversiones transparentes e ininterrumpidas entre sistemas criptográficos diferentes. Un experto en la materia reconocerá a partir de la descripción de este documento un gran número de ventajas e implementaciones del sistema interoperable precedente. Por ejemplo, la etapa precedente (986) del proceso de interoperabilidad (970) puede incluir ventajosamente aspectos de arbitraje de confianza, analizados con más detalle más adelante, donde la autoridad de certificación puede aceptar, bajo circunstancias especiales, niveles más bajos de certificación cruzada. Además, el proceso de interoperabilidad (970) puede incluir asegurar la interoperabilidad entre y el empleo de revocaciones de certificados estándar tales como empleando listas de revocación de certificados (CRL), protocolos de estado de certificados en línea (OCSP) o similares.

La figura 10 ilustra un flujo de datos de un proceso de autenticación (1000) de acuerdo con aspectos de una realización de la invención. De acuerdo con una realización, el proceso de autenticación (1000) incluye recopilar datos de autenticación actuales procedentes de un usuario y compararlos con los datos de autenticación de inscripción del usuario. Por ejemplo, el proceso de autenticación (1000) comienza en la etapa (1005) donde un usuario desea realizar una transacción con, por ejemplo, un vendedor. Tales transacciones pueden incluir, por ejemplo, seleccionar una opción de adquisición, solicitar acceso a un área restringida o dispositivo del sistema de vendedor (120) o similares. En la etapa (1010), un vendedor proporciona al usuario una ID de transacción y una solicitud de autenticación. La ID de transacción puede incluir ventajosamente una cantidad de 192 bits que tiene una marca de tiempo de 32 bits concatenada con una cantidad aleatoria de 128 bits o un “valor ocasional”, concatenado con una constante específica del vendedor de 32 bits. Tal ID de transacción identifica de manera única la transacción de modo que las transacciones imitadoras pueden ser rechazadas por el motor de confianza (110).

La solicitud de autenticación puede incluir ventajosamente qué nivel de autenticación es necesario para una transacción particular. Por ejemplo, el vendedor puede especificar un nivel particular de confidencia que es requerido para la transacción en cuestión. Si no puede efectuarse la autenticación a este nivel de confidencia, como se analiza más adelante, la transacción no se producirá sin autenticación adicional por parte del usuario para aumentar el nivel de confidencia o un cambio en los términos de la autenticación entre el vendedor y el servidor. Estas cuestiones se analizan de manera más completa más adelante.

De acuerdo con una realización, la ID de transacción y la solicitud de autenticación pueden ser generadas ventajosamente por una miniaplicación del lado del vendedor u otro programa de software. Además, la transmisión de la ID de transacción y los datos de autenticación puede incluir uno o más documentos XML cifrados usando tecnología SSL convencional como, por ejemplo, ½ SSL o, en otras palabras, SSL autenticada en el lado del vendedor.

Después de que el sistema de usuario (105) recibe la ID de transacción y la solicitud de autenticación, el sistema de usuario (105) recopila los datos de autenticación actuales, incluyendo potencialmente información biométrica actual, del usuario. El sistema de usuario (105), en la etapa (1015), cifra al menos los datos de autenticación actuales “B” y la ID de transacción, con la clave pública del motor de autenticación (215) y transfiere los datos al motor de confianza (110). La transmisión comprende preferentemente documentos XML cifrados con al menos tecnología ½ SSL convencional. En la etapa (1020), el motor de transacción (205) recibe la transmisión, reconoce preferentemente el formato de datos o la solicitud en el URL o el URI y reenvía la transmisión al motor de autenticación (215).

Durante las etapas (1015) y (1020), el sistema de vendedor (120), en la etapa (1025), reenvía la ID de transacción y

la solicitud de autenticación al motor de confianza (110), usando la tecnología SSL completa preferente. Esta comunicación también puede incluir una ID de vendedor, aunque la identificación de vendedor también puede ser comunicada a través de una porción no aleatoria de la ID de transacción. En las etapas (1030) y (1035), el motor de transacción (205) recibe la comunicación, crea un registro en el registro de auditoría, y genera una solicitud para que los datos de autenticación de inscripción del usuario sean ensamblados desde las instalaciones de almacenamiento de datos (D1) a (D4). En la etapa (1040), el sistema de depósito (700) transfiere las porciones de los datos de autenticación de inscripción que corresponden al usuario al motor de autenticación (215). En la etapa (1045), el motor de autenticación (215) descifra la transmisión usando su clave privada y compara los datos de autenticación de inscripción con los datos de autenticación actuales proporcionados por el usuario.

La comparación de la etapa (1045) puede aplicar ventajosamente autenticación heurística sensible al contexto, como a la que se hace referencia en lo anterior y se analiza con más detalle más adelante. Por ejemplo, si la información biométrica recibida no coincide perfectamente, se obtiene como resultado una confidencia más baja. En realizaciones particulares, se sopesan el nivel de confidencia de la autenticación y la naturaleza de la transacción y los deseos tanto del usuario como del vendedor. De nuevo, esto se analiza con mayor detalle más adelante.

En la etapa (1050), el motor de autenticación (215) rellena la solicitud de autenticación con el resultado de la comparación de la etapa (1045). De acuerdo con una realización de la invención, la solicitud de autenticación se rellena con un resultado SÍ/NO o VERDADERO/FALSO del proceso de autenticación (1000). En la etapa (1055) la solicitud de autenticación rellenada es devuelta al vendedor para que el vendedor actúe en consecuencia, por ejemplo, permitiendo que el usuario complete la transacción que inició la solicitud de autenticación. De acuerdo con una realización, se pasa un mensaje de confirmación al usuario.

Basándose en lo anterior, el proceso de autenticación (1000) guarda ventajosamente los datos sensibles seguros y produce resultados configurados para mantener la integridad de los datos sensibles. Por ejemplo, los datos sensibles son ensamblados solo dentro del motor de autenticación (215). Por ejemplo, los datos de autenticación de inscripción son indescifrables hasta que son ensamblados en el motor de autenticación (215) por el módulo de ensamblaje de datos, y los datos de autenticación actuales son indescifrables hasta que son desempaquetados por la tecnología SSL convencional y la clave privada del motor de autenticación (215). Por otra parte, el resultado de la autenticación transmitido al vendedor no incluye los datos sensibles, y el usuario ni siquiera puede saber si produjo datos de autenticación válidos.

Aunque el proceso de autenticación (1000) de describe con referencia a sus realizaciones preferentes y alternativas, la invención no pretende estar limitada por las mismas. Más bien, un experto en la materia reconocerá a partir de la descripción de este documento un gran número de alternativas para el proceso de autenticación (1000). Por ejemplo, el vendedor puede ser sustituido ventajosamente por casi cualquier aplicación de solicitud, incluso las que residen con el sistema de usuario (105). Por ejemplo, una aplicación cliente, tal como Microsoft Word, puede usar una interfaz de programa de aplicación (API) o una API criptográfica (CAPI) para solicitar autenticación antes de desbloquear un documento. Alternativamente, un servidor de correo, una red, un teléfono celular, un dispositivo informático personal o móvil, una estación de trabajo o similares, pueden efectuar todos ellos solicitudes de autenticación que pueden ser rellenadas por el proceso de autenticación (1000). De hecho, después de proporcionar el proceso de autenticación de confianza anterior (1000), la aplicación o el dispositivo solicitante pueden proporcionar acceso a, o usar un gran número de dispositivos o sistemas electrónicos o informáticos.

Por otra parte, el proceso de autenticación (1000) puede emplear un gran número de procedimientos alternativos en caso de fallo de autenticación. Por ejemplo, un fallo de autenticación puede mantener la misma ID de transacción y solicitar que el usuario vuelva a introducir sus datos de autenticación actuales. Como se menciona en lo anterior, el uso de la misma ID de transacción permite que el comparador del motor de autenticación (215) monitorice y limite el número de intentos de autenticación para una transacción particular, creando de ese modo un sistema criptográfico más seguro (100).

Además, el proceso de autenticación (1000) puede emplearse ventajosamente para desarrollar soluciones elegantes de inicio de sesión único, tales como desbloquear una bóveda de datos sensibles. Por ejemplo, la autenticación exitosa o positiva puede proporcionar al usuario autenticado la capacidad de acceder automáticamente a cualquier número de contraseñas para un número casi ilimitado de sistemas y aplicaciones. Por ejemplo, la autenticación de un usuario puede proporcionar al usuario acceso a una contraseña, registro, credenciales financieras o similares, asociados con múltiples vendedores en línea, una red de área local, diversos dispositivos informáticos personales, proveedores de servicios de internet, proveedores de subastas, correderías de inversiones o similares. Empleando una bóveda de datos sensibles, los usuarios pueden escoger contraseñas verdaderamente grandes y aleatorias

porque ya no necesitan recordarlas mediante asociación. En cambio, el proceso de autenticación (1000) proporciona acceso a las mismas. Por ejemplo, un usuario puede escoger una cadena alfanumérica aleatoria que sea de una longitud de veinte dígitos en adelante en lugar de algo asociado con unos datos memorizables, un nombre, etc.

De acuerdo con una realización, una bóveda de datos sensibles asociada con un usuario dado puede ser almacenada ventajosamente en las instalaciones de almacenamiento de datos del depósito (210) o ser dividida y almacenada en el sistema de depósito (700). De acuerdo con esta realización, después de la autenticación de usuario positiva, el motor de confianza (110) entrega los datos sensibles solicitados como, por ejemplo, la contraseña apropiada a la aplicación solicitante. De acuerdo con otra realización, el motor de confianza (110) puede incluir un sistema separado para almacenar la bóveda de datos sensibles. Por ejemplo, el motor de confianza (110) puede incluir un motor de software independiente que implementa la funcionalidad de bóveda de datos y que reside de manera figurada “detrás” del sistema de seguridad de extremo frontal precedente del motor de confianza (110). De acuerdo con esta realización, el motor de software entrega los datos sensibles solicitados después de que el motor de software recibe una señal que indica la autenticación de usuario positiva procedente del motor de confianza (110).

En otra realización, la bóveda de datos puede implementarse mediante un sistema de terceros. De manera similar a la realización del motor de software, el sistema de terceros puede entregar ventajosamente los datos sensibles solicitados después de que el sistema de terceros recibe una señal que indica la autenticación de usuario positiva procedente del motor de confianza (110). De acuerdo con otra realización, la bóveda de datos puede implementarse en el sistema de usuario (105). Un motor de software del lado usuario puede entregar ventajosamente los datos anteriores después de recibir una señal que indica la autenticación de usuario positiva procedente del motor de confianza (110).

Aunque las bóvedas de datos anteriores se describen con referencia a realizaciones alternativas, un experto en la materia reconocerá a partir de la descripción de este documento un gran número de implementaciones adicionales de los mismos. Por ejemplo, una bóveda de datos particular puede incluir aspectos de algunas o todas las realizaciones anteriores. Además, cualquiera de las bóvedas de datos anteriores puede emplear una o más solicitudes de autenticación en momentos variables. Por ejemplo, cualquiera de las bóvedas de datos puede requerir autenticación cada una o más transacciones, periódicamente, cada una o más sesiones, cada acceso a una o más páginas web o sitios web, en uno o más intervalos especificados o similares.

La figura 11 ilustra un flujo de datos de un proceso de firma (1100) de acuerdo con aspectos de una realización de la invención. Como se muestra en la figura 11, el proceso de firma (1100) incluye etapas similares a las del proceso de autenticación (1000) descrito en lo anterior con referencia a la figura 10. De acuerdo con una realización de la invención, el proceso de firma (1100) en primer lugar autentica al usuario y luego realiza una o más de varias funciones de firma digital como se analizará con más detalle más adelante. De acuerdo con otra realización, el proceso de firma (1100) puede almacenar ventajosamente datos relacionados con el mismo, tales como troceos de mensajes o documentos o similares. Estos datos pueden usarse ventajosamente en una auditoría o cualquier otro evento como, por ejemplo, cuando una parte participante intenta rechazar una transacción.

Como se muestra en la figura 11, durante las etapas de autenticación, el usuario y el vendedor pueden ponerse de acuerdo ventajosamente en un mensaje como, por ejemplo, un contrato. Durante la firma, el proceso de firma (1100) asegura ventajosamente que el contrato firmado por el usuario es idéntico al contrato suministrado por el vendedor. Por lo tanto, de acuerdo con una realización, durante la autenticación, el vendedor y el usuario incluyen un troceo de sus copias respectivas del mensaje o contrato, en los datos transmitidos al motor de autenticación (215). Empleando solo un troceo de un mensaje o contrato, el motor de confianza (110) puede almacenar ventajosamente una cantidad de datos reducida significativamente, proporcionando un sistema criptográfico más eficiente y económico. Además, el troceo almacenado puede ser comparado ventajosamente con un troceo de un documento en cuestión para determinar si el documento en cuestión coincide con uno firmado por cualquiera de las partes. La capacidad de determinar si el documento es idéntico al relacionado con una transacción proporciona una prueba adicional que puede usarse contra una reivindicación de rechazo por una parte a una transacción.

En la etapa (1103), el motor de autenticación (215) ensambla los datos de autenticación de inscripción y los compara con los datos de autenticación actuales proporcionados por el usuario. Cuando el comparador del motor de autenticación (215) indica que los datos de autenticación de inscripción coinciden con los datos de autenticación actuales, el comparador del motor de autenticación (215) también compara el troceo del mensaje suministrado por el vendedor con el troceo del mensaje suministrado por el usuario. Así, el motor de autenticación (215) asegura ventajosamente que el mensaje aceptado por el usuario es idéntico al aceptado por el vendedor.

En la etapa (1105), el motor de autenticación (215) transmite una solicitud de firma digital al motor criptográfico (220). De acuerdo con una realización de la invención, la solicitud incluye un troceo del mensaje o contrato. Sin embargo, un experto en la materia reconocerá a partir de la descripción de este documento que el motor criptográfico (220) puede cifrar prácticamente cualquier tipo de dato, incluyendo, pero no limitado a, vídeo audio, biometría, imágenes o texto para formar la firma digital deseada. Volviendo a la etapa (1105), la solicitud de firma digital comprende preferentemente un documento XML comunicado mediante tecnologías SSL convencionales.

En la etapa (1110), el motor de autenticación (215) transmite una solicitud a cada una de las instalaciones de almacenamiento de datos (D1) a (D4), de modo que cada una de las instalaciones de almacenamiento de datos (D1) a (D4) transmite su porción respectiva de la clave o claves criptográficas que corresponden a una parte firmante. De acuerdo con otra realización, el motor criptográfico (220) emplea algunas o todas las etapas del proceso de interoperabilidad (970) analizado en lo anterior, de modo que el motor criptográfico (220) en primer lugar determina la clave o claves apropiadas que solicitar del depósito (210) o el sistema de depósito (700) para la parte firmante y adopta acciones para proporcionar claves coincidentes apropiadas. De acuerdo con otra realización, el motor de autenticación (215) o el motor criptográfico (220) pueden solicitar ventajosamente una o más de las claves asociadas con la parte firmante y almacenadas en el depósito (210) el sistema de depósito (700).

De acuerdo con una realización, la parte firmante incluye uno de entre el usuario y el vendedor o ambos. En tal caso, el motor de autenticación (215) solicita ventajosamente las claves criptográficas que corresponden al usuario y/o el vendedor. De acuerdo con otra realización, la parte firmante incluye el motor de confianza (110). En esta realización, el motor de confianza (110) está certificando que el proceso de autenticación (1000) autenticó correctamente al usuario, al vendedor o a ambos. Por lo tanto, el motor de autenticación (215) solicita la clave criptográfica del motor de confianza (110) como, por ejemplo, la clave que pertenece al motor criptográfico (220) para realizar la firma digital. De acuerdo con otra realización, el motor de confianza (110) realiza una función similar a un notario. En esta realización, la parte firmante incluye el usuario, el vendedor o ambos, junto con el motor de confianza (110). Así, el motor de confianza (110) proporciona la firma digital del usuario y/o el vendedor y luego indica con su propia firma digital que el usuario y/o el vendedor fueron autenticados correctamente. En esta realización, el motor de autenticación (215) puede solicitar ventajosamente el ensamblaje de las claves criptográficas que corresponden al usuario, el vendedor o ambos. De acuerdo con otra realización, el motor de autenticación (215) puede solicitar ventajosamente el ensamblaje de las claves criptográficas que corresponden al motor de confianza (110).

De acuerdo con otra realización, el motor de confianza (110) realiza funciones similares a un poder notarial. Por ejemplo, el motor de confianza (110) puede firmar digitalmente el mensaje en nombre de un tercero. En tal caso, el motor de autenticación (215) solicita las claves criptográficas asociadas con el tercero. De acuerdo con esta realización, el proceso de firma (1100) puede incluir ventajosamente la autenticación del tercero, antes de permitir las funciones similares a un poder notarial. Además, el proceso de autenticación (1000) puede incluir una comprobación de restricciones de terceros como, por ejemplo, la lógica de negocio o similares que dicta cuándo y en qué circunstancias puede usarse la firma de un tercero particular.

Basándose en lo anterior, en la etapa (1110), el motor de autenticación solicitaba las claves criptográficas procedentes de las instalaciones de almacenamiento de datos (D1) a (D4) que corresponden a la parte firmante. En la etapa (1115), las instalaciones de almacenamiento de datos (D1) a (D4) transmiten sus porciones respectivas de la clave criptográfica que corresponden a la parte firmante al motor criptográfico (220). De acuerdo con una realización, las transmisiones anteriores incluyen tecnologías SSL. De acuerdo con otra realización, las transmisiones anteriores pueden ser ventajosamente supercifradas con la clave pública del motor criptográfico (220).

En la etapa (1120), el motor criptográfico (220) ensambla las claves criptográficas anteriores de la parte firmante y cifra el mensaje con las mismas, formando de ese modo la(s) firma(s) digital(es). En la etapa (1125) del proceso de firma (1100), el motor criptográfico (220) transmite la(s) firma(s) digital(es) al motor de autenticación (215). En la etapa (1130), el motor de autenticación (215) transmite la solicitud de autenticación rellenada junto con una copia del mensaje troceado y la(s) firma(s) digital(es) al motor de transacción (205). En la etapa (1135), el motor de transacción (205) transmite un recibo que comprende la ID de transacción, una indicación de si la autenticación resultó exitosa y la(s) firma(s) digital(es) al vendedor. De acuerdo con una realización, la transmisión precedente puede incluir ventajosamente la firma digital del motor de confianza (110). Por ejemplo, el motor de confianza (110) puede cifrar el troceo del recibo con su clave privada, formando de ese modo una firma digital que ha de adjuntarse a la transmisión al vendedor.

De acuerdo con una realización, el motor de transacción (205) también transmite un mensaje de confirmación al

usuario. Aunque el proceso de firma (1100) se describe con referencia a sus realizaciones preferentes y alternativas, la invención no pretende estar limitada por las mismas. Más bien, un experto en la materia reconocerá a partir de la descripción de este documento un gran número de alternativas para el proceso de firma (1100). Por ejemplo, el vendedor puede ser sustituido por una aplicación de usuario, tal como una aplicación de correo electrónico. Por ejemplo, el usuario puede desear firmar digitalmente un correo electrónico particular con su firma digital. En tal realización, la transmisión a lo largo de todo el proceso de firma (1100) puede incluir ventajosamente solo una copia de un troceo del mensaje. Por otra parte, un experto en la materia reconocerá a partir de la descripción de este documento que un gran número de aplicaciones cliente pueden solicitar firmas digitales. Por ejemplo, las aplicaciones cliente pueden comprender procesadores de texto, hojas de cálculo, correos electrónicos, correo de voz, acceso a áreas restringidas del sistema o similares.

Además, un experto en la materia reconocerá a partir de la descripción de este documento que las etapas (1105) a (1120) del proceso de firma (1100) pueden emplear ventajosamente algunas o todas las etapas del proceso de interoperabilidad (970) de la figura (9B), proporcionando de ese modo interoperabilidad entre diferentes sistemas criptográficos que pueden, por ejemplo, necesitar procesar la firma digital bajo diferentes tipos de firma.

La figura 12 ilustra un flujo de datos de un proceso de cifrado/descifrado (1200) de acuerdo con aspectos de una realización de la invención. Como se muestra en la figura 12, el proceso de descifrado (1200) comienza autenticando el usuario que usa el proceso de autenticación (1000). De acuerdo con una realización, el proceso de autenticación (1000) incluye en la solicitud de autenticación, una clave de sesión síncrona. Por ejemplo, en las tecnologías de PKI convencionales, se entiende por parte de los expertos en la materia que cifrar o descifrar datos usando claves públicas y privadas es matemáticamente intensivo y puede requerir significativos recursos del sistema. Sin embargo, en los sistemas criptográficos de clave simétrica, o los sistemas donde el remitente y el receptor de un mensaje comparten una única clave común que se usa para cifrar y descifrar un mensaje, las operaciones matemáticas son significativamente más sencillas y más rápidas. Así, en las tecnologías PKI convencionales, el remitente de un mensaje generará la clave de sesión síncrona y cifrará el mensaje usando el sistema de clave simétrica más sencillo y más rápido. Después, el remitente cifrará la clave de sesión con la clave pública del receptor. La clave de sesión cifrada será adjuntada al mensaje cifrado de manera síncrona y ambos datos son enviados al receptor. El receptor usa su clave privada para descifrar la clave de sesión, y después usa la clave de sesión para descifrar el mensaje. Basándose en lo anterior, el sistema de clave simétrica más sencillo y más rápido se usa para la mayoría del proceso de cifrado/descifrado. Así, en el proceso de descifrado (1200), el descifrado supone ventajosamente que una clave síncrona ha sido cifrada con la clave pública del usuario. Así, como se menciona en lo anterior, la clave de sesión cifrada está incluida en la solicitud de autenticación.

Volviendo al proceso de descifrado (1200), después de que el usuario ha sido autenticado en la etapa (1205), el motor de autenticación (215) reenvía la clave de sesión cifrada al motor criptográfico (220). En la etapa (1210), el motor de autenticación (215) reenvía una solicitud a cada una de las instalaciones de almacenamiento de datos, (D1) a (D4), solicitando los datos de clave criptográfica del usuario. En la etapa (1215), cada instalación de almacenamiento de datos, (D1) a (D4), transmite su porción respectiva de la clave criptográfica al motor criptográfico (220). De acuerdo con una realización, la transmisión precedente es cifrada con la clave pública del motor criptográfico (220).

En la etapa (1220) del proceso de descifrado (1200), el motor criptográfico (220) ensambla la clave criptográfica y descifra la clave de sesión con la misma. En la etapa (1225), el motor criptográfico reenvía la clave de sesión al motor de autenticación (215). En la etapa (1227), el motor de autenticación (215) rellena la solicitud de autenticación incluyendo la clave de sesión descifrada, y transmite la solicitud de autenticación rellenada al motor de transacción (205). En la etapa (1230), el motor de transacción (205) reenvía la solicitud de autenticación junto con la clave de sesión a la aplicación o el vendedor solicitante. Después, de acuerdo con una realización, la aplicación o el vendedor solicitante usa la clave de sesión para descifrar el mensaje cifrado.

Aunque el proceso de descifrado (1200) se describe con referencia a sus realizaciones preferentes y alternativas, un experto en la materia reconocerá a partir de la descripción de este documento un gran número de alternativas para el proceso de descifrado (1200). Por ejemplo, el proceso de descifrado (1200) puede prescindir de cifrado de clave síncrona y confiar en tecnología de clave pública completa. En tal realización, la aplicación solicitante puede transmitir todo el mensaje al motor criptográfico (220), o puede emplear algún tipo de compresión o troceo reversible con el fin de transmitir el mensaje al motor criptográfico (220). Un experto en la materia también reconocerá a partir de la descripción de este documento que las comunicaciones anteriores pueden incluir ventajosamente documentos XML envueltos en tecnología SSL.

El proceso de cifrado/descifrado (1200) también permite cifrado de documentos u otros datos. Así, en la etapa (1235), una aplicación o un vendedor solicitante pueden transmitir ventajosamente al motor de transacción (205) del motor de confianza (110) una solicitud de la clave pública del usuario. La aplicación o el vendedor solicitante efectúan esta solicitud porque la aplicación o el vendedor solicitante usa la clave pública del usuario, por ejemplo, para cifrar la clave de sesión que se usará para cifrar el documento o mensaje. Como se menciona en el proceso de inscripción (900), el motor de transacción (205) almacena una copia del certificado digital del usuario, por ejemplo, en la memoria de almacenamiento masivo (225). Así, en la etapa (1240) del proceso de cifrado (1200), el motor de transacción (205) solicita el certificado digital al usuario procedente de la memoria de almacenamiento masivo (225). En la etapa (1245), la memoria de almacenamiento masivo (225) transmite el certificado digital que corresponde al usuario, al motor de transacción (205). En la etapa (1250), el motor de transacción (205) transmite el certificado digital a la aplicación o el vendedor solicitante. De acuerdo con una realización, la porción de cifrado del proceso de cifrado (1200) no incluye la autenticación de un usuario. Esto es porque el vendedor solicitante solo necesita la clave pública del usuario y no está solicitando ningún dato sensible.

Un experto en la materia reconocerá a partir de la descripción de este documento que si un usuario particular no tiene un certificado digital el motor de confianza (110) puede emplear algo de, o todo el proceso de inscripción (900) con el fin de generar un certificado digital para ese usuario particular. Después, el motor de confianza (110) puede iniciar el proceso de cifrado/descifrado (1200) y proporcionar de ese modo el certificado digital apropiado. Además, un experto en la materia reconocerá a partir de la descripción de este documento que las etapas (1220) y (1235) a (1250) del proceso de cifrado/descifrado (1200) pueden emplear ventajosamente algunas o todas las etapas del proceso de interoperabilidad de la figura 9B, proporcionado de ese modo interoperabilidad entre sistemas criptográficos diferentes que pueden, por ejemplo, necesitar procesar el cifrado.

La figura 13 ilustra un diagrama de bloques simplificado de un sistema de motor de confianza (1300) de acuerdo con aspectos de otra realización de la invención. Como se muestra en la figura 13, el sistema de motor de confianza (1300) comprende una pluralidad de motores de confianza distintos (1305), (1310), (1315) y (1320), respectivamente. Para facilitar una comprensión más completa de la invención, la figura 13 ilustra cada motor de confianza, (1305), (1310), (1315) y (1320) como teniendo un motor de transacción, un depósito y un motor de autenticación. Sin embargo, un experto en la materia reconocerá que cada motor de transacción puede comprender ventajosamente alguno, una combinación, o todos los elementos y canales de comunicación descritos con referencia a las figuras 1-8. Por ejemplo, una realización puede incluir ventajosamente motores de confianza que tienen uno o más motores de transacción, depósitos, y servidores criptográficos o cualquier combinación de los mismos.

De acuerdo con una realización de la invención, cada uno de los motores de confianza (1305), (1310), (1315) y (1320) están separados geográficamente, de modo que, por ejemplo, el motor de confianza (1305) puede residir en una primera ubicación, el motor de confianza (1310) puede residir en una segunda ubicación, el motor de confianza (1315) puede residir en una tercera ubicación y el motor de confianza (1320) puede residir en una cuarta ubicación. La separación geográfica precedente disminuye ventajosamente el tiempo de respuesta del sistema mientras que aumenta la seguridad del sistema de motor de confianza global (1300).

Por ejemplo, cuando un usuario se registra en el sistema criptográfico (100), el usuario puede ser el más cercano a la primera ubicación y puede desear ser autenticado. Como se describe con referencia a la figura 10, para ser autenticado, el usuario proporciona datos de autenticación actuales, tales como una biometría o similares, y los datos de autenticación actuales son comparados con los datos de autenticación de inscripción de ese usuario. Por lo tanto, de acuerdo con un ejemplo, el usuario proporciona ventajosamente datos de autenticación actuales al motor de confianza más cercano geográficamente (1305). El motor de transacción (1321) del motor de confianza (1305) reenvía entonces los datos de autenticación actuales al motor de autenticación (1322) que también reside en la primera ubicación. De acuerdo con otra realización, el motor de transacción (1321) reenvía los datos de autenticación actuales a uno o más de los motores de autenticación de los motores de confianza (1310), (1315), o (1320).

El motor de transacción (1321) también solicita el ensamblaje de los datos de autenticación de inscripción procedentes de los depósitos de, por ejemplo, cada uno de los motores de confianza, (1305) a (1320). De acuerdo con esta realización, cada depósito proporciona su porción de los datos de autenticación de inscripción al motor de autenticación (1322) del motor de confianza (1305). El motor de autenticación (1322) emplea entonces las porciones de datos cifrados procedentes de, por ejemplo, los dos primeros depósitos para responder, y ensambla los datos de autenticación de inscripción en forma descifrada. El motor de autenticación (1322) compara los datos de autenticación de inscripción con los datos de autenticación actuales y devuelve un resultado de autenticación al motor de transacción (1321) del motor de confianza (1305).

Basándose en lo anterior, el sistema de motor de confianza (1300) emplea el más cercano de una pluralidad de motores de confianza separados geográficamente, (1305) a (1320), para realizar el proceso de autenticación. De acuerdo con una realización de la invención, el encaminamiento de información al motor de transacción más cercano puede realizarse ventajosamente en miniaplicaciones del lado del cliente que se ejecutan en uno o más del sistema de usuario (105), el sistema de vendedor (120) o la autoridad de certificación (115). De acuerdo con una realización alternativa, puede emplearse un proceso de decisión más sofisticado para seleccionar de entre los motores de confianza (1305) a (1320). Por ejemplo, la decisión puede estar basada en la disponibilidad, la capacidad de funcionamiento, la velocidad de las conexiones, la carga, el rendimiento, la proximidad geográfica, o una combinación de los mismos, de un motor de confianza dado.

De este modo, el sistema de motor de confianza (1300) reduce su tiempo de respuesta mientras que mantiene las ventajas de seguridad asociadas con las instalaciones de almacenamiento de datos remotas geográficamente, tales como las analizadas con referencia a la figura 7 donde cada instalación de almacenamiento de datos almacena porciones aleatorizadas de datos sensibles. Por ejemplo, un compromiso de seguridad en, por ejemplo, el depósito (1325) del motor de confianza (1315) no compromete necesariamente los datos sensibles del sistema de motor de confianza (1300). Esto es porque el depósito (1325) contiene solo datos aleatorizados no descifrables que, sin más, son completamente inútiles.

De acuerdo con otra realización, el sistema de motor de confianza (1300) puede incluir ventajosamente múltiples motores criptográficos dispuestos de manera similar a los motores de autenticación. Los motores criptográficos pueden realizar ventajosamente funciones criptográficas tales como las descritas con referencia a las figuras 1-8. De acuerdo con otra realización, el sistema de motor de confianza (1300) puede sustituir ventajosamente los motores de autenticación múltiples por motores criptográficos múltiples, realizando de ese modo funciones criptográficas tales como las descritas con referencia a las figuras 1-8. De acuerdo con otra realización de la invención, el sistema de motor de confianza (1300) puede sustituir cada motor de autenticación múltiple por un motor que tiene algunas o todas las funcionalidades de los motores de autenticación, los motores criptográficos o ambos, como se describe en lo anterior.

Aunque el sistema de motor de confianza (1300) se describe con referencia a sus realizaciones preferentes y alternativas, un experto en la materia reconocerá que el sistema de motor de confianza (1300) puede comprender porciones de los motores de confianza (1305) a (1320). Por ejemplo, el sistema de motor de confianza (1300) puede incluir uno o más motores de transacción, uno o más depósitos, uno o más motores de autenticación o uno o más motores criptográficos o combinaciones de los mismos.

La figura 14 ilustra un diagrama de bloques simplificado de un sistema de motor de confianza (1400) de acuerdo con aspectos de otra realización de la invención. Como se muestra en la figura 14, el sistema de motor de confianza (1400) incluye múltiples motores de confianza (1405), (1410), (1415) y (1420). De acuerdo con una realización, cada uno de los motores de confianza (1405), (1410), (1415) y (1420), comprende algunos o todos los elementos del motor de confianza (110) descrito con referencia a las figuras 1-8. De acuerdo con esta realización, cuando las miniaplicaciones del lado del cliente del sistema de usuario (105), el sistema de vendedor (120), o la autoridad de certificación (115), se comunican con el sistema de motor de confianza (1400), esas comunicaciones son enviadas a la dirección IP de cada uno de los motores de confianza (1405) a (1420). Además, cada motor de transacción de cada uno de los motores de confianza (1405), (1410), (1415) y (1420), se comporta de manera similar al motor de transacción (1321) del motor de confianza (1305) descrito con referencia a la figura 13. Por ejemplo, durante un proceso de autenticación, cada motor de transacción de cada uno de los motores de confianza (1405), (1410), (1415) y (1420) transmite los datos de autenticación actuales a sus motores de autenticación respectivos y transmite una solicitud para ensamblar los datos aleatorizados almacenados en cada uno de los depósitos de cada uno de los motores de confianza (1405) a (1420). La figura 14 no ilustra todas estas comunicaciones, ya que tal ilustración de volvería demasiado compleja. Continuando con el proceso de autenticación, cada uno de los depósitos comunica entonces su porción de los datos aleatorizados a cada uno de los motores de autenticación de cada uno de los motores de confianza (1405) a (1420). Cada uno de los motores de autenticación de cada uno de los motores de confianza emplea su comparador para determinar si los datos de autenticación actuales coinciden con los datos de autenticación de inscripción proporcionados por los depósitos de cada uno de los motores de confianza (1405) a (1420). De acuerdo con esta realización, el resultado de la comparación por parte de cada uno de los motores de autenticación es transmitido entonces a un módulo de redundancia de los otros tres motores de confianza. Por ejemplo, el resultado del motor de autenticación procedente del motor de confianza (1405) es transmitido a los módulos de de redundancia de los motores de confianza (1410), (1415) y (1420). Así, el módulo de redundancia del motor de confianza (1405) recibe asimismo el resultado de los motores de autenticación procedente de los motores

de confianza (1410), (1415) y (1420).

La figura 15 ilustra un diagrama de bloques del módulo de redundancia de la figura 14. El módulo de redundancia comprende un comparador configurado para recibir el resultado de autenticación procedente de tres motores de autenticación y transmitir ese resultado al motor de transacción del cuarto motor de confianza. El comparador compara el resultado de autenticación procedente de los tres motores de autenticación y, si dos de los resultados concuerdan, el comparador concluye que el resultado de autenticación debería coincidir con el de los dos motores de autenticación concordantes. Este resultado es transmitido entonces de vuelta al motor de transacción que corresponde al motor de confianza no asociado con los tres motores de autenticación.

Basándose en lo anterior, el módulo de redundancia determina un resultado de autenticación a partir de los datos recibidos de motores de autenticación que están preferentemente alejados geográficamente del motor de confianza del módulo de redundancia. Proporcionando tal funcionalidad de redundancia, el sistema de motor de confianza (1400) asegura que un compromiso del motor de autenticación de uno de los motores de confianza (1405) a (1420), sea insuficiente para comprometer el resultado de autenticación del módulo de redundancia de ese motor de confianza particular. Un experto en la materia reconocerá que la funcionalidad de módulo de redundancia del sistema de motor de confianza (1400) también puede aplicarse al motor criptográfico de cada uno de los motores de confianza (1405) a (1420). Sin embargo, tal comunicación del motor criptográfico no se mostraba en la figura 14 para evitar la complejidad. Por otra parte, un experto en la materia reconocerá que un gran número de algoritmos alternativos de resolución de conflictos resultado de la autenticación para el comparador de la figura 15 son adecuados para su uso en la presente invención.

De acuerdo con otra realización de la invención, el sistema de motor de confianza (1400) puede emplear ventajosamente el módulo de redundancia durante las etapas de comparación criptográfica. Por ejemplo, algo o toda la descripción de módulo de redundancia precedente con referencia a las figuras 14 y 15 puede implementarse ventajosamente durante una comparación de troceo de documentos proporcionados por una o más partes durante una transacción particular.

Aunque la invención precedente se ha descrito en cuanto a ciertas realizaciones preferentes y alternativas, otras realizaciones resultarán evidentes para cualquier experto en la materia a partir de la descripción de este documento. Por ejemplo, el motor de confianza (110) puede expedir certificados a corto plazo, donde la clave criptográfica privada se da a conocer al usuario durante un periodo de tiempo predeterminado. Por ejemplo, los estándares de certificación actuales incluyen un campo de validez que puede establecerse que concluya después de una cantidad de tiempo predeterminada. Así, el motor de confianza (110) puede dar a conocer una clave privada a un usuario donde la clave privada sería válida, por ejemplo, durante 24 horas. De acuerdo con tal realización, el motor de confianza (110) puede expedir ventajosamente un nuevo par de claves criptográficas que han de ser asociadas con un usuario particular y después da a conocer la clave privada del nuevo par de claves criptográficas. Después, una vez que se da a conocer la clave criptográfica privada, el motor de confianza (110) concluye inmediatamente cualquier uso válido interno de tal clave privada, puesto que ya no puede ser garantizada por el motor de confianza (110).

Además, un experto en la materia reconocerá que el sistema criptográfico (100) o el motor de confianza (110) pueden incluir la capacidad de reconocer cualquier tipo de dispositivo tales como, pero no limitados a, un ordenador portátil; un teléfono celular, una red, un dispositivo biométrico o similares. De acuerdo con una realización, tal reconocimiento puede proceder de datos suministrados en la solicitud de un servicio particular tal como una solicitud de autenticación que conduce a acceso o uso, una solicitud de funcionalidad criptográfica o similares. De acuerdo con una realización, la solicitud precedente puede incluir un identificador de dispositivo único como, por ejemplo, un ID de procesador. Alternativamente, la solicitud puede incluir datos en un formato de datos reconocible particular. Por ejemplo, los teléfonos móviles y por satélite a menudo no incluyen la potencia de procesamiento para certificados de cifrado pesados de tipo X509.v3 completo y, por lo tanto, no los solicitan. De acuerdo con esta realización, el motor de confianza (110) puede reconocer el tipo de formato de datos presentado y responder solo de la misma manera.

En un aspecto adicional del sistema descrito anteriormente, puede proporcionarse autenticación sensible al contexto usando diversas técnicas como se describirá más adelante. La autenticación sensible al contexto, por ejemplo como se muestra en la figura 16, proporciona la posibilidad de evaluar no solo los datos actuales que son enviados por el usuario cuando intenta autenticarse, sino también las circunstancias que rodean la generación y distribución de esos datos. Tales técnicas también pueden soportar arbitraje de confianza específico de la transacción entre el usuario y el motor de confianza (110) o entre el vendedor y el motor de confianza (110), como se describirá más adelante.

Como se discutió anteriormente, la autenticación es el proceso de probar que un usuario es quien dice ser. Generalmente, la autenticación requiere demostrar algún hecho a una autoridad de autenticación. El motor de confianza (110) de la presente invención representa la autoridad en la cual un usuario debe autenticarse. El usuario debe demostrar al motor de confianza (110) que es quien dice ser: conociendo algo que solo debería conocer el usuario (autenticación basada en el conocimiento), teniendo algo que solo debería tener el usuario (autenticación basada en testigo) o siendo algo que solo debería ser el usuario (autenticación basada en biometría).

Ejemplos de autenticación basada en el conocimiento incluyen sin limitación una contraseña, un número PIN o una combinación de bloqueo. Ejemplos de autenticación basada en testigo incluyen sin limitación una llave de casa, una tarjeta de crédito física, un permiso de conducir o un número de teléfono particular. Ejemplos de autenticación basada en biometría incluyen sin limitación una huella dactilar, análisis de escritura a mano, escáner facial, escáner de mano, escáner de oreja, escáner de iris, patrón vascular, ADN, análisis de voz o un escáner de retina.

Cada tipo de autenticación tiene ventajas y desventajas particulares y cada una proporciona un nivel de seguridad diferente. Por ejemplo, generalmente es más difícil crear una huella dactilar falsa que coincida con la de cualquier otra persona que oír por casualidad la contraseña de alguien y repetirla. Cada tipo de autenticación también requiere que la autoridad de autenticación conozca un tipo de datos diferente con el fin de verificar a alguien usando esa forma de autenticación.

Tal como se usa en este documento, “autenticación” se referirá en líneas generales al proceso global de verificar que la identidad de alguien es quien dice ser. Una “técnica de autenticación” se referirá a un tipo de autenticación particular basada en un conocimiento, testigo físico o lectura biométrica particular. “Datos de autenticación” se refiere a información que es enviada a, o demostrada de otro modo a, una autoridad de autenticación con el fin de establecer la identidad. “Datos de inscripción” se referirá a los datos que son presentados inicialmente a una autoridad de autenticación con el fin de establecer una línea base para la comparación con datos de autenticación. Una “instancia de autenticación” se referirá a los datos asociados con un intento de autenticar mediante una técnica de autenticación.

Los protocolos y comunicaciones internos implicados en el proceso de autenticar un usuario se describen con referencia a la figura 10 anterior. La parte de este proceso dentro de la cual tiene lugar la autenticación sensible al contexto se produce dentro de la etapa de comparación mostrada en la etapa (1045) de la figura 10. Esta etapa tiene lugar dentro del motor de autenticación (215) e implica ensamblar los datos de inscripción (410) recuperados del depósito (210) y comparar los datos de autenticación proporcionados por el usuario al mismo. Una realización particular de este proceso se muestra en la figura 16 y se describe más adelante.

Los datos de autenticación actuales proporcionados por el usuario y los datos de inscripción recuperados del depósito (210) son recibidos por el motor de autenticación (215) en la etapa (1600) de la figura 16. Estos dos conjuntos de datos pueden contener datos que están relacionados con técnicas de autenticación separadas. El motor de autenticación (215) separa los datos de autenticación asociados con cada instancia de autenticación individual en la etapa (1605). Esto es necesario para que los datos de autenticación sean comparados con el subconjunto apropiado de los datos de inscripción para el usuario (por ejemplo, los datos de autenticación por huella dactilar deberían ser comparados con los datos de inscripción por huella dactilar, en vez de los datos de inscripción por contraseña).

Generalmente, autenticar un usuario implica una o más instancias de autenticación individuales, dependiendo de las técnicas de autenticación de las que disponga el usuario. Estos procedimientos están limitados por los datos de inscripción que fueron proporcionados por el usuario durante su proceso de inscripción (si el usuario no proporcionó un escáner de retina cuando se inscribió, no podrá autenticarse usando un escáner de retina), así como los medios de los que puede disponer actualmente el usuario (por ejemplo, si el usuario no tiene un lector de huella dactilar en su ubicación actual, no será práctica la autenticación por huella dactilar). En algunos casos, una sola instancia de autenticación puede ser suficiente para autenticar un usuario; sin embargo, en ciertas circunstancias puede usarse una combinación de múltiples instancias de autenticación con el fin de autenticar de manera más confidencial un usuario para una transacción particular.

Cada instancia de autenticación consiste en datos relacionados con una técnica de autenticación particular (por ejemplo, huella dactilar, contraseña, tarjeta inteligente, etc.) y las circunstancias que rodean la captación y distribución de los datos para esa técnica particular. Por ejemplo, una instancia particular de intentar autenticar mediante contraseña generará no solo los datos relacionados con la contraseña en sí, sino también datos

circunstanciales, conocidos como “metadatos”, relacionados con ese intento de contraseña. Estos datos circunstanciales incluyen información tal como: el momento en que tuvo lugar la instancia de autenticación particular, la dirección de red desde la cual se distribuyó la información de autenticación, así como cualquier otra información conocida por los expertos en la materia que pueda determinarse acerca del origen de los datos de autenticación (el tipo de conexión, el número de serie del procesador, etc.).

En muchos casos, solo se dispondrá de una pequeña cantidad de metadatos circunstanciales. Por ejemplo, si el usuario está ubicado en una red que usa apoderados o traducción de dirección de red u otra técnica que enmascare la dirección del ordenador de partida, solo puede determinarse la dirección del apoderado o el encaminador. De manera similar, en muchos casos no se dispondrá de información tal como el número de serie del procesador debido a limitaciones del hardware o del sistema operativo que se use, la desactivación de tales características por parte del operador del sistema u otras limitaciones de la conexión entre el sistema del usuario y el motor de confianza (110).

Como se muestra en la figura 16, una vez que las instancias de autenticación individuales representadas dentro de los datos de autenticación son extraídas y separadas en la etapa (1605), el motor de autenticación (215) evalúa la fiabilidad de cada instancia al indicar que el usuario es quien reivindica ser. La fiabilidad para una sola instancia de autenticación se determinará generalmente basándose en varios factores. Estos pueden agruparse como factores relacionados con la fiabilidad asociada con la técnica de autenticación, que son evaluados en la etapa (1610) y factores relacionados con la fiabilidad de los datos de autenticación particulares proporcionados que son evaluados en la etapa (1815). El primer grupo incluye sin limitación la fiabilidad inherente de la técnica de autenticación que se usa, y la fiabilidad de los datos de inscripción que se usan con ese procedimiento. El segundo grupo incluye sin limitación el grado de coincidencia entre los datos de inscripción y los datos proporcionados con la instancia de autenticación, y los metadatos asociados con esa instancia de autenticación. Cada uno de estos factores puede variar independientemente de los otros.

La fiabilidad inherente de una técnica de autenticación está basada en cómo de difícil es para un impostor proporcionar datos correctos de cualquier otra persona, así como las tasas de error globales para la técnica de autenticación. Para procedimientos de autenticación basados en contraseñas y conocimiento, esta fiabilidad a menudo es bastante baja porque no hay nada que impida que alguien revele su contraseña a otra persona y que esa segunda persona use esa contraseña. Incluso un sistema basado en el conocimiento más complejo puede tener solo una fiabilidad relativamente moderada ya que el conocimiento puede ser transferido de persona a persona bastante fácilmente. La autenticación basada en testigo, tal como tener una tarjeta inteligente apropiada o usar un terminal particular para realizar la autenticación, es igualmente de baja fiabilidad usada por sí misma, ya que no existe garantía de que la persona correcta esté en posesión del testigo apropiado.

Sin embargo, las técnicas biométricas son más fiables inherentemente porque generalmente es difícil proporcionar a alguien más la capacidad de usar tus huellas dactilares de manera conveniente, incluso intencionadamente. Como subvertir las técnicas de autenticación biométrica es más difícil, la fiabilidad inherente de los procedimientos biométricos es generalmente más alta que la de las técnicas de autenticación basadas meramente en el conocimiento o un testigo. Sin embargo, incluso las técnicas biométricas pueden tener algunas ocasiones en las cuales se genera una aceptación falsa o un rechazo falso. Estos casos pueden verse reflejados por diferentes fiabilidades para diferentes implementaciones de la misma técnica biométrica. Por ejemplo, un sistema de coincidencia de huella dactilar proporcionado por una compañía puede proporcionar una fiabilidad más alta que uno proporcionado por una compañía diferente porque una usa óptica de mayor calidad o una mejor resolución de escaneo o alguna otra mejora que reduzca la aparición de aceptaciones falsas o rechazos falsos.

Obsérvese que esta fiabilidad puede expresarse de diferentes maneras. La fiabilidad se expresa deseablemente en alguna métrica que pueda ser usada por la heurística (530) y los algoritmos del motor de autenticación (215) para calcular el nivel de confianza de cada autenticación. Un modo preferente de expresar estas fiabilidades es como un porcentaje o fracción. Por ejemplo, a las huellas dactilares se les podría asignar una fiabilidad inherente del 97 % mientras que a las contraseñas solo se les podría asignar una fiabilidad inherente del 50 %. Los expertos en la materia reconocerán que estos valores particulares son meramente ejemplares y pueden variar entre implementaciones específicas.

El segundo factor para el cual debe evaluarse la fiabilidad es la fiabilidad de la inscripción. Esto es parte del proceso de “inscripción graduada” referido anteriormente. Este factor de fiabilidad refleja la fiabilidad de la identificación proporcionada durante el proceso de inscripción inicial. Por ejemplo, si el individuo se inscribe inicialmente de una manera en la que produce físicamente una prueba de su identidad ante un notario u otro funcionario público y, en ese momento, los datos de inscripción son registrados y notariados, los datos serán más fiables que los datos que

son proporcionados por una red durante la inscripción y solo son refrendados por una firma digital u otra información que no está ligada verdaderamente al individuo.

Otras técnicas de inscripción con niveles variables de fiabilidad incluyen sin limitación: la inscripción en una oficina física del operador del motor de confianza (110); la inscripción de el lugar de trabajo de un usuario; la inscripción en una oficina de correos o un organismo de expedición de pasaportes; la inscripción a través de una parte afiliada o de confianza en el operador del motor de confianza (110); la inscripción anónima o pseudoanónima en la cual la identidad inscrita todavía no está identificada con un individuo real particular, así como otros de tales medios conocidos en la técnica.

Estos factores reflejan la confianza entre el motor de confianza (110) y la fuente de identificación proporcionada durante el proceso de inscripción. Por ejemplo, si la inscripción se realiza en asociación con un empleador durante el proceso inicial de proporcionar una prueba de identidad, esta información puede considerarse sumamente fiable para los fines internos de la compañía, pero puede ser de menor grado de confianza para una agencia gubernamental o para un competidor. Por lo tanto, los motores de confianza manejados por cada una de estas otras organizaciones pueden asignar diferentes niveles de fiabilidad a esta inscripción.

De manera similar, los datos adicionales que son presentados a través de una red, pero que están autentificados por otros datos de confianza proporcionados durante una inscripción previa con el mismo motor de confianza (110) pueden considerarse tan fiables como lo eran los datos de inscripción originales, aun cuando los últimos datos fueran presentados a través de una red abierta. En tales circunstancias, una notarización posterior aumentará eficazmente el nivel de fiabilidad asociado con los datos de inscripción originales. De este modo, por ejemplo, una inscripción anónima o pseudoanónima puede ser elevada entonces a una inscripción plena demostrando a algún funcionario de inscripción la identidad del individuo que coincide con los datos inscritos.

Los factores de fiabilidad analizados anteriormente son generalmente valores que pueden determinarse con antelación a cualquier instancia de autenticación particular. Esto es porque están basados en la inscripción y la técnica, más que la autenticación real. En una realización, la etapa de generar fiabilidad basándose en estos factores implica consultar valores determinados previamente para esta técnica de autenticación particular y los datos de inscripción del usuario. En un aspecto adicional de una realización ventajosa de la presente invención, tales fiabilidades pueden estar incluidas con los datos de inscripción en sí. De este modo, estos factores son distribuidos automáticamente al motor de autenticación (215) junto con los datos de inscripción enviados desde el depósito (210).

Aunque estos factores pueden determinarse generalmente con antelación a cualquier instancia de autenticación individual, aun así tienen un efecto sobre cada instancia de autenticación que usa esa técnica particular de autenticación para ese usuario. Además, aunque los valores pueden cambiar a lo largo del tiempo (por ejemplo, si el usuario vuelve a inscribirse de una manera más fiable), no dependen de los datos de autenticación en sí. En comparación, los factores de fiabilidad asociados con datos de una sola instancia específica pueden variar en cada ocasión. Estos factores, como se analiza más adelante, deben ser evaluados para cada nueva autenticación con el fin de generar puntuaciones de fiabilidad en la etapa (1815).

La fiabilidad de los datos de autenticación refleja la coincidencia entre los datos proporcionados por el usuario en una instancia de autenticación particular y los datos proporcionados durante la inscripción de autenticación. Esta es la cuestión fundamental de si los datos de autenticación coinciden con los datos de inscripción para el individuo que el usuario está reivindicando ser. Normalmente, cuando los datos no coinciden, se considera que el usuario no está autenticado satisfactoriamente y la autenticación falla. La manera en que se evalúa esto puede cambiar dependiendo de la técnica de autenticación usada. La comparación de tales datos es realizada por la función del comparador (515) del motor de autenticación (215) como se muestra en la figura 5.

Por ejemplo, las coincidencias de contraseñas son evaluadas generalmente de manera binaria. En otras palabras, una contraseña es una coincidencia perfecta o una coincidencia fallida. Habitualmente no es deseable aceptar como incluso una coincidencia parcial una contraseña que sea parecida a la contraseña correcta si no es correcta exactamente. Por lo tanto, cuando se evalúa una autenticación por contraseña, la fiabilidad de la autenticación devuelta por el comparador (515) es típicamente o bien el 100 % (correcta) o bien el 0 % (incorrecta), sin posibilidad de valores intermedios.

Reglas similares a las de para las contraseñas se aplican generalmente a los procedimientos de autenticación basada en testigo, tal como tarjetas inteligentes. Esto es porque tener una tarjeta inteligente que tiene un

identificador similar o que es similar al correcto, aun así es exactamente tan incorrecto como tener cualquier otro testigo incorrecto. Por lo tanto, los testigos también tienden a ser autenticadores binarios: un usuario o tiene el testigo correcto o no lo tiene.

Sin embargo, ciertos tipos de datos de autenticación, tales como cuestionarios y biometrías, generalmente no son autenticadores binarios. Por ejemplo, una huella dactilar puede coincidir con una huella dactilar en grados variables. Hasta cierto punto, esto puede deberse a variaciones en la calidad de los datos captados ya sea durante la inscripción inicial o en autenticaciones posteriores. (Una huella dactilar puede estar emborronada o una persona puede tener una cicatriz o una quemadura aún curándose en un dedo particular). En otros casos los datos pueden coincidir imperfectamente porque la información en sí es un tanto variable y está basada en coincidencia de patrones. (Un análisis de voz puede parecer próximo pero no bastante correcto debido al ruido de fondo o la acústica del entorno en el que se graba la voz o porque la persona tiene un resfriado). Por último, en situaciones en las que se están comparando grandes cantidades de datos, simplemente puede darse el caso de que muchos de los datos coinciden bien, pero algunos no. (Un cuestionario de diez preguntas puede resultar en ocho respuestas correctas a preguntas personales, pero dos respuestas incorrectas). Por cualquiera de estas razones, a la coincidencia entre los datos de inscripción y los datos para una instancia de autenticación particular se le puede asignar deseablemente un valor de coincidencia parcial por parte el comparador (515). De este modo, podría decirse que la huella dactilar coincide en el 85 %, la impresión de voz coincide en el 65 % y el cuestionario coincide en el 80 %, por ejemplo.

Esta medida (grado de coincidencia) producida por el comparador (515) es el factor que representa la cuestión básica de si una autenticación es correcta o no. Sin embargo, como se analiza anteriormente, este es solo uno de los factores que pueden usarse al determinar la fiabilidad de una instancia de autenticación dada. Obsérvese también que aun cuando puede determinarse una coincidencia hasta algún grado parcial que, en última instancia, puede ser deseable proporcionar un resultado binario basándose en una coincidencia parcial. En un modo de funcionamiento alternativo, también es posible tratar las coincidencias parciales como binarias, es decir, o coincidencias perfectas (100 %) o fallidas (0 %), basándose en si el grado de coincidencia pasa o no un nivel de coincidencia umbral particular. Tal proceso puede usarse para proporcionar un nivel de coincidencia de simple aprobado/suspenso para sistemas que, de otro modo, producirían coincidencias parciales.

Otro factor que ha de considerarse al evaluar la fiabilidad de una instancia de autenticación dada concierne a las circunstancias bajo las cuales se proporcionan los datos de autenticación para esta instancia particular. Como se analiza anteriormente, las circunstancias se refieren a los metadatos asociados con una instancia de autenticación particular. Esto puede incluir sin limitación información tal como: la dirección de red del autenticador, hasta el punto en que pueda determinarse; el momento de la autenticación; el modo de transmisión de los datos de autenticación (línea telefónica, celular, red, etc.) y el número de serie del sistema del autenticador.

Estos factores pueden usarse para producir un perfil del tipo de autenticación que es solicitada normalmente por el usuario. Después, esta información puede usarse para determinar la fiabilidad al menos de dos maneras. Una manera es considerar si el usuario está solicitando autenticación de una manera que es coherente con el perfil normal de autenticación por parte de este usuario. Si el usuario normalmente efectúa solicitudes de autenticación desde una dirección de red durante días laborables (cuando está en el trabajo) y desde una dirección de red diferente durante las noches o los fines de semana (cuando está en casa), una autenticación que se produzca desde la dirección de casa durante el día laborable es menos fiable porque está fuera del perfil de autenticación normal. De manera similar, si el usuario se autentica normalmente usando una biometría de huella dactilar y por las noches, una autenticación que se origina durante el día usando solo una contraseña es menos fiable.

Un modo adicional en el que los metadatos circunstanciales pueden usarse para evaluar la fiabilidad de una instancia de autenticación es determinar cuánta corroboración proporciona la circunstancia de que el autenticador es el individuo que reivindica ser. Por ejemplo, si la autenticación procede de un sistema con un número de serie conocido que ha de ser asociado con el usuario, esto es un buen indicador circunstancial de que el usuario es quien reivindica ser. A la inversa, si la autenticación procede de una dirección de red que se sabe que está en Los Ángeles cuando se sabe que el usuario reside en Londres, esto es una indicación de que esta autenticación es menos fiable basándose en sus circunstancias.

También es posible que se ponga una *cookie* u otros datos electrónicos en el sistema que es usado por un usuario cuando interactúan con un sistema de vendedor o con el motor de confianza (110). Estos datos son escritos en la memoria del sistema del usuario y pueden contener una identificación que puede ser leída por un navegador web u otro software en el sistema de usuario. Si se permite que estos datos residan en el sistema de usuario entre

sesiones (una “*cookie* persistente”), pueden ser enviados con los datos de autenticación como prueba adicional del uso pasado de este sistema durante la autenticación de un usuario particular. En efecto, los metadatos de una instancia dada, particularmente una *cookie* persistente, pueden formar una especie de autenticador basado en testigo en sí.

Una vez que los factores de fiabilidad apropiados basados en la técnica y los datos de la instancia de autenticación se generan como se describió anteriormente en las etapas (1610) y (1615) respectivamente, se usan para producir una fiabilidad global para la instancia de autenticación proporcionada en la etapa (1620). Un medio de hacer esto es simplemente expresar cada fiabilidad como un porcentaje y luego multiplicarlas entre sí.

Por ejemplo, supongamos que los datos de autenticación están siendo enviados desde una dirección de red conocida por ser el ordenador doméstico del usuario completamente de acuerdo con el perfil de autenticación pasado del usuario (100 %), y la técnica que se usa es la identificación por huella dactilar (97 %) y los datos de huella dactilar iniciales fueron incluidos en la lista a través del empleador del usuario con el motor de confianza (110) (90 %) y la coincidencia entre los datos de autenticación y la plantilla de huella dactilar original en los datos de inscripción es muy buena (99 %). La fiabilidad global de esta instancia de autenticación podría calcularse entonces como el producto de estas fiabilidades: 100 % * 97 % * 90 % * 99 % - 86,4 % de fiabilidad.

Esta fiabilidad calculada representa la fiabilidad de una sola instancia de autenticación. La fiabilidad global de una sola instancia de autenticación también puede calcularse usando técnicas que tratan los diferentes factores de fiabilidad de manera diferente, por ejemplo usando fórmulas donde se asignan diferentes coeficientes de ponderación a cada factor de fiabilidad. Además, los expertos en la materia reconocerán que los valores reales usados pueden representar valores distintos de porcentajes y pueden usar sistemas no aritméticos. Una realización puede incluir un módulo usado por un solicitante de autenticación para fijar los coeficientes de ponderación para cada factor y los algoritmos usados al establecer la fiabilidad global de la instancia de autenticación.

El motor de autenticación (215) puede usar las técnicas anteriores y variaciones de las mismas para determinar la fiabilidad de una sola instancia de autenticación, indicada como la etapa (1620). Sin embargo, puede resultar útil en muchas situaciones de autenticación que múltiples instancias de autenticación sean proporcionadas al mismo tiempo. Por ejemplo, al intentar autenticarse uno mismo usando el sistema de la presente invención, un usuario puede proporcionar una identificación de usuario, datos de autenticación por huella dactilar, una tarjeta inteligente y una contraseña. En tal caso, se están proporcionando tres instancias de autenticación independientes al motor de confianza (110) para su evaluación. Pasando a la etapa (1625), si el motor de autenticación (215) determina que los datos proporcionados por el usuario incluyen más de una instancia de autenticación, entonces cada instancia será seleccionada a su vez como se muestra en la etapa (1630) y evaluada como se describe anteriormente en las etapas (1610), (1615) y (1620).

Obsérvese que muchos de los factores de fiabilidad analizados pueden variar de una de estas instancias a otra. Por ejemplo, la fiabilidad inherente de estas técnicas es probable que sea diferente, así como el grado de coincidencia proporcionado entre los datos de autenticación y los datos de inscripción. Además, el usuario puede haber proporcionado datos de inscripción en diferentes momentos y bajo diferentes circunstancias para cada una de estas técnicas, proporcionando diferentes fiabilidades de inscripción para cada una de estas instancias también. Por último, aun cuando las circunstancias bajo las cuales están siendo presentados los datos para cada una de estas instancias sean las mismas, el uso de tales técnicas puede ajustarse cada una al perfil del usuario de manera diferente, y por eso pueden asignarse diferentes fiabilidades circunstanciales. (Por ejemplo, el usuario puede usar normalmente su contraseña y su huella dactilar, pero no su tarjeta inteligente).

Como resultado, la fiabilidad final para cada una de estas instancias de autenticación puede ser diferente de una a otra. Sin embargo, usando múltiples instancias juntas, el nivel de confidencia global para la autenticación tenderá a aumentar.

Una vez que el motor de autenticación ha realizado las etapas (1610) a (1620) para todas las instancias de autenticación proporcionadas en los datos de autenticación, la fiabilidad de cada instancia se usa en la etapa (1635) para evaluar el nivel de confidencia de autenticación global. Este proceso de combinar las fiabilidades de instancias de autenticación individuales dentro del nivel de confidencia de autenticación puede ser modelado mediante diversos procedimientos relacionados con las fiabilidades individuales producidas y también puede encargarse de la interacción particular entre algunas de estas técnicas de autenticación. (Por ejemplo, múltiples sistemas basados en el conocimiento tales como contraseñas pueden producir menos confidencia que una sola contraseña e incluso una biometría bastante débil, tal como un análisis de voz básico).

Un medio en el que el motor de autenticación (215) puede combinar las fiabilidades de múltiples instancias de autenticación simultáneas para generar un nivel de confidencia final es multiplicar la falta de fiabilidad de cada instancia para llegar a una falta de fiabilidad total. La falta de fiabilidad es generalmente el porcentaje complementario de la fiabilidad. Por ejemplo, una técnica que tenga el 84 % de fiabilidad tiene el 16 % de falta de fiabilidad. Las tres instancias de autenticación descritas anteriormente (huella dactilar, tarjeta inteligente, contraseña) que producen fiabilidades del 86 %, el 75 % y el 72 % tendrían faltas de fiabilidad correspondientes del (100-86) %, (100-75) % y (100-72) % o el 14 %, el 25 % y el 28 %, respectivamente. Multiplicando estas faltas de fiabilidad, se obtiene una falta de fiabilidad acumulativa del 14 % * 25 % * 28 % - ,98 % de falta de fiabilidad, que corresponde a una fiabilidad del 99,02 %.

En un modo de funcionamiento adicional, pueden aplicarse factores y heurísticas adicionales (530) dentro del motor de autenticación (215) para dar cuenta de la interdependencia de diversas técnicas de autenticación. Por ejemplo, si alguien tiene acceso no autorizado a un ordenador doméstico particular, probablemente tiene acceso a la línea telefónica de esa dirección también. Por lo tanto, la autenticación basada en un número telefónico de origen así como en el número de serie del sistema autenticador no añade mucho a la confidencia global en la autenticación. Sin embargo, la autenticación basada en el conocimiento es independiente en gran parte de la autenticación basada en testigo (es decir, si alguien le roba su teléfono celular o sus claves, no es más probable que conozca su PIN o su contraseña que si no lo tuvieran).

Además, diferentes vendedores u otros solicitantes de autenticación pueden desear ponderar diferentes aspectos de la autenticación de manera diferente. Esto puede incluir el uso de factores de ponderación o algoritmos separados usados al calcular la fiabilidad de instancias independientes así como el uso de diferentes medios para evaluar eventos de autenticación con múltiples instancias.

Por ejemplo, los vendedores para ciertos tipos de transacciones, por ejemplo sistemas de correo electrónico corporativo, pueden desear autenticarse principalmente basándose en heurística y otros datos circunstanciales por defecto. Por lo tanto, pueden aplicar coeficientes de ponderación elevados a los factores relacionados con los metadatos y otra información relacionada con el perfil asociada con las circunstancias que rodean los eventos de autenticación. Esta disposición podría usarse para aliviar la carga sobre los usuarios durante las horas de funcionamiento normal, al requerir del usuario nada más que se registre en la máquina correcta durante las horas laborables. Sin embargo, otro vendedor puede ponderar las autenticaciones procedentes de una técnica particular con más peso, por ejemplo la coincidencia de huella dactilar, debido a una decisión política de que tal técnica es la más adecuada para la autenticación para los fines del vendedor particular.

Tales coeficientes de ponderación variables pueden ser definidos por el solicitante de autenticación al generar la solicitud de autenticación y enviados al motor de confianza (110) con la solicitud de autenticación en un modo de funcionamiento. Tales opciones también podrían ser fijadas como preferencias durante un proceso de inscripción inicial para el solicitante de autenticación y almacenadas dentro del motor de autenticación en otro modo de funcionamiento.

Una vez que el motor de autenticación (215) produce un nivel de confidencia de autenticación para los datos de autenticación proporcionados, este nivel de confidencia se usa para completar la solicitud de autenticación en la etapa (1640) y esta información es reenviada del motor de autenticación (215) al motor de transacción (205) para su inclusión en un mensaje al solicitante de autenticación.

El proceso descrito anteriormente es meramente ejemplar y los expertos en la materia reconocerán que las etapas no tienen que realizarse en el orden mostrado o que solo se desea que se realicen ciertas etapas o que puede desearse una diversidad de combinaciones de etapas. Además, ciertas etapas, tales como la evaluación de la fiabilidad de cada instancia de autenticación proporcionada, pueden llevarse a cabo en paralelo unas con otras si las circunstancias lo permiten.

En un aspecto adicional de esta invención, se proporciona un procedimiento para tener en cuenta las condiciones cuando el nivel de confidencia de autenticación producido por el proceso descrito anteriormente no satisface el nivel de confianza requerido del vendedor u otra parte que requiera la autenticación. En circunstancias tales como estas donde existe una brecha entre el nivel de confidencia proporcionado y el nivel de confianza deseado, el operador del motor de confianza (110) está en una posición para proporcionar oportunidades para que una o ambas partes proporcionen datos o requisitos alternativos con el fin de cerrar esta brecha de confianza. Este proceso se denominará “arbitraje de confianza” en este documento.

El arbitraje de confianza puede tener lugar dentro de una estructura de autenticación criptográfica como se describe anteriormente con referencia a las figuras 10 y 11. Como se muestra en las mismas, un vendedor u otra parte solicitarán autenticación de un usuario particular en asociación con una transacción particular. En una circunstancia, el vendedor simplemente solicita una autenticación, ya sea positiva o negativa, y después de recibir datos apropiados procedentes del usuario, el motor de confianza (110) proporcionará tal autenticación binaria. En circunstancias tales como estas, el grado de confidencia requerido con el fin de asegurar una autenticación positiva se determina basándose en preferencias fijadas dentro del motor de confianza (110).

Sin embargo, también es posible que el vendedor pueda solicitar un nivel particular de confianza con el fin de completar una transacción particular. Este nivel requerido puede estar incluido con la solicitud de autenticación (por ejemplo, autenticar este usuario al 98 % de confidencia) o puede ser determinado por el motor de confianza (110) basándose en otros factores asociados con la transacción (es decir, autenticar este usuario según resulte apropiado para esta transacción). Uno de tales factores podría ser el valor económico de la transacción. Para transacciones que tengan mayor valor económico, puede requerirse un grado de confianza más alto. De manera similar, para transacciones con alto grado de riesgo puede requerirse un alto grado de confianza. A la inversa, para transacciones de riesgo bajo o de valor bajo, pueden requerirse niveles de confianza más bajos por parte del vendedor u otro solicitante de autenticación.

El proceso del arbitraje de confianza se produce entre las etapas del motor de confianza (110) que reciben los datos de autenticación en la etapa (1050) de la figura 10 y la devolución de un resultado de autenticación al vendedor en la etapa (1055) de la figura 10. Entre estas etapas, el proceso que conduce a la evaluación de niveles de confianza y el arbitraje de confianza potencial se produce como se muestra en la figura 17. En circunstancias en las que se realiza una simple autenticación binaria, el proceso mostrado en la figura 17 se reduce a que el motor de transacción (205) compare directamente los datos de autenticación proporcionados con los datos de inscripción para el usuario identificado como se analiza anteriormente con referencia a la figura 10, señalando cualquier diferencia como una autenticación negativa.

Como se muestra en la figura 17, la primera etapa después de recibir los datos en la etapa (1050) es para que el motor de transacción (205) determine el nivel de confianza que se requiere para una autenticación positiva para esta transacción particular en la etapa (1710). Esta etapa puede ser realizada por uno de varios procedimientos diferentes. El nivel de confianza requerido puede ser especificado al motor de confianza (110) por el solicitante de autenticación en el momento en que se efectúa la solicitud de autenticación. El solicitante de autenticación también puede fijar una preferencia de antemano que es almacenada dentro del depósito (210) u otra memoria que sea accesible por parte del motor de transacción (205). Esta preferencia puede entonces ser leída y usada cada vez que se efectúa una solicitud de autenticación por parte de este solicitante de autenticación. La preferencia también puede estar asociada con un usuario particular como una medida de seguridad de modo que siempre se requiera un nivel particular de confianza con el fin de autenticar ese usuario, siendo almacenada la preferencia de usuario en el depósito (210) u otro medio de almacenamiento accesible por el motor de transacción (205). El nivel requerido también puede ser deducido por el motor de transacción (205) o el motor de autenticación (215) basándose en información proporcionada en la solicitud de autenticación, tal como el valor y el nivel de riesgo de la transacción que ha de ser autenticada.

En un modo de funcionamiento, un módulo de gestión de política u otro software que se use cuando se genera la solicitud de autenticación se usa para especificar el grado requerido de confianza para la autenticación de la transacción. Esto puede usarse para proporcionar una serie de reglas que se han de seguir cuando se asigna el nivel requerido de confianza basándose en las políticas que son especificadas dentro del módulo de gestión de política. Un modo ventajoso de funcionamiento para tal módulo es que esté incorporado con el servidor web de un vendedor con el fin de determinar correctamente el nivel requerido de confianza para transacciones iniciadas con el servidor web del vendedor. De este modo, a las solicitudes de transacción procedentes de usuarios se les puede asignar un nivel de confianza requerido de acuerdo con las políticas del vendedor y tal información puede ser reenviada al motor de confianza (110) junto con la solicitud de autenticación.

Este nivel de confianza requerido se correlaciona con el grado de certeza que el vendedor quiere tener de que el individuo que es autenticado es de hecho quien se identifica como tal. Por ejemplo, si la transacción es una donde el vendedor quiere un grado razonable de certeza porque las mercancías están cambiando de manos, el vendedor puede requerir un nivel del confianza del 85 %. Para una situación en la que el vendedor simplemente está autenticando el usuario para permitirle ver contenido solo para miembros o ejercer privilegios en una sala de charla, el riesgo de deterioro de la situación puede ser suficientemente pequeño como para que el vendedor requiera solo

un 60 % de nivel de confianza. Sin embargo, para entrar en un contrato de producción con un valor de decenas de miles de dólares, el vendedor puede requerir un nivel de confianza del 99 % o más.

Este nivel de confianza requerido representa una métrica con la cual el usuario debe autenticarse a sí mismo con el fin de completar la transacción. Si el nivel de confianza requerido es el 85 % por ejemplo, el usuario debe proporcionar autenticación al motor de confianza (110) suficiente para que el motor de confianza (110) diga con el 85 % de confidencia que el usuario es quien dice ser. Es el equilibrio entre este nivel de confianza requerido y el nivel de confidencia de autenticación que el produce o bien una autenticación positiva (a satisfacción del vendedor) o bien una posibilidad de arbitraje de confianza).

Como se muestra en la figura 17, después de que el motor de transacción (205) recibe el nivel de confianza requerido, compara en la etapa (1720) el nivel de confianza requerido con el nivel de confidencia de autenticación que el motor de autenticación (215) calculó para la autenticación actual (como se analiza con referencia a la figura 16). Si el nivel de confidencia de autenticación es más alto que el nivel de confianza requerido para la transacción en la etapa (1730), entonces el proceso pasa a la etapa (1740) donde una autenticación positiva para esta transacción es producida por el motor de transacción (205). Entonces será insertado un mensaje a este efecto dentro de los resultados de autenticación y será devuelto al vendedor por el motor de transacción (205) como se muestra en la etapa (1055) (véase la figura 10).

Sin embargo, si el nivel de confidencia de autenticación no cumple con el nivel de confianza requerido en la etapa (1730), entonces existe una brecha de confidencia para la autenticación actual, y en la etapa (1750) se lleva a cabo arbitraje de confianza. El arbitraje de confianza se describe de manera más completa con referencia a la figura 18 más adelante. Este proceso como se describe más adelante tiene lugar dentro del motor de transacción (205) del motor de confianza (110). Como no son necesarias la autenticación ni otras operaciones criptográficas para ejecutar el arbitraje de confianza (aparte de las requeridas para la comunicación SSL entre el moto de transacción (205) y otros componentes), el proceso puede realizarse fuera del motor de autenticación (215). Sin embargo, como se analiza más adelante, cualquier reevaluación de datos de autenticación u otros eventos criptográficos o de autenticación requerirá que el motor de transacción (205) vuelva a presentar los datos apropiados al motor de autenticación (215). Los expertos en la materia reconocerán que el proceso de arbitraje de confianza podría estar estructurado alternativamente para que tenga lugar parcialmente o por entero dentro del motor de autenticación (215) en sí.

Como se menciona anteriormente, el arbitraje de confianza es un proceso en el que el motor de confianza (110) media en una negociación entre el vendedor y el usuario en un intento de asegurar una autenticación positiva cuando sea apropiado. Como se muestra en la etapa (1805), el motor de transacción (205) en primer lugar determina si la situación actual es apropiada o no para el arbitraje de confianza. Esto puede determinarse basándose en las circunstancias de la autenticación, por ejemplo si esta autenticación ya ha sido a través de múltiples ciclos de arbitraje, así como siguiendo las preferencias del vendedor o el usuario, como se analizará con más detalle más adelante.

En las circunstancias tales que el arbitraje no es posible, el proceso pasa a la etapa (1810) donde el motor de transacción (205) genera una autenticación negativa y después la inserta dentro de los resultados de autenticación que son enviados al vendedor en la etapa (1055) (véase la figura 10). Un límite que puede usarse ventajosamente para impedir que las autenticaciones estén pendientes indefinidamente es fijar un periodo de tiempo límite desde la solicitud de autenticación inicial. De este modo, a cualquier transacción que no sea autenticada positivamente dentro del límite de tiempo se le deniega un arbitraje adicional y es autenticada negativamente. Los expertos en la materia reconocerán que tal límite de tiempo puede variar dependiendo de las circunstancias de la transacción y los deseos del usuario y el vendedor. También pueden establecerse limitaciones sobre el número de intentos que pueden efectuarse a la hora de proporcionar una autenticación satisfactoria. Tales limitaciones pueden ser tratadas por un limitador de intentos (535) como se muestra en la figura 5.

Si en la etapa (1805) no se prohíbe el arbitraje, el motor de transacción (205) entonces entablará negociación con una o las dos partes de la transacción. El motor de transacción (205) puede enviar un mensaje al usuario solicitando alguna forma de autenticación adicional con el fin de incrementar el nivel de confidencia de autenticación producido como se muestra en la etapa (1820). En la forma más simple, esto puede indicar simplemente que la autenticación fue insuficiente. También puede enviarse una solicitud para producir una o más instancias de autenticación adicionales para mejorar el nivel de confidencia global de la autenticación.

Si el usuario proporciona alguna instancia de autenticación adicional en la etapa (1825), entonces el motor de

transacción (205) añade estas instancias de autenticación a los datos de autenticación para la transacción y los reenvía al motor de autenticación (215) como se muestra en la etapa (1015) (véase la figura 10), y la autenticación es reevaluada basándose tanto en las instancias de autenticación preexistentes para esta transacción como en las instancias de autenticación recién proporcionadas.

Un tipo adicional de autenticación puede ser una solicitud procedente del motor de confianza (110) para efectuar alguna forma de contacto de persona a persona entre el operador del motor de confianza (110) (o un socio de confianza) y el usuario, por ejemplo, mediante llamada telefónica. Esta llamada telefónica u otra autenticación no informática puede usarse para proporcionar contacto personal con el individuo y también para llevar a cabo alguna forma de autenticación basada en cuestionario. Esto también puede ofrecer la oportunidad de verificar un número de teléfono de origen y potencialmente un análisis de voz del usuario cuando llama. Aunque no puedan proporcionarse datos de autenticación adicionales, el contexto adicional asociado con el número de teléfono del usuario puede mejorar la fiabilidad del contexto de autenticación. Cualquier dato o circunstancia revisados basándose en esta llamada telefónica se suministra al motor de confianza (110) para uso en consideración a la solicitud de autenticación.

Además, en la etapa (1820) el motor de confianza (110) puede proporcionar una oportunidad de que el usuario adquiera un seguro, adquiriendo eficazmente una autenticación de más confianza. El operador del motor de confianza (110) puede, a veces, querer solo disponer de tal opción si el nivel de confidencia de la autenticación está por encima de un cierto umbral con el que empezar. En efecto, este seguro por parte del usuario es un modo de que el motor de confianza (110) refrende al usuario cuando la autenticación satisface el nivel de confianza requerido del motor de confianza (110) para la autenticación, pero no satisface el nivel de confianza requerido del vendedor para esta transacción. De este modo, el usuario aun así puede autenticarse satisfactoriamente a un nivel muy alto como el que puede ser requerido por el vendedor, aun cuando solo tenga instancias de autenticación que produzcan confidencia suficiente para el motor de confianza (110).

Esta función del motor de confianza (110) permite que el motor de confianza (110) refrende a alguien que está autenticado a satisfacción del motor de confianza (110), pero no del vendedor. Esto es análogo a la función realizada por un notario que añade su firma a un documento con el fin de indicar a alguien que lea el documento en un momento posterior que la persona cuya firma aparece en el documento es, de hecho, la persona que lo firmó. La firma del notario testifica el acto de firmar por parte del usuario. Del mismo modo, el motor de confianza está proporcionando una indicación de que la persona que realiza la transacción es quien dice ser.

Sin embargo, como el motor de confianza (110) está incrementando artificialmente el nivel de confidencia proporcionado por el usuario, existe un mayor riesgo para el operador del motor de confianza (110), ya que el usuario no está satisfaciendo realmente el nivel de confianza requerido del vendedor. El coste del seguro está designado para compensar el riesgo de una autenticación positiva falsa en el motor de confianza (110) (quien puede notariar efectivamente las autenticaciones del usuario). El usuario paga al operador del motor de confianza (110) para que asuma el riesgo de autenticar a un nivel de confidencia más alto que el que ha sido proporcionado realmente.

Como tal sistema de seguro permite que alguien compre efectivamente un índice de confidencia más alto del motor de confianza (110), tanto el vendedor como los usuarios desean impedir el uso de un seguro por parte del usuario en ciertas transacciones. Los vendedores pueden desear limitar las autenticaciones positivas a circunstancias en las que sepan que los datos de autenticación reales soportan el grado de confidencia que ellos requieren y por tanto pueden indicar al motor de confianza (110) que no ha de permitirse un seguro por parte del usuario. De manera similar, para proteger su identidad en línea, un usuario puede desear impedir el uso de un seguro por parte del usuario en su cuenta, o puede desear limitar su uso a situaciones en las que el nivel de confidencia de autenticación sin el seguro es superior a un cierto límite. Esto puede usarse como medida de seguridad para impedir que alguien oiga por casualidad una contraseña o robe una tarjeta inteligente y las use para autenticarse falsamente a un nivel de confidencia bajo, y luego compre un seguro para producir un nivel de (falsa) confidencia muy alto. Estos factores pueden evaluarse al determinar si se permite un seguro por parte del usuario.

Si el usuario adquiere un seguro en la etapa (1840), entonces el nivel de confidencia de autenticación se ajusta basándose en el seguro adquirido en la etapa (1845), y el nivel de confidencia de autenticación y el nivel de confianza requerido son comparados de nuevo en la etapa (1730) (véase la figura 17). El proceso continúa desde ahí, y puede conducir o bien a una autenticación positiva en la etapa (1740) (véase la figura 17), o bien de vuelta al proceso de arbitraje de confianza en la etapa (1750) para, o bien un nuevo arbitraje (si se permite), o bien una autenticación negativa en la etapa (1810) sin está prohibido un nuevo arbitraje.

Además de enviar un mensaje al usuario en la etapa (1820), el motor de transacción (205) también puede enviar un mensaje al vendedor en la etapa (1830) que indica que una autenticación pendiente está actualmente por debajo del nivel de confianza requerido. El mensaje también puede ofrecer diversas opciones sobre cómo dirigirse al vendedor. Una de estas opciones es simplemente informar al vendedor de cuál es el nivel de confidencia de autenticación actual y preguntar si el vendedor desea mantener su nivel de confianza requerido insatisfecho actual. Esto puede ser beneficioso porque, en algunos casos, el vendedor puede tener medios independientes para autenticar la transacción o puede haber estado usando una conjunto de requisitos predeterminados que generalmente resultan en que se especifique inicialmente un nivel requerido más alto que el que es realmente necesario para la transacción particular en cuestión.

Por ejemplo, puede ser una práctica estándar que todas las transacciones de pedidos de adquisición entrantes con el vendedor se espere que satisfagan un nivel de confianza del 98 %. Sin embargo, si un pedido fue discutido por teléfono entre el vendedor y un antiguo cliente, e inmediatamente después la transacción es autenticada, pero solo a un nivel de confidencia del 93 %, el vendedor puede desear simplemente rebajar el umbral de aceptación para esta transacción, porque la llamada telefónica proporciona efectivamente autenticación adicional al vendedor. En ciertas circunstancias, el vendedor puede estar deseando rebajar su nivel de confianza requerido, pero no hasta el nivel de la confidencia de autenticación actual. Por ejemplo, el vendedor en el ejemplo anterior podría considerar que la llamada telefónica anterior al pedido podría merecer una reducción del 4 % en el grado de confianza necesario; sin embargo, aún así esto es mayor que la confidencia del 93 % producida por el usuario.

Si el vendedor ajusta su nivel de confianza requerido en la etapa (1835), entonces el nivel de confidencia de autenticación producido por la autenticación y el nivel de confianza requerido son comparados en la etapa (1730) (véase la figura 17). Si el nivel de confidencia ahora supera el nivel de confianza requerido, puede generarse una autenticación positiva en el motor de transacción (205) en la etapa (1740) (véase la figura 17). Si no, puede intentarse un nuevo arbitraje como se analizó anteriormente si está permitido.

Además de solicitar un ajuste en el nivel de confianza requerido, el motor de transacción (205) también puede ofrecer un seguro por parte del vendedor al vendedor que solicita la autenticación. Este seguro sirve para un fin similar al descrito anteriormente para el seguro por parte del usuario. Aquí, sin embargo, en lugar de que el coste que corresponde al riesgo que es asumido por el motor de confianza (110) al autenticar por encima del nivel de confidencia de autenticación real producido, el coste del seguro corresponde al riesgo que es asumido por el vendedor al aceptar un nivel de confianza más bajo en la autenticación.

En lugar de simplemente rebajar su nivel de confianza requerido, el vendedor tiene la opción de adquirir un seguro para protegerse del riesgo adicional asociado con un nivel de confianza más bajo en la autenticación del usuario. Como se describe anteriormente, puede ser ventajoso para el vendedor considerar solo adquirir tal seguro para cubrir la brecha de confianza en las condiciones en que la autenticación existente ya está por encima de un cierto umbral.

La disponibilidad de tal seguro por parte del vendedor permite al vendedor la opción de o bien: rebajar su requisito de confianza directamente sin coste adicional para sí mismo, corriendo el riesgo de una falsa autenticación de sí mismo (basándose en el nivel de confianza más bajo requerido); o bien, adquirir el seguro para la brecha de confianza entre el nivel de confidencia de autenticación y su requisito, con el operador del motor de confianza (110) corriendo el riesgo del nivel de confianza más bajo que se ha proporcionado. Adquiriendo el seguro, el vendedor mantiene eficazmente su requisito de nivel de confianza alto, porque el riesgo de una autenticación falsa es trasladado al operador del motor de confianza (110).

Si el vendedor adquiere el seguro en la etapa (1840), el nivel de confidencia de autenticación y los niveles de confianza requeridos son comparados en la etapa (1730) (véase la figura 17), y el proceso continúa como se describe anteriormente.

Obsérvese que también es posible que tanto el usuario como el vendedor respondan a mensajes procedentes del motor de confianza (110). Los expertos en la materia reconocerán que existen múltiples maneras en las que pueden tratarse tales situaciones. Un modo ventajoso de tratar la posibilidad de múltiples respuestas es simplemente tratar las respuestas en una manera de primera en llegar, primera en ser atendida. Por ejemplo, si el vendedor responde con un nivel de confianza requerido rebajado e inmediatamente después el usuario también adquiere un seguro para aumentar su nivel de autenticación, la autenticación en primer lugar es reevaluada basándose en el requisito de confianza rebajado del vendedor. Si la autenticación ahora es positiva, se ignora la adquisición de seguro del

usuario. En otro modo ventajoso de funcionamiento, al usuario se le podría cobrar solo el nivel de seguro requerido para satisfacer el nuevo requisito de confianza rebajado del vendedor (si seguía habiendo una brecha de confianza incluso con el requisito de confianza rebajado del vendedor).

Si no se recibe respuesta de ninguna parte durante el proceso de arbitraje de confianza en la etapa (1850) dentro del límite de tiempo fijado para la autenticación, el arbitraje es reevaluado en la etapa (1805). Esto comienza efectivamente el proceso de arbitraje de nuevo. Si el límite de tiempo fuera final u otras circunstancias impiden un nuevo arbitraje en la etapa (1805), se genera una autenticación negativa por parte del motor de transacción (205) en la etapa (1810) y se devuelve al vendedor en la etapa (1055) (véase la figura 10). Si no, pueden enviarse nuevos mensajes al usuario y al vendedor, y el proceso puede repetirse según se desee.

Obsérvese que para ciertos tipos de transacciones, por ejemplo, firmar digitalmente documentos que no forman parte de una transacción, puede no haber necesariamente un vendedor u otro tercero; por lo tanto, la transacción es principalmente entre el usuario y el motor de confianza (110). En circunstancias tales como estas, el motor de confianza (110) tendrá su propio nivel de confianza requerido que debe ser satisfecho con el fin de generar una autenticación positiva. Sin embargo, en tales circunstancias, a menudo no será deseable que el motor de confianza (110) ofrezca un seguro al usuario con el fin de que aumente la confidencia de su propia firma.

El proceso descrito anteriormente y mostrado en las figuras 16-18 puede llevarse a cabo usando diversos modos de comunicaciones como se describe anteriormente con referencia al motor de confianza (110). Por ejemplo, los mensajes pueden ser basados en web y enviados usando conexiones SSL entre el motor de confianza (110) y miniaplicaciones descargadas en tiempo real a navegadores que se ejecutan en los sistemas del usuario o el vendedor. En un modo alternativo de funcionamiento, ciertas aplicaciones dedicadas pueden estar en uso por parte del usuario y el vendedor que facilitan tales transacciones de arbitraje y seguro. En otro modo alternativo de funcionamiento, pueden usarse operaciones de correo electrónico seguro para mediar en el arbitraje descrito anteriormente, permitiendo de ese modo evaluaciones aplazadas y procesamiento de autenticaciones por lotes. Los expertos en la materia reconocerán que pueden usarse diferentes modos de comunicaciones según resulte apropiado para las circunstancias y los requisitos de autenticación del vendedor.

La siguiente descripción con referencia a la figura 19 describe una transacción de muestra que integra los diversos aspectos de la presente invención como se describen anteriormente. Este ejemplo ilustra el proceso global entre un usuario y un vendedor con la mediación del motor de confianza (110). Aunque las diversas etapas y componentes descritos como se describe en detalle anteriormente pueden usarse para llevar a cabo la siguiente transacción, el proceso ilustrado se centra en la interacción entre el motor de confianza (110), el usuario y el vendedor.

La transacción comienza cuando el usuario, mientras que ve páginas web en línea, rellena un formulario de pedido en el sitio web del vendedor en la etapa (1900). El usuario desea presentar este formulario de pedido al vendo, firmado con su firma digital. Para hacer esto, el usuario presenta el formulario de pedido con su solicitud de una firma al motor de confianza (110) en la etapa (1905). El usuario también proporcionará datos de autenticación que serán usados como se describe anteriormente para autenticar su identidad.

En la etapa (1910) los datos de autenticación son comparados con los datos de inscripción por el motor de confianza (110) como se analiza anteriormente, y si se produce una autenticación positiva, el troceo del formulario de pedido, firmado con la clave privada del usuario, es reenviado al vendedor junto con el formulario de pedido en sí.

El vendedor recibe el formulario firmado en la etapa (1915), y entonces el vendedor generará una factura u otro contrato relacionado con la adquisición que ha de efectuarse en la etapa (1920). Este contrato es enviado de vuelta al usuario con una solicitud de una firma en la etapa (1925). El vendedor también envía una solicitud de autenticación de esta transacción de contrato al motor de confianza (110) en la etapa (1930) que incluye un troceo del contrato que será firmado por ambas partes. Para permitir que el contrato sea firmado digitalmente por ambas partes, el vendedor también incluye datos de autenticación para él mismo de modo que la firma del vendedor en el momento del contrato pueda ser verificada más adelante si es necesario.

Como se analiza anteriormente, el motor de confianza (110) verifica entonces los datos de autenticación proporcionados por el vendedor para confirmar la identidad del vendedor, y si los datos producen una autenticación positiva en la etapa (1935), continúa con la etapa (1955) cuando los datos son recibidos desde el usuario. Si los datos de autenticación del vendedor no coinciden con los datos de inscripción del vendedor hasta el grado deseado, se devuelve un mensaje al vendedor solicitando una nueva autenticación. Aquí puede realizarse el arbitraje de confianza si es necesario, como se describe anteriormente, con el fin de que el vendedor se autentique

satisfactoriamente en el motor de confianza (110).

Cuando el usuario recibe el contrato en la etapa (1940), lo revisa, genera datos de autenticación para firmarlo si es aceptable en la etapa (1945), y luego envía un troceo del contrato y sus datos de autenticación al motor de confianza (110) en la etapa (1950). El motor de confianza (110) verifica los datos de autenticación en la etapa (1955) y si la autenticación es buena, pasa a procesar el contrato como se describe más adelante. Como se analiza anteriormente con referencia a las figuras 17 y 18, el arbitraje de confianza puede realizarse según resulte apropiado para cerrar cualquier brecha de confianza que exista entre el nivel de confidencia de autenticación y el nivel de autenticación requerido para la transacción.

El motor de confianza (110) firma el troceo del contrato con la clave privada del usuario, y envíe este troceo firmado al vendedor en la etapa (1960), firmando el mensaje completo en su propio nombre, es decir, incluyendo un troceo del mensaje completo (incluyendo la firma del usuario) cifrado con la clave privada (510) del motor de confianza (110). Este mensaje es recibido por el vendedor en la etapa (1965). El mensaje representa un contrato firmado (el troceo del contrato cifrado usando la clave privada del usuario) y un recibo procedente del motor de confianza (110) (el troceo del mensaje que incluye el contrato firmado, cifrado usando la clave privada del motor de confianza (110)).

El motor de confianza (110) prepara de manera similar un troceo del contrato con la clave privada del vendedor en la etapa (1970), y reenvía este al usuario, firmado por el motor de confianza (110). De este modo, el usuario también recibe una copia del contrato, firmada por el vendedor, así como un recibo, firmado por el motor de confianza (110), para distribución del contrato firmado en la etapa (1975).

Además de lo anterior, un aspecto adicional de la invención proporciona un módulo proveedor de servicio (SPM) que puede estar a disposición de una aplicación del lado del cliente como medio para acceder a funciones proporcionadas por el motor de confianza (110) descritas anteriormente. Un modo ventajoso de proporcionar tal servicio es que el SPM criptográfico medie en las comunicaciones entre una interfaz de programación de aplicaciones (API) y un motor de confianza (110) que sea accesible a través de una red u otra conexión remota. Más adelante se describe un SPM criptográfico de muestra con referencia a la figura 20.

Por ejemplo, en un sistema típico, varias API están a disposición de los programadores. Cada API proporciona un conjunto de llamadas a funciones que pueden efectuarse mediante una aplicación (2000) que se ejecuta en el sistema. Ejemplos de API que proporcionan interfaces de programación adecuadas para funciones criptográficas, funciones de autenticación, y otra función de seguridad incluyen la API criptográfica (CAPI) (2010) proporcionada por Microsoft con sus sistemas operativos Windows, y la arquitectura común de seguridad de datos (CDSA), patrocinada por IBM, Intel y otros miembros del Open Group. En la siguiente discusión se usará CAPI como una API de seguridad ejemplar. Sin embargo, podría usarse el SPM criptográfico con CDSA u otras API de seguridad tal como se conocen en la técnica.

Esta API es usada por un sistema de usuario (105) o un sistema de vendedor (120) cuando se efectúa una llamada para una función criptográfica. Incluidas entre estas funciones pueden estar solicitudes asociadas con la realización de diversas operaciones criptográficas, tales como cifrar un documento con una clave particular, firmar un documento, solicitar un certificado digital, verificar una firma en un documento firmado, y otras de tales funciones criptográficas como se describen en este documento o conocidas por los expertos en la materia.

Tales funciones criptográficas normalmente son realizadas localmente al sistema en el que está ubicada la CAPI (2010). Esto es porque, generalmente, las funciones llamadas requieren el uso de o bien recursos del sistema de usuario local (105), tales como un lector de huella dactilar, o bien funciones de software que son programadas usando bibliotecas que son ejecutadas en la máquina local. El acceso a estos recursos locales normalmente es proporcionado por uno o más módulos proveedores de servicios (SPM) (2015), (2020) a los que se hace referencia anteriormente, que proporcionan recursos con los cuales se llevan a cabo las funciones criptográficas. Tales SPM puede incluir bibliotecas de software (2015) para realizar el cifrado o descifrado de operaciones, o controladores y aplicaciones (2020) que son capaces de acceder a hardware especializado (2025), tales como dispositivos de escaneo biométrico. Así como la CAPI (2010) proporciona funciones que pueden ser usadas por una aplicación (2000) del sistema (105), los SPM (2015), (2020) proporcionan CAPI con acceso a las funciones y recursos de nivel más bajo asociados con los servicios disponibles en el sistema.

De acuerdo con la invención, es posible proporcionar un SPM criptográfico (2030) que es capaz de acceder a las funciones criptográficas proporcionadas por el motor de confianza (110) y poner estas funciones a disposición de una aplicación (2000) a través de la CAPI (2010). A diferencia de las realizaciones donde la CAPI (2010) solo puede

acceder a recursos que están disponibles localmente a través de los SPM (2015), (2020), un SPM criptográfico (2030) como se describe en este documento podría presentar solicitudes de operaciones criptográficas a un motor de confianza accesible por red ubicado a distancia (110) con el fin de realizar las operaciones deseadas.

Por ejemplo, si una aplicación (2000) tiene una necesidad de una operación criptográfica, tal como firmar un documento, la aplicación (2000) efectúa una llamada de función a la función de la CAPI (2010) apropiada. La CAPI (2010) a su vez ejecutará esta función, haciendo uso de los recursos que fueron puestos a su disposición por los SPM (2015), (2020) y el SPM criptográfico (2030). En el caso de una función de firma digital, el SPM criptográfico (2030) generará una solicitud apropiada que será enviada al motor de confianza (110) a través del enlace de comunicación (125).

Las operaciones que se producen entre el SPM criptográfico (2030) y el motor de confianza (110) son las mismas operaciones que serían posibles entre cualquier otro sistema y el motor de confianza (110). Sin embargo, estas funciones se ponen eficazmente a disposición de un sistema de usuario (105) a través de la CAPI (2010) de modo que parecen estar disponibles localmente en el sistema de usuario (105) en sí. Sin embargo, a diferencia de los SPM ordinarios (2015), (2020), las funciones se están llevando a cabo en el motor de confianza remoto (110) y los resultados se retransmiten al criptográfico SPM (2030) en respuesta a solicitudes apropiadas a través del enlace de comunicación (125).

Este SPM criptográfico (2030) pone a disposición del sistema de usuario (105) o un sistema de vendedor (120) varias operaciones que de otro modo podrían no estar disponibles. Estas funciones incluyen sin limitación: cifrado y descifrado de documentos; expedición de certificados digitales; firma digital de documentos; verificación de firmas digitales; y otras de tales operaciones como resultará evidente para los expertos en la materia.

En una realización separada, la presente invención comprende un sistema completo para realizar los procedimientos de seguridad de datos de la presente invención sobre cualquier conjunto de datos. El sistema informático de esta realización comprende un módulo de división de datos que comprende la funcionalidad mostrada en la figura 8 y descrita en este documento. En una realización de la presente invención, el módulo de división de datos, a veces denominado en este documento analizador sintáctico de datos seguros, comprende un programa analizador sintáctico o un paquete de software que comprende funcionalidad de división, cifrado y descifrado, reconstitución y reensamblaje de datos. Esta realización además puede comprender también una instalación de almacenamiento de datos o múltiples instalaciones de almacenamiento de datos. El módulo de división de datos, o el analizador sintáctico de datos seguros, comprende un paquete de módulos de software de plataformas cruzadas que integra en su interior una infraestructura electrónica, o como un añadido a cualquier aplicación que requiera la seguridad definitiva de sus elementos de datos. Este proceso de análisis sintáctico opera sobre cualquier tipo de conjunto de datos, y sobre cualquiera y todo tipo de archivos, o en una base de datos sobre cualquier fila, columna o celda de datos en esa base de datos.

El proceso de análisis sintáctico de la presente invención puede, en una realización, estar diseñado por niveles modulares, y cualquier proceso de cifrado es adecuado para uso en el proceso de la presente invención. Los niveles modulares del proceso de análisis sintáctico y división de la presente invención pueden incluir, pero no están limitados a, 1) división criptográfica, dispersada y almacenada con seguridad en múltiples ubicaciones; 2) cifrado, división criptográfica, dispersada y almacenada con seguridad e múltiples ubicaciones; 3) cifrado, división criptográfica, cifrado de cada cuota, luego dispersadas y almacenadas con seguridad en múltiples ubicaciones; y 4) cifrado, división criptográfica, cifrado de cada cuota con un tipo de cifrado diferente del usado en la primera etapa, luego dispersada y almacenada con seguridad en múltiples ubicaciones.

El proceso comprende, en una realización, la división de los datos de acuerdo con el contenido de un número aleatorio generado, o clave, y realizar la misma división criptográfica de la clave usada en el cifrado de división de los datos que han de ser asegurados en dos o más porciones, o cuotas, de los datos analizados sintácticamente y divididos, y en una realización, preferentemente en cuatro o más porciones de datos analizados sintácticamente y divididos, cifrar todas las porciones, luego dispersar y volver a almacenar estas porciones dentro de la base de datos, o reubicarlos en cualquier dispositivo indicado, fijo o extraíble, dependiendo de la necesidad de privacidad y seguridad del solicitante. Alternativamente, en otra realización, el cifrado puede producirse antes de la división del conjunto de datos por parte del módulo de división o el analizador sintáctico de datos seguros. Los datos originales procesados como se describe en este documento son cifrados y ofuscados y son asegurados. La dispersión de los elementos cifrados, si se desea, puede ser prácticamente en cualquier parte, incluyendo, pero no limitada a, un solo servidor o dispositivo de almacenamiento de datos, o entre instalaciones o dispositivos de almacenamiento de datos separados. La gestión de claves de cifrado en una realización puede estar incluida dentro del paquete de software, o

en otra realización puede estar integrada en una infraestructura existente o cualquier otra ubicación deseada.

Una división criptográfica (criptodivisión) parte los datos en un número N de cuotas. La partición puede ser en cualquier unidad de tamaño de datos, incluyendo un bit individual, bits, *bytes*, *kilobytes*, *megabytes*, o unidades más grandes, así como cualquier patrón o combinación de tamaños de unidad de datos ya sea predeterminado o generado aleatoriamente. Las unidades también pueden ser dimensionadas de manera diferente, basándose en un conjunto de valores aleatorio o predeterminado. Esto significa que los datos pueden verse como una secuencia de estas unidades. De esta manera, el tamaño de las unidades de tamaño en sí puede hacer que los datos resulten más seguros, por ejemplo usando uno o más patrones, secuencias o combinaciones de tamaños de unidades de datos predeterminados o generados aleatoriamente. Las unidades después son distribuidas (ya sea aleatoriamente o por un conjunto predeterminado de valores) dentro de las N cuotas. Esta distribución también podría implicar una transposición del orden de las unidades en las cuotas. Resulta inmediatamente evidente para cualquier experto en la materia que la distribución de las unidades de datos dentro de las cuotas puede realizarse de acuerdo con una amplia variedad de selecciones posibles, incluyendo, pero no limitadas a fijada por tamaño, tamaños predeterminados, o una o más combinaciones, patrones o secuencias de tamaños de unidad de datos que son predeterminados o generados aleatoriamente.

En algunas realizaciones de este proceso de división por criptodivisión, los datos pueden ser de cualquier número adecuado de *bytes* de tamaño, tal como uno, dos, tres, cinco, veinte, cincuenta, cien, más de cien, o N *bytes* de tamaño. Un ejemplo particular de este proceso de división criptográfica, o criptodivisión, sería considerar que los datos son de 23 *bytes* de tamaño, con el tamaño de unidad de datos escogido para que sea un *byte*, y con el número de cuotas seleccionadas para que sean 4. Cada *byte* estaría distribuido en una de las 4 cuotas. Suponiendo una distribución aleatoria, se obtendría una clave para crear una secuencia de 23 números aleatorios (r1, r2, r3 a r23), cada uno con un valor entre 1 y 4 que corresponde a las cuatro cuotas. Cada una de las unidades de datos (en este ejemplo 23 *bytes* de datos individuales) está asociado con uno de los 23 números aleatorios que corresponden a una de las cuatro cuotas. La distribución de los *bytes* de datos dentro de las cuatro cuotas se produciría poniendo el primer *byte* de los datos dentro de la cuota número r1, el *byte* dos dentro de la cuota r2, el *byte* tres dentro de la cuota r3, hasta el *byte* de datos 23º dentro de la cuota r23. Resulta inmediatamente evidente para cualquier experto en la materia que en el proceso de criptodivisión de la presente invención puede usarse una amplia variedad de otras posibles etapas o combinación o secuencia de etapas, incluyendo el tamaño de las unidades de datos, y el ejemplo anterior es una descripción no limitativa de un proceso para criptodividir datos. Para recrear los datos originales, se realizaría la operación inversa.

En otra realización del proceso de criptodivisión de la presente invención, una opción para el proceso de criptodivisión es proporcionar suficiente redundancia en las cuotas de modo que solo es necesario un subconjunto de las cuotas para volver a ensamblar o restaurar los datos a su forma original o utilizable. Como ejemplo no limitativo, la criptodivisión puede hacerse como una criptodivisión de “3 de 4” de modo que solo sean necesarias tres de las cuatro cuotas para volver a ensamblar o restaurar los datos a su forma original o utilizable. Esto también se denomina “criptodivisión M de N” donde N es el número total de cuotas, y M es al menos uno menos que N. Resulta inmediatamente evidente para cualquier experto en la materia que existen muchas posibilidades para crear esta redundancia en el proceso de criptodivisión de la presente invención.

En una realización del proceso de criptodivisión de la presente invención, cada unidad de datos es almacenada en dos cuotas, la cuota primaria y la cuota de copia de seguridad. Usando el proceso de criptodivisión de “3 de 4” descrito anteriormente, puede faltar una cuota cualquiera, y esto es suficiente para volver a ensamblar los datos originales sin que falten unidades de datos ya que solo se requieren tres de las cuatro cuotas totales. Como se describe en este documento, se genera un número aleatorio que corresponde a una de las cuotas. El número aleatorio es asociado con una unidad de datos, y almacenado en la cuota correspondiente, basándose en una clave. Se usa una clave, en esta realización, para generar el número aleatorio de cuotas primarias y de copia de seguridad. Como se describe en este documento para el proceso de criptodivisión de la presente invención, se genera un conjunto de números aleatorios (también denominados números de cuotas primarias) de 0 a 3 igual al número de unidades de datos. Después se genera otro conjunto de números aleatorios (también denominados números de cuotas de copia de seguridad) de 1 a 3 igual al número de unidades de datos. Cada unidad de datos es asociada después con un número de cuotas primarias y un número de cuotas de copia de seguridad. Alternativamente, puede generarse un conjunto de números aleatorios que es menor que el número de unidades de datos, y repetir el conjunto de números aleatorios, pero esto puede reducir la seguridad de los datos sensibles. El número de cuotas primarias se usa para determinar dentro de qué cuotas es almacenada la unidad de datos. El número de cuotas de copia de seguridad se combina con el número de cuotas primarias para crear un tercer número de cuotas entre 0 y 3, y este número se usa para determinar dentro de qué cuota es almacenada la unidad de datos. En este ejemplo, la

ecuación para determinar el tercer número de cuotas es:

(número de cuotas primarias + número de cuotas de copia de seguridad) MOD 4 = tercer número de cuotas.

En la realización descrita anteriormente donde el número de cuotas primarias está entre 0 y 3, y el número de cuotas de copia de seguridad está entre 1 y 3 asegura que el tercer número de cuotas es diferente del número de cuotas primarias. Esto tiene como resultado que la unidad de datos es almacenada en dos cuotas diferentes. Resulta inmediatamente evidente para cualquier experto en la materia que existen muchos modos de realizar criptodivisión redundante y criptodivisión no redundante además de las realizaciones descritas en este documento. Por ejemplo, las unidades de datos en cada cuota podrían ser transpuestas utilizando un algoritmo diferente. Esta transposición de unidades de datos puede realizarse cuando los datos originales son divididos en las unidades de datos, o después de que las unidades de datos son colocadas dentro de las cuotas, o después de que la cuota está llena, por ejemplo.

Los diversos procesos de criptodivisión y procedimientos de transposición de datos descritos en este documento, y todas las demás realizaciones de los procesos de criptodivisión y transposición de datos de la presente invención pueden realizarse en unidades de datos de cualquier tamaño, incluyendo, pero no limitado a, tan pequeño como un bit individual, bits, *bytes*, *kilobytes*, *megabytes* o mayor.

Un ejemplo de una realización de código fuente que realizaría el proceso de criptodivisión descrito en este documento es:

```
                DATA [1:24] – matriz de bytes con los datos que han de ser divididos
                SHARES[0:3; 1:24] – matriz bidimensional con cada fila representando una de las cuotas
                RANDOM[1:24] – matriz de números aleatorios en el intervalo de 0..3
                S1 = 1;
                S2 = 1;
                S3 = 1;
                S4 = 1;

For J = 1 to 24 do
                Begin
                IF RANDOM[J[ ==0 then
                                Begin
                                SHARES[1,S1] = DATA [J];
                                S1 = S1 + 1;
                                End
                ELSE IF RANDOM [J[ ==1 then
                                Begin
                                SHARES[2,52] = DATA [J];
                                S2=S2+1;
                                END
                ELSE IF RANDOM[J[ ==2 then
                                Begin
                                Shares[3,S3] = data [J];
                                S3=S3+1;
                                End
                Else begin
                                Shares[4,S4] = data [J];
                                S4=S4+1;
                                End;
                END;
```

Un ejemplo de una realización de código fuente que realizaría el proceso de criptodivisión RAID descrito en este documento es:

Generar dos conjuntos de números, PrimaryShare es 0 a 3, BackupShare es 1 a 3. Luego poner cada unidad de datos dentro de share[primaryshare[1]] y share[(primaryshare[1]+backupcuota[1]) mod 4, con el mismo proceso que en la criptodivisión descrita anteriormente. Este procedimiento será escalable a cualquier tamaño N, donde solo son

necesarias N-1 cuotas para restaurar los datos.

La recuperación, recombinación, reensamblaje o reconstitución de los elementos de datos cifrados pueden utilizar cualquier número de técnicas de autenticación, incluyendo, pero no limitadas a, biometría, tal como reconocimiento de huella dactilar, escáner facial, escáner de mano, escáner de iris, escáner de retina, escáner de oreja, reconocimiento de patrón vascular o análisis de ADN. Los módulos de división de datos y/o analizadores sintácticos de la presente invención pueden estar integrados dentro de una amplia variedad de productos de infraestructura o aplicaciones según se desee.

Las tecnologías de cifrado tradicionales conocidas en la técnica están basadas en una o más claves usadas para cifrar los datos y hacer que resulten inutilizables sin la clave. Los datos, sin embargo, siguen estando enteros e intactos y sujetos a ataque. El analizador sintáctico de datos seguros de la presente invención, en una realización, se ocupa de este problema realizando un análisis sintáctico criptográfico y división del archivo cifrado en dos o más porciones o cuotas, y en otra realización, preferentemente cuatro o más cuotas, añadiendo otra capa de cifrado a cada cuota de los datos, después almacenando las cuotas en diferentes ubicaciones físicas y/o lógicas. Cuando una o más cuotas de datos son eliminadas físicamente del sistema, ya sea usando un dispositivo extraíble, tal como un dispositivo de almacenamiento de datos, o poniendo la cuota bajo control de otra parte, se elimina eficazmente cualquier posibilidad de compromiso de los datos asegurados.

Un ejemplo de una realización del analizador sintáctico de datos seguros de la presente invención y un ejemplo de cómo puede utilizarse se muestra en la figura 21 y se describe más adelante. Sin embargo, resulta inmediatamente evidente para cualquier experto en la materia que el analizador sintáctico de datos seguros de la presente invención puede utilizarse en una amplia variedad de modos además del ejemplo no limitativo de más adelante. Como opción de despliegue, y en una realización, el analizador sintáctico de datos seguros puede implementarse con gestión de clave de sesión externa o almacenamiento interno seguro de claves de sesión. Tras la implementación, se generará una clave maestra de analizador sintáctico que se usará para asegurar la aplicación y con fines de cifrado. También cabe destacar que la incorporación de la clave maestra de analizador sintáctico en los datos asegurados resultantes permite una flexibilidad de compartición de los datos asegurados por parte de los individuos dentro de un grupo de trabajo, empresa o público ampliado.

Como se muestra en la figura 21, esta realización de la presente invención muestra las etapas del proceso realizado por el analizador sintáctico de datos seguros sobre los datos para almacenar la clave maestra de sesión con los datos analizados sintácticamente:

1. Generar una clave maestra de sesión y cifrar los datos usando cifrado en flujo RS1.
2. Separar los datos cifrados resultantes en cuatro cuotas o porciones de datos analizados sintácticamente de acuerdo con el patrón de la clave maestra de sesión.
3. En esta realización del procedimiento, la clave maestra de sesión será almacenada junto con las cuotas de datos asegurados en un depósito de datos. Separar la clave maestra de sesión de acuerdo con el patrón de la clave maestra analizada sintácticamente y adjuntar los datos de clave a los datos analizados sintácticamente cifrados.
4. Las cuatro cuotas de datos resultantes contendrán porciones cifradas de los datos originales y porciones de la clave maestra de sesión. Generar una clave de cifrado en flujo para cada una de las cuatro cuotas de datos.
5. Cifrar cada cuota, después almacenar las claves de cifrado en ubicaciones diferentes de las porciones o cuotas de datos cifrados: la cuota 1 obtiene la clave 4, la cuota 2 obtiene la clave 1, la cuota 3 obtiene la clave 2, la cuota 4 obtiene la clave 3.

Para restaurar el formato de datos original, se invierten las etapas.

Resulta inmediatamente evidente para cualquier experto en la materia que ciertas etapas de los procedimientos descritos en este documento pueden realizarse en diferente orden, o repetirse múltiples veces, según se desee. También resulta inmediatamente evidente para los expertos en la materia que las porciones de los datos pueden ser tratadas de manera diferente unas de otras. Por ejemplo, pueden realizarse múltiples etapas de análisis sintáctico sobre solo una porción de los datos analizados sintácticamente. Cada porción de datos analizados sintácticamente puede ser asegurada de manera única de cualquier modo deseable solo siempre que los datos puedan volver a ser ensamblados, reconstituidos, reformados, descifrados o restaurados a su forma original u otra forma utilizable.

Como se muestra en la figura 22 y se describe en este documento, otra realización de la presente invención comprende las etapas del proceso realizado por el analizador sintáctico de datos seguros sobre los datos para almacenar los datos de clave maestra de sesión en una o más tablas de gestión de claves separadas:

1. Generar una clave maestra de sesión y cifrar los datos usando cifrado en flujo RS1.
2. Separar los datos cifrados resultantes en cuatro cuotas o porciones de datos analizados sintácticamente de acuerdo con el patrón de la clave maestra de sesión.
3. En esta realización del procedimiento de la presente invención, la clave maestra de sesión será almacenada en una tabla de gestión de claves separada en un depósito de datos. Generar una ID de transacción única para esta transacción. Almacenar la ID de transacción y la clave maestra de sesión en una tabla de gestión de claves separada. Separar la ID de transacción de acuerdo con el patrón de la clave maestra de analizador sintáctico y adjuntar los datos a los datos analizados sintácticamente cifrados o separados.
4. Las cuatro cuotas de datos resultantes contendrán porciones cifradas de los datos originales y porciones de la ID de transacción.
5. Generar una clave de cifrado en flujo de las cuatro cuotas de datos.
6. Cifrar cada cuota, después almacenar las claves de cifrado en ubicaciones diferentes de las porciones o cuotas de datos cifrados: la cuota 1 obtiene la clave 4, la cuota 2 obtiene la clave 1, la cuota 3 obtiene la clave 2, la cuota 4 obtiene la clave 3.

Para restaurar el formato de datos original, se invierten las etapas.

Resulta inmediatamente evidente para cualquier experto en la materia que ciertas etapas del procedimiento descrito en este documento pueden realizarse en diferente orden, o repetirse múltiples veces, según se desee. También resulta inmediatamente evidente para los expertos en la materia que las porciones de los datos pueden ser tratadas de manera diferente unas de otras. Por ejemplo, pueden realizarse múltiples etapas de separación o análisis sintáctico sobre solo una porción de los datos analizados sintácticamente. Cada porción de datos analizados sintácticamente puede ser asegurada de manera única de cualquier modo deseable solo siempre que los datos puedan volver a ser ensamblados, reconstituidos, reformados, descifrados o restaurados a su forma original u otra forma utilizable.

Como se muestra en la figura 23, esta realización de la presente invención muestra las etapas del proceso realizado por el analizador sintáctico de datos seguros sobre los datos para almacenar la clave maestra de sesión con los datos analizados sintácticamente:

1. Acceder a la clave maestra de analizador sintáctico asociada con el usuario autenticado.
2. Generar una clave maestra de sesión única.
3. Deducir una clave intermedia a partir de una función OR exclusiva de la clave maestra de analizador sintáctico y la clave maestra de sesión.
4. Cifrado opcional de los datos usando un algoritmo de cifrado existente o nuevo, codificado con la clave intermedia.
5. Separar los datos cifrados opcionalmente resultantes en cuatro porciones alícuotas o porciones de datos analizados sintácticamente de acuerdo con el patrón de la clave intermedia.
6. En esta realización del procedimiento, la clave maestra de sesión será almacenada junto con las cuotas de datos asegurados en un depósito de datos. Separar la clave maestra de sesión de acuerdo con el patrón de la clave maestra de analizador sintáctico y adjuntar los datos de clave a las cuotas de datos analizados sintácticamente cifrados opcionalmente.
7. Las múltiples cuotas de datos resultantes contendrán porciones cifradas opcionalmente de los datos originales y porciones de la clave maestra de sesión.
8. Generar opcionalmente una clave de cifrado para cada una de las cuatro cuotas de datos.
9. Cifrar opcionalmente cada cuota con un algoritmo de cifrado existente o nuevo, después almacenar las claves de cifrado en ubicaciones diferentes de las porciones o cuotas de datos cifrados: por ejemplo, la cuota 1 obtiene la clave 4, la cuota 2 obtiene la clave 1, la cuota 3 obtiene la clave 2, la cuota 4 obtiene la clave 3.

Para restaurar el formato de datos original, se invierten las etapas.

Resulta inmediatamente evidente para cualquier experto en la materia que ciertas etapas de los procedimientos descritos en este documento pueden realizarse en diferente orden, o repetirse múltiples veces, según se desee. También resulta inmediatamente evidente para los expertos en la materia que las porciones de los datos pueden ser tratadas de manera diferente unas de otras. Por ejemplo, pueden realizarse múltiples etapas de análisis sintáctico sobre solo una porción de los datos analizados sintácticamente. Cada porción de datos analizados sintácticamente puede ser asegurada de manera única de cualquier modo deseable solo siempre que los datos puedan volver a ser ensamblados, reconstituidos, reformados, descifrados o restaurados a su forma original u otra forma utilizable.

Como se muestra en la figura 24 y se describe en este documento, otra realización de la presente invención comprende las etapas del proceso realizado por el analizador sintáctico de datos seguros sobre los datos para almacenar los datos de clave maestra de sesión en una o más tablas de gestión de claves separadas:

1. Acceder a la clave maestra de analizador sintáctico asociada con el usuario autenticado.
2. Generar una clave maestra de sesión única.
3. Deducir una clave intermedia a partir de una función OR exclusiva de la clave maestra de analizador sintáctico y la clave maestra de sesión.
4. Cifrar opcionalmente los datos usando un algoritmo de cifrado existente o nuevo codificado con la clave intermedia.
5. Separar los datos cifrados opcionalmente resultantes en cuatro porciones alícuotas o porciones de datos analizados sintácticamente de acuerdo con el patrón de la clave intermedia.
6. En esta realización del procedimiento de la presente invención, la clave maestra de sesión será almacenada en una tabla de gestión de claves separada en un depósito de datos. Generar una ID de transacción única para esta transacción. Almacenar la ID de transacción y la clave maestra de sesión en una tabla de asignación de claves separada o pasar la clave maestra de sesión y la ID de transacción de vuelta al programa llamante para gestión externa. Separar la ID de transacción de acuerdo con el patrón de la clave maestra de analizador sintáctico y adjuntar los datos a los datos analizados sintácticamente cifrados opcionalmente o separados.
7. Las cuatro cuotas de datos resultantes contendrán porciones cifradas opcionalmente de los datos originales y porciones de la ID de transacción.
8. Generar opcionalmente una clave de cifrado para cada una de las cuatro cuotas de datos.
9. Cifrar opcionalmente cada cuota, después almacenar las claves de cifrado en ubicaciones diferentes de las porciones o cuotas de datos cifrados. Por ejemplo, la cuota 1 obtiene la clave 4, la cuota 2 obtiene la clave 1, la cuota 3 obtiene la clave 2, la cuota 4 obtiene la clave 3.

Para restaurar el formato de datos original, se invierten las etapas.

Resulta inmediatamente evidente para cualquier experto en la materia que ciertas etapas del procedimiento descrito en este documento pueden realizarse en diferente orden, o repetirse múltiples veces, según se desee. También resulta inmediatamente evidente para los expertos en la materia que las porciones de los datos pueden ser tratadas de manera diferente unas de otras. Por ejemplo, pueden realizarse múltiples etapas de separación o análisis sintáctico sobre solo una porción de los datos analizados sintácticamente. Cada porción de datos analizados sintácticamente puede ser asegurada de manera única de cualquier modo deseable solo siempre que los datos puedan volver a ser ensamblados, reconstituidos, reformados, descifrados o restaurados a su forma original u otra forma utilizable.

Una amplia variedad de metodologías de cifrado son adecuadas para uso en los procedimientos de la presente invención, como resulta inmediatamente evidente para los expertos en la materia. El algoritmo One Time Pad (libreta de un solo uso) a menudo se considera uno de los procedimientos de cifrado más seguros, y es adecuado para uso en el procedimiento de la presente invención. Usar el algoritmo One Time Pad requiere que se genere una clave que sea tan larga como los datos que han de ser asegurados. El uso de este procedimiento puede ser menos deseable en ciertas circunstancias tales como las que tienen como resultado la generación y gestión de claves muy largas debido al tamaño del conjunto de datos que ha de ser asegurado. En un algoritmo One Time Pad (OTP), se usa la función or exclusiva simple, XOR. Para dos flujos binarios x e y de la misma longitud, x XOR y significa la or exclusiva a nivel de bit de x e y.

Al nivel de bit se genera:

0 XOR 0 = 0
0 XOR 1 = 1
1 XOR 0 = 1
1 XOR 1 = 0

En este documento se describe un ejemplo de este proceso para un secreto de n *bytes*, s, (o conjunto de datos) que ha de ser dividido. El proceso generará un valor aleatorio de n *bytes*, a, y luego establecerá: b = a XOR s.

Obsérvese que se puede deducir “s” por la ecuación:

s = a XOR b.

Los valores a y b se denominan cuotas o porciones y están situados en depósitos separados. Una vez que el secreto s es dividido en dos o más cuotas, es desechado de una manera segura.

El analizador sintáctico de datos seguros de la presente invención puede utilizar esta función, realizando múltiples funciones XOR que incorporan múltiples valores de clave secreta distintos: K1, K2, K3, Kn, K5. Al principio de la operación, los datos que han de ser asegurados se hacen pasar a través de la primera operación de cifrado, datos seguros = datos XOR clave secreta 5:

S = D XOR K5

Con el fin de almacenar con seguridad los datos cifrados resultantes en, por ejemplo, cuatro cuotas, S1, S2, S3, Sn, los datos son analizados sintácticamente y divididos en “n” segmentos, o cuotas, de acuerdo con el valor de K5. Esta operación tiene como resultado “n” cuotas pseudoaleatorias de los datos cifrados originales. Después pueden realizarse funciones XOR subsiguientes sobre cada cuota con los valores de clave secreta restantes, por ejemplo: Segmento de datos seguros 1 = cuota de datos cifrados 1 XOR clave secreta 1:

SD1 = S1 XOR K1

SD2 = S2 XOR K2

SD3 = S3 XOR K3

SDn = Sn XOR Kn

En una realización, puede no desearse tener un depósito cualquiera que contenga suficiente información para descifrar la información allí guardada, así que la clave requerida para descifrar la cuota es almacenada en un depósito de datos diferente:

Depósito 1: SD1, Kn
Depósito 2: SD2, K1
Depósito 3: SD3, K2
Depósito n: SDn, K3.

Además, adjunta a cada cuota puede estar la información requerida para recuperar la clave de cifrado de sesión original, K5. Por lo tanto, en el ejemplo de gestión de claves descrito en este documento, se hace referencia a la clave maestra de sesión original por una ID de transacción dividida en “n” cuotas de acuerdo con el contenido de la clave maestra de analizador sintáctico dependiente de la instalación (TID1, TID2, TID3, TIDn):

Depósito 1: SD1, Kn, TID1
Depósito 2: SD2, K1, TID2
Depósito 3: SD3, K2, TID3
Depósito n: SDn, K3, TIDn.

En el ejemplo de clave de sesión incorporada descrito en este documento, la clave maestra de sesión es dividida en “n” cuotas de acuerdo con el contenido de la clave maestra de analizador sintáctico dependiente de la instalación (SKI, SK2, SK3, SKn):

Depósito 1: SD1, Kn, SK1
Depósito 2: SD2, K1, SK2
Depósito 3: SD3, K2, SK3
Depósito n: SDn, K3, SKn.

A menos que sean recuperadas las cuatro cuotas, los datos no pueden volver a ser ensamblados de acuerdo con este ejemplo. Aunque sean captadas las cuatro cuotas, no existe posibilidad de volver a ensamblar o restaurar la información original sin acceder a la clave maestra de sesión y la clave maestra de analizador sintáctico.

Este ejemplo ha descrito una realización del procedimiento de la presente invención, y también describe, en otra

realización, el algoritmo usado para poner las cuotas dentro de depósitos de modo que las cuotas procedentes de todos los depósitos puedan ser combinadas para formar el material de autenticación secreto. Los cálculos necesarios son muy sencillos y rápidos. Sin embargo, con el algoritmo One Time Pad (OTP) puede haber circunstancias que hagan que sea menos deseable, tales como que haya de ser asegurado un gran conjunto de datos, porque el tamaño de clave es el mismo tamaño que los datos que han de ser almacenados. Por lo tanto, existiría una necesidad de almacenar y transmitir aproximadamente el doble de la cantidad de los datos originales, lo cual puede ser menos deseable bajo ciertas circunstancias.

Cifrado en flujo RS1

La técnica de división por cifrado en flujo RS1 es muy similar a la técnica de división por OTP descrita en este documento. En lugar de un valor aleatorio de n *bytes*, se genera un valor aleatorio de n' = min(n, 16) *bytes* y se usa para codificar el algoritmo de cifrado en flujo RS1. La ventaja del algoritmo de cifrado en flujo RS1 es que se genera una clave pseudoaleatoria a partir de un número generador mucho más pequeño. La velocidad de ejecución del cifrado por cifrado en flujo RS1 también está graduada a aproximadamente 10 veces la velocidad del cifrado DES triple bien conocido en la técnica sin comprometer la seguridad. El algoritmo de cifrado en flujo RS1 es bien conocido en la técnica, y puede usarse para generar las claves usadas en la función XOR. El algoritmo de cifrado en flujo RS1 puede interactuar con otros algoritmos de cifrado en flujo disponibles comercialmente, tales como el algoritmo de cifrado en flujo RC4™ de RSA Security, Inc, y es adecuado para uso en los procedimientos de la presente invención.

Usando la notación de claves anterior, K1 a K5 ahora son valores aleatorios de n' *bytes* y se establece:

SD1 = S1 XOR E(K1)
SD2 = S2 XOR E(K2)
SD3 = S3 XOR E(K3)
SDn = Sn XOR E(Kn)

donde E(K1) a E(Kn) son los primeros n' *bytes* de salida del algoritmo de cifrado en flujo RS1 codificados por K1 a Kn. Las cuotas ahora se ponen dentro de depósitos de datos como se describe en este documento.

En este algoritmo RS1 de cifrado en flujo, los cálculos requeridos necesarios son casi tan simples y rápidos como el algoritmo OTP. El beneficio en este ejemplo usando el cifrado en flujo RS1 es que el sistema necesita almacenar y transmitir de media solo aproximadamente 16 *bytes* más que el tamaño de los datos originales que han de ser asegurados por cuota. Cuando el tamaño de los datos originales es más de 16 *bytes*, este algoritmo RS1 es más eficiente que el algoritmo OTP porque es simplemente más corto. Resulta inmediatamente evidente para cualquier experto en la materia que una amplia variedad de procedimientos o algoritmos de cifrados son adecuados para uso en la presente invención, incluyendo, pero no limitados a RS1, OTP, RC4™, DES triple, y AES.

Existen ventajas fundamentales proporcionadas por los procedimientos de seguridad de datos y los sistemas informáticos de la presente invención sobre los procedimientos de cifrado tradicionales. Una ventaja es la seguridad conseguida de mover las cuotas de los datos a diferentes ubicaciones en uno o más depósitos de datos o dispositivos de almacenamiento, que pueden estar en diferentes ubicaciones lógicas, físicas o geográficas. Cuando las cuotas de datos son divididas físicamente y están bajo el control de diferente personal, por ejemplo, se reduce en gran medida la posibilidad de comprometer los datos.

Otra ventaja proporcionada por los procedimientos y el sistema de la presente invención es la combinación de las etapas del procedimiento de la presente invención para asegurar datos para proporcionar un proceso completo de mantenimiento de la seguridad de los datos sensibles. Los datos son cifrados con una clave segura y divididos en una o más cuotas, y en una realización, cuatro cuotas, de acuerdo con la clave segura. La clave segura es almacenada con seguridad con un puntero de referencia que es asegurado dentro de cuatro cuotas de acuerdo con una clave segura. Después, las cuotas de datos son cifradas individualmente y las claves son almacenadas con seguridad con diferentes cuotas cifradas. Cuando se combinan, todo el proceso para asegurar datos de acuerdo con los procedimientos descritos en este documento se convierte en un paquete completo para seguridad de datos.

Los datos asegurados de acuerdo con los procedimientos de la presente invención son recuperables fácilmente y restaurados, reconstituidos, vueltos a ensamblar, descifrados, o devueltos de otro modo a su forma original u otra forma adecuada para su uso. Con el fin de restaurar los datos originales, pueden utilizarse los siguientes elementos:

1. Todas las cuotas o porciones del conjunto de datos.
2. El conocimiento de, y la capacidad de reproducir el flujo de proceso del procedimiento usado para asegurar los datos.
3. El acceso a la clave maestra de sesión.
4. El acceso a la clave maestra de analizador sintáctico.

Por lo tanto, puede ser deseable planear una instalación segura donde al menos uno de los elementos anteriores pueda estar separado físicamente de los restantes componentes del sistema (bajo el control de un administrador de sistema diferente, por ejemplo).

La protección contra una aplicación incontrolable que invoca la aplicación de procedimientos de seguridad de datos puede verse impuesta por el uso de la clave maestra de analizador sintáctico. En esta realización de la presente invención puede requerirse una toma de contacto de autenticación mutua entre el analizador sintáctico de datos seguros y la aplicación antes de adoptar cualquier acción.

La seguridad del sistema dicta que no hay un procedimiento “encubierto” para la recreación de los datos originales. Para instalaciones donde pueden surgir problemas de recuperación de datos, el analizador sintáctico de datos seguros puede ser mejorado para proporcionar una réplica de las cuatro cuotas y el depósito de clave maestra de sesión. Las opciones de hardware tales como RAID (batería redundante de discos de bajo coste, usada para dispersar la información por varios discos) y las opciones de software tales como la replicación pueden ayudar también en la planificación de recuperación de datos.

Gestión de claves

En una realización de la presente invención, el procedimiento de seguridad de datos usa tres conjuntos de claves para una operación de cifrado. Cada conjunto de claves puede tener opciones de almacenamiento, reparación, seguridad y recuperación de claves individuales, basadas en la instalación. Las claves que pueden usarse incluyen, pero no están limitadas a:

La clave maestra de analizador sintáctico

Esta clave es una clave individual asociada con la instalación del analizador sintáctico de datos seguros. Está instalada en el servidor en el cual ha sido desplegado el analizador sintáctico de datos seguros. Existe una diversidad de opciones adecuadas para asegurar esta clave, incluyendo, pero no limitadas a, una tarjeta inteligente, almacén de claves por hardware separado, almacenes de claves estándar, almacenes de claves personalizados o dentro de una tabla de base de datos asegurada, por ejemplo.

La clave maestra de sesión

Puede generarse una clave maestra de sesión cada vez que son asegurados datos. La clave maestra de sesión se usa para cifrar los datos antes de las operaciones de análisis sintáctico y división. También puede incorporarse (si la clave de sesión maestra no está integrada en los datos analizados sintácticamente) como medio de análisis sintáctico de los datos cifrados. La clave maestra de sesión puede ser asegurada de varias maneras, incluyendo, pero no limitadas a, un almacén de claves estándar, un almacén de claves personalizado, una tabla de base de datos separada, o asegurada dentro de las cuotas cifradas, por ejemplo.

Las claves de cifrado de cuotas

Para cada cuota o porción de un conjunto de datos que se crea, puede generarse una clave de cifrado de cuota individual para cifrar aún más las cuotas. Las claves de cifrado de cuotas pueden ser almacenadas en cuotas diferentes de la cuota que fue cifrada.

Resulta inmediatamente evidente para cualquier experto en la materia que los procedimientos de seguridad de datos y el sistema informático de la presente invención son ampliamente aplicables a cualquier tipo de datos en cualquier escenario o entorno. Además de aplicaciones comerciales llevadas a cabo por internet o entre clientes y vendedores, los procedimientos de seguridad de datos y los sistemas informáticos de la presente invención son muy aplicables a escenarios o entornos no comerciales o privados. Cualquier conjunto de datos que se desee mantener a salvo de cualquier usuario no autorizado puede ser asegurado usando los procedimientos y sistemas descritos en este documento. Por ejemplo, el acceso a una base de datos particular dentro de una compañía u organización

puede ser restringido ventajosamente a solo usuarios seleccionados empleando los procedimientos y sistemas de la presente invención para asegurar datos. Otro ejemplo es la generación, modificación o acceso a documentos donde se desea restringir el acceso o impedir el acceso no autorizado o accidental o la revelación fuera de un grupo de individuos, ordenadores o estaciones de trabajo seleccionados. Estos y otros ejemplos de los modos en que los procedimientos y sistemas de seguridad de datos de la presente invención son aplicables a cualquier entorno o escenario no comercial o comercial para cualquier escenario, incluyendo, pero no limitado a cualquier organización, agencia gubernamental o corporación.

En otra realización de la presente invención, el procedimiento de seguridad de datos usa tres conjuntos de claves para una operación de cifrado. Cada conjunto de claves puede tener opciones de almacenamiento, reparación, seguridad y recuperación de claves individuales, basadas en la instalación. Las claves que pueden usarse incluyen, pero no están limitadas a:

1. La clave maestra de analizador sintáctico

Esta clave es una clave individual asociada con la instalación del analizador sintáctico de datos seguros. Está instalada en el servidor en el cual ha sido desplegado el analizador sintáctico de datos seguros. Existe una diversidad de opciones adecuadas para asegurar esta clave, incluyendo, pero no limitadas a, una tarjeta inteligente, almacén de claves por hardware separado, almacenes de claves estándar, almacenes de claves personalizados o dentro de una tabla de base de datos asegurada, por ejemplo.

2. La clave maestra de sesión

Puede generarse una clave maestra de sesión cada vez que son asegurados datos. La clave maestra de sesión se usa conjuntamente con la clave maestra de analizador sintáctico para deducir la clave intermedia. La clave maestra de sesión puede ser asegurada de varias maneras, incluyendo, pero no limitadas a, un almacén de claves estándar, un almacén de claves personalizado, una tabla de base de datos separada, o asegurada dentro de las cuotas cifradas, por ejemplo.

3. La clave intermedia

Puede generarse una clave intermedia cada vez que son asegurados datos. La clave intermedia se usa para cifrar los datos antes de la operación de análisis sintáctico y división. También puede incorporarse como medio de análisis sintáctico de los datos cifrados.

4. Claves de cifrado de cuotas

Para cada cuota o porción de un conjunto de datos que se crea, puede generarse una clave de cifrado de cuota individual para cifrar aún más las cuotas. Las claves de cifrado de cuotas pueden ser almacenadas en cuotas diferentes de la cuota que fue cifrada.

Resulta inmediatamente evidente para cualquier experto en la materia que los procedimientos de seguridad de datos y el sistema informático de la presente invención son ampliamente aplicables a cualquier tipo de datos en cualquier escenario o entorno. Además de aplicaciones comerciales llevadas a cabo por internet o entre clientes y vendedores, los procedimientos de seguridad de datos y los sistemas informáticos de la presente invención son muy aplicables a escenarios o entornos no comerciales o privados. Cualquier conjunto de datos que se desee mantener a salvo de cualquier usuario no autorizado puede ser asegurado usando los procedimientos y sistemas descritos en este documento. Por ejemplo, el acceso a una base de datos particular dentro de una compañía u organización puede ser restringido ventajosamente a solo usuarios seleccionados empleando los procedimientos y sistemas de la presente invención para asegurar datos. Otro ejemplo es la generación, modificación o acceso a documentos donde se desea restringir el acceso o impedir el acceso no autorizado o accidental o la revelación fuera de un grupo de individuos, ordenadores o estaciones de trabajo seleccionados. Estos y otros ejemplos de los modos en que los procedimientos y sistemas de seguridad de datos de la presente invención son aplicables a cualquier entorno o escenario no comercial o comercial para cualquier escenario, incluyendo, pero no limitado a cualquier organización, agencia gubernamental o corporación.

Seguridad de datos por grupo de trabajo, proyecto, ordenador personal/portátil individual o de plataformas cruzadas

Los procedimientos de seguridad de datos y los sistemas informáticos de la presente invención también son útiles

para asegurar datos por grupo de trabajo, proyecto, ordenador personal/portátil individual y cualquier otra plataforma que esté en uso en, por ejemplo, negocios, oficinas, agencias gubernamentales, o cualquier escenario en el que se crean, manipulan o almacenan datos sensibles. La presente invención proporciona procedimientos y sistemas informáticos para asegurar datos que se sabe que son buscados por organizaciones, tales como el gobierno de EE.UU., para su implementación por toda la organización gubernamental o entre gobiernos a nivel estatal o federal.

Los procedimientos de seguridad de datos y los sistemas informáticos de la presente invención proporcionan la capacidad no solo de analizar sintácticamente y dividir archivos planos sino también campos, conjuntos o tablas de datos de cualquier tipo. Además, toda forma de datos es capaz de ser asegurada bajo este proceso, incluyendo, pero no limitados a datos de texto, vídeo, imágenes, biometría y voz. La escalabilidad, la velocidad y la producción de datos de los procedimientos de seguridad de datos de la presente invención solo están limitados al hardware que el usuario tiene a su disposición.

En una realización de la presente invención, los procedimientos de seguridad de datos se utilizan como se describe más adelante en un entorno de grupo de trabajo. En una realización, como se muestra en la figura 23 y se describe más adelante, el procedimiento de seguridad de datos a escala de grupo de trabajo de la presente invención usa la funcionalidad de gestión de claves privadas del motor de confianza para almacenar las relaciones usuario/grupo y las claves privadas asociadas (claves maestras de grupo de analizador sintáctico) necesarias para que un grupo de usuarios compartan los datos seguros. El procedimiento de la presente invención tiene la capacidad de asegurar datos para una empresa, un grupo de trabajo, o un usuario individual, dependiendo de cómo fue desplegada la clave maestra de analizador sintáctico.

En una realización, pueden estar previstos programas adicionales de gestión de claves y de gestión de usuarios/grupos. La generación, gestión y revocación de claves son tratadas por el programa de mantenimiento único, volviéndose todos ellos especialmente importantes a medida que aumenta el número de usuarios. En otra realización, también puede establecerse gestión de claves a través de uno o varios administradores de sistemas diferentes, que pueden no permitir que ninguna persona o grupo controle los datos según sea necesario. Esto permite que la gestión de datos asegurados se obtenga por papeles, responsabilidades, pertenencia, derechos, etc., tal como se defina por una organización, y el acceso a los datos asegurados puede ser limitado solo a quienes se les permita o sea necesario que tengan acceso únicamente a la porción en la que están trabajando, mientras que otros, tales como directores o ejecutivos, pueden tener acceso a todos los datos asegurados. Esta realización permite la compartición de datos asegurados entre diferentes grupos dentro de una compañía u organización mientras que al mismo tiempo solo permite que ciertos individuos seleccionados, tales como quienes tienen los papeles y responsabilidades autorizados y predeterminados, observen los datos en conjunto. Además, esta realización de los procedimientos y sistemas de la presente invención también permite la compartición de datos entre, por ejemplo, compañías separadas, o departamentos o divisiones de compañías separados, o cualquier departamento de organización, grupo, agencia, u oficina o similar separado, de cualquier gobierno u organización de cualquier clase, donde se requiera algo de compartición, pero no que a cualquier parte se le permita tener acceso a todos los datos. Ejemplos particularmente evidentes de la necesidad y utilidad de tal procedimiento y sistema de la presente invención son permitir la compartición, pero mantener la seguridad, entre áreas, agencias y oficinas gubernamentales, y entre diferentes divisiones, departamentos u oficinas de una gran compañía, o cualquier otra organización, por ejemplo.

Un ejemplo de la aplicación de los procedimientos de la presente invención a menor escala es el siguiente. Se usa una clave maestra de analizador sintáctico como serialización o creación de marca del analizador sintáctico de datos seguros a una organización. A medida que la escala de uso de la clave maestra de analizador sintáctico se reduce de toda la empresa a un grupo de trabajo más pequeño, los procedimientos de seguridad de datos descritos en este documento se usan para compartir archivos dentro de grupos de usuarios.

En el ejemplo mostrad en la figura 25 y descrito más adelante, hay seis usuarios definidos junto con su tratamiento o papel dentro de la organización. La barra lateral representa cinco posibles grupos a los que pueden pertenecer los usuarios de acuerdo con su papel. La flecha representa la pertenencia del usuario a uno o más de los grupos.

Cuando se configura el analizador sintáctico de datos seguros para su uso en este ejemplo, el administrador del sistema accede a la información de usuarios y grupos desde el sistema operativo mediante un programa de mantenimiento. Este programa de mantenimiento genera y asigna claves maestras de grupo de analizador sintáctico a los usuarios basándose en su pertenencia a grupos.

En este ejemplo, hay tres miembros en el grupo de altos cargos. Para este grupo, las acciones serían:

1. Acceder a la clave maestra de grupo de analizador sintáctico para el grupo de altos cargos (generar una clave si no se dispone de ella);
2. Generar un certificado digital que asocia el CEO con el grupo de altos cargos;
3. Generar un certificado digital que asocia el CFO con el grupo de altos cargos;
4. Generar un certificado digital que asocia el vicepresidente de marketing con el grupo de altos cargos.

Se realizaría el mismo conjunto de acciones para cada grupo, y cada miembro dentro de cada grupo. Cuando el programa de mantenimiento está terminado, la clave maestra de grupo de analizador sintáctico se convierte en una credencial compartida para cada miembro del grupo. La revocación del certificado digital asignado puede realizarse automáticamente cuando un usuario es eliminado de un grupo mediante el programa de mantenimiento sin afectar al resto de los miembros del grupo.

Una vez que las credenciales compartidas han sido definidas, el proceso de análisis sintáctico y división sigue siendo el mismo. Cuando un archivo, documento o elemento de datos ha de ser asegurado, se consulta al usuario qué grupo objetivo ha de usarse al asegurar los datos. Los datos asegurados resultantes solo son accesibles por parte de otros miembros del grupo objetivo. Esta funcionalidad de los procedimientos y sistemas de la presente invención puede usarse con cualquier otro sistema informático o plataforma de software, y puede estar integrada, por ejemplo, en programas de aplicación existentes o usarse independientemente para seguridad de archivos.

Resulta inmediatamente evidente para cualquier experto en la materia que uno cualquiera o una combinación de algoritmos de cifrado son adecuados para uso en los procedimientos y sistemas de la presente invención. Por ejemplo, las etapas de cifrado, en una realización, pueden repetirse para producir un esquema de cifrado de múltiples capas. Además, puede usarse un algoritmo de cifrado diferente, o una combinación de algoritmos de cifrado, en etapas de cifrado repetidas de modo que se aplican diferentes algoritmos de cifrado a las diferentes capas del esquema de cifrado de capas múltiples. Como tal, el esquema de cifrado en sí puede convertirse en un componente de los procedimientos de la presente invención para asegurar datos sensibles contra un uso o acceso no autorizado.

El analizador sintáctico de datos seguros puede incluir como componente interno, como componente externo, o como ambos un componente de comprobación de errores. Por ejemplo, en una estrategia adecuada, como las porciones de datos se crean usando el analizador sintáctico de datos seguros de acuerdo con la presente invención, para garantizar la integridad de los datos dentro de una porción, se toma un valor de troceo a intervalos prefijados dentro de la porción y se adjunta al final del intervalo. El valor de troceo es una representación numérica predecible y reproducible de los datos. Si algún bit dentro de los datos cambia, el valor de troceo sería diferente. Un módulo de escaneo (ya sea como un componente independiente externo al analizador sintáctico de datos seguros o como un componente interno) puede entonces escanear las porciones de datos generadas por el analizador sintáctico de datos seguros. Cada porción de datos (o alternativamente, menos de la totalidad de las porciones de datos de acuerdo con algún intervalo o mediante un muestreo aleatorio o pseudoaleatorio) es comparada con el valor o los valores de troceo adjuntos y puede adoptarse una acción. Esta acción puede incluir un informe de los valores que coinciden y no coinciden, una alerta para los valores que no coinciden, o la invocación de algún programa externo o interno para activar una recuperación de los datos. Por ejemplo, la recuperación de los datos podría realizarse invocando un módulo de recuperación basándose en el concepto de que pueden ser necesarias menos de la totalidad de las porciones para generar datos originales de acuerdo con la presente invención.

Cualquier otra comprobación de integridad adecuada puede implementarse usando cualquier información de integridad adecuada adjunta en alguna parte en todas o en un subconjunto de porciones de datos. La información de integridad puede incluir cualquier información adecuada que pueda usarse para determinar la integridad de las porciones de datos. Ejemplos de información de integridad pueden incluir valores de troceo calculados basándose en cualquier parámetro adecuado (por ejemplo, basándose en porciones de datos respectivas), información de firma digital, información de código de autenticación de mensaje (MAC), cualquier otra información adecuada, o cualquier combinación de los mimos.

El analizador sintáctico de datos seguros de la presente invención puede usarse en cualquier aplicación adecuada. Concretamente, el analizador sintáctico de datos seguros descrito en este documento tiene una diversidad de aplicaciones en diferentes áreas de la computación y la tecnología. Varias de tales áreas se analizan más adelante. Se entenderá que estas son de naturaleza meramente ilustrativa y que cualquier otra aplicación adecuada puede hacer uso del analizador sintáctico de datos seguros. Además se entenderá que los ejemplos descritos son realizaciones meramente ilustrativas que pueden modificarse de cualquier manera adecuada con el fin de satisfacer

cualquier deseo adecuado. Por ejemplo, el análisis sintáctico y la división pueden estar basados en cualquier unidad adecuada, tal como por bits, por *bytes*, por *kilobytes*, por *megabytes*, por cualquier combinación de las mismas o por cualquier otra unidad adecuada.

El analizador sintáctico de datos seguros de la presente invención puede usarse para implementar testigos físicos seguros, por lo que los datos almacenados en un testigo físico pueden requerirse con el fin de acceder a datos adicionales almacenados en otra área de almacenamiento. En una estrategia adecuada, puede usarse un testigo físico, tal como una unidad flash USB compacta, un disco flexible, un disco óptico, una tarjeta inteligente, o cualquier otro testigo físico adecuado, para almacenar una de al menos dos porciones de datos analizados sintácticamente de acuerdo con la presente invención. Con el fin de acceder a los datos originales, tendría que accederse a la unidad flash USB. Así, un ordenador personal que guarda una porción de los datos analizados sintácticamente tendría que tener la unidad flash USB, que tiene la otra porción de datos analizados sintácticamente, conectada antes de que pueda accederse a los datos originales. La figura 26 ilustra esta aplicación. El área de almacenamiento (2500) incluye una porción de datos analizados sintácticamente (2502). El testigo físico (2504), que tiene una porción de datos analizados sintácticamente (2506) tendría que ser acoplado al área de almacenamiento (2500) usando cualquier interfaz de comunicaciones adecuada (2508) (por ejemplo, USB, en serie, en paralelo, Bluetooth, IR, IEEE 1394, Ethernet, o cualquier otra interfaz de comunicaciones adecuada) con el fin de acceder a los datos originales. Esto resulta útil en una situación en la que, por ejemplo, los datos sensibles de un ordenador se dejan solos y sujetos a intentos de acceso no autorizado. Extrayendo el testigo físico (por ejemplo, la unidad flash USB), los datos sensibles son inaccesibles. Se entenderá que puede usarse cualquier otra estrategia adecuada para usar testigos físicos.

El analizador de datos seguros de la presente invención puede usarse para implementar un sistema de autenticación segura por el cual los datos de inscripción de usuario (por ejemplo, contraseñas, claves de cifrado privadas, plantillas de huellas dactilares, datos biométricos o cualquier otro datos de inscripción de usuario adecuado) son analizados sintácticamente y divididos usando el analizador sintáctico de datos seguros. Los datos de inscripción de usuario pueden ser analizados sintácticamente y divididos por lo que una o más porciones son almacenadas en una tarjeta inteligente, una tarjeta de acceso común gubernamental, cualquier dispositivo de almacenamiento físico adecuado (por ejemplo, disco magnético u óptico, unidad de llave USB, etc.), o cualquier otro dispositivo adecuado. Una u otras porciones más de los datos de inscripción de usuario analizados sintácticamente pueden ser almacenadas en el sistema que realiza la autenticación. Esto proporciona un nivel de seguridad añadido al proceso de autenticación (por ejemplo, además de la información de autenticación biométrica obtenida de la fuente biométrica, los datos de inscripción de usuario también pueden obtenerse por medio de la porción de datos analizados sintácticamente y divididos apropiada).

El analizador sintáctico de datos seguros de la presente invención puede estar integrado dentro de cualquier sistema existente adecuado con el fin de proporcionar el uso de su funcionalidad en el entorno respectivo de cada sistema. La figura 27 muestra un diagrama de bloques de un sistema ilustrativo (2600), que puede incluir software, hardware o ambos para implementar cualquier aplicación adecuada. El sistema (2600) puede ser un sistema existente en el cual el analizador sintáctico de datos seguros (2602) puede ser actualizado como un componente integrado. Alternativamente, el analizador sintáctico de datos seguros (2602) puede ser integrado dentro de cualquier sistema (2600) adecuado, por ejemplo, desde su fase de diseño más temprana. El analizador sintáctico de datos seguros (2600) puede ser integrado en cualquier nivel adecuado del sistema (2600). Por ejemplo, el analizador sintáctico de datos seguros (2602) puede ser integrado dentro del sistema (2600) a un nivel suficientemente de extremo trasero de modo que la presencia del analizador sintáctico de datos seguros (2602) puede ser sustancialmente transparente para un usuario final del sistema (2600). El analizador sintáctico de datos seguros (2602) puede usarse para analizar sintácticamente y dividir datos entre uno o más dispositivos de almacenamiento (2604) de acuerdo con la presente invención. Más adelante se analizan algunos ejemplos ilustrativos de sistemas que tienen el analizador sintáctico de datos seguros integrado en los mismos.

El analizador sintáctico de datos seguros de la presente invención puede ser integrado en un núcleo de sistema operativo (por ejemplo, Linux, Unix, o cualquier otro sistema operativo comercial o en propiedad adecuado). Esta integración puede usarse para proteger datos al nivel de dispositivo por lo que, por ejemplo, los datos que generalmente serían almacenados en uno o más dispositivos son separados en un cierto número de porciones por el analizador sintáctico de datos seguros integrado dentro del sistema operativo y almacenadas entre el 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 analizados sintácticamente en los datos originales de un modo que puede ser transparente para el usuario final.

El analizador sintáctico de datos seguros de la presente invención puede estar integrado dentro de un administrador de volúmenes o cualquier otro componente adecuado de un sistema de almacenamiento para proteger el almacenamiento de datos locales y conectado en red a través de cualquiera de las plataformas soportada o todas ellas. Por ejemplo, con el analizador sintáctico de datos seguros integrado, un sistema de almacenamiento puede hacer uso de la redundancia ofrecida por el analizador sintáctico de datos seguros (es decir, el que se usa para implementar la característica de necesitar menos de la totalidad de las porciones separadas de los datos con el fin de reconstruir los datos originales) para proteger contra la pérdida de datos. El analizador sintáctico de datos seguros también permite que todos los datos escritos en dispositivos de almacenamiento, ya sea usando redundancia o no, estén en 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 administrador de volúmenes u otro componente adecuado del sistema de almacenamiento, puede recombinar las porciones de datos analizadas sintácticamente en los datos originales de un modo que puede ser transparente para el usuario final.

En una estrategia adecuada, el analizador sintáctico de datos seguros de la presente invención puede estar integrado dentro de un controlador RAID (ya sea como hardware o como software). Esto permite el almacenamiento seguro de datos en múltiples unidades en tanto que manteniendo la tolerancia a fallos en caso de fallo de una unidad.

El analizador sintáctico de datos seguros de la presente invención puede estar integrado dentro de una base de datos con el fin, por ejemplo, de proteger información en tablas sensible. Por ejemplo, en una estrategia adecuada, los datos asociados con celdas particulares de una tabla de base de datos (por ejemplo, celdas individuales, una o más columnas particulares, una o más filas particulares, cualquier combinación de las mismas, o una tabla de base de datos entera) pueden ser analizados sintácticamente y separados de acuerdo con la presente invención (por ejemplo, cuando las diferentes porciones son almacenadas en uno o más dispositivos de almacenamiento en una o más ubicaciones o en un solo dispositivo de almacenamiento). El acceso para recombinar las porciones con el fin de ver los datos originales puede ser concedido mediante procedimientos de autenticación tradicionales (por ejemplo, la indagación de nombre de usuario y contraseña).

El analizador sintáctico de datos seguros de la presente invención puede estar integrado en cualquier sistema adecuado que implique datos en movimiento (es decir, transferencia de datos de una ubicación a otra). Tales sistemas incluyen, por ejemplo, correo electrónico, difusiones de datos de transmisión continua, y comunicaciones inalámbricas (por ejemplo, WiFi). Con respecto al correo electrónico, en una estrategia adecuada, el analizador sintáctico de datos seguros puede usarse para analizar sintácticamente los mensajes salientes (es decir, que contienen texto, datos binarios o ambos (por ejemplo, archivos adjuntos a un mensaje de correo electrónico)) y enviar las diferentes porciones de los datos analizados sintácticamente a lo largo de diferentes trayectos creando así múltiples trenes de datos. Si uno cualquiera de estos trenes de datos se ve comprometido, el mensaje original permanece seguro porque el sistema puede requerir que sean combinadas más de una de las porciones, de acuerdo con la presente invención, con el fin de generar los datos originales. En otra estrategia adecuada, las diferentes porciones de datos pueden ser comunicadas a lo largo de un trayecto secuencialmente de modo que si se obtiene una porción, puede no ser suficiente para generar los datos originales. Las diferentes porciones llegan a la ubicación del receptor deseado y pueden ser combinadas para generar los datos originales de acuerdo con la presente invención.

Las figuras 28 y 29 son diagramas de bloques ilustrativos de tales sistemas de correo electrónico. La figura 28 muestra un sistema remitente (2700), que puede incluir cualquier hardware adecuado, tal como un terminal de ordenador, un ordenador personal, un dispositivo de mano (por ejemplo, PDA, Blackberry), un teléfono celular, una red de ordenadores, o cualquier otro hardware adecuado, o cualquier combinación de los mismos. El sistema remitente (2700) se usa para generar y/o almacenar un mensaje (2704), que puede ser, por ejemplo, un mensaje de correo electrónico, un archivo de datos binarios (por ejemplo, gráficos, voz, vídeo, etc.) o ambos. El mensaje (2704) es analizado sintácticamente y dividido por el analizador sintáctico de datos seguros (2702) de acuerdo con la presente invención. Las porciones de datos resultantes pueden ser comunicadas a través de uno o más trayectos de comunicaciones separados (2706) a través de la red (2708) (por ejemplo, internet, una intranet, una LAN, WiFi, Bluetooth, cualquier otro medio de comunicaciones por cable o inalámbricas adecuado, o cualquier combinación de los mismos) al sistema receptor (2710). Las porciones de datos pueden ser comunicadas en paralelo en el tiempo o alternativamente, de acuerdo con cualquier retardo adecuado entre la comunicación de las diferentes porciones de datos. El sistema receptor (2710) puede ser cualquier hardware adecuado como se describe anteriormente con respecto al sistema remitente (2700). Las porciones de datos separadas transportadas a lo largo de los trayectos de comunicaciones (2706) son recombinadas en el sistema receptor (2710) para generar el mensaje o los datos

originales de acuerdo con la presente invención.

La figura 29 muestra un sistema remitente (2800), que puede incluir cualquier hardware adecuado, tal como un terminal de ordenador, un ordenador personal, un dispositivo de mano (por ejemplo, PDA) , un teléfono celular, una red de ordenadores, cualquier otro hardware adecuado, o cualquier combinación de los mismos. El sistema remitente (2800) se usa para generar y/o almacenar un mensaje (2804), que puede ser, por ejemplo, un mensaje de correo electrónico, un archivo de datos binarios (por ejemplo, gráficos, voz, vídeo, etc.) o ambos. El mensaje (2804) es analizado sintácticamente y dividido por el analizador sintáctico de datos seguros (2802) de acuerdo con la presente invención. Las porciones de datos resultantes pueden ser comunicadas a través de uno o más trayectos de comunicaciones individuales (2806) por la red (2808) (por ejemplo, internet, una intranet, una LAN, WiFi, Bluetooth, cualquier otro medio de comunicaciones adecuado, o cualquier combinación de los mismos) al sistema receptor (2810). Las porciones de datos pueden ser comunicadas en serie a través del trayecto de comunicaciones (2806) unas respecto a otras. El sistema receptor (2810) puede ser cualquier hardware adecuado como se describe anteriormente con respecto al sistema remitente (2800). Las porciones de datos separadas transportadas a lo largo del trayecto de comunicaciones (2806) son recombinadas en el sistema receptor (2810) para generar el mensaje o los datos originales de acuerdo con la presente invención.

Se entenderá que las disposiciones de las figuras 28 y 29 son meramente ilustrativas. Puede usarse cualquier otra disposición adecuada. Por ejemplo, en otra estrategia adecuada, las características de los sistemas de las figuras 28 y 29 pueden combinarse por lo que se usa la estrategia multitrayecto de la figura 28 y en la cual se usan uno o más trayectos de comunicaciones (2706) para transportar más de una porción de datos como lo hace el trayecto de comunicaciones (2806) en el contexto de la figura 29.

El analizador sintáctico de datos seguros puede estar integrado en cualquier nivel adecuado de un sistema de datos en movimiento. Por ejemplo, en el contexto de un sistema de correo electrónico, el analizador sintáctico de datos seguros puede estar integrado en el nivel de interfaz de usuario (por ejemplo, dentro de Microsoft® Outlook), en cuyo caso el usuario puede tener control sobre el uso de las características de analizador sintáctico de datos seguros cuando usa el correo electrónico. Alternativamente, el analizador sintáctico de datos seguros puede implementarse en un componente de extremo trasero tal como en el servidor de intercambio, en cuyo caso los mensajes pueden ser analizados sintácticamente, divididos y comunicados automáticamente a lo largo de diferentes trayectos de acuerdo con la presente invención sin ninguna intervención por parte del usuario.

De manera similar, en el caso de difusiones de datos de transmisión continua (por ejemplo, audio, vídeo), los datos salientes pueden ser analizados sintácticamente y separados en múltiples trenes que contienen cada uno una porción de los datos analizados sintácticamente. Los múltiples trenes pueden ser transmitidos a lo largo de uno o más trayectos y recombinados en la ubicación del receptor de acuerdo con la presente invención. Uno de los beneficios de esta estrategia es que evita la tara relativamente grande asociada con el cifrado tradicional de datos seguido por la transmisión de los datos cifrados por un único canal de comunicaciones. El analizador sintáctico de datos seguros de la presente invención permite que los datos en movimiento sean enviados en múltiples trenes paralelos, aumentando la velocidad y la eficiencia.

Se entenderá que el analizador sintáctico de datos seguros puede estar integrado para protección y tolerancia a fallos de cualquier tipo de datos en movimiento a través de cualquier medio de transporte, incluyendo, por ejemplo, por cable, inalámbrico, o físico. Por ejemplo, las aplicaciones de voz sobre protocolo internet (VoIP) pueden hacer uso del analizador sintáctico de datos seguros de la presente invención. El transporte de datos inalámbrico o por cable desde o hacia cualquier dispositivo asistente digital personal (PDA) adecuado tal como Blackberries o teléfonos inteligentes puede asegurarse usando el analizador sintáctico de datos seguros de la presente invención. Las comunicaciones que usan protocolos inalámbricos 802.11 para redes inalámbricas entre pares y basadas en nodo centralizado, comunicaciones por satélite, comunicaciones inalámbricas punto a punto, comunicaciones cliente/servidor por internet, o cualquier otra comunicación adecuada pueden implicar las capacidades de datos en movimiento del analizador sintáctico de datos seguros de acuerdo con la presente invención. La comunicación entre un dispositivo periférico informático (por ejemplo, un impresora, un escáner, un monitor, un teclado, un encaminador de red, un dispositivo de autenticación biométrica (por ejemplo, un escáner de huella digital), o cualquier otro dispositivo periférico adecuado) entre un ordenador y un dispositivo periférico informático, entre un dispositivo periférico informático 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 al presente invención también pueden aplicarse al transporte físico de cuotas seguras usando, por ejemplo, rutas separadas, vehículos, procedimientos, y cualquier otro transporte físico

adecuado, o cualquier combinación de los mismos. Por ejemplo, el transporte físico de datos puede tener lugar en cintas digitales/magnéticas, discos flexibles, discos ópticos, testigos físicos, unidades USB, unidades rígidas extraíbles, dispositivos electrónicos de consumo con memoria flash (por ejemplo, IPOD de Apple u otros reproductores MP3), memoria flash, y cualquier otro medio adecuado usado para transportar datos, o cualquier combinación de los mismos.

El analizador sintáctico de datos seguros de la presente invención puede proporcionar seguridad con la capacidad de recuperación ante desastres. De acuerdo con la presente invención, pueden ser necesarias menos de la totalidad de las porciones de los datos separados generados por el analizador sintáctico de datos seguros con el fin de recuperar los datos originales. Es decir, de m porciones almacenadas, n puede ser el número mínimo de estas m porciones necesarias para recuperar los datos originales, donde n <= m. Por ejemplo, si cada una de las cuatro porciones es almacenada en una ubicación física diferente en relación con las otras tres porciones, entonces, si n=2 en este ejemplo, dos de las ubicaciones pueden verse comprometidas por lo que los datos son destruidos o son inaccesibles, y aun así los datos originales pueden ser recuperados a partir de las porciones de las otras dos ubicaciones. Puede usarse cualquier valor adecuado para n o m.

Además, la característica de n de m de la presente invención puede usarse para crear una “regla de dos hombres” por la que con el fin de evitar confiar a un solo individuo o cualquier otra entidad con pleno acceso lo que pueden ser datos sensibles, dos o más entidades distintas, cada una con una porción de los datos separados analizados sintácticamente por el analizador sintáctico de datos seguros de la presente invención pueden tener que ponerse de acuerdo en juntar sus porciones con el fin de recuperar los datos originales.

El analizador sintáctico de datos seguros de la presente invención puede usarse para proporcionar a un grupo de entidades una clave de todo el grupo que permite a los miembros del grupo acceder a información particular a la que ese grupo particular está autorizado a acceder. La clave de grupo puede ser una de las porciones de datos generadas por el analizador sintáctico de datos seguros de acuerdo con la presente invención que puede requerirse que sea combinada con otra porción almacenada centralmente, por ejemplo con el fin de recuperar la información buscada. Esta característica permite, por ejemplo, la colaboración segura entre un grupo. Puede aplicarse, por ejemplo, en redes dedicadas, redes privadas virtuales, intranets, o cualquier otra red adecuada.

Aplicaciones específicas de este uso del analizador sintáctico de datos seguros incluyen, por ejemplo, la compartición de información de coalición en la que, por ejemplo, a unas fuerzas multinacionales de gobiernos amigos se les da la capacidad de comunicar datos operativos y sensibles de otro tipo sobre un nivel de seguridad autorizado a cada país respectivo por una sola red o una red doble (es decir, comparada con las muchas redes que implican procesos manuales relativamente sustanciales usadas actualmente). Esta capacidad también es aplicable para compañías u otras organizaciones en las cuales la información que necesita ser conocida por uno o más individuos específicos (dentro o fuera de la organización) puede ser comunicada por una sola red sin la necesidad de preocuparse porque individuos no autorizados vean la información.

Otra aplicación específica incluye una jerarquía de seguridad multinivel para sistemas gubernamentales. Es decir, el analizador sintáctico de datos seguros de la presente invención puede proporcionar la capacidad de operar un sistema gubernamental a diferentes niveles de información clasificada (por ejemplo, desclasificada, clasificada, secreta, de alto secreto) usando una sola red. Si se desea, pueden usarse más redes (por ejemplo, una red separada para alto secreto), pero la presente invención permite sustancialmente menos que la disposición actual en la cual se usa una red separada para cada nivel de clasificación.

Se entenderá que puede usarse cualquier combinación de las aplicaciones descritas anteriormente del analizador sintáctico de datos seguros de la presente invención. Por ejemplo, puede usarse la aplicación de clave de grupo junto con la aplicación de seguridad de datos en movimiento (es decir, por la cual a los datos que son comunicados por una red solo puede acceder un miembro del grupo respectivo y donde, mientras los datos están en movimiento, son divididos en múltiples trayectos (o enviados en porciones secuenciales) de acuerdo con la presente invención).

El analizador sintáctico de datos seguros de la presente invención puede estar integrado dentro de cualquier aplicación de middleware para permitir que las aplicaciones almacenen con seguridad datos en diferentes productos de base de datos o en diferentes dispositivos sin modificación en las aplicaciones o la base de datos. Middleware es un término general para cualquier producto que permite que dos programas separados y ya existentes se comuniquen. Por ejemplo, en una estrategia adecuada, puede usarse middleware que tiene integrado el analizador sintáctico de datos seguros para permitir que los programas escritos para una base de datos particular se comuniquen con otras bases de datos sin codificación personalizada.

El analizador sintáctico de datos seguros de la presente invención puede implementarse con cualquier combinación de cualquier capacidad adecuada, tales como las analizadas en este documento. En algunas realizaciones de la presente invención, por ejemplo, en analizador sintáctico de datos seguros puede implementarse con solo ciertas capacidades mientras que otras capacidades pueden obtenerse mediante el uso de software o hardware externo, o ambos, interconectados o bien directamente o bien indirectamente con el analizador sintáctico de datos seguros.

La figura 30, por ejemplo, muestra una implementación ilustrativa del analizador sintáctico de datos seguros como en analizador sintáctico de datos seguros (3000). El analizador sintáctico de datos seguros (3000) puede implementarse con muy pocas capacidades integradas. Como se ilustra, el analizador sintáctico de datos seguros (3000) puede incluir capacidades integradas para analizar sintácticamente y dividir datos en porciones (también denominadas en este documento como cuotas) de datos usando el módulo (3002) de acuerdo con la presente invención. El analizador sintáctico de datos seguros (3000) también puede incluir capacidades integradas para realizar redundancia con el fin de poder implementar, por ejemplo, la característica de m de n descrita anteriormente (es decir, recrear los datos originales usando menos de la totalidad de las cuotas de datos analizados sintácticamente y divididos) usando el módulo (3004). El analizador sintáctico de datos seguros (3000) también puede incluir capacidades de distribución de cuotas usando el módulo (3006) para poner las cuotas de datos dentro de memorias intermedias desde las cuales son enviadas para comunicación a una ubicación remota, para almacenamiento, etc. de acuerdo con la presente invención. Se entenderá que cualquier otra capacidad adecuada puede integrarse dentro del analizador sintáctico de datos seguros (3000).

La memoria intermedia de datos ensamblados (3008) puede ser cualquier memoria adecuada usada para almacenar los datos originales (aunque no necesariamente en su forma original) que serán analizados sintácticamente y divididos por el analizador sintáctico de datos seguros (3000). En una operación de división, la memoria intermedia de datos ensamblados (3008) proporciona entrada al analizador sintáctico de datos seguros (3008). En una aplicación de restauración, la memoria intermedia de datos ensamblados (3008) puede usarse para almacenar la salida del analizador sintáctico de datos seguros (3000).

Las memorias intermedias de cuotas divididas (3010) pueden ser uno o más módulos de memoria que pueden usarse para almacenar las múltiples cuotas de datos que resultaron del análisis sintáctico y la división de los datos originales. En una operación de división, las memorias intermedias de cuotas divididas (3010) guardan la salida del analizador sintáctico de datos seguros. En una operación de restauración, las memorias intermedias de cuotas divididas guardan la entrada al analizador sintáctico de datos seguros (3000).

Se entenderá que puede integrarse cualquier otra disposición adecuada de capacidades para el analizador sintáctico de datos seguros (3000). Puede integrarse cualquier característica adicional y cualquiera de las características ilustradas puede eliminarse, hacerse más robusta, hacerse menos robusta, o modificarse si no de cualquier manera adecuada. Las memorias intermedias (3008) y (3010) son asimismo meramente ilustrativas y pueden modificarse, eliminarse, o añadirse de cualquier manera adecuada.

Cualquier módulo adecuado implementado en software, hardware o ambos puede ser llamado por o puede llamar al analizador sintáctico de datos seguros (3000). Si se desea, incluso las capacidades que están integradas en el analizador sintáctico de datos seguros (3000) pueden ser reemplazadas por uno o más módulos externos. Como se ilustra, algunos módulos externos incluyen el generador de números aleatorios (3012), el generador de claves de realimentación de cifrado (3014), el algoritmo de troceo (3016), uno cualquiera o más tipos de cifrado (3018), y la gestión de claves (3020). Se entenderá que estos son módulos externos meramente ilustrativos. Puede usarse cualquier otro módulo adecuado además de o en lugar de los ilustrados.

El generador de claves de realimentación de cifrado (3014) puede, externamente al analizador sintáctico de datos seguros (3000), generar para cada operación del analizador sintáctico de datos seguros, una clave única, o un número aleatorio (usando, por ejemplo, el generador de números aleatorios (3012), que ha de usarse como valor generador para una operación que amplía un tamaño de clave de sesión original (por ejemplo, un valor de 128, 256, 512, o 1024 bits) a un valor igual a la longitud de los datos que han de ser analizados sintácticamente y divididos. Puede usarse cualquier algoritmo adecuado para la generación de claves de realimentación de cifrado, incluyendo, por ejemplo, el algoritmo de generación de claves de realimentación de cifrado AES.

Con el fin de facilitar la integración del analizador sintáctico de datos seguros (3000) y sus módulos externos (es decir, la capa de analizador sintáctico de datos seguros (3026)) dentro de una capa de aplicación (3024) (por ejemplo, una aplicación de correo electrónico, una aplicación de base de datos, etc.), puede usarse una capa de

envoltura que puede hacer uso de, por ejemplo, llamadas de función API. Puede usarse cualquier otra disposición adecuada para facilitar la integración de la capa de analizador sintáctico de datos seguros (3026) dentro de la capa de aplicación (3024).

La figura 31 muestra ilustrativamente cómo puede usarse la disposición de la figura 30 cuando es emitido un comando de escritura (por ejemplo, en un dispositivo de almacenamiento), inserción (por ejemplo, en un campo de base de datos), o transmisión (por ejemplo, por una red) en la capa de aplicación (3024). En la etapa (3100) se identifican los datos que han de ser asegurados y se hace una llamada al analizador sintáctico de datos seguros. La llamada se pasa a través de la capa de envoltura (3022) donde en la etapa (3102) la capa de envoltura (3022) transmite los datos de entrada identificados en la etapa (3100) a la memoria intermedia de datos ensamblados (3008). También en la etapa (3012), cualquier información de cuota, nombres de archivos, cualquier otra información adecuada, o cualquier combinación de las mismas puede ser almacenada (por ejemplo, como información (3106) en la capa de envoltura (3022)). El procesador de datos seguros (3000) entonces analiza sintácticamente y divide los datos que toma como entrada procedentes de la memoria intermedia de datos ensamblados (3008) de acuerdo con la presente invención. Produce como salida las cuotas de datos dentro de las memorias intermedias de cuotas divididas (3010). En la etapa (3104), la capa de envoltura (3022) obtiene de la información almacenada (3106) cualquier información de cuota adecuada (es decir, almacenada por la envoltura (3022) en la etapa (3102) y la(s) ubicación(es) de cuotas (por ejemplo, de uno o más archivos de configuración). La capa de envoltura (3022) escribe entonces las cuotas de salida (obtenidas de las memorias intermedias de cuotas divididas (3010)) apropiadamente (por ejemplo, escritas en un o más dispositivos de almacenamiento, comunicadas sobre una red, etc.).

La figura 32 muestra ilustrativamente cómo puede usarse la disposición de la figura 30 cuando se produce una lectura (por ejemplo, de un dispositivo de almacenamiento), selección (por ejemplo, de un campo de base de datos), o recepción (por ejemplo, de una red). En la etapa (3200), los datos que han de ser restaurados son identificados y se hace una llamada al analizador sintáctico de datos seguros (3000) desde la capa de aplicación (3024). En la etapa (3202), de la capa de envoltura (3022) se obtiene cualquier información de cuota adecuada y se determina la ubicación de la cuota. La capa de envoltura (3022) carga las porciones de datos identificadas en la etapa (3200) en memorias intermedias de cuotas divididas (3010). El analizador sintáctico de datos seguros (3000) procesa entonces estas cuotas de acuerdo con la presente invención (por ejemplo, si solo se dispone de tres de las cuatro cuotas, entonces pueden usarse las capacidades de redundancia del analizador sintáctico de datos seguros (3000) para restaurar los datos originales usando solo las tres cuotas). Los datos restaurados se almacenan entonces en la memoria intermedia de datos ensamblados (3008). En la etapa (3204), la capa de aplicación (3022) convierte los datos almacenados en la memoria intermedia de datos ensamblados (3008) a su formato de datos original (si es necesario) y proporciona los datos originales en su formato original a la capa de aplicación (3024).

Se entenderá que el análisis sintáctico y la división de los datos originales ilustrados en la figura 31 y la restauración de porciones de datos en datos originales ilustrada en la figura 32 son meramente ilustrativos. Puede usarse cualquier otro proceso, componente o ambos además de o en lugar de los ilustrados.

La figura 33 es un diagrama de bloques de un flujo de proceso ilustrativo para analizar sintácticamente y dividir los datos originales en dos o más porciones de datos de acuerdo con una realización de la presente invención. Como se ilustra, los datos originales que se desea que sean analizados sintácticamente y divididos es el texto plano (3306) (es decir, la palabra “SUMMIT” se usa como ejemplo). Se entenderá que cualquier otro tipo de datos puede ser analizado sintácticamente y dividido de acuerdo con la presente invención. Se genera una clave de sesión (3300). Si la longitud de la clave de sesión (3300) no es compatible con la longitud de los datos originales (3306), entonces puede generarse la clave de sesión de realimentación de cifrado (3304).

En una estrategia adecuada, los datos originales (3306) pueden ser cifrados antes del análisis sintáctico, la división o ambos. Por ejemplo, como ilustra la figura 33, los datos originales (3306) pueden ser XORed con cualquier valor adecuado (por ejemplo, con la clave de sesión de realimentación de cifrado (3304), o con cualquier otro valor adecuado). Se entenderá que puede usarse cualquier otra técnica de cifrado adecuada en lugar de o además de la técnica XOR ilustrada. Se entenderá además que aunque la figura 33 se ilustra en cuanto a operaciones de *byte* por *byte*, la operación puede tener lugar al nivel de bit o a cualquier otro nivel adecuado. Se entenderá además que, si se desea, no tiene que haber ningún cifrado sean cuales sean los datos originales (3306).

Los datos cifrados resultantes (o los datos originales si no tuvo lugar cifrado) son entonces troceados para determinar cómo dividir los datos cifrados (u originales) entre los sectores de almacenamiento de salida (por ejemplo, de los cuales hay cuatro en el ejemplo ilustrado). En el ejemplo ilustrado, el troceo tiene lugar por *bytes* y es una función de la clave de sesión de realimentación de cifrado (3304). Se entenderá que esto es meramente

ilustrativo. El troceo puede realizarse a nivel de bit, si se desea. El troceo puede ser una función de cualquier otro valor adecuado además de la clave de sesión de realimentación de cifrado (3304). En otra estrategia adecuada, no tiene que usarse troceo. En cambio, puede emplearse cualquier otra técnica adecuada para dividir datos.

La figura 34 es un diagrama de bloques de un flujo de proceso ilustrativo para restaurar los datos originales (3306) a partir de dos o más porciones analizadas sintácticamente y divididas de los datos originales (3306) de acuerdo con una realización de la presente invención. El proceso implica trocear las porciones al revés (es decir, respecto al proceso de la figura 33) como una función de la clave de sesión de realimentación de cifrado (3304) para restaurar los datos originales cifrados (o los datos originales si no hubo cifrado antes del análisis sintáctico y la división). La clave de cifrado puede usarse entonces para restaurar los datos originales (es decir, en el ejemplo ilustrado, la clave de sesión de realimentación de cifrado (3304) se usa para descifrar el cifrado XOR aplicándole XOR con los datos cifrados). Esto restaura entonces los datos originales (3306).

La figura 35 muestra cómo puede implementarse la división en bits en el ejemplo de las figuras 33 y 34. Puede usarse un troceo (por ejemplo, como una función de la clave de sesión de realimentación de cifrado, como una función de cualquier otro valor adecuado) para determinar un valor de bit al cual dividir cada *byte* de datos. Se entenderá que esta es una manera meramente ilustrativa en la cual implementar la división al nivel de bit. Puede usarse cualquier otra técnica adecuada.

Se entenderá que cualquier referencia a la funcionalidad de troceo hecha en este documento puede hacerse con respecto a cualquier algoritmo de troceo adecuado. Estos incluyen, por ejemplo, MD5 y SHA-1. Pueden usarse diferentes algoritmos de troceo en diferentes momentos y por diferentes componentes de la presente invención.

Después de haberse determinado un punto de división de acuerdo con el procedimiento ilustrativo anterior o mediante cualquier otro procedimiento o algoritmo, puede efectuarse una determinación con respecto a qué porciones de datos ajuntar cada uno de los segmentos izquierdo y derecho. Puede usarse cualquier algoritmo adecuado para efectuar esta determinación. Por ejemplo, en una estrategia adecuada, puede crearse una tabla de todas las distribuciones posibles (por ejemplo, en forma de parejas de destinos para el segmento izquierdo y para el segmento derecho), por lo que puede determinarse un valor de cuota de destino para cada uno de los segmentos izquierdo y derecho usando cualquier función de troceo adecuada sobre los datos correspondientes en la clave de sesión, la clave de sesión de realimentación de cifrado, o cualquier otro valor aleatorio o pseudoaleatorio adecuado, que pueda ser generado y ampliado al tamaño de los datos originales. Por ejemplo, puede efectuarse una función de troceo de un *byte* correspondiente en el valor aleatorio o pseudoaleatorio. La salida de la función de troceo se usa para determinar qué pareja de destinos (es decir, uno para el segmento izquierdo y uno para el segmento derecho) seleccionar de la tabla de todas las combinaciones de destinos. Basándose en este resultado, cada segmento de la unidad de datos divididos es adjuntado a las dos cuotas respectivas indicadas por el valor de la tabla seleccionado como resultado de la función de troceo.

Puede adjuntarse información de redundancia a las porciones de datos de acuerdo con la presente invención para permitir la restauración de los datos originales usando menos de la totalidad de las porciones de datos. Por ejemplo, si se desea que dos de cuatro porciones sean suficientes para la restauración de datos, entonces datos adicionales procedentes de las cuotas pueden adjuntarse en consecuencia a cada cuota, por ejemplo, de una manera ordenada cíclicamente (por ejemplo, cuando el tamaño de los datos originales es 4 MB, entonces la cuota 1 obtiene sus propias cuotas así como las de las cuotas 2 y 3; la cuota 2 obtiene su propia cuota así como las de las cuotas 3 y 4; la cuota 3 obtiene su propia cuota así como las de las cuotas 4 y 1; y la cuota 4 obtiene sus propias cuotas así como las de las cuotas 1 y 2). Puede usarse cualquiera de tales redundancias adecuadas de acuerdo con la presente invención.

Se entenderá que puede usarse cualquier otra estrategia adecuada de análisis sintáctico y división para generar porciones de datos a partir de un conjunto de datos originales de acuerdo con la presente invención. Por ejemplo, el análisis sintáctico y la división pueden ser procesados de manera aleatoria o pseudoaleatoria sobre una base de bit por bit. Puede usarse un valor aleatorio o pseudoaleatorio (por ejemplo, la clave de sesión, la clave de sesión de realimentación de cifrado, etc.) por lo que para cada bit de los datos originales, el resultado de una función de troceo sobre los datos correspondientes en el valor aleatorio o pseudoaleatorio puede indicar a qué cuota adjuntar el bit respectivo. En una estrategia adecuada el valor aleatorio o pseudoaleatorio puede generarse como, o ampliarse hasta, 8 veces el tamaño de los datos originales de modo que la función de troceo puede realizarse sobre un *byte* correspondiente del valor aleatorio o pseudoaleatorio con respecto a cada bit de los datos originales. Puede usarse cualquier otro algoritmo adecuado para analizar sintácticamente y dividir datos a nivel de bit por bit de acuerdo con la presente invención. Se apreciará además que pueden adjuntarse datos de redundancia a las cuotas de datos

como, por ejemplo, de la manera descrita inmediatamente antes de acuerdo con la presente invención.

En una estrategia adecuada, el análisis sintáctico y la división no tienen que ser aleatorios o pseudoaleatorios. En cambio, puede usarse cualquier algoritmo determinista adecuado para analizar sintácticamente y dividir los datos. Por ejemplo, puede emplearse una descomposición de los datos originales en cuotas secuenciales como algoritmo de análisis sintáctico y división. Otro ejemplo es analizar sintácticamente y dividir los datos originales bit por bit, adjuntando cada bit respectivo a las cuotas de datos secuencialmente de manera ordenada cíclicamente. Se apreciará además que pueden adjuntarse datos de redundancia a las cuotas de datos como, por ejemplo, de la manera descrita anteriormente de acuerdo con la presente invención.

En una realización de la presente invención, después de que el analizador sintáctico de datos seguros genera un número de porciones de datos originales, con el fin de restaurar los datos originales, pueden ser obligatorias ciertas una o más de las porciones generadas. Por ejemplo, si una de las porciones se usa como cuota de autenticación (por ejemplo, guardada en un dispositivo de testigo físico), y si se está usando la característica de tolerancia a fallos del analizador sintáctico de datos seguros (es decir, cuando son necesarias menos de la totalidad de las porciones para restaurar los datos originales), entonces aun cuando el analizador sintáctico de datos seguros pueda tener acceso a un número suficiente de porciones de los datos originales con el fin de restaurar los datos originales, puede requerir la cuota de autenticación almacenada en el dispositivo de testigo físico antes de que restaure los datos originales. Se entenderá que puede requerirse cualquier número y tipo de cuota particular basándose en, por ejemplo, la aplicación, el tipo de datos, el usuario, cualquier otro factor adecuado, o cualquier combinación de los mismos.

En una estrategia adecuada, el analizador sintáctico de datos seguros o algún componente externo al analizador sintáctico de datos seguros puede cifrar una o más porciones de los datos originales. Puede requerirse que las porciones cifradas sean proporcionadas y descifradas con el fin de restaurar los datos originales. Las diferentes porciones cifradas pueden ser cifradas con diferentes claves de cifrado. Por ejemplo, esta características pueden usarse para implementar una “regla de dos hombres” más segura por lo que un primer usuario necesitaría tener una cuota particular cifrada usando un primer cifrado y un segundo usuario necesitaría tener una cuota particular cifradas usando una segunda clave de cifrado. Con el fin de acceder a los datos originales, ambos usuarios necesitarían tener sus claves de cifrado respectivas y proporcionar sus porciones respectivas de los datos originales. En una estrategia adecuada, puede usarse una clave pública para cifrar una o más porciones de datos que pueden ser una cuota obligatoria para restaurar los datos originales. Después puede usarse una clave privada para descifrar la cuota con el fin de ser usada para restaurar a los datos originales.

Puede usarse cualquier paradigma adecuado que haga uso de cuotas obligatorias cuando sean necesarios menos de todas las cuotas para restaurar los datos originales.

En una realización adecuada de la presente invención, la distribución de datos en un número finito de cuotas de datos puede ser procesada de manera aleatoria o pseudoaleatoria de modo que, desde una perspectiva estadística, la probabilidad de que cualquier cuota de datos particular reciba una unidad de datos particular es igual a la probabilidad de que una cualquiera de las cuotas restantes reciba la unidad de datos. Como resultado, cada cuota de datos tendrá una cantidad de bits de datos aproximadamente igual.

De acuerdo con otra realización de la presente invención, cada una del número finito de cuotas de datos no necesitan tener una probabilidad igual de recibir unidades de datos procedentes del análisis sintáctico y la división de los datos originales. En cambio, ciertas una o más cuotas pueden tener una probabilidad más alta o más baja que las cuotas restantes. Como resultado, ciertas cuotas pueden ser mayores o menores en cuanto al tamaño de bits en relación con las otras cuotas. Por ejemplo, en un escenario de dos cuotas, una cuota puede tener un 1 % de probabilidad de recibir una unidad de datos mientras que la segunda cuota tiene un 99 % de probabilidad. Debería desprenderse, por lo tanto, que una vez que las unidades de datos han sido distribuidas por el analizador sintáctico de datos seguros entre las dos cuotas, la primera cuota debería tener aproximadamente el 1 % de los datos y la segunda cuota el 99 %. Puede usarse cualquier probabilidad adecuada de acuerdo con la presente invención.

Se entenderá que el analizador sintáctico de datos seguros puede ser programado para distribuir datos a las cuotas de acuerdo también con un porcentaje exacto (o casi exacto). Por ejemplo, el analizador sintáctico de datos seguros puede ser programado para distribuir el 80 % de los datos a una primera cuota y el 20 % restante de los datos a una segunda cuota.

De acuerdo con otra realización de la presente invención, el analizador sintáctico de datos seguros puede generar

cuotas de datos, de las cuales una o más tienen tamaños predefinidos. Por ejemplo, el analizador sintáctico de datos seguros puede dividir los datos originales en porciones de datos donde una de las porciones es exactamente 256 bits. En una estrategia adecuada, si no es posible generar una porción de datos que tenga el tamaño requerido, entonces el analizador sintáctico de datos seguros puede rellenar la porción para hacerla del tamaño correcto. Puede usarse cualquier tamaño adecuado.

En una estrategia adecuada, el tamaño de una porción de datos puede ser el tamaño de una clave de cifrado, una clave de división, cualquier otra clave adecuada, o cualquier otro elemento de datos adecuado.

Como se analiza anteriormente, el analizador sintáctico de datos seguros puede usar claves en el análisis sintáctico y la división de los datos. Por claridad y brevedad, estas claves se denominarán en este documento como “claves de división”. Por ejemplo, la clave maestra de sesión, presentada previamente, es un tipo de clave de división. Además, como se analiza anteriormente, las claves de división pueden ser aseguradas dentro de cuotas de datos generadas por el analizador sintáctico de datos seguros. Puede usarse cualquier algoritmo adecuado para asegurar claves de división para asegurarlas entre las cuotas de datos. Por ejemplo, puede usarse el algoritmo de Shamir para asegurar las claves de división por medio del cual se genera la información que puede usarse para reconstruir una clave de división y se adjunta a las cuotas de datos. Puede usarse cualquier otro algoritmo adecuado de acuerdo con la presente invención.

De manera similar, cualquier clave de cifrado adecuada puede ser asegurada dentro de una o más cuotas de datos de acuerdo con cualquier algoritmo adecuado tal como el algoritmo Shamir. Por ejemplo, las claves de cifrado usadas para cifrar un conjunto de datos antes del análisis sintáctico y la división, las claves de cifrado usadas para cifrar una porción de datos después del análisis sintáctico y la división, o ambas pueden ser aseguradas usando, por ejemplo, el algoritmo Shamir o cualquier otro algoritmo adecuado.

De acuerdo con una realización de la presente invención, puede usarse una transformada de todo o nada (AoNT), tal como una transformada de paquete completo, para asegurar más los datos trasformando las claves de división, las claves de cifrado, cualquier otro elemento de datos adecuado, o cualquier combinación de los mismos. Por ejemplo, una clave de cifrado usada para cifrar un conjunto de datos antes del análisis sintáctico y la división de acuerdo con la presente invención puede ser transformada por algoritmo AoNT. La clave de cifrado transformada puede ser distribuida entonces entre las cuotas de datos de acuerdo con, por ejemplo, el algoritmo de Shamir o cualquier otro algoritmo asociado. Con el fin de reconstruir la clave de cifrado, el conjunto de datos cifrados debe ser restaurado (por ejemplo, no necesariamente usando todas las cuotas de datos si se usó redundancia de acuerdo con la presente invención) con el fin de acceder a la información necesaria respecto a la transformación de acuerdo con AoNT como es bien sabido por un experto en la materia. Cuando la clave de cifrado original es recuperada, puede usarse para descifrar el conjunto de datos cifrados para recuperar el conjunto de datos originales. Se entenderá que pueden usarse las características de tolerancia a fallos de la presente invención conjuntamente con la característica de AoNT. Concretamente, puede incluirse datos de redundancia en las porciones de datos de modo que sean necesarias menos de todas las porciones de datos para restaurar el conjunto de datos cifrados.

Se entenderá que la AoNT puede aplicarse a claves de cifrado usadas para cifrar las porciones de datos después del análisis sintáctico y la división ya sea en lugar de o además del cifrado y la AoNT de la clave de cifrado respectiva que corresponde al conjunto de datos antes del análisis sintáctico y la división. Asimismo, puede aplicarse la AoNT a la división de claves.

En una realización de la presente invención, las claves de cifrado, las claves de división, o ambas tal como se usan de acuerdo con la presente invención pueden ser cifradas nuevamente usando, por ejemplo, una clave de grupo de trabajo con el fin de proporcionar un nivel extra de seguridad a un conjunto de datos asegurados.

En una realización de la presente invención, puede estar provisto un módulo de auditoría que realiza un seguimiento siempre que es invocado el analizador sintáctico de datos seguros para dividir los datos.

La figura 36 ilustra opciones (3600) para usar los componentes del analizador sintáctico de datos seguros de acuerdo con la invención. Cada combinación de opciones es explicada resumidamente más adelante y está etiquetada con los números de etapa apropiados de la figura 36. El analizador sintáctico de datos seguros puede ser de naturaleza modular, permitiendo que se use cualquier algoritmo conocido dentro de cada uno de los bloques de función mostrados en la figura 36. Por ejemplo, pueden usarse otros algoritmos división de clave (por ejemplo, compartición de secreto) tales como el Blakely en lugar del Shamir, o el cifrado AES podría sustituirse por otros algoritmos de cifrado conocidos tales como DES triple. Las etiquetas mostradas en el ejemplo de la figura 36

representan meramente una posible combinación de algoritmos para uso en una realización de la invención. Debería entenderse que puede usarse cualquier algoritmo adecuado o combinación de algoritmos en lugar de los algoritmos etiquetados.

1) (3610, 3612, 3614, 3615, 3616, 3617, 3618, 3619)
Usando los datos cifrados anteriormente en la etapa (3610), los datos pueden ser divididos finalmente en un número predefinido de cuotas. Si el algoritmo de división requiere una clave, puede generarse una clave de cifrado de división en la etapa (3612) usando un generador de números pseudoaleatorios criptográficamente seguros. La clave de cifrado de división puede ser transformada opcionalmente usando una transformada de todo o nada (AoNT) en una clave de división de transformada en la etapa (3614) antes de ser dividida por clave en el número predefinido de cuotas con tolerancia a fallos en la etapa (3615). Los datos pueden ser divididos entonces en el número predefinido de cuotas en la etapa (3616). Puede usarse un esquema tolerante a fallos en la etapa (3617) para permitir la regeneración de los datos a partir de menos del número total de cuotas. Una vez que las cuotas están creadas, puede insertarse información de autenticación/integridad dentro de las cuotas en la etapa (3618). Cada cuota puede ser postcifrada opcionalmente en la etapa (3619).
2) (3111, 3612, 3614, 3616, 3617, 3618, 3619)
En algunas realizaciones, los datos de entrada pueden ser cifrados usando una clave de cifrado proporcionada por un usuario o un sistema externo. La clave externa es proporcionada en la etapa (3611). Por ejemplo, la clave puede ser proporcionada desde un almacén de claves externo. Si el algoritmo de división requiere una clave, la clave de cifrado de división puede generarse usando un generador de números pseudoaleatorios criptográficamente seguros en la etapa (3612). La clave de división puede ser transformada opcionalmente usando una transformada de todo o nada (AoNT) en una clave de cifrado de división de transformada en la etapa (3614) antes de ser dividida por clave en el número predefinido de cuotas con tolerancia a fallos en la etapa (3615). Los datos son divididos entonces en un número predefinido de cuotas en la etapa (3616). Puede usarse un esquema de tolerancia a fallos en la etapa (3617) para permitir la regeneración de los datos a partir de menos del número total de cuotas. Una vez que las cuotas están creadas, puede insertarse información de autenticación/integridad dentro de las cuotas en la etapa (3618). Cada cuota puede ser postcifrada opcionalmente en la etapa (3619).
3) (3612, 3613, 3614, 3615, 3612, 3614, 3615, 3616, 3617, 3618, 3619)
En algunas realizaciones, puede generarse una clave de cifrado usando un generador de números pseudoaleatorios criptográficamente seguros en la etapa (3612) para transformar los datos. El cifrado de los datos usando la clave de cifrado generada puede producirse en la etapa (3613). La clave de cifrado puede ser transformada opcionalmente usando una transformada de todo o nada (AoNT) en una clave de cifrado de transformada en la etapa (3614). La clave de cifrado de transformada y/o la clave de cifrado generada pueden ser divididas entonces en el número predefinido de cuotas con tolerancia a fallos en la etapa (3615). Si el algoritmo de división requiere una clave, la generación de la clave de cifrado de división usando un generador de números pseudoaleatorios criptográficamente seguros puede producirse en la etapa (3612). La clave de división puede ser trasformada opcionalmente usando una transformada de todo o nada (AoNT) en una clave de cifrado de división de transformada en la etapa (3614) antes de ser dividida por clave en el número predefinido de cuotas con tolerancia a fallos en la etapa (3615). Los datos pueden ser divididos entonces en un número predefinido de cuotas en la etapa (3616). Puede usarse un esquema tolerante a fallos en la etapa (3617) para permitir la regeneración de los datos a partir de menos del número total de cuotas. Una vez que las cuotas están creadas, se insertará información de autenticación/integridad dentro de las cuotas en la etapa (3618). Cada cuota puede entonces ser postcifrada opcionalmente en la etapa (3619).
4) (3612, 3614, 3615, 3616, 3617, 3618, 3619)

En algunas realizaciones, los datos pueden ser divididos en un número predefinido de cuotas. Si el algoritmo de división requiere una clave, la generación de la clave de cifrado de división usando un generador de números aleatorios criptográficamente seguros puede producirse en la etapa (3612). La clave de división puede ser transformada opcionalmente usando una transformada de todo o nada (AoNT) en una clave de división transformada en la etapa (3614) antes de ser dividida por clave en el número predefinido de cuotas con tolerancia a fallos en la etapa (3615). Los datos pueden ser divididos entonces en la etapa (3616). Puede usarse un esquema tolerante a fallos en la etapa (3617) para permitir la regeneración de los datos a partir de menos del número total de cuotas. Una vez que las cuotas están creadas, puede insertarse información de autenticación/integridad dentro de las cuotas en la etapa (3618). Cada cuota puede ser postcifrada opcionalmente en la etapa (3619).

Aunque las cuatro combinaciones de opciones anteriores se usan preferentemente en algunas realizaciones de la invención, en otras realizaciones puede usarse cualquier otra combinación adecuada de características, etapas, u opciones con el analizador sintáctico de datos seguros.

El analizador sintáctico de datos seguros puede ofrecer protección de datos flexible facilitando la separación física.

Los datos pueden ser cifrados en primer lugar, luego divididos en cuotas con tolerancia a fallos “m de n”. Esto permite la regeneración de la información original cuando se dispone de menos del número total de cuotas. Por ejemplo, algunas cuotas pueden perderse o corromperse en la transmisión. Las cuotas perdidas o corruptas pueden ser recreadas a partir de la tolerancia a fallos o información de integridad adjunta a las cuotas, como se analiza con más detalle más adelante.

Con el fin de crear las cuotas, opcionalmente son utilizadas varias claves por el analizador sintáctico de datos seguros. Estas claves pueden incluir uno o más de lo siguiente:

Clave de precifrado: cuando se selecciona precifrado de las cuotas, puede pasarse una clave externa al analizador sintáctico de datos seguros. Esta clave puede ser generada y almacenada externamente en un almacén de claves (u otra ubicación) y puede usarse para cifrar opcionalmente datos antes de la división de datos.

Clave de cifrado de división: esta clave puede ser generada internamente y usada por el analizador sintáctico de datos seguros para cifrar los datos antes de la división. Esta clave puede ser almacenada con seguridad dentro de las cuotas usando un algoritmo de división de clave.

Clave de sesión de división: esta clave no se usa con un algoritmo de cifrado; en cambio, puede usarse para codificar los algoritmos de partición de datos cuando se selecciona división aleatoria. Cuando se usa una división aleatoria, puede generarse internamente una clave de sesión de división y usarse por el analizador sintáctico de datos seguros para partir los datos en cuotas. Esta clave puede ser almacenada con seguridad dentro de las cuotas usando un algoritmo de división de clave.

Clave de postcifrado: cuando se selecciona postcifrado de las cuotas, puede pasarse una clave externa al analizador sintáctico de datos seguros y usarse para postcifrar las cuotas individuales. Esta clave puede ser generada y almacenada externamente en un almacén de claves u otra ubicación adecuada.

En algunas realizaciones, cuando los datos son asegurados usando de este modo el analizador sintáctico de datos seguros, la información solo puede volver a ser ensamblada siempre que estén presentes todas las cuotas requeridas y las claves de cifrado externas.

La figura 37 muestra el proceso de vista general ilustrativo (3700) para usar el analizador sintáctico de datos seguros de la presente invención en algunas realizaciones. Como se describe anteriormente, dos funciones indicadas para el analizador sintáctico de datos seguros (3706) pueden incluir el cifrado (3702) y la copia de seguridad (3704). Como tal, el analizador sintáctico de datos seguros (3706) puede estar integrado con un sistema RAID o de copia de seguridad o un motor de cifrado por hardware o por software en algunas realizaciones.

Los procesos de clave primaria asociados con el analizador sintáctico de datos seguros (3706) pueden incluir uno o más del proceso de precifrado (3708), el proceso de cifrado/transformada (3710), el proceso de clave segura (3712), el proceso de análisis sintáctico/distribución (3714), el proceso de tolerancia a fallos (3716), el proceso de autenticación de cuota (3716), y el proceso de postcifrado (3720). Estos procesos pueden ejecutarse en varios órdenes o combinaciones, como se detalla en la figura 36. La combinación y el orden de los procesos usados pueden depender de la aplicación o el uso particular, el nivel de seguridad deseado, si se desea precifrado, postcifrado o ambos opcionales, la redundancia deseada, las capacidades o el rendimiento de un sistema subyacente o integrado, o cualquier otro factor o combinación de factores adecuados.

La salida del proceso ilustrativo (3700) puede ser dos o más cuotas (3722). Como se describe anteriormente, los datos pueden ser distribuidos a cada una de estas cuotas de manera aleatoria (o pseudoaleatoria) en algunas realizaciones. En otras realizaciones, puede usarse un algoritmo determinista (o alguna combinación adecuada algoritmos aleatorios, pseudoaleatorios, y deterministas).

Además de la protección individual de activos de información, a veces existe un requisito de compartir información entre diferentes grupos de usuarios o comunidades de interés. Entonces puede ser necesario o bien controlar el acceso a las cuotas individuales dentro de ese grupo de usuarios o bien compartir las credenciales entre esos usuarios que solo permitirían a los miembros del grupo volver a ensamblar las cuotas. Con este fin, puede ser desplegada una clave de grupo de trabajo a los miembros del grupo en algunas realizaciones de la invención. La clave de grupo de trabajo debería ser protegida y mantenida confidencial, ya que el compromiso de la clave de grupo de trabajo puede permitir potencialmente que quienes están fuera del grupo accedan a la información. Más adelante se analizan algunos sistemas y procedimientos para despliegue y protección de clave de grupo de trabajo.

El concepto de clave de grupo de trabajo permite la protección mejorada de activos de información cifrando la información clave almacenada dentro de las cuotas. Una vez que se realiza esta operación, aunque sean descubiertas todas las cuotas requeridas y las claves externas, un atacante no tiene esperanza de recrear la información sin acceder a la clave de grupo de trabajo.

La figura 38 muestra el diagrama de bloques ilustrativo (3800) para almacenar los componentes de clave y datos dentro de las cuotas. En el ejemplo del diagrama (3800), se omiten las etapas opcionales de precifrado y postcifrado, aunque estas etapas pueden estar incluidas en otras realizaciones.

El proceso simplificado de dividir los datos incluye cifrar los datos usando la clave de cifrado (3804) en la fase de cifrado (3802). Las porciones de la clave de cifrado (3804) entonces pueden ser divididas y almacenadas dentro de las cuotas (3810) de acuerdo con la presente invención. Las porciones de la clave de cifrado de división (3806) también pueden ser almacenadas dentro de las cuotas (3810). Usando la clave de cifrado de división, después los datos (3808) son divididos y almacenados en las cuotas (3810).

Con el fin de restaurar los datos, la clave de cifrado de división (3806) puede ser recuperada y restaurada de acuerdo con la presente invención. La operación de división puede invertirse entonces para restaurar el texto cifrado. La clave de cifrado (3804) también puede ser recuperada y restaurada, y el texto cifrado puede ser descifrado entonces usando la clave de cifrado.

Cuando se utiliza una clave de grupo de trabajo, el proceso anterior puede cambiarse ligeramente para proteger la clave de cifrado con la clave de grupo de trabajo. La clave de cifrado puede ser cifrada entonces con la clave de grupo de trabajo antes de ser almacenada dentro de las cuotas. Las etapas modificadas se muestran en el diagrama de bloques ilustrativo (3900) de la figura 39.

El proceso simplificado para dividir los datos usando una clave de grupo de trabajo incluye en primer lugar cifrar los datos usando la clave de cifrado en la fase (3902). La clave de cifrado puede entonces ser cifrada con la clave de grupo de trabajo en la fase (3904). La clave de cifrado cifrada con la clave de grupo de trabajo puede entonces ser dividida en porciones y almacenada con las cuotas (3912). La clave de división (3908) también puede ser dividida y almacenada en las cuotas (3912). Por último, las porciones de datos (3910) son divididas y almacenadas en las cuotas (3912) usando la clave de división (3908).

Con el fin de restaurar los datos, la clave de división puede ser recuperada y restaurada de acuerdo con la presente invención. La operación de división puede invertirse entonces para restaurar el texto cifrado de acuerdo con la presente invención. La clave de cifrado (que fue cifrada con la clave de grupo de trabajo) puede ser recuperada y restaurada. La clave de cifrado puede entonces ser descifrada usando la clave de grupo de trabajo. Por último, el texto cifrado puede ser descifrado usando la clave de cifrado.

Existen varios procedimientos seguros para desplegar y proteger claves de grupo de trabajo. La selección de qué procedimiento usar para una aplicación particular depende de varios factores. Estos factores pueden incluir el nivel de seguridad requerido, el coste, la conveniencia, y el número de usuarios en el grupo de trabajo. Más adelante se proporcionan algunas técnicas usadas comúnmente en algunas realizaciones:

Almacenamiento de claves basado en hardware

Las soluciones basadas en hardware generalmente proporcionan las garantías más fuertes para la seguridad de las claves de cifrado/descifrado en un sistema de cifrado. Ejemplos de soluciones de almacenamiento basado en hardware incluyen dispositivos de testigo de clave inviolables que almacenan claves en un dispositivo portátil (por ejemplo, una tarjeta inteligente/llave electrónica), o periféricos de almacenamiento de claves no portátiles. Estos dispositivos están diseñados para impedir la fácil duplicación del material clave por partes no autorizadas. Las claves pueden ser generadas por una autoridad de confianza y distribuidas a los usuarios, o generadas dentro del hardware. Además, muchos sistemas de almacenamiento permiten una autenticación multifactor, donde el uso de las claves requiere acceso tanto a un objeto físico (testigo) como a una frase de paso o una biometría.

Almacenamiento de claves basado en software

Aunque el almacenamiento basado en hardware dedicado puede ser deseable para despliegues o aplicaciones de alta seguridad, otros despliegues pueden elegir almacenar claves directamente en hardware local (por ejemplo,

discos, almacenes RAM o RAM no volátil tales como unidades USB). Esto proporciona un nivel de protección más bajo frente a los atacantes infiltrados, o en los casos en los que un atacante es capaz de acceder directamente a la máquina de cifrado.

Para asegurar claves en discos, la gestión de claves basada en software a menudo protege las claves almacenándolas en forma cifrada bajo una clave deducida de una combinación de otras métricas de autenticación, incluyendo: contraseñas y frases de paso, presencia de otras claves (por ejemplo, de una solución basada en hardware), biometrías, o cualquier combinación adecuada de lo anterior. El nivel de seguridad proporcionado por tales técnicas puede comprender desde los mecanismos de protección de claves relativamente débiles proporcionados por algunos sistemas operativos (por ejemplo, MS Windows y Linux), hasta soluciones más robustas implementadas usando autenticación multifactor.

El analizador sintáctico de datos seguros de la presente invención puede usarse ventajosamente en varias aplicaciones y tecnologías. Por ejemplo, un sistema de correo electrónico, sistemas RAID, sistemas de difusión de vídeo, sistemas de bases de datos, sistemas de copia de seguridad en cinta, o cualquier otro sistema adecuado puede tener el analizador sintáctico de datos seguros integrado a cualquier nivel adecuado. Como se analiza anteriormente, se entenderá que el analizador sintáctico de datos seguros también puede estar integrado para protección y tolerancia a fallos de cualquier tipo de datos en movimiento a través de cualquier medio de transporte, incluyendo, por ejemplo, medios de transporte por cable, inalámbricos, o físicos. Como un ejemplo, las aplicaciones de voz sobre protocolo internet (VoIP) pueden hacer uso del analizador sintáctico de datos seguros de la presente invención para solucionar problemas relacionados con ecos y retardos que se encuentran comúnmente en VoIP. La necesidad de reintento de conexión a red sobre los paquetes perdidos puede eliminarse usando tolerancia a fallos, la cual garantiza la distribución de paquetes incluso con la pérdida de un número predeterminado de cuotas. Los paquetes de datos (por ejemplo, paquetes de red) también pueden ser divididos y restaurados eficientemente “sobre la marcha” con retardo y almacenamiento en memoria intermedia mínimos, con el resultado de una solución exhaustiva para diversos tipos de datos en movimiento. El analizador sintáctico de datos seguros puede actuar sobre paquetes de datos por red, paquetes de voz por red, bloques de datos del sistema de archivos, o cualquier otra unidad de información adecuada. Además de estar integrado con una aplicación de VoIP, el analizador sintáctico de datos seguros puede estar integrado con una aplicación de compartición de archivos (por ejemplo, una aplicación de compartición de archivos entre pares), una aplicación de difusión de vídeo, una aplicación de votación o encuesta electrónica (que puede implementar un protocolo de votación electrónica 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, el soporte de datos de red en movimiento puede ser proporcionado por el analizador sintáctico de datos seguros de la presente invención en dos fases distintas – una fase de generación de encabezamiento y una fase de partición de datos. El proceso de generación de encabezamiento simplificado (4000) y el proceso de partición de datos simplificado (4010) se muestran en las figuras 40A y 40B, respectivamente. Uno de estos procesos o ambos, puede realizarse sobre paquetes de red, bloques del sistema de archivos, o cualquier otra información adecuada.

En algunas realizaciones, el proceso de generación de encabezamiento (4000) puede realizarse una vez al inicio de un tren de paquetes de red. En la etapa (4002), puede generarse una clave de cifrado de división aleatoria (o pseudoaleatoria), K. La clave de cifrado de división, K, puede entonces ser cifrada opcionalmente (por ejemplo, usando la clave de grupo de trabajo descrita anteriormente) en la etapa de envoltura de clave AES (4004). Aunque en algunas realizaciones puede usarse una envoltura de clave AES, en otras realizaciones puede usarse cualquier algoritmo de cifrado de clave o de envoltura de clave adecuado. La etapa de envoltura de clave AES (4004) puede operar sobre toda la clave de cifrado de división, K, o la clave de cifrado de división puede ser analizada sintácticamente en varios bloques (por ejemplo, bloques de 64 bits). La etapa de envoltura de clave AES (4004) puede operar entonces sobre bloques de la clave de cifrado de división, si se desea.

En la etapa (4006), puede usarse un algoritmo de compartición de secreto (por ejemplo, Shamir) para dividir la clave de cifrado de división, K, en cuotas de clave. Cada cuota de clave puede entonces insertarse en una de las cuotas de salida (por ejemplo, en los encabezamientos de cuota). Por último, un bloque de integridad de cuotas y (opcionalmente) una etiqueta de postautenticación (por ejemplo, MAC) pueden adjuntarse al bloque de encabezamiento de cada cuota. Cada bloque de encabezamiento puede estar diseñado para ajustar dentro de un solo paquete de datos.

Después de completarse la generación de encabezamiento (por ejemplo, usando el proceso de generación de

encabezamiento simplificado (4000)), el analizador sintáctico de datos seguros puede entrar en la fase de partición de datos usando el proceso de división de datos simplificado (4010). Cada paquete de datos o bloque de datos entrante del tren es cifrado usando la clave de cifrado de división, K, en la etapa (4012). En la etapa (4014), puede calcularse la información de integridad de cuotas (por ejemplo, un troceo H) sobre el texto cifrado que resulta de la etapa (4012). Por ejemplo, puede calcularse un troceo SHA-256. En la etapa (4016), el paquete de datos o el bloque de datos puede entonces ser partido en dos o más cuotas de datos usando uno de los algoritmos de división de datos descritos anteriormente de acuerdo con la presente invención. En algunas realizaciones, el paquete de datos o el bloque de datos puede ser dividido de modo que cada cuota de datos contiene una distribución sustancialmente aleatoria del paquete de datos o el bloque de datos cifrado. La información de integridad (por ejemplo, el troceo H) puede entonces adjuntarse a cada cuota de datos. También puede calcularse una etiqueta de postautenticación opcional (por ejemplo, MAC) y adjuntarse a cada cuota de datos en algunas realizaciones.

Cada cuota de datos puede incluir metadatos, que pueden ser necesarios para permitir la reconstrucción correcta de los bloques de datos o paquetes de datos. Esta información puede estar incluida en el encabezamiento de cuota. Los metadatos pueden incluir información tal como cuotas de claves criptográficas, identidades de claves, valores ocasionales de cuota, firmas/valores MAC, y bloques de integridad. Con el fin de maximizar la eficiencia de la anchura de banda, los metadatos pueden almacenarse en un formato binario compacto.

Por ejemplo, en algunas realizaciones, el encabezamiento de cuota incluye un fragmento de encabezamiento de texto claro, que no está cifrado y puede incluir elementos tales como la cuota de clave Shamir, el valor ocasional por sesión, el valor ocasional por cuota, identificadores de claves (por ejemplo, un identificador de clave de grupo de trabajo y un identificador de clave postautenticación). El encabezamiento de cuota también puede incluir un fragmento de encabezamiento cifrado, que está cifrado con la clave de cifrado de división. Un fragmento de encabezamiento de integridad, que puede incluir comprobaciones de integridad para cualquier número de bloques previos (por ejemplo, los dos bloques previos) también puede estar incluido en el encabezamiento. En el encabezamiento de cuota también puede estar incluido cualquier otro valor o información adecuados.

Como se muestra en el formato de cuota ilustrativo (4100) de la figura 41, el bloque de encabezamiento (4102) puede estar asociado con dos o más bloques de salida (4104). Cada bloque de encabezamiento, tal como el bloque de encabezamiento (4102), puede estar diseñado para ajustar dentro de un solo paquete de datos de red. En algunas realizaciones, después de que el bloque de encabezamiento (4102) es transmitido desde una primera ubicación hasta una segunda ubicación, los bloques de salida pueden entonces ser transmitidos. Alternativamente, el bloque de encabezamiento (4102) y los bloques de salida (4104) pueden ser transmitidos al mismo tiempo en paralelo. La transmisión puede producirse por uno o más trayectos de comunicaciones similares o distintos.

Cada bloque de salida puede incluir la porción de datos (4106) y la porción de integridad/autenticidad (4108). Como se describe anteriormente, cada cuota de datos puede ser asegurada usando una porción de integridad de cuota que incluye información de integridad de cuota (por ejemplo, un troceo SHA-256) de los datos cifrados, partidos previamente. Para verificar la integridad de los bloques de salida en el momento de la recuperación, el analizador sintáctico de datos seguros puede comparar los bloques de integridad de cuota de cada cuota y luego invertir el algoritmo de división. El troceo de los datos recuperados puede entonces ser verificado frente al troceo de cuotas.

Como se mencionó anteriormente, en algunas realizaciones de la presente invención, el analizador sintáctico de datos seguros puede usarse conjuntamente con un sistema de copia de seguridad en cinta. Por ejemplo, puede usarse una cinta individual como nodo (es decir, porción/cuota) de acuerdo con la presente invención. Puede usarse cualquier otra disposición adecuada. Por ejemplo, una biblioteca o subsistema de cintas, que está constituido por dos o más cintas, puede tratarse como un solo nodo.

También puede usarse redundancia con las cinta de acuerdo con la presente invención. Por ejemplo, si un conjunto de datos está repartido entre cuatro cintas (es decir, porciones/cuotas), entonces dos de las cuatro cintas pueden ser necesarias con el fin de restaurar los datos originales. Se entenderá que puede requerirse cualquier número de nodos adecuado (es decir, menos del número total de nodos) para restaurar los datos originales de acuerdo con las característica de redundancia de la presente invención. Esto aumenta sustancialmente la probabilidad de restauración cuando concluyen una o más cintas.

Cada cinta también puede estar protegida digitalmente con un valor de troceo SHA-256, HMAC, cualquier otro valor adecuado, o cualquier combinación de los mismos como garantía contra la manipulación. Si cambia algún dato de la cinta o el valor de troceo, la cinta no será una candidata para la restauración y se usaría cualquier número de cintas mínimo requerido de las cintas restantes para restaurar los datos.

En los sistemas de copia de seguridad en cinta convencionales, cuando un usuario solicita que se escriban datos en una cinta o se lean datos de una cinta, el sistema de gestión de cintas (TMS) presenta un número que corresponde a un soporte de cinta física. Este soporte de cinta apunta a una unidad física donde serán montados los datos. La cinta es cargada ya sea por un operador de cintas humano o por un robot de cintas en un silo de cintas.

Bajo la presente invención, el soporte de cinta física puede considerarse un punto de soporte lógico que apunta a varias cintas físicas. Esto no solo aumenta la capacidad de datos sino que también mejora el rendimiento debido al paralelismo.

Para un mayor rendimiento los nodos de cinta pueden ser o pueden incluir una batería de discos RAID usada para almacenar imágenes de cintas. Esto permite la restauración a alta velocidad porque los datos siempre están disponibles en la RAID.

En cualquiera de las realizaciones anteriores, los datos que han de ser asegurados pueden ser distribuidos en una pluralidad de cuotas usando técnicas de distribución de datos deterministas, probabilistas, o tanto deterministas como probabilistas. Con el fin de impedir que un atacante comience un ataque criptográfico sobre cualquier bloque de cifrado, los bits de los bloques de cifrado pueden ser distribuidos de manera determinista en las cuotas. Por ejemplo, la distribución puede realizarse usando la rutina BitSegment, o la rutina BlockSegment puede ser modificada para permitir la distribución de porciones de bloques en múltiples cuotas. Esta estrategia puede defender contra un atacante que tenga acumuladas menos de “M” cuotas.

En algunas realizaciones, puede emplearse una rutina de compartición de secreto codificada que usa dispersión de información codificada (por ejemplo, mediante el uso de un algoritmo de dispersión de información codificada o “IDA”). L clave para el IDA codificado también puede ser protegida por una o más claves de grupo de trabajo externas, una o más claves compartidas, o cualquier combinación de claves de grupo de trabajo y claves compartidas. De este modo, puede emplearse un esquema de compartición de secreto multifactor. Para reconstruir los datos, en algunas realizaciones pueden requerirse al menos “M” cuotas más la(s) clave(s) de grupo de trabajo (y/o la(s) clave(s) compartida(s)). El IDA (o la clave para el IDA) también puede ser metido en el proceso de cifrado. Por ejemplo, la transformada puede ser metida en el texto claro (por ejemplo, durante la capa de preprocesamiento antes del cifrado) y puede proteger más el texto claro antes de que sea cifrado.

Por ejemplo, en algunas realizaciones, se usa dispersión de información codificada para distribuir porciones únicas de datos procedentes de un conjunto de datos en dos o más cuotas. La dispersión de información codificada puede usar una clave de sesión para, en primer lugar, cifrar el conjunto de datos, para distribuir porciones únicas de datos cifrados procedentes del conjunto de datos en dos o más cuotas de conjunto de datos cifrados, o tanto cifrar el conjunto de datos como distribuir porciones únicas de datos cifrados procedentes del conjunto de datos en las dos o más cuotas de datos cifrados. Por ejemplo, para distribuir porciones únicas del conjunto de datos o el conjunto de datos cifrados, puede usarse compartición de secreto (o los procedimientos descritos anteriormente, tales como BitSegment o BlockSegment). La clave de sesión puede entonces ser transformada opcionalmente (por ejemplo, usando una transformada de paquete completo o AoNT) y compartida usando, por ejemplo, compartición de secreto (o la dispersión de información codificada y la clave de sesión).

En algunas realizaciones, la clave de sesión puede ser cifrada usando una clave compartida (por ejemplo, una clave de grupo de trabajo) antes de que las porciones únicas de la clave sean distribuidas o compartidas en dos o más cuotas de clave de sesión. Entonces pueden formarse dos o más cuotas de usuario combinando al menos una cuota de conjunto de datos cifrados y al menos una cuota de clave de sesión. Al formar una cuota de usuario, en algunas realizaciones, la al menos una cuota de clave de sesión puede ser entrelazada dentro de una cuota de conjunto de datos cifrados. En otras realizaciones, la al menos una cuota de clave de sesión puede ser insertada dentro de una cuota de conjunto de datos cifrados en una ubicación basándose al menos en parte en la clave de grupo de trabajo compartida. Por ejemplo, puede usarse dispersión de información codificada para distribuir cada cuota de clave de sesión en una única cuota de conjunto de datos cifrados para formar una cuota de usuario. El entrelazado o la inserción de una cuota de clave de sesión dentro de una cuota de conjunto de datos cifrados en una ubicación basándose al menos en parte en el grupo de trabajo compartido pueden proporcionar mayor seguridad frente a ataques criptográficos. En otras realizaciones, una o más cuotas de clave de sesión pueden adjuntarse al principio o el final de una cuota de conjunto de datos cifrados para formar una cuota de usuario. La colección de cuotas de usuario puede entonces ser almacenada por separado en al menos un depósito de datos. El depósito o los depósitos de datos pueden estar ubicados en la misma ubicación física (por ejemplo, en el mismo dispositivo de almacenamiento magnético o de cinta) o separados geográficamente (por ejemplo, en servidores separados

físicamente en diferentes ubicaciones geográficas). Para reconstruir el conjunto de datos originales, puede requerirse un conjunto autorizado de usuarios y la clave de grupo de trabajo compartida.

La dispersión de información codificada puede ser segura incluso frente a oráculos de recuperación de clave. Por ejemplo, tomemos un cifrado en bloque *E* y un oráculo de recuperación de clave para *E* que toma una lista $(X_1, Y_1),..., (X_c, Y_c)$ de pares de entrada/salida al cifrado en bloque, y devuelve una clave *K* que es consistente con los ejemplos de entrada/salida (por ejemplo, $Y_i = E_K(X_i)$ para todo *i*). El oráculo puede devolver el valor distinguido $\perp$ si no hay una clave consistente. Este oráculo puede modelar un ataque criptoanalítico que puede recuperar una clave de una lista de ejemplos de entrada/salida.

Los esquemas basados en cifrado de bloque estándar pueden fallar en presencia de un oráculo de recuperación de clave. Por ejemplo, el cifrado CBC o el CBC MAC puede volverse completamente inseguros en presencia de un oráculo de recuperación de clave.

Si Π^{IDA} es un esquema IDA y Π^{Enc} es un esquema de cifrado dado por un modo de operación de algún cifrado de bloque *E*, entonces (Π^{IDA}, Π^{Enc}) proporciona seguridad frente a un ataque de recuperación de clave si los dos esquemas, cuando se combinan con un esquema de compartición de secreto perfecto arbitrario (PSS) de acuerdo con HK1 o HK2, logran el objetivo de compartición de secreto computacional robusto (RCSS), pero en el modelo en el cual el adversario tiene un oráculo de recuperación de clave.

Si existe un esquema IDA Π^{IDA} y un esquema de cifrado Π^{Enc} de modo que el par de esquemas proporciona seguridad frente a ataques de recuperación de clave, entonces un modo de lograr este par es tener un IDA “inteligente” y un esquema de cifrado “elemental”. Otro modo de lograr este par de esquemas puede ser tener un IDA “elemental” y un esquema de cifrado “inteligente”.

Para ilustrar el uso de un IDA inteligente y un esquema de cifrado elemental, en algunas realizaciones, el esquema de cifrado puede ser CBC y el IDA puede tener una propiedad de “privacidad débil”. La propiedad de privacidad débil significa, por ejemplo, que si la entrada al IDA es una secuencia aleatoria de bloques $M = M_1 ...M_1$, y el adversario obtiene las cuotas de una colección no autorizada, entonces existe algún índice de bloque i tal que es inviable que el adversario calcule M_i. Tal IDA débilmente privado puede ser construido aplicando en primer lugar a *M* una AoNT de información teórica, tal como la AoNT de Stinson, y luego aplicando un IDA simple tal como BlockSegment, o un IDA eficiente en cuanto a bits como el esquema de Rabin (por ejemplo, la codificación de Reed-Solomon).

Para ilustrar el uso de un IDA elemental y un esquema de cifrado inteligente, en algunas realizaciones, se puede usar un modo CBC con cifrado doble en lugar de cifrado único. Ahora puede usarse cualquier IDA, incluso duplicación. Tener el oráculo de recuperación de clave para el cifrado de bloque sería inútil para un adversario, ya que al adversario se le denegará cualquier ejemplo de entrada/salida con cifrado único.

Aunque un IDA tiene valor, también puede resultar no esencial en algunos contextos, en el sentido de que los “inteligentes” necesarios para proporcionar seguridad frente a un ataque de recuperación de clave pueden haber sido “empujados” a otro sitio. Por ejemplo, en algunas realizaciones, no importa lo inteligente que sea el IDA, y para qué objetivo está intentando lograrse con el IDA en el contexto de HK1/HK2, los inteligentes pueden ser empujados fuera del IDA y dentro del esquema de cifrado, quedándose con un IDA fijo y elemental.

Basándose en lo anterior, en algunas realizaciones, puede usarse un IDA inteligente “universalmente sano” Π^{IDA}. Por ejemplo, se proporciona un IDA de modo que para todo esquema de cifrado Π^{Enc}, el par (Π^{IDA}, Π^{Enc}) proporciona universalmente seguridad frente a ataques de recuperación de clave.

En algunas realizaciones, se proporciona un esquema de cifrado que es RCSS seguro frente a un oráculo de recuperación de clave. El esquema puede estar integrado con HK1/HK2, con *cualquier* IDA, para lograr seguridad frente a la recuperación de clave. Usar el nuevo esquema puede resultar particularmente útil, por ejemplo, para hacer los esquemas de cifrado simétrico más seguros contra ataques de recuperación de clave.

Como se menciona anteriormente, las nociones de compartición de secreto clásicas típicamente son sin codificar. Así, un secreto es descompuesto en cuotas, o reconstruido a partir de ellas, de un modo que no requiere que ni el comerciante ni la parte que reconstruyen el secreto guarden ninguna clase de clave simétrica o asimétrica. El analizador sintáctico de datos seguros descrito en este documento, sin embargo, es codificado opcionalmente. El comerciante puede proporcionar una clave simétrica que, si se usa para compartición de datos, puede requerirse para recuperación de datos. El analizador sintáctico de datos seguros puede usar la clave simétrica para dispersar o

distribuir porciones únicas del mensaje que ha de ser asegurado en dos o más cuotas.

La clave compartida puede permitir compartición de secreto multifactor o de dos factores (2FSS). Entonces puede requerirse al adversario que navegue por dos tipos de seguridad fundamentalmente diferentes con el fin de romper el mecanismo de seguridad. Por ejemplo, para violar los objetivos de compartición de secreto, el adversario (1) puede necesitar obtener las cuotas de un conjunto autorizado de jugadores, *y* (2) puede necesitar obtener una clave secreta que no debería poder obtener (o romper el mecanismo criptográfico que es codificado por esa clave).

En algunas realizaciones, se añade un nuevo conjunto de requisitos adicionales al objetivo de RCSS. Los requisitos adicionales pueden incluir la posesión de la clave de "segundo factor". Estos requisitos adicionales pueden añadirse sin disminuir el conjunto de requisitos original. Un conjunto de requisitos puede estar relacionado con la incapacidad del adversario de romper el esquema si conoce la clave secreta pero no obtiene suficientes cuotas (por ejemplo, los requisitos *clásicos* o *de primer factor*) mientras que el otro conjunto de requisitos puede estar relacionado con la incapacidad del adversario de romper el esquema si tiene la clave secreta pero se las arregla para apropiarse de todas las cuotas (por ejemplo, los requisitos *nuevos* o *de segundo factor*).

En algunas realizaciones, puede haber dos requisitos de segundo factor: un requisito de privacidad y un requisito de autenticidad. En el requisito de privacidad, puede estar implicado un juego en el que una clave secreta *K* y un bit *b* son seleccionados por el entorno. El adversario ahora suministra un par de mensajes de igual longitud en el dominio del esquema de compartición de secreto, M_1^0 y M_1^1. El entorno calcula las cuotas de M_1^b para obtener un vector de cuotas, $\boldsymbol{S}_1 = (\boldsymbol{S}_1[1], ..., \boldsymbol{S}_1[n])$, y da las cuotas $\boldsymbol{S}_1$ al adversario (todas ellas). El adversario ahora puede escoger otro par de mensajes (M_2^0, M_2^1) y todo continúa como antes, usando la misma clave *K* y el bit oculto *b*. El trabajo del adversario es producir el bit *b'* que cree que es *b*. La privacidad del adversario es uno menos el doble de la probabilidad de que *b = b'.* Este juego capta la noción de que, incluso aprendiendo todas las cuotas, el adversario aun así no puede aprender nada acerca del secreto compartido si carece de la clave secreta.

En el requisito de autenticidad, puede estar implicado un juego donde el entorno escoge una clave secreta *K* y usa esta en las llamadas subsiguientes a *Cuota* y *Recuperar. Cuota* y *Recuperar* pueden tener su sintaxis modificada, en algunas realizaciones, para reflejar la presencia de esta clave. Luego el adversario hace solicitudes de *Cuota* para cualquier mensaje $M_1, ..., M_q$ que elija en el dominio del esquema de compartición de secreto. En respuesta a cada solicitud de *Cuota* obtiene el n-vector correspondiente de cuotas, $\boldsymbol{S}_1, ..., \boldsymbol{S}_q$. El propósito del adversario es *falsificar* un nuevo texto plano: gana si produce un vector de cuotas **S'** tal que, cuando es suministrado al algoritmo de *Recuperación*, resulta en algo que *no está* en $\{M_1, ..., M_q\}$. Esta es una noción de "integridad de texto plano".

Existen dos estrategias para lograr compartición de secreto multifactor. La primera es una estrategia genérica – genérica en el sentido de usar un esquema (R)CSS subyacente a modo de caja negra. Se usa un esquema de cifrado autenticado para cifrar el mensaje que ha de ser compartido por CSS, y luego el texto de cifrado resultante puede ser compartido, por ejemplo, usando un algoritmo de compartición de secreto, tal como Blakely o Shamir.

Una estrategia potencialmente más eficiente es permitir que la clave compartida sea la clave de grupo de trabajo. Concretamente, (1) la clave de sesión generada aleatoriamente del esquema (R)CSS puede ser cifrada usando la clave compartida, y (2) el esquema de cifrado aplicado al mensaje (por ejemplo, el archivo) puede ser sustituido por un esquema de cifrado autenticado. Esta estrategia puede implicar solo una mínima degradación de rendimiento.

Aunque anteriormente se describen algunas aplicaciones del analizador sintáctico de datos seguros, debería entenderse claramente que la presente invención puede ser integrada con cualquier aplicación de red con el fin de aumentar la seguridad, la tolerancia a fallos, el anonimato, o cualquier combinación de lo anterior.

En algunas realizaciones de la presente invención, el analizador sintáctico de datos seguros puede implementarse en un servicio de apoderado seguro para asegurar datos en movimiento. Como se describe anteriormente, el analizador sintáctico de datos seguros es una biblioteca criptográfica que proporciona servicios de cifrado/autenticación tradicionales para aplicaciones, así como una propiedad de seguridad adicional lograda separando los datos protegidos (ya sea físicamente, temporalmente, o por alguna otra forma de confianza). El analizador sintáctico de datos seguros está diseñado para aplicaciones donde la amenaza de que un adversario comprometa el sistema es real, ya sea obteniendo claves criptográficas, acceso físico a un medio de transmisión, u obteniendo cualquier conocimiento que normalmente vencería a la seguridad. El servicio de apoderado seguro proporciona una capa adicional de seguridad para proteger de estas mismas amenazas, y es preferentemente flexible de modo que pueda implementarse en una amplia gama de sistemas – (por ejemplo, servidores empresariales, ordenadores personales, cualquier otra combinación de los mismos). El servicio de apoderado

seguro se describe más adelante con respecto a las figuras 42-50.

El servicio de apoderado seguro se usa para asegurar datos en movimiento entre dos dispositivos. En particular, el servicio de apoderado seguro se ejecuta en un primer dispositivo y proporciona comunicaciones habilitadas por analizador sintáctico de datos seguros para aplicaciones por una red. Estos dispositivos pueden ser cualquier par adecuado de dispositivos incluidos en el sistema criptográfico (100) (figura 1). Por ejemplo, el servicio de apoderado seguro puede establecerse entre el sistema de usuario (105) y el sistema de vendedor (120), tales como un ordenador personal y un servidor web. En otro ejemplo, el servicio de apoderado seguro puede establecerse entre sistemas de usuario separados (105), tales como un ordenador personal y un NAS, un ordenador personal y un encaminador doméstico, un NAS y un encaminador doméstico, o cualquier combinación adecuada de sistemas de usuario (105). La comunicación entre dispositivos que usan el servicio de apoderado seguro se asemeja a la de un cliente que se conecta a una web o un servidor de correo electrónico.

En algunas realizaciones, un cliente, tal como el sistema de usuario (105), y un servidor, tal como el sistema de vendedor (120), pueden establecer comunicaciones seguras usando el servicio de apoderado seguro. Al establecer el servicio de apoderado seguro, el sistema de usuario (105) y el sistema de vendedor (120) pueden ser actualizados a una configuración adecuada para el servicio de apoderado seguro. En tales realizaciones, cuando el cliente se conecta al servidor, la conexión se establece entre los dos servicios de apoderado seguro. En el servidor, el servicio de apoderado seguro está configurado para reenviar los datos que recibe a una aplicación servidor. La aplicación servidor puede entonces encargarse de la solicitud y responder a través del servicio de apoderado seguro implementado localmente.

En algunas realizaciones, el servicio de apoderado seguro protege la confidencialidad, integridad y autenticidad de los datos transmitidos por una red basándose en la confianza distribuida entre cualquier número de autoridades de certificación, tales como las autoridades de certificación (115) (figura 1). En tales realizaciones, la confidencialidad, integridad y autenticidad de los datos puede protegerse siempre que se confíe en un *quorum* de autoridades de certificación. Si la confianza de la autoridad de certificación se ve comprometida, no puede garantizarse la autenticación mutua, y la confidencialidad, integridad y autenticidad de los mensajes intercambiados se derrumba. El servicio de apoderado seguro es una solución habilitada por analizador sintáctico de datos seguros que permite que la confianza puesta en una sola autoridad de certificación sea distribuida por cualquier número de autoridades de certificación (por ejemplo, dos, tres, cinco, diez, veinte, cincuenta, cien, o más de cien autoridades de certificación). Esta confianza distribuida permite que el intercambio de mensajes por el servicio de apoderado seguro permanezca seguro si existe un solo punto de fallo entre el conjunto de autoridades de certificación.

En algunas realizaciones, el servicio de apoderado seguro se implementa usando una adaptación de los protocolos SSL y/o TLS completa. Estos protocolos pueden ser adecuados para adaptación como parte del servicio de apoderado seguro porque están basados al menos en parte en la confianza de una autoridad de certificación para autenticar mutuamente ambas partes en una comunicación.

A continuación se describe una visión general del uso de autoridades de certificación en TLS completa. Para que se establezca una conexión habilitada por TLS completa entre dos dispositivos, los dos dispositivos se ponen de acuerdo sobre el paquete criptográfico de algoritmos que han de usar, e intercambian y autentican mutuamente las claves públicas de uno y otro. Las claves públicas de cada dispositivo son autenticadas mediante la validación de la firma de una autoridad de certificación de la clave pública. La confianza que los dos dispositivos están comunicándose genuinamente se establece por el hecho de que los dos confían en la autoridad de certificación, cuya firma de los certificados de los dispositivos no podría ser falsificada sin el compromiso de esa autoridad.

La autoridad de certificación crea para sí misma un par de clave pública y privada, (Pub_{CA}, Pri_{CA}). Además, la autoridad de certificación crea un certificado autofirmado para la clave pública:

$$Cert_{CA} = Pub_{CA}, Sig_{Pri\text{-}CA}(Pub_{CA}) \qquad (1)$$

Ambos dispositivos reciben el certificado $Cert_{CA}$ de la autoridad de certificación de acuerdo con la ecuación (1), una clave privada (Pri_{Dev1}, Pri_{Dev2}), y un certificado firmado por la autoridad de certificación:

$$Cert_{Dev1} = Pub_{Dev1}, Sig_{Pri\text{-}CA}(Pub_{Dev1}) \qquad (2)$$

$$Cert_{Dev2} = Pub_{Dev2}, Sig_{Pri\text{-}CA}(Pub_{Dev2}) \qquad (3)$$

Cuando comienza una comunicación, los dispositivos intercambian sus certificados respectivos en las ecuaciones (2) y (3), y verifican la autenticidad de estos certificados usando la clave pública de la autoridad de certificación. Por ejemplo, el primer dispositivo puede realizar la verificación ejecutando una función de verificación Verify($Cert_{Dev2}$, Pub_{CA}), y el segundo dispositivo puede realizar la verificación ejecutando una función de verificación Verify($Cert_{Dev1}$, Pub_{CA}). Si ambos dispositivos están satisfechos con la firma de la autoridad de certificación de las claves públicas intercambiadas, el primer dispositivo envía el material de clave de cifrado simétrica del segundo dispositivo usando la clave pública del segundo dispositivo. El primer dispositivo demuestra el conocimiento de la clave privada que corresponde a su certificado realizando una puesta a prueba de firma digital. Una vez que el primer dispositivo demuestra el conocimiento de la clave privada que corresponde a su certificado, el primer dispositivo y el segundo dispositivo pueden intercambiar mensajes con seguridad.

Si o bien el primer dispositivo o bien el segundo dispositivo se han visto comprometidos, sus claves privadas respectivas pueden verse comprometidas también y a partir de entonces el dispositivo comprometido podría ser suplantado. Si la autoridad de certificación se ve comprometida, pueden generarse certificados válidos para los cuales la autoridad de certificación conoce la clave privada correspondiente, y alguno de los dispositivos podría ser suplantado. Sin embargo, sin compromiso de los dispositivos o la autoridad de certificación, los dispositivos pueden garantizarse mutuamente que están hablando con la entidad correcta.

En algunas realizaciones, no toda la confianza es delegada en una sola autoridad de certificación. Puede resultar poco práctico crear, distribuir y validar constantemente certificados por parte de una sola autoridad de certificación. En cambio, puede establecerse una cadena de confianza en forma de una jerarquía de autoridades de certificación (4200), como se ilustra por la figura 42. La jerarquía de autoridades de certificación (4200) puede establecer una cadena de confianza en forma de árbol. En la copa del árbol está la autoridad de certificación raíz (4210) quien delga la autoridad en todos los descendientes (por ejemplo, hijos y nietos) de los certificados raíz (4210). La confianza en cada nivel de la jerarquía de autoridades de certificación (4200) está garantizada por la confianza de la autoridad de certificación raíz (4210).

En la jerarquía de autoridades de certificación (4200), la autoridad de certificación raíz (4210) puede firmar certificados para autoridades de certificación hijas (4220). Aunque en la figura 42 solo se muestra una autoridad de certificación raíz (CA-0), puede entenderse que en ciertas realizaciones la jerarquía de autoridades de certificación puede incluir cualquier número de autoridades de certificación raíces. Las autoridades de certificación hijas (4220) pueden firmar certificados para autoridades de certificación nietas (4230). Por ejemplo, como se ilustra en la figura 42, la autoridad de certificación raíz (CA-0) firma certificados para sus hijas (CA-1) y (CA-2), quienes a su vez firman certificados para sus hijas (CA-1.1), (CA-1.2), (CA-2.1) y (CA-2.2). Aunque en la figura 42 se ilustran solo tres niveles de autoridades de certificación, se entenderá que en ciertas realizaciones puede haber más o menos niveles de autoridades de certificación. Para garantizar el no rechazo de firmas, todas las entidades pueden generar sus propios certificados.

En un sistema criptográfico, un primer dispositivo puede haber recibido su certificado de una de las autoridades de certificación hijas (4220), y un segundo dispositivo en comunicación con el primer dispositivo puede recibir su certificado de una de las autoridades de certificación nietas (4230). La validación de los certificados para cada dispositivo puede realizarse obteniendo el certificado de la autoridad de certificación expedidora (por ejemplo, (CA-1) o (CA-2) para el primer dispositivo, y (CA-1.1), (CA-1.2), (CA-2.1), o (CA-2.2) para un segundo dispositivo) y verificando la firma del certificado del primer dispositivo o el segundo dispositivo (por ejemplo, verificando los certificados mostrados en las ecuaciones (2) o (3)). Si la confianza de la autoridad de certificación expedidora no puede establecerse, el dispositivo que realiza la verificación puede obtener el certificado del padre de la autoridad de certificación expedidora en cuestión y realizar una verificación similar para garantizar que la autoridad de certificación es válida. Este proceso puede continuar por parte de ambos dispositivo hasta llegar a la autoridad de certificación raíz (4210), que es de confianza para ambos dispositivos. En algunas realizaciones, cada dispositivo que está en comunicación puede estar asociado con más de una autoridad de certificación raíz (4210). En tales realizaciones, es posible que los dispositivos con certificados válidos procedentes de cualquiera de estas autoridades de certificación se comuniquen.

A partir de la descripción anterior del uso de autoridades de certificación con TLS, se entiende que la seguridad está basada en última instancia en la confianza de una sola autoridad de certificación raíz, o en menor medida, una de las autoridades de certificación descendientes dentro de la jerarquía de autoridades de certificación en la que los dispositivos en comunicación confían cómodamente. En algunas realizaciones, si cualquier autoridad de certificación en la jerarquía se ve comprometida, todos los descendientes de la autoridad de certificación comprometida también se ven comprometidos. Si este nodo comprometido es la raíz, entonces cada una de las autoridades de certificación

en la jerarquía puede verse comprometida.

En algunas realizaciones, el servicio de apoderado seguro puede usar el analizador sintáctico de datos seguros con TLS para distribuir la confianza puesta en una sola autoridad de certificación con la confianza de un *quorum* de autoridades de certificación. Este *quorum* puede ser un *quorum* de autoridades de certificación raíces (4210), o un *quorum* de autoridades de certificación menores dentro del árbol de una sola autoridad de certificación raíz. Por ejemplo, este *quorum* puede ser dos de las tres autoridades de certificación en el conjunto que consiste en (CA-1), (CA-1.1) y (CA-1.2), que son autoridades de certificación menores dentro del árbol de la autoridad de certificación raíz (CA-0).

En algunas realizaciones, la jerarquía de autoridades de certificación (4200) puede ser recorrida por cualquier algoritmo gráfico adecuado. Este recorrido puede realizarse con el fin de obtener una lista de autoridades de certificación o una lista de certificados asociados con autoridades de certificación tan únicas, o tienen diferentes pares de claves públicas y privadas. En algunas realizaciones, el recorrido de la jerarquía de autoridades de certificación (4200) puede resultar en autoridades de certificación o certificados de autoridades de certificación que son autoridades de certificación raíces. En algunas realizaciones, el recorrido de la jerarquía de autoridades de certificación (4200) puede resultar en autoridades de certificación o certificados de autoridades de certificación que son autoridades de certificación menores dentro del árbol de una o más autoridades de certificación raíces.

Las figuras 44 a 50 detallan dos estrategias para implementar el servicio de apoderado seguro. Ambas estrategias son igualmente seguras. En algunas realizaciones, el analizador sintáctico de datos seguros puede estar integrado con TLS completa. Además, en cada estrategia la confianza se distribuye entre un conjunto de autoridades de certificación (por ejemplo, el *quorum* de autoridades de certificación analizado con respecto a la jerarquía de autoridades de certificación (4200) en la figura 42). En algunas realizaciones, el servicio de apoderado seguro puede implementarse integrando el analizador sintáctico de datos seguros con SSL, con SSL y TLS, o implementando el analizador sintáctico de datos seguros sin el uso de SSL y/o TLS. En algunas realizaciones, el servicio de apoderado seguro puede implementarse conjuntamente con uno cualquiera o más tipos de cifrado (3018) que pueden proporcionar cifrado seguro de datos en la capa de analizador sintáctico de daos seguros (3026) de la figura 30. Además, en algunas realizaciones el servicio de apoderado seguro puede implementarse conjuntamente con cualquier protocolo adecuado que haga uso de autoridades de certificación para garantizar la confidencialidad, integridad y autenticidad de los mensajes intercambiados.

En las realizaciones descritas con respecto a las figuras 44 a 46, el analizador sintáctico de datos seguros puede usarse para distribuir confianza en cualquier número de autoridades de certificación durante la negociación inicial (por ejemplo, la fase de establecimiento de clave) de una conexión entre dispositivos. Esto ofrece la garantía de que si alguna (pero menos que un *quorum*)*quorum* de las autoridades de certificación se han visto comprometidas, la conexión todavía puede establecerse, y los mensajes pueden intercambiarse sin alterar la confidencialidad, integridad y autenticidad de la comunicación. En las realizaciones descritas con respecto a las figuras 47 a 50, los datos son preprocesados usando el analizador sintáctico de datos seguros y luego dispersados en cuotas. Puede establecerse un conjunto de túneles de comunicación segura dentro de un canal de comunicación usando certificados expedidos por autoridades de certificación únicas, estas autoridades de certificación pueden usarse para cifrar datos para cada uno de los túneles, y las cuotas individuales pueden ser transmitidas por cada uno de los túneles. Así, en la segunda estrategia puede distribuirse confianza entre un conjunto de autoridades de certificación en la estructura del canal de comunicación en sí.

Con el fin de ilustrar cómo está integrado el analizador sintáctico de datos seguros con la TLS en algunas realizaciones del servicio de apoderado seguro, se describe una visión general de la fase de establecimiento de clave de TLS completa con respecto a la figura 43. La figura 43 muestra un flujo de proceso simplificado e ilustrativo (4300) para la fase de establecimiento de clave de TLS para comunicación entre dos dispositivos: el primer dispositivo (4310) y el segundo dispositivo (4320). El primer dispositivo (4310) y el segundo dispositivo (4320) pueden ser cualquier combinación de sistema de usuario (105) y/o sistema de vendedor (120) que se comunican por un enlace de comunicación, por ejemplo, el enlace de comunicación (125) como se muestra en la figura 1. Esta fase de establecimiento de clave puede incluir una toma de contacto y autenticación mutua. En la etapa (4312), el primer dispositivo (4310) genera un número aleatorio R_{Dev1} y envía el número aleatorio junto con su certificado $Cert_{Dev1}$ (como se calculó, por ejemplo, en la ecuación (2)) al segundo dispositivo (4320).

En la etapa (4322), el segundo dispositivo (4320) genera su propio número aleatorio R_{Dev2}, y envía el número aleatorio junto con su certificado $Cert_{Dev2}$ (como se calculó en la ecuación (3)). En la etapa (4314), el cliente genera información secreta S_{Dev1}, la cifra bajo la clave pública del segundo dispositivo usando cualquier tipo de cifrado

adecuado, y la envía al segundo dispositivo. En la etapa (4324), el segundo dispositivo (4320) descifra la información secreta S_{Dev1} y calcula una clave de cifrado compartida K basándose en una función pseudoaleatoria G y los valores aleatorio y secreto que han sido intercambiados (es decir, R_{Dev1}, R_{Dev2}, y S_{Dev1}). De manera similar, en la etapa (4316) el segundo dispositivo (4310) calcula una clave de cifrado compartida K basándose en una función pseudoaleatoria G y los valores aleatorio y secreto que han sido intercambiados (es decir, R_{Dev1}, R_{Dev2}, y S_{Dev1}). En la etapa (4330), el primer dispositivo (4310) y el segundo dispositivo (4320) intercambian mensajes cifrados con sus claves de cifrado compartidas calculadas independientemente. Si las claves de cifrado compartidas calculadas coinciden, el primer dispositivo (4310) y el segundo dispositivo (4320) pueden intercambiar mensajes que se garantiza que son confidenciales y auténticos. Como se analizará con respecto a las figuras 44 a 46, en algunas realizaciones, el servicio de analizador sintáctico de datos seguros puede modificar y/o añadir a las etapas del flujo de proceso (4300) con el fin de integrar el analizador sintáctico de datos seguros con TLS.

La figura 44 muestra un flujo de proceso simplificado e ilustrativo (4400) para un servicio de apoderado seguro, que puede usarse en cualquier combinación adecuada, con cualquier añadido, eliminación o modificación adecuados de acuerdo con una realización de la presente invención. En el flujo de proceso (4400), la confianza se distribuye en un conjunto de autoridades de certificación durante la negociación inicial de una conexión entre dispositivos. En algunas realizaciones, el flujo de proceso (4400) puede ejecutarse como parte de la fase de establecimiento de clave de un intercambio seguro de información entre dos dispositivos. Esta fase de establecimiento de clave puede formar parte de uno o más de los procesos asociados con el analizador sintáctico de datos seguros (3706) como se ilustra en la figura 37, o puede ser un proceso independiente. Por ejemplo, las etapas (4410), (4420), (4430), (4440), (4450) y (4460) pueden ser parte de uno o más del proceso de precifrado (3708), el proceso de cifrado/transformada (3710), el proceso de clave segura (3712), o el proceso de análisis sintáctico/distribución (3714) asociados con el analizador sintáctico de datos seguros (3706) como se ilustra en la figura 37, o puede ser un proceso independiente.

El flujo de proceso (4400) comienza en la etapa (4410). En la etapa (4410), un primer dispositivo al que le gustaría intercambiar con seguridad información con el segundo dispositivo puede generar información secreta. Esta información secreta puede ser cualquier cantidad de números aleatorios adecuados (por ejemplo, uno, dos, cinco, veinte, cien, o más de cien números aleatorios) generados por un generador de números aleatorios. Por ejemplo, la información secreta puede ser un número aleatorio generado por el generador de números aleatorios (3012) del analizador sintáctico de datos seguros (3026) como se muestra en la figura 30. El flujo de proceso (4400) pasa a la etapa (4420).

En la etapa (4420), el primer dispositivo puede dispersar la información secreta generada en la etapa (4410) en cuotas. En algunas realizaciones, la información secreta puede ser dispersada en cuotas usando un proceso de criptodivisión, tal como una “criptodivisión M de N”. Esta “criptodivisión M de N” puede lograrse usando el analizador sintáctico de datos seguros de la presente invención. Por ejemplo, la criptodivisión puede lograrse usando cualquiera de las técnicas de división de datos analizadas con respecto a la figura 21 a la figura 24. En tales realizaciones, las cuotas dispersas pueden ser recuperables a partir de al menos un subconjunto de las cuotas recombinando al menos un *quorum* de las cuotas. Además, en algunas realizaciones, la división de información secreta puede producirse sustancialmente a través de cualquier número de usos del analizador sintáctico de datos seguros esbozados con respecto a la figura 33, la figura 35 y la figura 36. Por ejemplo, el analizador sintáctico de datos seguros puede recibir información secreta descifrada en la etapa (3610). Si la información secreta va a ser dividida con un algoritmo que requiere una clave, se genera una clave de cifrado de división en la etapa (3612). La información secreta puede ser dividida en cuotas en la etapa (3616) (por ejemplo, de acuerdo con cualquiera de las técnicas descritas con respecto a la figura 33, la figura 35 y la figura 36). Puede usarse un esquema tolerante a fallos en la etapa (3617) para cifrar la clave de cifrado de división y permitir la regeneración de la información secreta a partir de menos del número total de cuotas. Además, en la etapa (3617) puede añadirse información a las cuotas de información secreta que se usa para reconstruir las cuotas. En algunas realizaciones, esta información puede insertarse dentro de encabezamientos de cuota. Además, una vez que se crean las cuotas, puede insertarse información de autenticación/integridad dentro de los encabezamientos de las cuotas de información secreta en la etapa (3618). Cada cuota puede ser postcifrada usando claves públicas de diferentes autoridades de certificación como se describirá con respecto a la etapa (4430).

Además, en algunas realizaciones, la dispersión de la información secreta en cuotas puede producirse, por ejemplo, de acuerdo con el proceso de generación de encabezamiento simplificado (4000) como se muestra en la figura 40A. Por ejemplo, en la etapa (4002), puede generarse la información secreta. La información secreta puede entonces ser cifrada opcionalmente (por ejemplo, usando la clave de grupo de trabajo descrita con respecto a la figura 39) en la etapa (4004). En la etapa (4006), puede usarse una “criptodivisión M de N” para dividir la información secreta en cuotas de información secreta. La información asociada con la división de información secreta puede entonces

insertarse dentro de un encabezamiento de cuota. Por último, un bloque de integridad de cuota y una etiqueta de postautenticación (por ejemplo, MAC) pueden adjuntarse al bloque de encabezamiento de cada cuota. Cada bloque de encabezamiento puede estar diseñado para ajustar dentro de un solo paquete de datos.

En algunas realizaciones, las cuotas de información secreta generadas en la etapa (4420) pueden generarse usando un esquema de compartición de secreto multifactor. Este esquema de compartición de secreto multifactor puede ser, por ejemplo, el algoritmo de dispersión de información codificada analizado después de la figura 41. Por ejemplo, las cuotas de información secreta pueden ser distribuidas con los datos que han de ser asegurados en una pluralidad de cuotas usando técnicas de distribución de datos deterministas, probabilistas, o tanto deterministas como probabilistas. Una vez que la información secreta ha sido dispersada en cuotas, el flujo de proceso (4400) puede pasar a la etapa (4430).

En la etapa (4430), las cuotas que resultan de la división de información secreta calculada en la etapa (4420) son cifradas por el primer dispositivo basándose en claves públicas de autoridades de certificación únicas. Por ejemplo, si existen tres cuotas de información secreta, la primera cuota puede ser cifrada bajo la clave pública de una primera autoridad de certificación, la segunda cuota puede ser cifrada bajo la clave pública de una segunda autoridad de certificación, y la tercera cuota puede ser cifrada bajo la clave pública de una tercera autoridad de certificación. Cada autoridad de certificación puede ser única porque los certificados expedidos por cada una tienen diferentes pares de clave pública y privada. En algunas realizaciones, las autoridades de certificación únicas pueden ser autoridades de certificación raíces. En otras realizaciones, las autoridades de certificación únicas pueden ser autoridades de certificación menores dentro del árbol de una sola autoridad de certificación raíz, como se analiza con respecto a la jerarquía de autoridades de certificación (4200) en la figura 42.

Como se analiza anteriormente con respecto a la etapa (4420), en algunas realizaciones la información relacionada con la dispersión de información secreta puede insertarse dentro de encabezamientos de cuota. Por ejemplo, si la información secreta es dividida en la etapa (4420) en cuatro cuotas, pueden generarse cuatro encabezamientos que incluyen cada uno información asociada con las cuotas de información secreta dispersadas.

En algunas realizaciones, las cuotas pueden ser protegidas por una o más claves de grupo de trabajo externas, una o más claves compartidas, o cualquier combinación de claves de grupo de trabajo y claves de cuota. Una vez que las cuotas de información secreta son cifradas, el primer dispositivo puede enviar las cuotas cifradas al segundo dispositivo. El flujo de proceso (4400) pasa entonces a la etapa (4440).

En la etapa (4440), el segundo dispositivo puede intentar recuperar la información secreta cifrada. Este proceso de recuperación puede depender de cómo las cuotas de información secreta fueron dispersadas en la etapa (4420) y cifradas en la etapa (4430). Por ejemplo, la información secreta puede haber sido dispersada en cuotas usando una “criptodivisión M de N” y cifradas usando una clave de grupo de trabajo en la etapa (4420), y luego esas cuotas pueden ser cifradas basándose en claves públicas de diferentes autoridades de certificación en la etapa (4430). El proceso de recuperación puede descifrar las cuotas en primer lugar usando las claves públicas de las diferentes autoridades de certificación, luego descifrar las cuotas basándose en la clave de grupo de trabajo, y luego usa una función de restauración del analizador sintáctico de datos seguros para reconstruir las cuotas de información secreta dispersadas en la información secreta original basándose en la “criptodivisión M de N”.

Si el proceso de recuperación es exitoso, la información secreta calculada puede coincidir con la información secreta original. Esta coincidencia puede ser confirmada mutuamente entre los dispositivos mediante el cálculo independiente por parte de cada dispositivo de una clave de cifrado compartida. Por ejemplo, un primer dispositivo puede calcular una clave de cifrado compartida basándose en la información secreta original, mientras que el segundo dispositivo calcula una clave de cifrado compartida basándose en la información secreta recuperada o restaurada. En algunas realizaciones, si el segundo dispositivo recupera la información secreta original y posteriormente calcula una clave de cifrado compartida válida, el flujo de proceso (4400) pasa a la etapa (4450), y se intercambian mensajes. En algunas realizaciones, estos mensajes pueden ser intercambiados con seguridad basándose en las claves de cifrado compartidas calculadas por el primer dispositivo y el segundo dispositivo. En algunas realizaciones, si el segundo dispositivo no recupera la información secreta original, el flujo de proceso (4400) pasa a la etapa (4460), y no se intercambian mensajes. Por ejemplo, puede que los mensajes no puedan intercambiarse porque la clave de cifrado compartida del primer dispositivo no coincide con la del segundo dispositivo.

La figura 45 muestra un flujo de proceso simplificado e ilustrativo (4500) para establecer un servicio de apoderado seguro entre dos dispositivos, que puede usarse en cualquier combinación adecuada, con cualquier añadido,

eliminación o modificación adecuados de acuerdo con una realización de la presente invención. En el flujo de proceso (4500), la confianza se distribuye en un conjunto de autoridades de certificación durante la negociación inicial de una conexión entre dispositivos. En algunas realizaciones, el flujo de proceso (4500) puede ejecutarse como parte de la fase de establecimiento de clave de un intercambio seguro de información entre dos dispositivos. Esta fase de establecimiento de clave, incluyendo cada una de las etapas en el flujo de proceso (4500), puede ser parte de uno o más de los procesos asociados con el analizador sintáctico de datos seguros, por ejemplo, de manera similar a cómo las etapas del flujo de proceso (4400) están asociadas con el analizador sintáctico de datos seguros.

El flujo de proceso (4500) comienza en la etapa (4510). En la etapa (4510), los dispositivos intercambian números aleatorios y certificados asociados con claves públicas, cada clave pública expedida por una autoridad de certificación única. En algunas realizaciones, estos dispositivos pueden ser, por ejemplo, el primer dispositivo (4310) y el segundo dispositivo (4320) como se describe con respecto al flujo de proceso (4300) en la figura 43. Los números aleatorios intercambiados pueden ser generados por cada dispositivo usando el generador de números aleatorios (3012) del analizador sintáctico de datos seguros (3026) como se muestra en la figura 30. Los certificados intercambiados pueden ser generados a partir del recorrido de la jerarquía de autoridades de certificación (4200) como se muestra en la figura 42. Por ejemplo, cualquier algoritmo gráfico adecuado puede recorrer la jerarquía de certificación (4200) para calcular una lista de los certificados de las autoridades de certificación raíces, o una lista de los certificados de las autoridades de certificación menores dentro del árbol de una sola autoridad de certificación raíz dentro de la jerarquía de certificación (4200). En algunas realizaciones, los certificados intercambiados pueden determinarse basándose en parámetros de cifrado acordados por el primer y el segundo dispositivo. Estos parámetros pueden estar asociados con la implementación de dispersión de las cuotas de información secreta acordada por el primer y el segundo dispositivo. Por ejemplo, si las técnicas de dispersión usadas en la etapa (4520) dispersan información secreta en cinco cuotas, los certificados intercambiados pueden incluir cinco certificados de autoridades de certificación únicas del primer dispositivo, y cinco certificados de autoridades de certificación únicas del segundo dispositivo.

En algunas realizaciones, puede obtenerse una clave pública única para cada certificado único del primer dispositivo o el segundo dispositivo. En algunas realizaciones, los parámetros de cifrado pueden ser fijados por el usuario del servicio de apoderado seguro, tal como el usuario de un ordenador personal que quiere conectar con el servidor de una institución financiera usando el servicio de apoderado seguro. En algunas realizaciones, los parámetros de cifrado pueden ser fijados por un administrador del servicio de apoderado seguro, tal como el administrador de los servidores de una institución financiera que quiere ofrecer conexiones habilitadas para servicio de apoderado seguro a sus clientes. Además, el algunas realizaciones, las listas de certificados intercambiadas pueden estar basadas en un proceso de inscripción (900) llevado a cabo con el usuario de uno de los dispositivos como se describe con respecto a la figura 9. El flujo de proceso (4500) pasa entonces a la etapa (4515).

En la etapa (4515), el primer dispositivo genera información secreta. Esta información secreta puede ser generada, por ejemplo, de acuerdo con la etapa (4410) descrita con respecto al flujo de proceso (4400) de la figura 44. El flujo de proceso (4500) pasa entonces a la etapa (4520). En la etapa (4520), el primer dispositivo dispersa la información secreta generada en la etapa (4515) en cuotas usando cualquier técnica de dispersión adecuada. Por ejemplo, el primer dispositivo puede realizar una “criptodivisión M de N” de la información secreta usando el analizador sintáctico de datos seguros de la presente invención de acuerdo con, por ejemplo, la etapa (4420) descrita con respecto al flujo de proceso (4400) de la figura 44. En algunas realizaciones, las cuotas de información secreta que resultan de las técnicas de dispersión pueden ser recuperables a partir de al menos un subconjunto de las cuotas recombinando al menos un *quorum* de las cuotas. Además, en algunas realizaciones, puede aplicarse una rutina de compartición de secreto codificada a las cuotas de información secreta usando un IDA codificado. La clave para el IDA codificado puede ser protegida por una o más claves de grupo de trabajo externas, una o más claves compartidas, o cualquier combinación de claves compartidas y de grupo de trabajo. El flujo de proceso (4500) pasa entonces a la etapa (4525).

En la etapa (4525), el primer dispositivo cifra cada cuota de información secreta basándose en una clave pública expedida por una autoridad de certificación diferente. Las claves públicas pueden ser claves públicas obtenidas de los certificados enviados al segundo dispositivo desde el primer dispositivo en la etapa (4510). En algunas realizaciones, la etapa (4525) puede estar incluida como parte de la etapa (4520). Por ejemplo, la rutina de compartición de secreto codificada descrita con respecto a la etapa (4520) puede aplicarse a las cuotas de información secreta, donde las claves para el IDA codificado son las claves públicas asociadas con la lista de certificados enviada al segundo dispositivo desde el primer dispositivo. En otro ejemplo, las claves públicas asociadas con la lista de certificados pueden usarse como claves de división para cifrar las cuotas de información

secreta como se describe con respecto a las opciones (3600) de la figura 36. El proceso (4500) pasa entones a la etapa (4530), o puede pasar opcionalmente a la etapa (4527).

En la etapa opcional (4527), el primer dispositivo puede realizar una envoltura de clave sobre las claves aplicadas a las cuotas de información secreta en la etapa (4525). En algunas realizaciones, la envoltura de clave puede ser cualquier algoritmo de cifrado de clave o de envoltura de clave adecuado. La envoltura de clave puede operar sobre todas las cuotas de información secreta dispersada producidas en la etapa (4520). Alternativamente, las cuotas dispersadas pueden ser dispersadas adicionalmente en varios bloques, y la envoltura de clave puede operar sobre estos bloques. El flujo de proceso (4500) pasa entonces a la etapa (4530).

En la etapa (4530), el primer dispositivo transmite las cuotas de información secreta cifradas al segundo dispositivo. Esta transmisión puede producirse por cualquier canal de comunicación adecuado, tal como el descrito con respecto al enlace de comunicación (105) en la figura 1. El primer dispositivo en el flujo de proceso (4500) pasa entonces a la etapa (4545), mientras que el segundo dispositivo pasa a la etapa (4535).

En la etapa (4535), el segundo dispositivo puede intentar descifrar las cuotas cifradas recibidas del primer dispositivo. El proceso de descifrado puede estar basado en cómo fueron cifradas las cuotas de información secreta en la etapa (4520) y la etapa (4525). Por ejemplo, en la etapa (4520), las cuotas de información secreta pueden haber sido producidas a partir de técnicas de dispersión que producen cuotas de información secreta que pueden ser recuperables a partir de al menos un subconjunto de las cuotas recombinando al menos un *quorum* de cuotas. En la etapa (4525), cada parta alícuota dispersada puede haber sido cifrada usando las claves públicas obtenidas por diferentes autoridades de certificación que corresponden a los certificados del segundo dispositivo. En la etapa (4527), las cuotas pueden haber sido cifradas adicionalmente usando una envoltura de clave basado en una clave de grupo de trabajo. Basándose en este cifrado, en la etapa (4535) el segundo dispositivo puede descifrar en primer lugar las cuotas de información secreta cifradas basándose en las claves públicas expedidas por autoridades de certificación únicas, luego descifrar las cuotas de información secreta basándose en la clave de grupo de trabajo de la envoltura de clave aplicada en la etapa (4527). Se entenderá que más allá de este ejemplo particular, en la etapa (4535) puede realizarse cualquier número y tipo adecuado de etapas de descifrado. El flujo de proceso (4500) pasa entonces a la etapa (4540).

En la etapa (4540), el segundo dispositivo puede intentar restaurar la información secreta original basándose en las cuotas descifradas calculadas en la etapa (4535). Este proceso de restauración puede estar basado en cómo la información secreta generada en la etapa (4515) fue dispersada en la etapa (4520). Por ejemplo, en la etapa (4520), las cuotas de información secreta pueden haber sido producidas usando funciones de dispersión del analizador sintáctico de datos seguros de acuerdo con cualquiera de las técnicas descritas con respecto a la figura 33, la figura 35 y la figura 36. Basándose en esta dispersión, en la etapa (4540) el segundo dispositivo puede restaurar la información secreta original a partir de la división usando funciones de restauración del analizador sintáctico de datos seguros de acuerdo con cualquiera de las técnicas descritas con respecto a la figura 34. El flujo de proceso (4500) pasa entonces a la etapa (4545).

En la etapa (4545), el primer y el segundo dispositivos pueden calcular independientemente una clave de cifrado compartida basándose en los números aleatorios intercambiados, e información secreta calculada u original. Por ejemplo, el primer dispositivo puede realizar varias firmas digitales, una para cada uno de sus certificados en su lista de certificados, usando su propio número aleatorio, el número aleatorio del segundo dispositivo, y la información secreta generada en la etapa (4515). Estas firmas digitales pueden entonces usarse como entrada a una función de generación de clave que calcula la clave de cifrado compartida para el primer dispositivo. El segundo dispositivo puede realizar firmas digitales similares para calcular su propia clave de cifrado compartida, pero usar la información secreta descifrada en lugar de la información secreta original. El proceso (4500) pasa entonces a la etapa (4550).

En algunas realizaciones, en la etapa (4550), el primer dispositivo y el segundo dispositivo determinan si están de acuerdo en las claves de cifrado compartidas calculadas independientemente en la etapa (4545). En algunas realizaciones, este acuerdo puede ser determinado por el primer y el segundo dispositivo intercambiado mensajes codificados con la clave de cifrado compartida. Por ejemplo, el primer dispositivo puede enviar al segundo dispositivo un mensaje cifrado con la clave de cifrado compartida. Si el segundo dispositivo es capaz de descifrar el mensaje cifrado y responder, por ejemplo, con un acuse de recibo apropiado, el primer dispositivo puede determinar que puede intercambiar mensajes con seguridad con el segundo dispositivo. Si no, el primer dispositivo puede determinar que no puede intercambiar mensajes con seguridad con el segundo dispositivo, y no se intercambian más mensajes. Se entenderá que puede producirse una determinación similar en el segundo dispositivo. En algunas realizaciones, el primer y el segundo dispositivos pueden determinar que sus claves de cifrado compartidas

calculadas independientemente coinciden intercambiando las claves de cifrado sin ningún mensaje. Si el primer y el segundo dispositivos no están de acuerdo en la clave de cifrado compartida, el proceso (4500) pasa a la etapa (4555). Si el primer y el segundo dispositivos están de acuerdo en la clave de cifrado compartida, el proceso (4500) pasa a la etapa (4560). En la etapa (4555), el primer y el segundo dispositivos no intercambian mensajes. En la etapa (4560), el primer y el segundo dispositivos intercambian mensajes. Después de cada una de las etapas (4555) y (4560), el flujo de proceso (4500) puede finalizar.

La figura 46 muestra un flujo de proceso simplificado e ilustrativo (4600) para establecer un servicio de apoderado seguro entre el cliente (4610) y el servidor (4620), que puede usarse en cualquier combinación adecuada, con cualquier añadido, eliminación o modificación adecuados de acuerdo con una realización de la presente invención. En el flujo de proceso (4600), la confianza se distribuye en un conjunto de autoridades de certificación durante la negociación inicial de una conexión entre el cliente (4610) y el servidor (5620). En algunas realizaciones, el flujo de proceso (4600) puede ejecutarse como parte de la fase de establecimiento de clave de un intercambio seguro entre el cliente (4610) y el servidor (4620). Esta fase de establecimiento de clave, que incluye cualquiera de las etapas del flujo de proceso (4600), puede formar parte de uno o más de los procesos asociados con el analizador sintáctico de datos seguros de acuerdo con, por ejemplo, cómo las etapas del flujo de proceso (4400) están asociadas con el analizador sintáctico de datos seguros. Además, el flujo de proceso (4600) puede ser un ejemplo del flujo de proceso (4500) como se analiza con respecto a la figura 45.

El flujo de proceso (4600) comienza en la etapa (4612). En la etapa (4612), el cliente (4610) envía al servidor (4620) un número aleatorio generado R_C y una lista de certificados Cert-CA1$_C$, Cert-CA2$_C$ y Cert-CA3$_C$. El cliente (4610) y el servidor (4620) pueden ser cualquier dispositivo cliente y servidor adecuados como se describe con respecto al sistema de usuario (105) y el sistema de vendedor (120) de la figura 1, respectivamente. R_C puede ser generado por el cliente (4610), de acuerdo con, por ejemplo, cómo fue generado el número aleatorio por el primer dispositivo en la etapa (4510) del flujo de proceso (4500) en la figura 45. Cada uno de estos certificados puede estar asociado con una clave pública expedida por una autoridad de seguridad diferente, de manera similar a las listas de certificados analizadas con respecto a la etapa (4510) del flujo de proceso (4500) en la figura 45. El flujo de proceso (4600) pasa entonces a la etapa (4622).

En la etapa (4622), el servidor (4620) envía al cliente (4610) su propio número aleatorio generado R_S y una lista de sus certificados Cert-CA1$_S$, Cert-CA2$_S$ y Cert-CA3$_S$. R_S puede ser generado por el servidor (4620) de acuerdo con el número aleatorio generado por el segundo dispositivo en la etapa (4510) del flujo de proceso (4500) en la figura 45. Cada uno de estos certificados puede estar asociado con una clave pública expedida por una autoridad de seguridad única, de manera similar a las claves públicas de las autoridades de certificación únicas analizadas con respecto a la etapa (4510) del flujo de proceso (4500) en la figura 45. El flujo de proceso (4600) pasa entonces a la etapa (4614).

En la etapa (4614), el cliente (4610) genera información secreta. Esta información secreta puede generarse de acuerdo con, por ejemplo, la etapa (4515) del flujo de proceso (4500) en la figura 45. También en la etapa (4614), el cliente (4610) dispersa la información secreta S_C en cuotas S1$_C$, S2$_C$ y S3$_C$. Esta dispersión puede realizarse de acuerdo con, por ejemplo, la dispersión de información secreta analizada con respecto a la etapa (4520) del flujo de proceso (4500) en la figura 45. También en la etapa (4614), el cliente (4610) cifra las cuotas de información secreta usando una clave diferente de las claves públicas del servidor. Por ejemplo, si “Enc” representa la función de cifrado ejecutada por el analizador sintáctico de datos seguros, y Pub1$_S$, Pub2$_S$ y Pub3$_S$ representan las claves públicas que corresponden a los certificados Cert-CA1$_S$, Cert-CA2$_S$ y Cert-CA3$_S$ del servidor, respectivamente, el cliente puede codificar S1$_C$ usando Pub1$_S$ ejecutando Enc(Pub1$_S$, S1$_C$), puede codificar S2$_C$ usando Pub2$_S$ ejecutando Enc(Pub2$_S$, S2$_C$), y puede codificar S3$_C$ usando Pub3$_S$ ejecutando Enc(Pub3$_S$, S3$_C$). La función de cifrado puede escogerse de cualquier combinación de los procedimientos de cifrado descritos con respecto a las etapas (4525) y (4527) del flujo de proceso (4500) en la figura 45. Una vez que la información secreta es generada, dispersada y cifrada, las cuotas cifradas son transmitidas al servidor (4620). El flujo de proceso (4600) pasa entonces a las etapas (4616) y (4624).

En la etapa (4624), las cuotas de información secreta S1$_C$, S2$_C$ y S3$_C$ pueden ser descifradas y restauradas a la información secreta original por el servidor (4620 usando cualquier técnica de descifrado y restauración adecuada descrita con respecto a las etapas (4525) y (4540) del flujo de proceso (4500) en la figura 45. El servidor (4620) puede entonces usar la información secreta restaurada para generar una clave de cifrado compartida K usando una función de generación de clave G. La función de generación de clave G puede tomar los números aleatorios R_C y R_S como entrada junto con la información secreta restaurada. En la etapa 4616, el cliente (4610) puede generar de manera similar su propia clave de cifrado compartida K usando una función de generación de clave G. Sin embargo,

la función de generación de clave ejecutada por el cliente (4610) puede usar la información secreta original generada por el cliente (4610) en lugar de la información secreta restaurada generada por el servidor (4620). El proceso (4600) pasa entonces a la etapa (4630).

En la etapa (4630), se intercambian mensajes entre el cliente (4610) y el servidor (4620) usando sus claves de cifrado compartidas respectivas K. En algunas realizaciones, el cliente (4610) y el servidor (4620) pueden determinar si sus claves de cifrado compartidas coinciden de manera similar al proceso descrito con respecto a la etapa (4550) del flujo de proceso (4500) en la figura 45. Si se determina que las claves de cifrado compartidas respectivas del cliente (4610) y el servidor (4620) no coinciden, no pueden intercambiarse mensajes o pueden dejar de intercambiarse entre el cliente (4610) y el servidor (4620). Si no, el intercambio de mensajes puede continuar de manera similar a la comunicación TLS o SSL normal después de la fase de establecimiento de clave.

En algunas realizaciones, un servicio de apoderado seguro puede residir en una aplicación cliente que se ejecuta en el cliente (4610). La aplicación cliente puede mantener una lista de servidores habilitados como servidor apoderado seguro, tales como el servidor (4620), basándose en la dirección IP o el URL y el número de puerto de los servidores. En algunas realizaciones, la aplicación cliente puede estar asociada con una dirección que es direccionable por los servidores. Cuando por parte del cliente se solicita una conexión para un servidor habilitado como servicio de apoderado seguro, la aplicación cliente puede establecer una conexión con el servicio de apoderado del servidor especificado utilizando las estrategias descritas en los flujos de proceso (4400), (4500) y (4600). Además, el servicio de apoderado seguro puede residir en una aplicación servidor que se ejecuta en el servicio (4620). La aplicación servidor puede aceptar conexiones desde la aplicación cliente, y reenviar los datos que recibe al puerto configurado como apoderado seguro apropiado basándose en reglas de reenvío de puertos. Estas reglas de reenvío de puertos pueden ser predeterminadas o acordadas mutuamente por la aplicación cliente y la aplicación servidor.

La fase de establecimiento de clave descrita por los flujos de proceso (4400), (4500) y (4600) ofrecen la garantía de que si algunas, pero menos que un *quorum*, de las autoridades de certificación se han visto comprometidas, aun así puede establecerse con seguridad la conexión entre dos dispositivos. Es decir, aunque las autoridades de certificación comprometidas tengan acceso a la información intercambiada entre los dispositivos, no tendrían suficiente información para alterar la confidencialidad o integridad de la comunicación. Por ejemplo, si hubiera tres cuotas de información secreta cifradas cada una con una clave pública de una autoridad de certificación diferente como se muestra en el flujo de proceso (4600), una de las autoridades de certificación podría verse comprometida y podría establecerse con seguridad la conexión entre dos dispositivos. Esta seguridad se garantiza porque aunque la autoridad de certificación comprometida tuviera acceso a los mensajes que se pasan entre dos dispositivos, el atacante asociado con la autoridad de certificación comprometida no tendría conocimiento del par de claves pública y privada de las otras dos autoridades de certificación, y de este modo como máximo podría recuperar una de las cuotas de información secreta. Además, como las cuotas de información secreta fueron dispersadas de modo que pudieran ser restauradas con al menos un subconjunto de las cuotas recombinando al menos un *quorum* de las cuotas, el atacante tras la autoridad de certificación comprometida no podría construir la información secreta original usando solo una cuota recuperada. Por consiguiente, el atacante tras la autoridad de certificación comprometida no podría recuperar la información secreta, y no podría calcular la clave de cifrado compartida usada para cifrar mensajes entre el primer dispositivo y el segundo dispositivo.

En diversas realizaciones se describe que los flujos de proceso (4400), (4500) y (4600) se producen entre dos dispositivos que desean establecer un medio de comunicación seguro entre ellos. Sin embargo, en algunas realizaciones el flujo de proceso (4400) puede producirse entre más de dos dispositivos. Por ejemplo, el flujo de proceso (4400) puede usarse para establecer un medio de comunicación seguro entre un ordenador personal, y un conjunto de servidores web. Cada servidor web del conjunto puede usar un conjunto diferente de autoridades de certificación únicas en la fase de establecimiento de clave de comunicación con el primer dispositivo.

La figura 47 y las figuras 48A y 48B muestran flujos de proceso simplificados e ilustrativos (4700), (4800) y (4850) para establecer un servicio de apoderado seguro entre dispositivos, que puede usarse en cualquier combinación adecuada, con cualquier añadido, eliminación o modificación adecuados de acuerdo con una realización de la presente invención. En los flujos de proceso (4700), (4800) y (4850), la confianza se distribuye entre un conjunto de autoridades de certificación en la estructura del canal de comunicación usado para intercambiar mensajes entre los dispositivos. En algunas realizaciones, el flujo de proceso (4700) puede ejecutarse después de la fase de establecimiento de clave de un intercambio seguro de información entre dispositivos, pero antes de que los dispositivos intercambien mensajes. Los flujos de proceso (4700), (4800) y (4850) pueden formar parte de uno o más de los procesos asociados con el analizador sintáctico de datos seguros (3706) como se ilustra en la figura 37,

o puede ser un proceso independiente. Por ejemplo, las etapas (4710), (4720), (4730), (4740), (4750) y (4760) pueden formar parte del proceso de postcifrado (3720) asociado con el analizador sintáctico de datos seguros (3706) como se ilustra en la figura 37, o puede ser un proceso independiente.

El flujo de proceso (4700) comienza en la etapa (4710). En la etapa (4710), se establece un canal de comunicación entre dispositivos. Este canal de comunicaciones puede establecerse usando cualquier motor de confianza adecuado (110) descrito con respecto a la figura 1 a la figura 14. En algunas realizaciones, este canal de comunicación puede ser asegurado usando cualquier tecnología de cifrado adecuada para asegurar datos en movimiento en cualquier comunicación adecuada. Por ejemplo, el canal de comunicación puede establecerse usando SSL, ½ SSL, SLL completa, TLS, TLS completa, RS1, OTP, RC4™, DES triple, AES, IPSec, cifrado de clave pública, cifrado de clave simétrica, cifrado de clave de división, cifrado multifactor, o cualquier combinación adecuada de tecnologías de cifrado convencionales. En algunas realizaciones, este canal de comunicación puede no ser seguro. Por ejemplo, el canal de comunicación establecido puede transportar datos mediante texto claro. En algunas realizaciones, estas tecnologías de cifrado pueden usar claves expedidas desde una autoridad de certificación. Esta autoridad de certificación puede denominarse “autoridad de certificación de nivel exterior” porque puede asegurar el primer canal de comunicación independientemente de cualquier autoridad de certificación usada para asegurar los túneles de comunicación segura descritos con respecto a la etapa (4730) más adelante.

Además, el canal de comunicación puede transportar datos asociados con correo electrónico, difusiones de datos de transmisión continua y comunicaciones WiFi. En algunas realizaciones, el canal de comunicación establecido puede utilizar cualquier número de tecnologías del lado del servidor o del lado del cliente, tales como guiones de CGI, ASP, o cualquier tecnología de servidor web adecuada. En algunas realizaciones, el canal de comunicación puede establecerse a través de varios medios de transporte físico o trayectos físicos. Por ejemplo, el canal de comunicación puede establecerse por una o más de internet, una intranet, una LAN; WiFi, Bluetooth, WiMax, o cualquier medio de comunicación por cable o inalámbrica, o cualquier combinación de los mismos. Cada medio de transporte físico puede tener una topología de red diferente entre los dispositivos que intercambian mensajes en el medio físico particular. El proceso (4700) pasa entonces a la etapa (4720).

En la etapa (4720), se establece cualquier número de túneles de comunicación segura dentro del primer canal de comunicación basándose en la confianza distribuida entre un conjunto de autoridades de certificación. Estas autoridades de certificación pueden denominarse “autoridades de certificación de nivel interior” porque pueden proteger las comunicaciones dentro de los túneles de comunicación segura independientemente de cualquier autoridad de certificación de nivel exterior. En algunas realizaciones, estos túneles de comunicación pueden establecerse usando cualquier fase de establecimiento de clave adecuada de cualquiera de las tecnologías de cifrado descritas con respecto a la etapa (4710). En algunas realizaciones, los túneles de comunicación segura se establecen usando una tecnología de cifrado que es diferente de la utilizada por el primer canal de comunicación. Por ejemplo, el canal de comunicación puede establecerse usando AES, mientras que los túneles de comunicación segura se establecen usando TLS completa. En este ejemplo, cada uno de los túneles de comunicación segura puede establecerse usando un proceso de establecimiento de clave similar al descrito con respecto al flujo de proceso (4300) de la figura 43. En algunas realizaciones, los túneles de comunicación segura se establecen usando la misma tecnología de cifrado que el primer canal de comunicación. Por ejemplo, el canal de comunicación y cada uno de los túneles de comunicación segura pueden establecerse usando TLS completa.

En algunas realizaciones, los túneles de comunicaciones seguras pueden establecerse usando la misma tecnología de cifrado, por ejemplo, cada canal de comunicación puede establecerse usando TLS completa. En otras realizaciones, los túneles de comunicación segura pueden establecerse usando diferentes tecnologías de cifrado, por ejemplo algunos de los túneles de cifrado pueden establecerse usando TLS completa, mientras que otros túneles se establecen usando AES. En algunas realizaciones, los túneles de comunicación segura pueden establecerse a través de varios medios físicos o trayectos físicos. Por ejemplo, los túneles de comunicación segura pueden establecerse por una o más de internet, una intranet, una LAN,WiFi, Bluetooth, WiMax, o cualquier medio de comunicación por cable o inalámbrico, o cualquier combinación de los mismos. Cada medio de transporte físico puede tener una topología de red diferente entre los dispositivos que intercambian mensajes en el medio físico particular.

Independientemente de qué tecnología de cifrado se usa para establecer los túneles de comunicación segura, los túneles se establecen en la etapa (4720) basándose en la confianza distribuida entre autoridades de certificación. En algunas realizaciones, esta confianza distribuida puede lograrse estableciendo cada túnel de comunicación segura basándose en una autoridad de certificación única. En algunas realizaciones, cada túnel de comunicación segura puede establecerse usando un certificado expedido por una de las autoridades de certificación únicas. En tales

realizaciones, el material de clave de cifrado simétrica puede comunicarse durante el establecimiento de cada canal usando el certificado expedido por la autoridad de certificación única asociada con ese canal. En tales realizaciones, el material de cifrado de clave simétrica puede ser, por ejemplo, el material de clave de cifrado simétrica analizado con respecto al uso de autoridades de certificación en TLS completa anteriormente. Cada autoridad de certificación puede ser única porque los certificados expedidos por cada una tienen pares de claves pública y privada diferentes. En algunas realizaciones, las autoridades de certificación únicas pueden ser autoridades de certificación raíces. En otras realizaciones, las autoridades de certificación únicas pueden ser autoridades de certificación menores dentro del árbol de una sola autoridad de certificación raíz, como se analiza con respecto a la jerarquía de autoridades de certificación (4200) en la figura 42. Los pares de claves pública y privada únicos de las diferentes autoridades de certificación pueden usarse durante el establecimiento de clave de cada túnel de comunicación segura. Por ejemplo, si los túneles de comunicación segura están basados en TLS, cada uno de los túneles puede establecerse como se describe con respecto al flujo de proceso (4300) de la figura 43 usando el certificado de una de las autoridades de certificación únicas. El proceso (4700) pasa entonces a la etapa (4730).

En la etapa (4730), se preparan paquetes de datos para transmisión por los túneles de comunicación segura basándose en el conjunto de autoridades de certificación y compartición de secreto multifactor. En algunas realizaciones, esta preparación puede incluir cifrar los paquetes de datos usando una clave desarrollada durante el establecimiento de un túnel diferente de los túneles de comunicación. En algunas realizaciones, esta clave puede ser una clave simétrica generada usando material de clave de cifrado simétrica que fue comunicado durante el establecimiento de cada canal usando un certificado de una autoridad de certificación única asociada con ese canal. Además, esta preparación puede incluir dispersar cada paquete de datos en cuotas basándose en compartición de secreto multifactor, y luego cifrando las cuotas resultantes usando los certificados de las autoridades de certificación únicas usadas para establecer los túneles de comunicación segura en la etapa (4720). Este proceso de dispersión puede lograrse usando cualquier división o criptodivisión de datos adecuada como se analiza con respecto al módulo de división de datos (520) o (610) de la figura 5 y la figura 6, y se explica en mayor detalle con respecto a la figura 8 y las figuras 20 a 24.

Además, en algunas realizaciones, los paquetes de datos pueden ser dispersados en cuotas sustancialmente mediante cualquier número de usos del analizador sintáctico de datos seguros explicado resumidamente con respecto a la figura 33, la figura 35 y la figura 36. Por ejemplo, el analizador sintáctico de datos seguros puede recibir paquetes de datos sin cifrar. Si los paquetes de datos van a ser divididos con un algoritmo que requiere una clave, se genera una clave de cifrado de división. En algunas realizaciones, los paquetes de datos pueden ser divididos en cuotas en una etapa de acuerdo con cualquiera de las técnicas descritas con respecto a la figura 33, la figura 35 y la figura 36. En algunas realizaciones, puede usarse un esquema tolerante a fallos para cifrar la clave de cifrado de división y permitir la regeneración de los paquetes de datos a partir de menos del número total de cuotas. Por ejemplo, los paquetes de datos pueden ser dispersados en cuotas usando cualquier técnica de dispersión de datos adecuada de modo que las cuotas sean recuperables a partir de al menos un subconjunto de las cuotas recombinando al menos un *quorum* de las cuotas. Además, puede añadirse información a las cuotas de paquetes de datos que se usan para reconstruir los paquetes de datos. Además, una vez que se crean las cuotas, puede insertarse información de autenticación/integridad dentro de las cuotas de paquetes de datos. Cada cuota puede ser postcifrada usando claves públicas de autoridades de certificación únicas usadas para establecer los túneles de comunicación segura en la etapa (4720).

Además, el algunas realizaciones, la dispersión de los paquetes de datos puede producirse en dos fases – una fase de generación de encabezamiento y una fase de partición de datos. Las fases pueden ser, por ejemplo, el proceso de generación de encabezamiento simplificado (4000) como se muestra en la figura 40A y el proceso de partición de datos simplificado (4010) como se muestra en la figura 40B. Uno de estos procesos o ambos pueden realizarse sobre los paquetes de datos. En algunas realizaciones, los paquetes de datos pueden ser precifrados basándose en la tecnología de cifrado usada para establecer el primer canal de comunicación. Los paquetes de datos precifrados pueden entonces ser ejecutados a través de los procesos (4000) y/o (4010) como se describe más adelante.

Como se muestra en la etapa (4002) de la figura 40A, pueden generarse claves de división. Los paquetes de datos sin cifrar o precifrados pueden entonces ser cifrados opcionalmente (por ejemplo, usando la clave de grupo de trabajo descrita con respecto a la figura 39) en la etapa (4004). En la etapa (4006), puede usarse una “criptodivisión M de N” para dividir los paquetes de datos en cuotas de información secreta usando la clave de división. Cada cuota del paquete de datos puede entonces insertarse dentro de un encabezamiento de cuota. Por último, un bloque de integridad de cuota y una etiqueta de postautenticación (por ejemplo, MAC) pueden adjuntarse al bloque de encabezamiento de cada cuota. Cada bloque de encabezamiento puede estar diseñado para ajustar dentro de un solo paquete de datos cifrado. Cada bloque de encabezamiento puede ser postcifrado usando una clave

desarrollada durante el establecimiento de un túnel diferente de los túneles de comunicación en la etapa (4720).

En algunas realizaciones, después de generarse los encabezamientos que incluyen las cuotas de información secreta, el analizador sintáctico de datos seguros puede entrar en una fase de partición de datos. Esta fase de partición de datos puede ser, por ejemplo, el proceso de división de datos simplificado (4010) como se muestra en la figura 40B. Por ejemplo, cada paquete de datos sin cifrar o precifrado entrante puede ser cifrado usando una o más claves, tal como una clave compartida o una clave de grupo de trabajo, en la etapa (4012). En algunas realizaciones, los datos que son cifrados pueden incluir los encabezamientos que contienen las cuotas de paquetes de datos calculados durante el proceso de generación de encabezamiento simplificado (4000). En la etapa (4014), puede calcularse la información de integridad de cuotas (por ejemplo, un troceo H) sobre el texto cifrado resultante de la etapa (4012). Por ejemplo, puede calcularse un troceo SHA-256 sobe los datos que son cifrados con una o más claves en la etapa (4012). En la etapa (4016), el paquete de datos puede entonces ser partido en dos o más cuotas de datos usando uno de los algoritmos de división de datos descritos anteriormente de acuerdo con la presente invención. En algunas realizaciones, el paquete de datos o el bloque de datos puede ser dividido de modo que cada cuota de datos contenga una distribución sustancialmente aleatoria del paquete de datos o el bloque de datos cifrado. La información de integridad (por ejemplo, troceo H) puede entonces adjuntarse a cada cuota de datos. También puede calcularse una etiqueta de postautenticación opcional (por ejemplo, MAC) y adjuntarse a cada cuota de datos en algunas realizaciones. Además, cada cuota de datos puede incluir metadatos como se describe con respecto a la figura 40B. Los metadatos pueden incluir información respecto a los paquetes de datos y las claves de grupo de trabajo usados para generar las cuotas de paquetes de datos. Cada cuota de paquete de datos puede ser postprocesada usando claves públicas de autoridades de certificación únicas usadas para establecer los túneles de comunicación segura en la etapa (4720).

En algunas realizaciones, las cuotas de paquetes de datos pueden ser asociadas con cuotas de una clave de cifrado o una clave de división de datos de manera similar a como la clave y los componentes de datos están almacenados dentro de cuotas como se muestra en los diagramas de bloques ilustrativos (3800) y (3900) en las figuras 38 y 39. Por ejemplo, las cuotas de los paquetes de datos pueden ser almacenadas de manera similar a como las porciones de la clave de cifrado (3804) es dividida y almacenada dentro de las cuotas (3810). Cuando se utiliza una clave de grupo de trabajo, las cuotas de datos pueden ser cifradas con la clave de grupo de trabajo antes de ser almacenadas dentro de las cuotas como se muestra en el diagrama de bloques ilustrativo (3900).

Independientemente de cómo los paquetes de datos son dispersados en cuotas, cada cuota puede ser postcifrada usando una clave desarrollada durante el establecimiento de un túnel diferente de los túneles de comunicación en la etapa (4720). Por ejemplo, en algunas realizaciones puede haber tres túneles de comunicación segura establecidos en la etapa (4720), cada uno con una autoridad de certificación única. Cada cuota producida en la etapa (4730) puede entonces ser cifrada usando la clave desarrollada durante el establecimiento de un túnel diferente de los túneles de comunicación. En algunas realizaciones, estas claves pueden ser claves simétricas generadas usando material de clave de cifrado simétrica que fue comunicado durante el establecimiento de cada canal usando las tres autoridades de certificación únicas. El proceso (4700) pasa entonces a la etapa (4740).

En la etapa (4740), los paquetes de datos preparados son transmitidos a su destino. Esta transmisión puede producirse por cualquier canal de comunicación adecuado, tal como se describe con respecto al enlace de comunicación (105) en la figura 1. En algunas realizaciones, el destino para los paquetes puede ser uno o más de los servidores habilitados como apoderado de datos seguro. Una aplicación cliente que se ejecuta en un dispositivo cliente puede mantener una lista de servidores habilitados como servidor apoderado seguro basándose en la dirección IP o el URL y el número de puerto de los servidores. En algunas realizaciones, la aplicación cliente puede estar asociada con una dirección que es direccionable por los servidores. Cuando por parte del cliente se solicita una conexión para un servidor habilitado como servicio de apoderado seguro, la aplicación cliente establece una conexión con el servicio de apoderado del servidor especificado, utilizando las estrategias descritas en las etapas (4710) y (4720). Una vez que los datos preparados son transmitidos a su destino, el proceso (4700) pasa entonces a la etapa (4750).

En la etapa (4750), los paquetes de datos transmitidos son recibidos. En algunas realizaciones, los paquetes de datos transmitidos pueden ser recibidos por un servicio de apoderado seguro que reside en una aplicación servidor que se ejecuta en un servidor habilitado como apoderado de datos seguro. La aplicación servidor puede aceptar conexiones desde la aplicación cliente, y reenvía los datos que recibe al puerto configurado como apoderado seguro correcto basándose en reglas de reenvío de puertos. Estas reglas de reenvío de puertos pueden ser predeterminadas o acordadas mutuamente por la aplicación cliente y la aplicación servidor. El proceso (4700) pasa entonces a la etapa (4760).

En la etapa (4760), los paquetes de datos son restaurados basándose en el conjunto de autoridades de certificación y la compartición de secreto multifactor. En algunas realizaciones, esta restauración puede ser un proceso duplicado del proceso de preparación usado para analizar sintácticamente y cifrar los paquetes de datos en la etapa (4730). Por ejemplo, en la etapa (4730), los paquetes de datos pueden haber sido cifrados usando claves asociadas con el establecimiento de los túneles de comunicación segura en la etapa (4720). Además, las cuotas de paquetes de datos sin cifrar o precifrados pueden haber sido producidas usando técnicas de dispersión del analizador sintáctico de datos seguros de acuerdo con cualquiera de las técnicas descritas con respecto a la figura 33, la figura 35 y la figura 36. En algunas realizaciones, las cuotas de paquetes de datos pueden ser cifradas basándose en la tecnología de cifrado usada para establecer el primer canal de comunicación.

Por consiguiente, las cuotas de paquetes de datos en primer lugar pueden ser descifradas basándose en las claves asociadas con el establecimiento de los túneles de comunicación segura en la etapa (4720). Las cuotas descifradas pueden entonces ser restauradas usando funciones de restauración del analizador sintáctico de datos seguros de acuerdo con cualquiera de las técnicas descritas con respecto a la figura 34. En algunas realizaciones, las cuotas restauradas pueden ser descifradas basándose en la tecnología de cifrado usada para establecer el primer canal de comunicación. En algunas realizaciones, las cuotas descifradas de los datos pueden insertarse en encabezamientos de cuota. En tales realizaciones, las cuotas de datos pueden ser extraídas de los encabezamientos de cuota descifrados, y restauradas usando las funciones de restauración del analizador sintáctico de datos seguros. El flujo de proceso (4700) entonces finaliza. En algunas realizaciones, las etapas (4730), (4740), (4750) y (4760) pueden repetirse según sea necesario para la transmisión de datos por los túneles de comunicación segura.

Describiendo las realizaciones del servicio de apoderado seguro con respecto a la figura 48A, el flujo de proceso (4800) puede ejecutarse en un primer dispositivo, tal como en una aplicación del lado del cliente que se ejecuta en un ordenador personal que solicita comunicarse usando el servicio de apoderado seguro con un segundo dispositivo, tal como un servidor web. El flujo de proceso (4800) comienza en la etapa (4810). En la etapa (4810), puede establecerse un primer canal de comunicación segura. Este canal de comunicación segura puede establecerse usando un proceso de establecimiento de clave con las claves de cualquier tecnología de cifrado adecuada como se describe con respecto a la etapa (4710) en el flujo de proceso (4700) de la figura 47. En algunas realizaciones, estas claves pueden ser expedidas desde una autoridad de certificación denominada “autoridad de certificación de nivel exterior”. Además, el canal de comunicación puede transportar datos asociados con cualquier aplicación adecuada como se analiza con respecto a la etapa (4710) en el flujo de proceso (4700) de la figura 47. Además, el canal de comunicación puede establecerse a través de varios medios de transporte físico como se describe con respecto a la etapa (4710) del flujo de proceso (4700) de la figura 47. El proceso (4800) pasa entonces a la etapa (4815).

En la etapa (4815), se establece cualquier número de túneles de comunicación segura dentro del primer canal de comunicación (por ejemplo, uno, dos, tres, cinco, diez, cincuenta, cien, o más de cien túneles de comunicación segura). Cada canal de comunicación segura puede establecerse usando un certificado obtenido de una autoridad de certificación única y cada túnel puede estar asociado con la autoridad de certificación única respectiva. En algunas realizaciones, el material de clave de cifrado simétrica puede comunicarse durante el establecimiento de cada canal usando el certificado expedido por la autoridad de certificación única asociada con ese canal. En tales realizaciones, el material de cifrado de clave simétrica puede ser, por ejemplo, el material de clave de cifrado simétrica analizado con respecto al uso de autoridades de certificación en TLS completa anteriormente. De manera similar al flujo de proceso (4700) de la figura 47, las autoridades de certificación únicas usadas para establecer los túneles de comunicación segura pueden denominarse “autoridades de certificación de nivel interior”. Cada uno de estos túneles de comunicación segura puede establecerse usando un proceso de establecimiento de clave con cualquier tecnología de cifrado adecuada por uno o más medios de transporte físico como se describe con respecto a la etapa (4720) del flujo de proceso (4700) de la figura 47. También de manera similar a la etapa (4720) del flujo de proceso (4700) de la figura 47, cada autoridad de certificación puede ser única porque los certificados expedidos por cada una tienen pares de claves pública y privada diferentes. En algunas realizaciones, cada túnel de comunicación segura puede estar asociado con una autoridad de certificación única respectiva porque todos los datos enviados por ese túnel son cifrados basándose en claves desarrolladas durante el establecimiento de los túneles de comunicación. En algunas realizaciones, esta asociación puede ser seguida en cualquier estructura de datos adecuada por el analizador sintáctico de datos seguros en una aplicación cliente, una aplicación servidor, o ambas. El proceso (4800) pasa entonces a la etapa (4820).

En la etapa (4820), los paquetes de datos entrantes pueden ser divididos criptográficamente en cualquier número de cuotas usando compartición de secreto multifactor. En algunas realizaciones, los paquetes de datos entrantes

pueden ser divididos en el mismo número de cuotas que el número de túneles de comunicación segura establecidos en la etapa (4815). La división criptográfica de los paquetes de datos entrantes puede lograrse de acuerdo con, por ejemplo, cualquier técnica de dispersión adecuada analizada con respecto a la etapa (4730) del flujo de proceso (4700) de la fig. 47. El proceso (4800) pasa entonces a la etapa (4825).

En la etapa (4825), cada una de las cuotas es cifrada usando una clave desarrollada durante el establecimiento de un túnel diferente de los túneles de comunicaciones seguras. En algunas realizaciones, la clave puede ser una clave de cifrado simétrica generada usando material de clave de cifrado simétrica que fue comunicado durante el establecimiento de cada canal usando un certificado de una autoridad de certificación única asociada con ese canal. En algunas realizaciones, este material de clave de cifrado simétrica puede ser, por ejemplo, el material de clave de cifrado simétrica analizado con respecto al uso de autoridades de certificación en TLS completa anteriormente. Puede entenderse, sin embargo, que las claves desarrolladas durante el establecimiento de los túneles de comunicación segura pueden ser cualquier clave de cifrado, información secreta, o cualquier otra información adecuada distinta de las claves de cifrado simétricas. Por ejemplo, las claves desarrolladas durante el establecimiento de los túneles de comunicación segura pueden ser claves de cifrado asimétricas. En algunas realizaciones, cada una de las cuotas que son producidas en la etapa (4820) es procesada y etiquetada con un o más bits que identifican cuál de las claves asociadas con el establecimiento de los túneles de comunicación debería usarse para cifrar cada una de las cuotas. El proceso (4800) pasa entonces a la etapa (4830).

En la etapa (4830), cada una de las cuotas cifradas es transmitida por el túnel asociado con la autoridad de certificación única bajo la cual se estableció ese túnel. Por ejemplo, si hubiera tres túneles de comunicación segura establecidos basados cada uno en una autoridad diferente de tres autoridades de certificación únicas, cada paquete de datos sin cifrar o precifrado entrante sería dividido criptográficamente en tres cuotas usando compartición de secreto multifactor y cifrado usando una clave diferente de tres claves desarrolladas durante el establecimiento de los tres túneles de comunicación segura usando una autoridad diferente de tres autoridades de certificación únicas. Por consiguiente, cada una de las tres cuotas cifradas sería transmitida por el túnel asociado con la autoridad de certificación única bajo la cual se estableció ese túnel. En algunas realizaciones, esta transmisión puede estar basada en la estructura de datos que mantiene las asociaciones entre las autoridades de certificación y los túneles.

En algunas realizaciones, la asociación entre una autoridad de certificación y los túneles de comunicación segura puede permanecer constate a lo largo de toda la duración de una transmisión de datos. En otras realizaciones, las asociaciones entre las autoridades de certificación y los túneles de comunicación segura pueden ser dinámicas. En tales realizaciones, las asociaciones pueden ser transpuestas en cualquier momento adecuado, tal como después de la transmisión de un paquete de datos entero. Por ejemplo, un primer paquete de datos puede ser procesado por el flujo de proceso (4800) donde el paquete de datos es criptodividido en tres cuotas en la etapa (4820). La primera cuota del primer paquete de datos puede ser cifrada usando una primera clave desarrollada durante el establecimiento de un primer túnel de comunicación segura usando una primera autoridad de certificación y transmitida por el primer túnel de comunicación. La segunda cuota del primer paquete de datos puede ser cifrada usando una segunda clave desarrollada durante el establecimiento de un segundo túnel de comunicación segura usando una segunda autoridad de certificación y transmitida por el segundo túnel de comunicación. Por último, la tercera cuota del primer paquete de datos puede ser cifrada usando una tercera clave desarrollada durante el establecimiento de un tercer túnel de comunicación segura usando una tercera autoridad de certificación y transmitida por el tercer túnel de comunicación.

En algunas realizaciones, después de ser transferidas las tres cuotas del primer paquete de datos, las asociaciones entre las autoridades de certificación y los canales de comunicación pueden ser transpuestas de modo que la primera cuota puede ser cifrada usando la tercera clave y transmitida por el tercer túnel, la segunda cuota puede ser cifrada usando la primera clave y transmitida por el primer túnel, y la tercera autoridad de certificación puede ser cifrada usando la segunda clave y transmitida por el segundo túnel. En tales realizaciones, estas asociaciones pueden ser almacenadas en cualquier depósito adecuado que sea accesible a los dispositivos en comunicación, tal como el depósito (210) de la figura 2.

Describiendo realizaciones del servicio de apoderado seguro con respecto a la figura 48B, el flujo de proceso (4850) puede ejecutarse en una aplicación servidor de apoderado seguro del lado del cliente que se ejecuta en un segundo dispositivo, tal como un servidor web, que está intercambiando información con un primer dispositivo, tal como un ordenador personal que ejecuta una aplicación de servicio de apoderado seguro del lado del cliente. El flujo de proceso (4850) comienza en la etapa (4835). En la etapa (4835), las cuotas de datos cifradas son recibidas cada una en un túnel de comunicación respectivo. La aplicación servidor puede aceptar conexiones procedentes de la aplicación cliente, y reenviar los datos que recibe al puerto configurado como apoderado seguro correcto basándose

en reglas de reenvío de puertos. Estas cuotas de datos pueden ser las mimas cuotas que fueron divididas criptográficamente, cifradas y transmitidas en las etapas (4820), (4825) y (4830) del flujo de proceso (4800) de la figura 48A, respectivamente. El flujo de proceso (4850) pasa entonces a la etapa (4840).

En la etapa (4840), cada una de las cuotas es descifrada basándose en la clave asociada con el establecimiento del túnel de comunicación segura respectivo en el que fue recibida la cuota. En algunas realizaciones, este proceso puede ser un duplicado del descrito con respecto a la etapa (4825) del flujo de proceso (4800) de la figura 48. El flujo de proceso (4850) pasa entonces a la etapa (4845).

En la etapa (4845), las cuotas de paquetes de datos descifradas son restauradas a los paquetes de datos originales. En algunas realizaciones, esta restauración puede ser un proceso duplicado de las técnicas de dispersión usadas en la etapa (4820) del flujo de proceso (4800) en la figura 48. En algunas realizaciones, las cuotas restauradas pueden ser descifradas basándose en las tecnologías de dispersión y/o cifrado de datos usadas para establecer el primer canal de comunicación. Entonces finaliza el flujo de proceso (4800). En algunas realizaciones, las etapas de los flujos de proceso (4800) y (4850) pueden repetirse según sea necesario para la transmisión de datos por los túneles de comunicación segura.

Los protocolos de comunicación descritos con respecto a los flujos de proceso (4700), (4800) y (4850) ofrecen la garantía de que si ciertas autoridades de certificación de nivel exterior o interior se han visto comprometidas, los datos serán intercambiados con seguridad entre dispositivos. Es decir, aunque las autoridades de certificación comprometidas tengan acceso a la información intercambiada basándose en las claves asociadas con esa autoridad de certificación, el atacante asociado con la autoridad de certificación comprometida no tendría acceso a suficiente información para alterar la confidencialidad o integridad de la comunicación. Por ejemplo, si la autoridad de certificación de nivel exterior estuviera comprometida pero las autoridades de certificación de nivel interior mantuvieran su integridad, el atacante podría observar los trenes de datos dentro de cada uno de los túneles de comunicación segura. Sin embargo, el atacante no tendría conocimiento del cifrado usado dentro de cada uno de los túneles de comunicación segura, incluyendo el conocimiento del certificado de cada una de las autoridades de certificación únicas usado para asegurar los datos por cada túnel de comunicación segura.

En otro ejemplo, si una o más de las autoridades de certificación de nivel interior se viera comprometida pero la autoridad de certificación de nivel exterior se mantuviera intacta, el atacante puede recuperar porciones divididas criptográficamente de los paquetes de datos, pero no puede descifrar las porciones divididas criptográficamente porque no tendría conocimiento del cifrado usado por la autoridad de certificación de nivel exterior. Además, si los paquetes de datos enviados a través de los túneles de comunicación segura están divididos criptográficamente de modo que pueden ser restaurados a partir de al menos un subconjunto de las cuotas recombinando al menos un *quorum* de las cuotas, el usuario del analizador sintáctico de datos seguros pueden tener la protección adicional de que si algunos, pero menos de un *quorum*, de los certificados asociados con los túneles de comunicación segura se han visto comprometidos, el atacante no podría restaurar los paquetes de datos criptodivididos.

La figura 48C es un diagrama de bloques simplificado de un servicio de apoderado seguro (4870) que distribuye confianza entre un conjunto de autoridades de certificación en la estructura de canales de comunicación, que puede usarse en cualquier combinación adecuada, con cualquier añadido, eliminación, o modificación adecuados de acuerdo con una realización de la presente invención. El servicio de apoderado seguro (4870) puede residir en cualquier motor de confianza adecuado (110) o módulo dentro del motor de confianza (110) como se describe con respecto a las figuras 1-8. Se ilustra que el servicio de apoderado seguro incluye un primer canal de comunicación (4880) y subcanales (es decir, túneles de comunicación segura) (4872), (4874) y (4876) que se establecen usando TLS completa. Sin embargo, se entenderá que estos canales de comunicación pueden establecerse y usarse con cualquier tecnología de cifrado adecuada, o sin cifrado, como se analiza con respecto a las etapas (4710) y (4720) del flujo de proceso (4700) en la figura 47, o como se analiza con respecto a las etapas (4810) y (4815) del flujo de proceso (4800) de la figura 48A. Además, aunque se ilustra que el servicio de apoderado seguro (4870) usa tres subcanales, puede usarse cualquier número de subcanales para transferir con seguridad información por el servicio de apoderado seguro (4870).

El servicio de apoderado seguro (4870) puede incluir paquetes de datos recibidos (4877). En algunas realizaciones, los paquetes de datos (4877) pueden ser paquetes de datos sin cifrar que han de ser procesados por el servicio de apoderado seguro (4870). Los paquetes de datos (4877) pueden ser recibidos desde cualquier fuente adecuada, tal como el depósito (210) descrito con respecto al motor de confianza (210) de la figura 2. En otras realizaciones, los paquetes de datos (4877) pueden ser precifrados de acuerdo con la tecnología de cifrado usada para establecer el canal de comunicación (4880). Por ejemplo, como se muestra en el servicio de apoderado seguro (4870), el canal de

comunicación (4880) se establece usando TLS completa. Este canal de comunicación de TLS completa puede establecerse de acuerdo con el flujo de proceso (4300) de la figura 43.

El servicio de apoderado seguro (4870) también puede incluir el módulo de división criptográfica de paquetes (4878). En algunas realizaciones, el módulo de división criptográfica de paquetes (4878) puede incluir cualquier circuito y/o instrucción para ejecutar y/o calcular cualquiera de las técnicas de cifrado y dispersión de datos analizadas con respecto a la etapa (4730) del flujo de proceso (4700) de la figura 47, o analizadas con respecto a la etapa (4820) y (4825) del flujo de proceso (4800) de la figura 48A. En algunas realizaciones, el módulo de división criptográfica de paquetes (4878) puede residir en un dispositivo cliente o una aplicación del lado del cliente que solicite comunicarse con un servidor. En otras realizaciones, el módulo de división criptográfica de paquetes (4878) puede residir o ejecutarse en cualquier dispositivo que sea adecuado para ejecutar el analizador sintáctico de datos seguros (3706) del proceso de vista general ilustrativo (3700) de la figura 37.

El servicio de apoderado seguro (4870) también puede incluir el canal de comunicación (4880). El canal de comunicación (4880) puede establecerse por uno o más medios físicos usando cualquier tecnología de cifrado adecuada, o sin cifrado, como se describe con respecto al primer canal de comunicación en la etapa (4710) del flujo de proceso (4700) de la figura 47, o como se describe con respecto al primer canal de comunicaciones seguras en la etapa (4810) del flujo de proceso (4800) de la figura 48A. Los subcanales (4872), (4874) y (4876) pueden establecerse basándose en el canal de comunicación (4880). Estos subcanales pueden establecerse por uno o más medios físicos basándose en un certificado de una autoridad de certificación única de acuerdo con, por ejemplo, cómo se describen los túneles de comunicación segura con respecto a la etapa (4720) del flujo de proceso (4700) de la figura 47, o se describen con respecto a la etapa (4815) del flujo de proceso (4800) de la figura 48A. De esta manera, cada subcanal puede estar asociado con una autoridad de certificación única.

Por ejemplo, como se muestra en el servicio de apoderado seguro (4870), el subcanal de TLS (4872) está asociado con la autoridad de certificación CA1, el subcanal de TLS (4874) está asociado con la autoridad de certificación CA2, y el subcanal de TLS (4876) está asociado con la autoridad de certificación CA3. En algunas realizaciones, las asociaciones entre subcanales y sus autoridades de certificación respectivas pueden mantenerse constante. En otras realizaciones, las asociaciones entre subcanales y sus autoridades de certificación respectivas pueden cambiar como se describe con respecto a la etapa (4830) del flujo de proceso (4800) de la figura 48A. El canal de comunicación (4880) y los subcanales (4872), (4873) y (4876) pueden establecerse por cualquier enlace de comunicación adecuado, tal como el enlace de comunicación (125) descrito con respecto al sistema criptográfico (100) de la figura 1.

En algunas realizaciones, el módulo de división criptográfica de paquetes (4878) puede transmitir cuotas de paquetes de datos dispersadas (4877) por los subcanales (4872), (4874) y (4876). Esta transmisión puede producirse de acuerdo con, por ejemplo, la etapa (4740) del flujo de proceso (4700) de la figura 47, o de acuerdo con, por ejemplo, la etapa (4830) del flujo de proceso (4800) de la figura 48A. En algunas realizaciones, el módulo de división criptográfica de paquetes (4878) puede transmitir una de las cuotas divididas por cada uno de los subcanales (4872), (4874) y (4876). En otras realizaciones, el módulo de división criptográfica de paquetes (4878) puede transmitir más de una cuota dividida por uno o más de los subcanales (4872), (4874) y (4876). Tales realizaciones pueden ser útiles cuando uno de los subcanales (4872), (4874) y (4876) resulta inutilizables debido a un fallo en el medio físico que soporta uno de los subcanales.

En algunas realizaciones, los subcanales (4872), (4874) y (4876) pueden incluir módulos de cifrado de datos (4871), (4873) y (4875), respectivamente. Los módulos de cifrado de datos (4871), (4873) y (4875) pueden estar asociados cada uno con una autoridad de certificación única asociada con uno de los subcanales. En algunas realizaciones, los módulos de cifrado de datos aplicarán cifrado de datos a cada cuota de un paquete de datos que pasa por el subcanal. Por ejemplo, como se muestra con respecto al servicio de apoderado (4870), el módulo de cifrado (4871) está asociado con la autoridad de certificación CA1 que está asociada con el subcanal de TLS (4872), y cifra cada cuota de un paquete de datos que pasa por el subcanal (4872) usando TLS completa basándose en una clave desarrollada durante el establecimiento de canal (4872). El establecimiento de canal (4872) puede haber usado un certificado obtenido de la autoridad de certificación CA1. El módulo de cifrado (4873) está asociado con la autoridad de certificación CA2 que está asociada con el subcanal de TLS (4874), y cifra cada cuota de un paquete de datos que pasa por el subcanal (4874) usando TLS completa basándose en una clave desarrollada durante el establecimiento del canal (4874). Este establecimiento de canal (4874) puede haber usado un certificado obtenido de la autoridad de certificación CA2. Por último, el módulo de cifrado (4875) está asociado con la autoridad de certificación CA3 que está asociada con el subcanal de TLS (4876), y cifra cada cuota de un paquete de datos que pasa por el subcanal (4876) usando TLS completa basándose en una clave desarrollada durante el establecimiento

del canal (4876). Este establecimiento de canal (4876) puede haber usado un certificado obtenido de la autoridad de certificación CA3. En algunas realizaciones, los módulos de cifrado (4872) pueden residir o ejecutarse en cualquier dispositivo que sea adecuado para ejecutar el analizador sintáctico de datos seguros (3706) del proceso ilustrativo (3700) de la figura 37.

El servicio de apoderado seguro (4870) también puede incluir el módulo de restauración de paquetes (4879). El módulo de restauración de paquetes puede recibir cuotas de paquetes de datos procedentes de los subcanales (4872), (4874) y (4876) como se describe con respecto a la etapa (4750) del flujo de proceso (4700) de la figura 47, o como se describe con respecto a la etapa (4835) del flujo de proceso (4850) de la figura 48B. En algunas realizaciones, el módulo de restauración de paquetes (4879) puede incluir cualquier circuito y/o instrucción para ejecutar y/o calcular cualquiera de las técnicas de descifrado o las técnicas de restauración de paquetes para producir paquetes de datos restaurados (4882) como se describe con respecto a la etapa (4760) del flujo de proceso (4700) de la figura 47 o las etapas (4840) y (4845) como se describe con respecto al flujo de proceso (4850) de la figura 48B. En algunas realizaciones, el módulo de restauración de paquetes (4879) puede residir en un dispositivo servidor o una aplicación del lado de servicio que recibe solicitudes procedentes de un dispositivo cliente o una aplicación del lado del cliente. En otras realizaciones, el módulo de restauración de paquetes (4879) puede residir o ejecutarse en cualquier dispositivo que sea adecuado para ejecutar el analizador sintáctico de datos seguros (3700) del proceso de visión general ilustrativo (3700) de la figura 37.

La figura 49 es un diagrama de flujo de proceso de etapas y características ilustradas para un servicio de apoderado seguro (4900) entre el cliente (4910) y el servidor (4920) que distribuye confianza entre un conjunto de autoridades de certificación en la estructura de canales de comunicación, que puede usarse en cualquier combinación adecuada, con cualquier añadido, eliminación o modificación adecuados de acuerdo con una realización de la presente invención. Por ejemplo, la confianza puede ser distribuida en la primera autoridad de certificación CA1, la segunda autoridad de certificación CA2 y la tercera autoridad de certificación CA3 como parte de la fase de establecimiento de clave (4570), como se describirá más adelante. En algunas realizaciones, el servicio de apoderado seguro (4900) puede ejecutarse durante y después de la fase de establecimiento de clave de un intercambio seguro de información entre el cliente (4910) y el servidor (4920), pero antes de que el cliente (4910) y el servidor (4920) intercambien mensajes. El servicio de apoderado seguro (4900) puede formar parte de uno o más de los procesos asociados con el analizador sintáctico de datos seguros de manera similar a como las etapas de los flujos de proceso (4700), (4800) y (4850) están asociadas con el analizador sintáctico de datos seguros. Además, el servicio de apoderado seguro (4900) puede ser un ejemplo de los flujos de proceso (4700), (4800) y (4850) de las figuras 47, 48A y 48B, o puede ser un ejemplo del funcionamiento del servicio de apoderado seguro (4870).

El servicio de apoderado seguro (4900) comienza en la etapa (4930). En la etapa (4930), el cliente (4910) establece un primer canal de comunicación (no mostrado) y túneles de comunicación segura como se describe con respecto al primer canal de comunicación y los túneles de comunicación segura en las etapas (4710) y (4720) del flujo de proceso (4700) de la figura 47, y un primer canal de comunicación segura y túneles de comunicación segura en las etapas (4810) y (4820) del flujo de proceso (4800) de la figura 48A. El servicio de apoderado seguro (4900) pasa entonces a la etapa (4912).

En la etapa (4912), el cliente (4910) puede generar encabezamientos de analizador sintáctico de datos seguros H_1, H_2 y H_3, y transmitirlos al servidor (4920). Los encabezamientos H_1, H_2 y H_3 pueden contener información relacionada con las técnicas de dispersión de datos acordadas por el cliente (4910) y el servidor (4920). Por ejemplo, en algunas realizaciones, el cliente (4910) y el servidor (4920) pueden acordar el uso de una “criptodivisión M de N” de cada mensaje intercambiado. Los encabezamientos H_1, H_2 y H_3 pueden ser cifrados basándose en claves asociadas con el establecimiento de los túneles de comunicación segura en la etapa (4930). En algunas realizaciones, este cifrado y generación de encabezamiento puede estar incluido como parre de cualquiera de las técnicas de dispersión de datos áridos de cifrado analizadas con respecto a la etapa (4730) del flujo de proceso (4700) de la figura 47, o analizadas con respecto a la etapa (4820) y (4825) del flujo de proceso (4800) de la figura 48A. Además, en algunas realizaciones, este proceso de generación de encabezamiento puede ser ejecutado por el módulo de división criptográfica de paquetes (4878) como se describe con respecto al servicio de apoderado seguro (4870) de la figura 48C. El cliente (4910) puede entonces transmitir los encabezamientos H_1, H_2 y H_3 al servidor (4920). Esta transmisión puede producirse de acuerdo con, por ejemplo, la etapa (4740) del flujo de proceso (4700) de la figura 47, o de acuerdo con, por ejemplo, la etapa (4830) del flujo de proceso (4800) de la figura 48A. Además, el módulo de división criptográfica de paquetes (4878) puede transmitir los encabezamientos H_1, H_2 y H_3 de los paquetes de datos (4877) por los subcanales (4872), (4874) y (4876) como se describe con respecto al servicio de apoderado seguro (4870) en la figura 48C. El servicio de apoderado seguro (4900) pasa entonces a la etapa (4922).

En la etapa (4922), el servidor (4920) puede recibir los encabezamientos H_1, H_2 y H_3 como se describe con respecto a la etapa (4750) del flujo de proceso (4700) de la figura 47, o como se describe con respecto a la etapa (4835) del flujo de proceso (4850) de la figura 48B. El cliente (4910) puede entonces dispersar los datos D en las cuotas D_1, D_2 y D_3. Las cuotas D_1, D_2 y D_3 pueden ser cifradas basándose en claves asociadas con el establecimiento de los túneles de comunicación segura en la etapa (4930). En algunas realizaciones, este proceso de dispersión puede estar incluido como parte de cualquiera de las técnicas de cifrad y dispersión de datos analizadas con respecto a la etapa (4730) del flujo de proceso (4700) de la figura 47, o analizadas con respecto a la etapa (4820) y (4825) del flujo de proceso (4800) de la figura 48A. El servicio de apoderado seguro (4900) transmite las cuotas de datos cifrados y analizados sintácticamente al cliente (4910). Esta transmisión puede producirse de acuerdo con, por ejemplo, la etapa (4740) del flujo de proceso (4700) de la figura 47, o de acuerdo con, por ejemplo, la etapa (4830) del flujo de proceso (4800) de la figura 48A. El servicio de apoderado seguro (4900) puede pasar a la etapa (4914).

En la etapa (4914), el cliente (4910) puede recibir las cuotas D_1, D_2 y D_3 como se describe con respecto a la etapa (4750) del flujo de proceso (4700) de la figura 47, o como se describe con respecto a la etapa (4835) del flujo de proceso (4850) de la figura 48B. En algunas realizaciones, un módulo de restauración de paquetes puede recibir cuotas de paquetes de datos procedentes de subcanales como se describe con respecto al módulo de restauración de paquetes (4879) del servicio de apoderado seguro (4870) en la figura 48C. El cliente (4910) puede entonces descifrar y restaurar las cuotas D_1, D_2 y D_3. Las cuotas pueden ser descifradas y restauradas de acuerdo con cualquier técnica de descifrado y restauración como se describe con respecto a la etapa (4760) del flujo de proceso (4700) de la figura 47 o las etapas (4840) y (4845) como se describe con respecto al flujo de proceso (4850) de la figura 48B. En algunas realizaciones, las cuotas D_1, D_2 y D_3 pueden ser descifradas y restauradas por un módulo de restauración de paquetes tal como el módulo de restauración de paquetes (4879) del servicio de apoderado seguro (4870) en la figura 48C. El cliente (4910) puede repetir cualquiera de las etapas (4912) y (4914), y el servidor (4920) puede repetir la etapa (4922), tantas veces como sea necesario para transmitir datos entre el cliente (4910) y el servidor (4920). Entonces finaliza el servicio de apoderado seguro (4900).

La fig. 50 es un diagrama de bloques simplificado de un servicio de apoderado seguro (5000) entre el cliente (5010) y el servidor (5020) que distribuye confianza entre un conjunto de autoridades de certificación en la estructura de canales de comunicación, que puede usarse en cualquier combinación adecuada, con cualquier añadido, eliminación o modificación adecuados de acuerdo con una realización de la presente invención. El servicio de apoderado seguro (5000) puede ser, por ejemplo, los servicios de apoderado seguro analizados con respecto al flujo de proceso (4700), (4800) o (4850), así como el servicio de apoderado seguro (4870) o (4900) como se describe con respecto a las figuras 47-49. El servicio de apoderado seguro (5000) puede implementarse de modo que cada uno de los túneles de comunicación segura (5030), (5040) y (5050) esté asociado con una autoridad de certificación de nivel exterior (no mostrada en la figura 50) como se describe con respecto a la etapa (4710) del flujo de proceso (4700) de la figura 47 y la etapa (4810) del flujo de proceso (4800) de la figura 48A. Además, el servicio de apoderado seguro (5000) puede implementarse de moco que cada uno de los túneles de comunicación segura (5030), (5040) y (5050) esté asociado con una autoridad diferente de una autoridad de certificación de nivel interior tal como la primera autoridad de certificación CA1, la segunda autoridad de certificación CA2 y la tercera autoridad de certificación CA3, y cada uno de los túneles de comunicación segura (5030), (5040) y (5050) se establecen por medios de transporte físico diferentes. Estos medios físicos diferentes pueden ser cualquier medio de transporte físico como se describe con respecto a la etapa (4710) del flujo de proceso (4700) de la figura 4700 o con respecto a la etapa (4810) del flujo de proceso (4800) de la figura 48A. Por ejemplo, como se ilustra en la figura 50, los túneles de comunicación segura (5030), (5040) y (5050) pueden establecerse por WiFi, Ethernet, y canales de comunicación celular, respectivamente.

Durante el funcionamiento normal del servicio de apoderado seguro (5000), el cliente (5010) puede enviar la primera cuota de datos (5012) por el primer túnel de comunicación segura (5030), la segunda cuota de datos (5014) por el segundo túnel de comunicación segura (5040) y la tercera cuota de datos (5016) por el tercer túnel de comunicación segura (5050). Las cuotas de datos (5012), (5014) y (5016) pueden ser cuotas de datos calculadas por el cliente (5010) usando cualquier técnica de dispersión y cifrado de datos adecuada analizada con respecto a la etapa (4730) del flujo de proceso (4700) de la figura 47, o analizada con respecto a la etapa (4820) y (4825) del flujo de proceso (4800) de la figura 48A. Aunque se ilustra que el servicio de apoderado seguro (5000) divide los datos en 3 cuotas de datos, puede entenderse que el servicio de apoderado seguro (5000) puede dispersar los datos en cualquier número adecuado de cuotas y transmitir cada una de ellas por cualquier número adecuado de túneles de comunicación segura.

En algunas realizaciones, uno de los medios físicos puede experimentar un fallo de red. Este fallo de red puede deberse a un mal funcionamiento estructural de los medios físicos. Por ejemplo, como se ilustra en el servicio de

apoderado seguro (5000), el canal de comunicación celular usado para establecer el tercer túnel de comunicación segura (5050) puede experimentar un fallo de red debido a daño en una torre celular.

En algunas realizaciones, el servicio de apoderado seguro (5000) puede no cambiar la transmisión de sus paquetes de datos por los túneles de comunicación segura (5030), (5040) y (5050) en respuesta al fallo de red (no ilustrado en la figura 50). En otras palabras, el cliente (5010) puede seguir enviando la primera cuota de datos (5012) por el primer túnel de comunicación segura (5030), y la segunda cuota de datos (5014) por el segundo túnel de comunicación segura (5040). En algunas realizaciones del servicio de apoderado seguro (5000), los paquetes de datos que incluyen la primera cuota de datos (5012) y la segunda cuota de datos (5014) pueden seguir intercambiándose sin una pérdida de integridad de datos. Por ejemplo, si los paquetes de datos procesados por el servicio de apoderado seguro (5000) son divididos usando un algoritmo de compartición de secreto (por ejemplo, el algoritmo de compartición de secreto de Shamir) de modo que solo es necesario un *quorum* de cuotas de datos (5012), (5014) y (5016) para recuperar cada paquete de datos transmitido, entonces puede que no haya pérdida de integridad de datos entre los paquetes intercambiados entre el cliente (5010) y el servidor (5020).

En algunas realizaciones, el servicio de apoderado seguro (5000) puede cambiar la transmisión de sus paquetes de datos por túneles de comunicación segura. Por ejemplo, la primera cuota de datos (5012) puede seguir siendo transmitida por el túnel de comunicación segura basado en WiFi (5030), mientras que la segunda cuota de datos (5014) y la tercera cuota de datos (5014) pueden ser transmitidas por el túnel de comunicación segura basado en Ethernet (5040). En tales realizaciones, uno o más de los túneles de comunicación segura pueden tener que ser divididos en uno o más túneles de comunicación segura usando procesos de establecimiento de clave adicionales. Esta división puede lograrse de acuerdo con, por ejemplo, cualquiera de las fases de establecimiento de clave descritas con respecto a la etapa (4720) del flujo de proceso (4700) de la figura 47 o la etapa (4820) del flujo de proceso (4800) de la figura 48. Después de estas fases de establecimiento de clave adicionales, las cuotas de datos de los paquetes de datos pueden reanudarse de acuerdo con la nueva configuración del servicio de apoderado seguro (5000).

En algunas realizaciones, esta nueva configuración del servicio de apoderado seguro (5000) puede cambiar cómo las cuotas de datos divididas son cifradas basándose en claves asociadas con el establecimiento de los túneles de comunicación segura o las porciones divididas de los túneles de comunicación segura. Por ejemplo, la primera cuota de datos (5012) puede ser cifrada basándose en una clave asociada con el establecimiento del primer túnel de comunicación segura basado en WiFi (5030), y luego transmitida por ese túnel. La segunda cuota de datos (5014) puede ser cifrada basándose en una clave asociada con el establecimiento de una primera porción dividida (5042) del segundo túnel de comunicación segura basado en Ethernet (5040) y transmitida por la primera porción dividida (5042), y la tercera cuota de datos (5016) puede ser cifrada basándose en una clave asociada con el establecimiento de una segunda porción dividida (5044) del túnel de comunicación segura basado en Ethernet (5040) y transmitida por la segunda porción dividida (5044). En algunas realizaciones, el primer túnel de comunicación segura (5030) puede establecerse usando el certificado obtenido de la autoridad de certificación CA1, la primera porción dividida (5042) del segundo túnel de comunicación segura basado en Ethernet (5040) puede establecerse usando el certificado obtenido de la autoridad de certificación CA2, y la segunda porción dividida (5044) del túnel de comunicación segura basado en Ethernet (5040) puede establecerse usando el certificado obtenido de la autoridad de certificación CA3. En algunas realizaciones, el servicio de apoderado seguro (5000) puede ejecutar estos procesos de establecimiento de clave adicionales de manera adaptativa cuando los canales de comunicación en los que se establecen los túneles de comunicación segura fallan o son restaurados. En realizaciones del servicio de apoderado seguro (5000) como se ilustra en la figura 50, el servicio de apoderado seguro (5000) puede denominarse “medio de comunicación redundante”.

En realizaciones del servicio de apoderado seguro (5000) como se ilustra en la figura 50, pueden intercambiarse datos entre el cliente (5010) y el servidor (5020) sin una pérdida de confidencialidad, integridad y autenticidad de datos. Es decir, aunque las autoridades de certificación comprometidas tengan acceso a la información intercambiada basándose en esa autoridad de certificación, el atacante asociado con esa autoridad de certificación puede no tener suficiente información para alterar la confidencialidad o integridad de la comunicación. Por ejemplo, si la autoridad de certificación de nivel exterior del servicio de apoderado seguro (5000) se viera comprometida pero se preservara la integridad de las autoridades de certificación de nivel interior, el atacante puede ser capaz de observar los trenes de datos por el canal de comunicación basado en WiFi y ambas porciones del canal de comunicación basado en Ethernet, pero puede no tener conocimiento del cifrado usado para asegurar los datos por cada túnel de comunicación segura.

En otro ejemplo, si una o más de las autoridades de certificación de nivel interior se viera comprometida pero la

autoridad de certificación de nivel exterior permaneciera intacta, el atacante puede ser capaz de recuperar algunas de las porciones divididas criptográficamente de los paquetes de datos, pero puede no ser capaz de descifrar los paquetes de datos en sí porque puede no tener conocimiento del cifrado usado por la autoridad de certificación de nivel exterior. Además, si los paquetes de datos enviados a través de los túneles de comunicación segura son divididos criptográficamente de modo que pueden ser restaurados a partir de al menos un subconjunto de las cuotas recombinando al menos un *quorum* de las cuotas, el usuario del analizador sintáctico de datos seguros puede tener la protección adicional de que si alguno, pero menos de un *quorum*, de los certificados asociados con los túneles de comunicación segura se han visto comprometidos, el atacante puede no ser capaz de restaurar los paquetes de datos criptodivididos.

Además, otras combinaciones, añadidos, sustituciones y modificaciones resultarán evidentes para un experto e la materia en vista de la descripción de este documento.

REIVINDICACIONES

1. Un procedimiento para calcular al menos una clave de cifrado compartida, que comprende:

generar información secreta original;
obtener claves públicas de autoridades de certificación únicas (4210, 4220, 4230);
dispersar la información secreta en cuotas; y
cifrar cada una de las cuotas basándose, al menos en parte, en la clave pública de una autoridad diferente de las autoridades de certificación únicas, donde las cuotas pueden ser restauradas a partir de al menos un subconjunto de las cuotas recombinando al menos un número umbral de las cuotas, donde el número umbral de cuotas incluye menos de la totalidad de las cuotas (4614);
calcular una primera clave de cifrado compartida basándose en un conjunto de números sustancialmente aleatorios y la información secreta original (4616);
recombinar el al menos un número umbral de las cuotas; y
calcular una segunda clave de cifrado compartida basándose en el conjunto de números sustancialmente aleatorios y las cuotas recombinadas (4624).

2. El procedimiento de acuerdo con la reivindicación 1, que comprende además:

transmitir datos basándose en las cuotas recombinadas.

3. El procedimiento de acuerdo con la reivindicación 1, que comprende además:

comparar la primera y la segunda clave de cifrado compartida;
determinar si transmitir datos basándose en la comparación; y
transmitir datos basándose en la determinación.

4. El procedimiento de acuerdo con la reivindicación 1, que comprende además cifrar cada una de las cuotas basándose en una envoltura de clave.

5. El procedimiento de acuerdo con la reivindicación -4, donde la envoltura de clave está basada en una clave de grupo de trabajo.

6. El procedimiento de acuerdo con la reivindicación 1, que comprende además:

generar una jerarquía de autoridades de certificación, donde la jerarquía de autoridades de certificación comprende autoridades de certificación raíces; y
cifrar cada una del conjunto de cuotas basándose en un certificado expedido por una autoridad de certificación raíz única de la jerarquía de autoridades de certificación.

7. El procedimiento de acuerdo con la reivindicación 1, que comprende además:

generar una jerarquía de autoridades de certificación, donde la jerarquía de autoridades de certificación comprende un conjunto de autoridades de certificación menores; y
cifrar cada una del conjunto de cuotas basándose en un certificado expedido por una autoridad de certificación menor única de la jerarquía de autoridades de certificación.

8. Un sistema para calcular al menos una clave de cifrado compartida, donde el sistema comprende un primer dispositivo que comprende un primer circuito de procesamiento configurado para:

generar información secreta original;
obtener claves públicas de autoridades de certificación únicas (4210, 4220, 4230);
dispersar la información secreta en cuotas; y
cifrar cada una de las cuotas basándose en la clave pública de una autoridad diferente de las autoridades de certificación únicas, donde las cuotas pueden ser restauradas a partir de al menos un subconjunto de las cuotas recombinando al menos un número umbral de las cuotas, donde el número umbral de cuotas incluye menos de la totalidad de las cuotas (4614);
calcular una primera clave de cifrado compartida basándose en un conjunto de números sustancialmente aleatorios y la información secreta original (4616);

recombinar el al menos un número umbral de las cuotas; y
calcular una segunda clave de cifrado compartida basándose en el conjunto de números sustancialmente aleatorios y las cuotas recombinadas (4624).

9. El sistema de acuerdo con la reivindicación 8, que incluye un segundo dispositivo que comprende un segundo circuito de procesamiento configurado además para:

transmitir datos basándose en las cuotas recombinadas.

10. El sistema de acuerdo con la reivindicación 8, que incluye el primer circuito de procesamiento configurado además para:

comparar la primera y la segunda clave de cifrado compartida;
determinar si transmitir datos basándose en la comparación; y
transmitir datos basándose en la determinación.

11. El sistema de acuerdo con la reivindicación 8, que incluye el primer circuito de procesamiento configurado además para cifrar cada una de las cuotas basándose en una envoltura de clave.

12. El sistema de acuerdo con la reivindicación 8, donde la envoltura de clave está basada en una clave de grupo de trabajo.

13. El sistema de acuerdo con la reivindicación 8, que incluye el primer circuito de procesamiento configurado además para:

generar una jerarquía de autoridades de certificación, donde la jerarquía de autoridades de certificación comprende autoridades de certificación raíces; y
cifrar cada una del conjunto de cuotas basándose en un certificado expedido por una autoridad de certificación raíz única de la jerarquía de autoridades de certificación.

14. El sistema de acuerdo con la reivindicación 8, que incluye el primer circuito de procesamiento configurado además para:

generar una jerarquía de autoridades de certificación, donde la jerarquía de autoridades de certificación comprende un conjunto de autoridades de certificación menores; y
cifrar cada una del conjunto de cuotas basándose en un certificado expedido por una autoridad de certificación menor única de la jerarquía de autoridades de certificación.

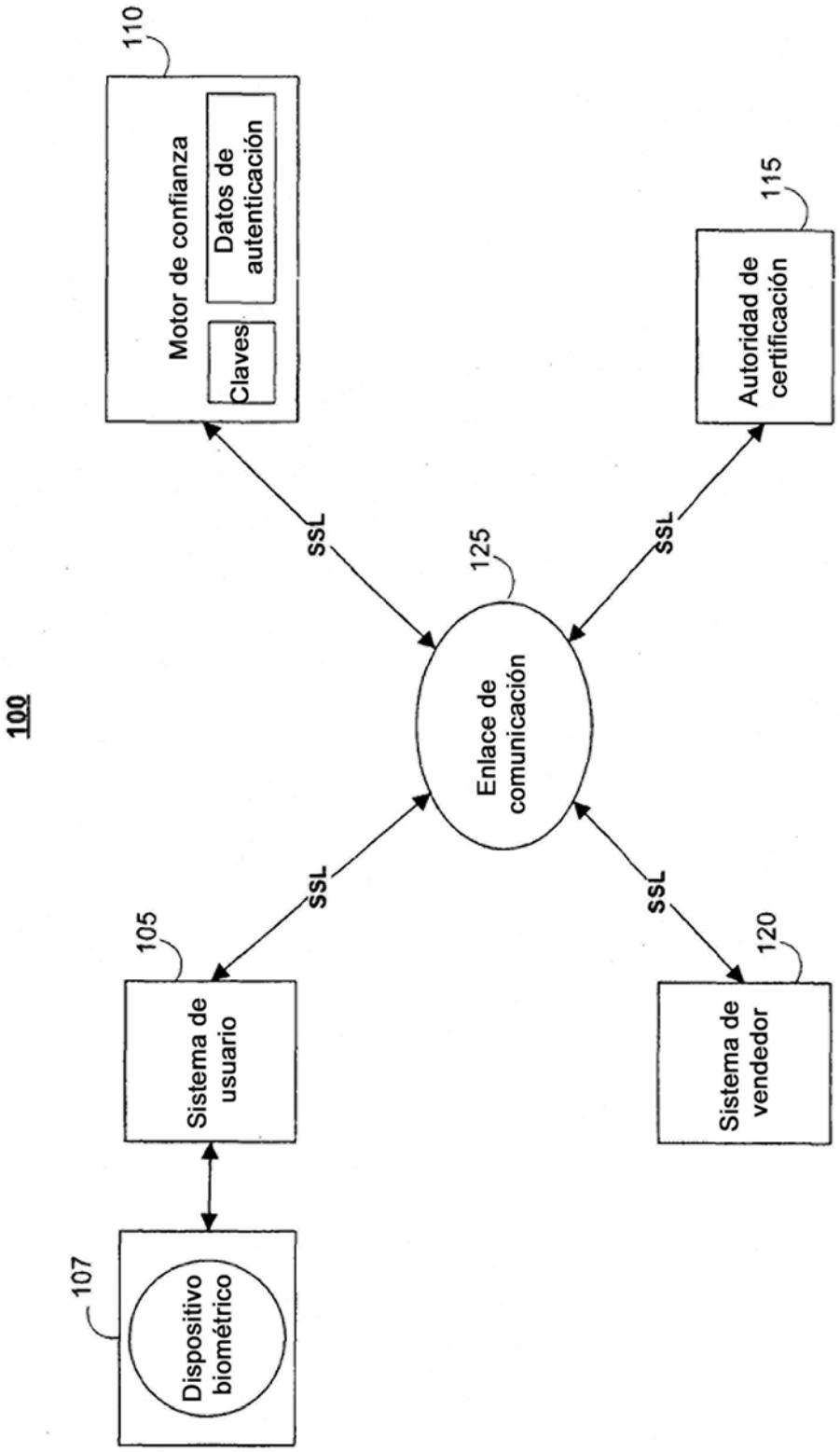

100
110
Motor de confianza
Claves
Datos de autenticación
115
Autoridad de certificación
SSL
SSL
125
Enlace de comunicación
SSL
SSL
105
Sistema de usuario
120
Sistema de vendedor
107
Dispositivo biométrico

FIG. 1

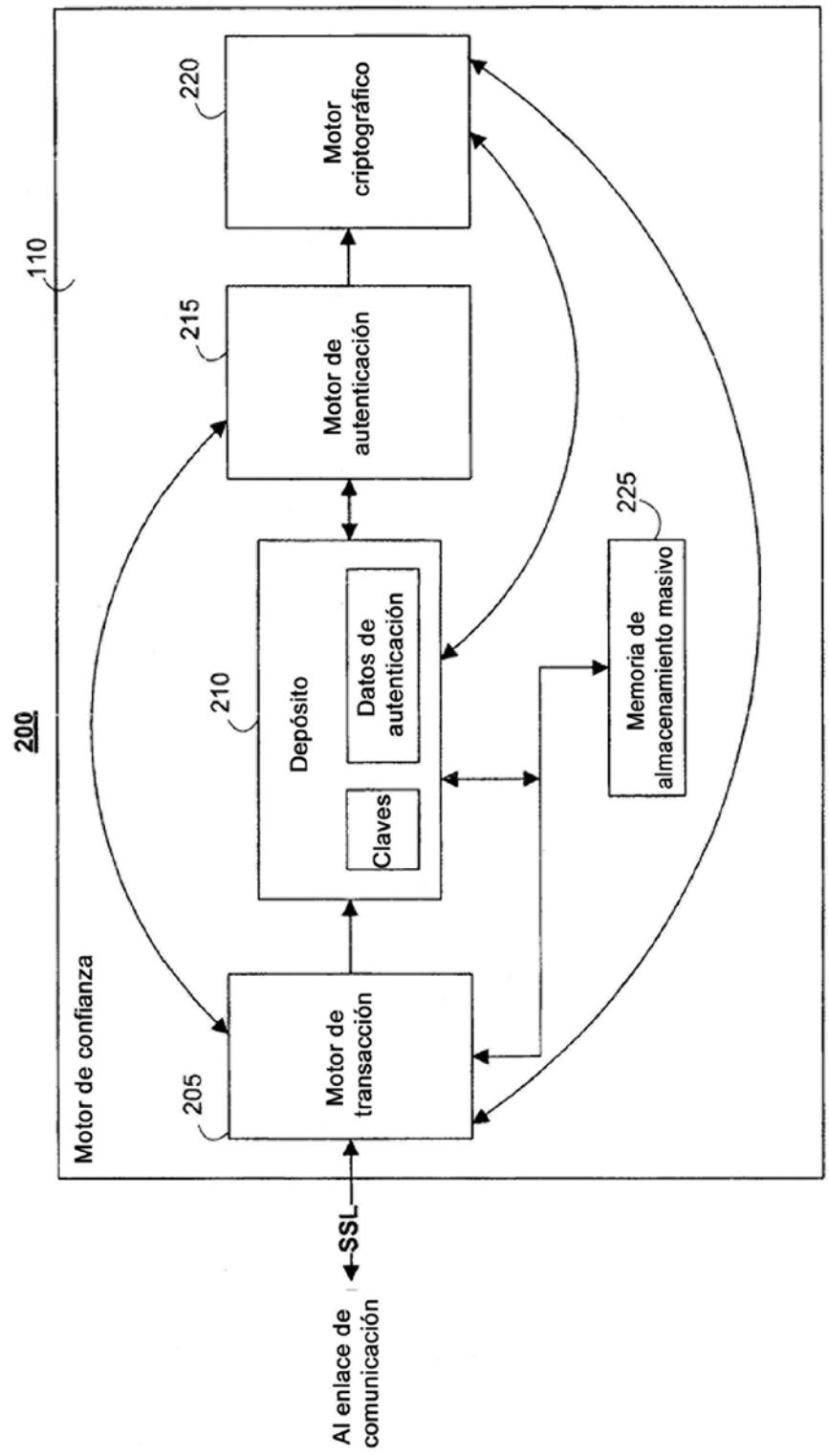

200
Motor de confianza
110
Motor de transacción
205
Depósito
210
Claves
Datos de autenticación
Motor de autenticación
215
Motor criptográfico
220
Memoria de almacenamiento masivo
225
SSL
Al enlace de comunicación

FIG. 2

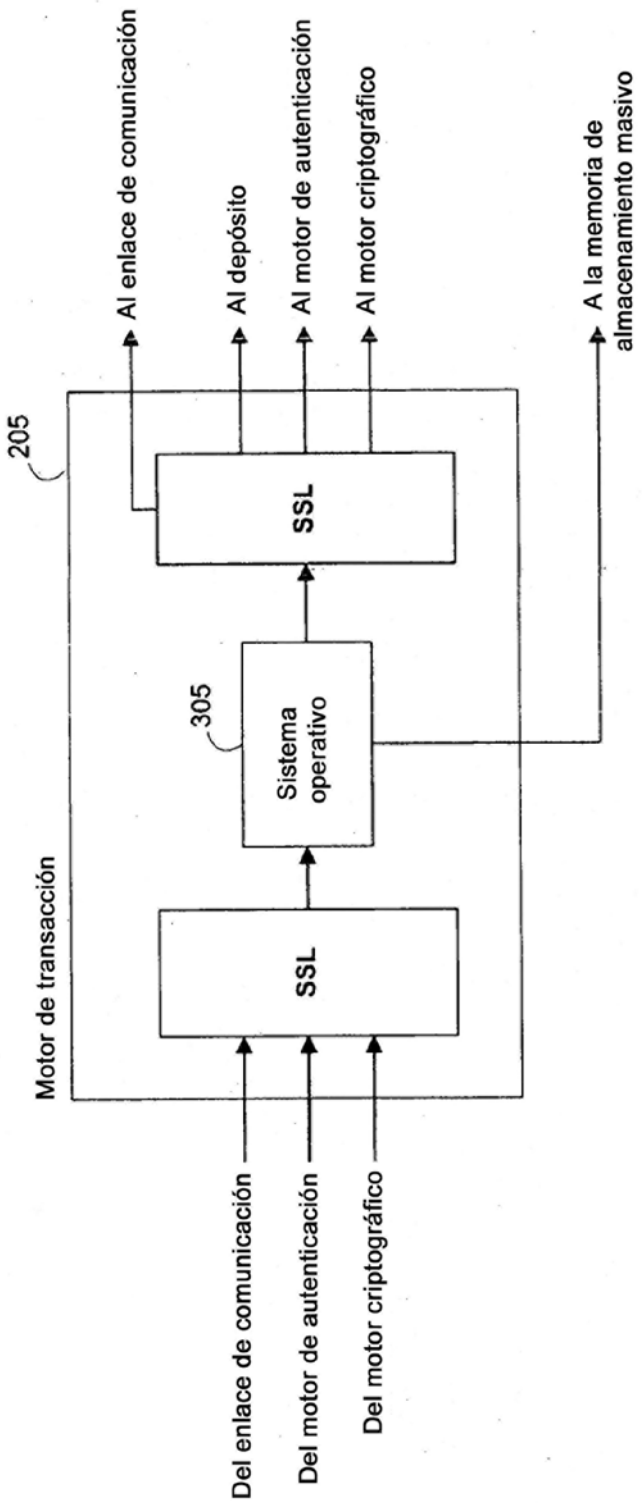

Al enlace de comunicación
Al depósito
Al motor de autenticación
Al motor criptográfico
A la memoria de almacenamiento masivo
205
SSL
305
Sistema operativo
SSL
Motor de transacción
Del enlace de comunicación
Del motor de autenticación
Del motor criptográfico

FIG. 3

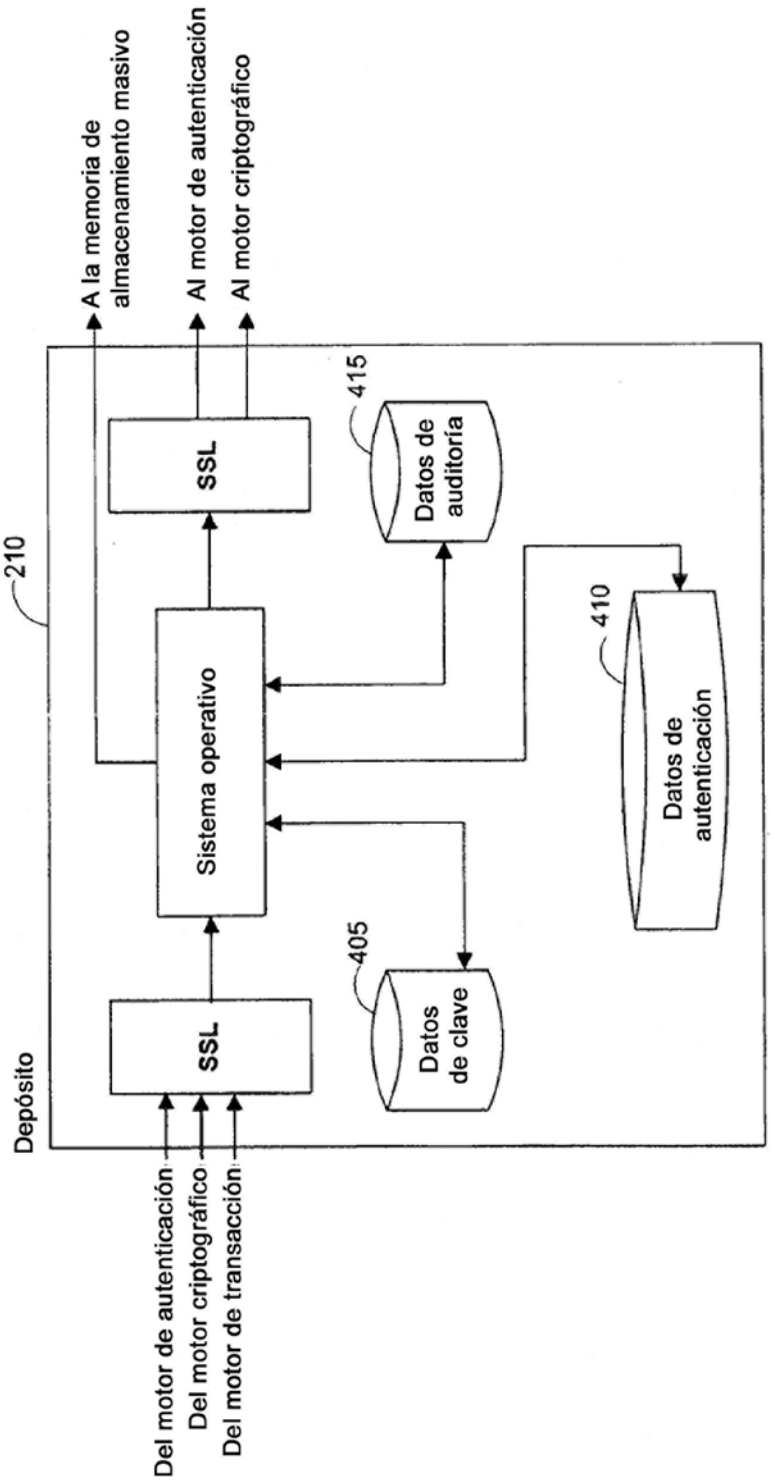

A la memoria de almacenamiento masivo
Al motor de autenticación
Al motor criptográfico
210
SSL
415
Datos de auditoría
Sistema operativo
410
Datos de autenticación
405
Datos de clave
SSL
Depósito
Del motor de autenticación
Del motor criptográfico
Del motor de transacción

FIG. 4

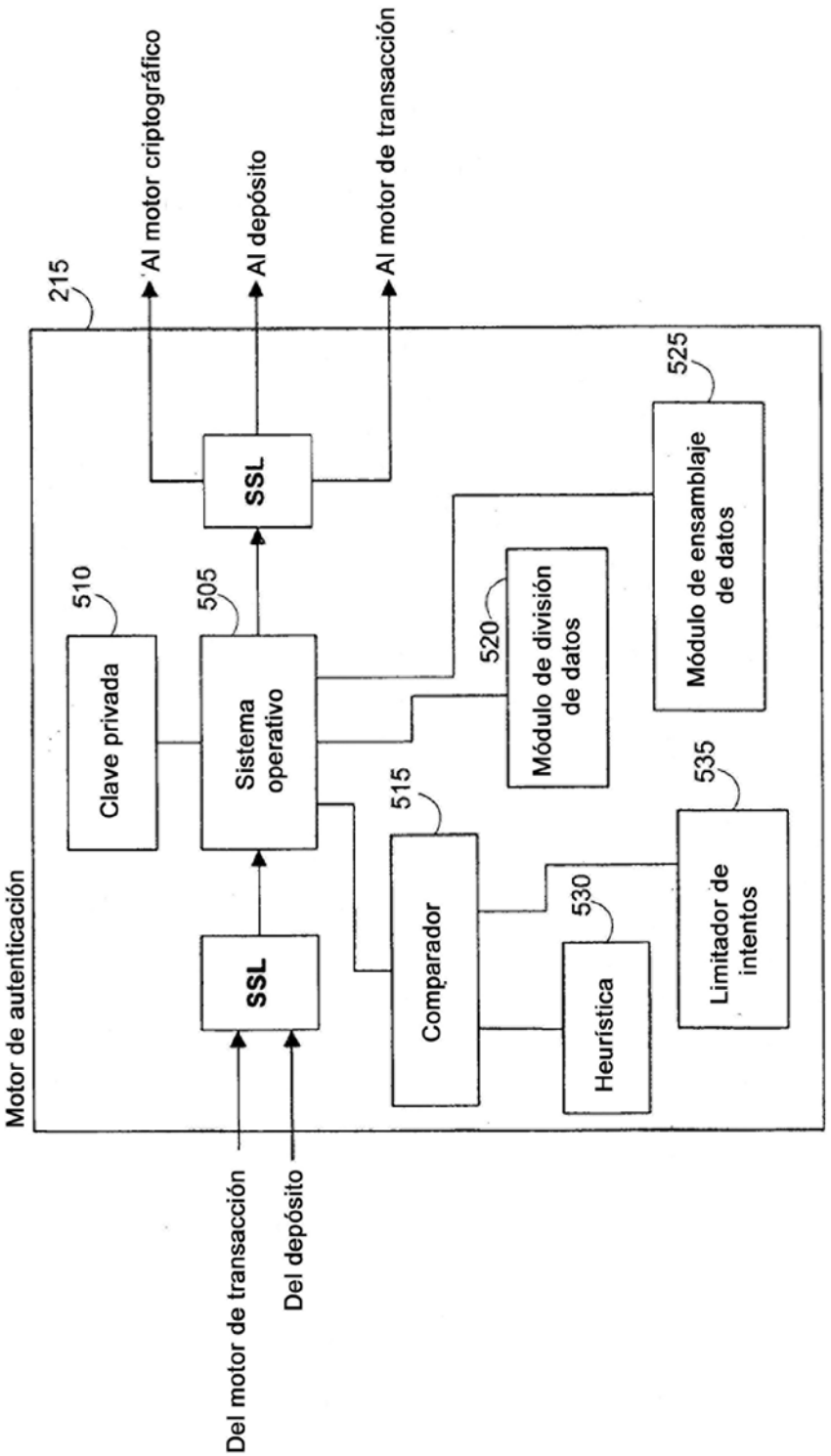

Motor de autenticación
215
Al motor criptográfico
Al depósito
Al motor de transacción
SSL
SSL
Clave privada
510
Sistema operativo
505
Módulo de división de datos
520
Módulo de ensamblaje de datos
525
Comparador
515
Heurística
530
Limitador de intentos
535
Del motor de transacción
Del depósito

FIG. 5

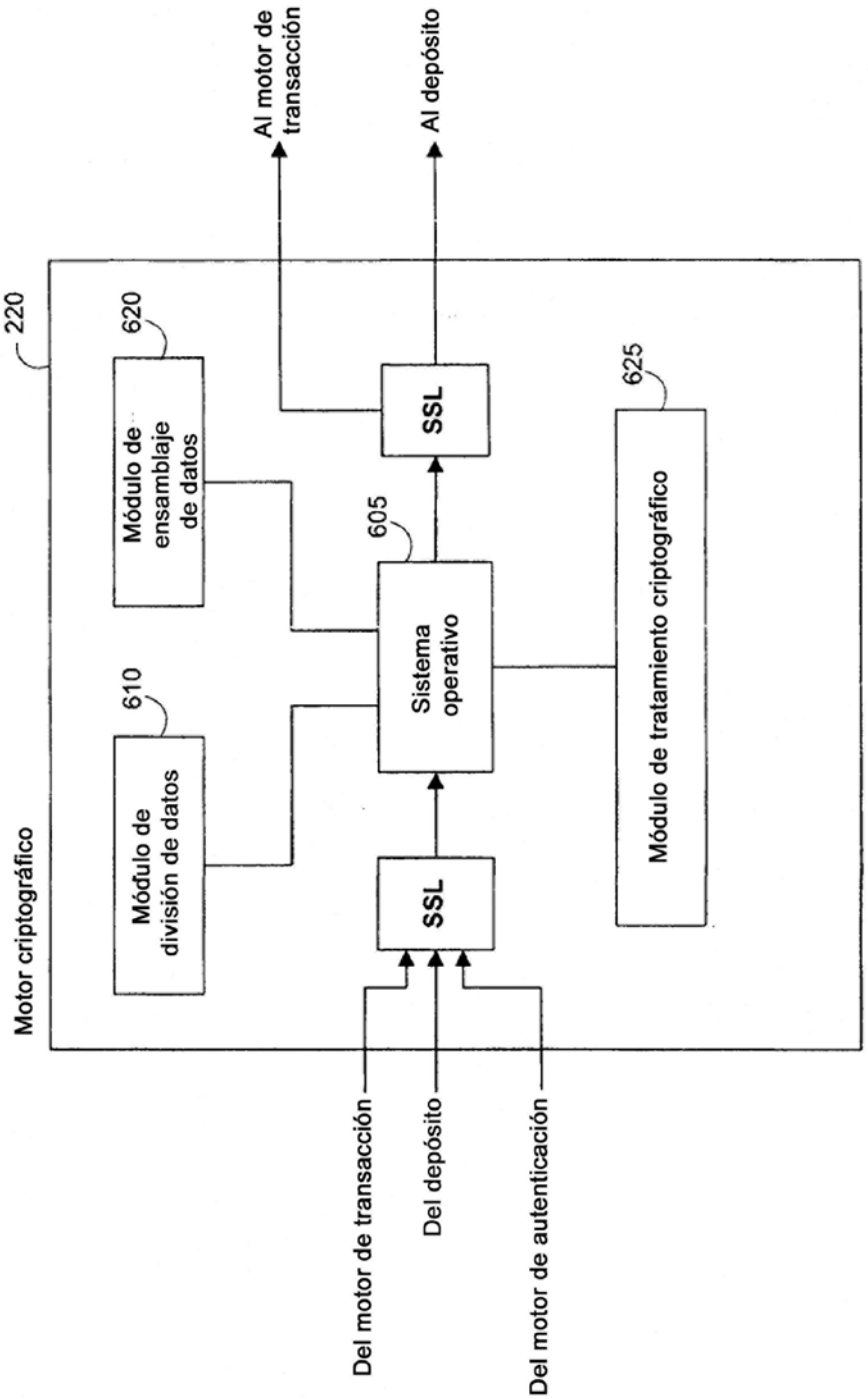

Motor criptográfico
220
Módulo de división de datos
610
Módulo de ensamblaje de datos
620
Sistema operativo
605
SSL
SSL
Módulo de tratamiento criptográfico
625
Del motor de transacción
Del depósito
Del motor de autenticación
Al motor de transacción
Al depósito

FIG. 6

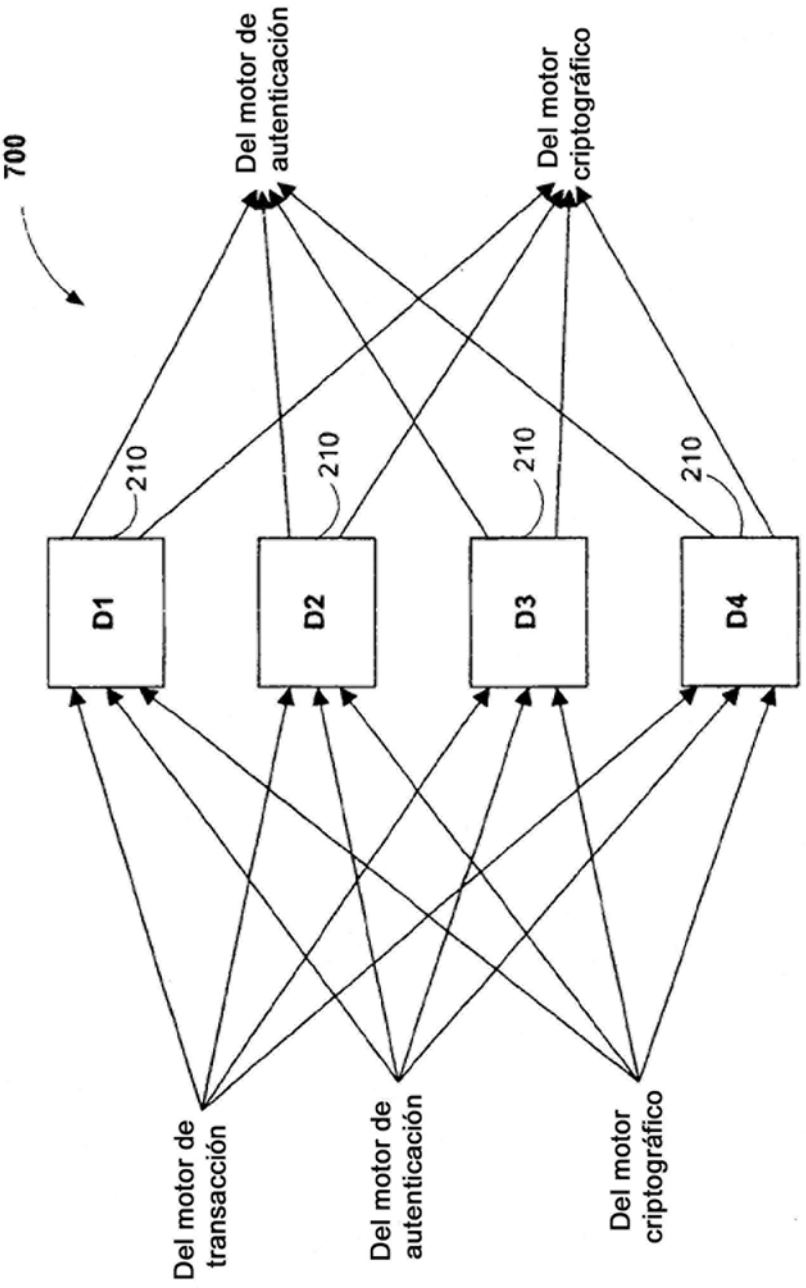

700
Del motor de autenticación
Del motor criptográfico
210
210
210
210
D1
D2
D3
D4
Del motor de transacción
Del motor de autenticación
Del motor criptográfico

FIG. 7

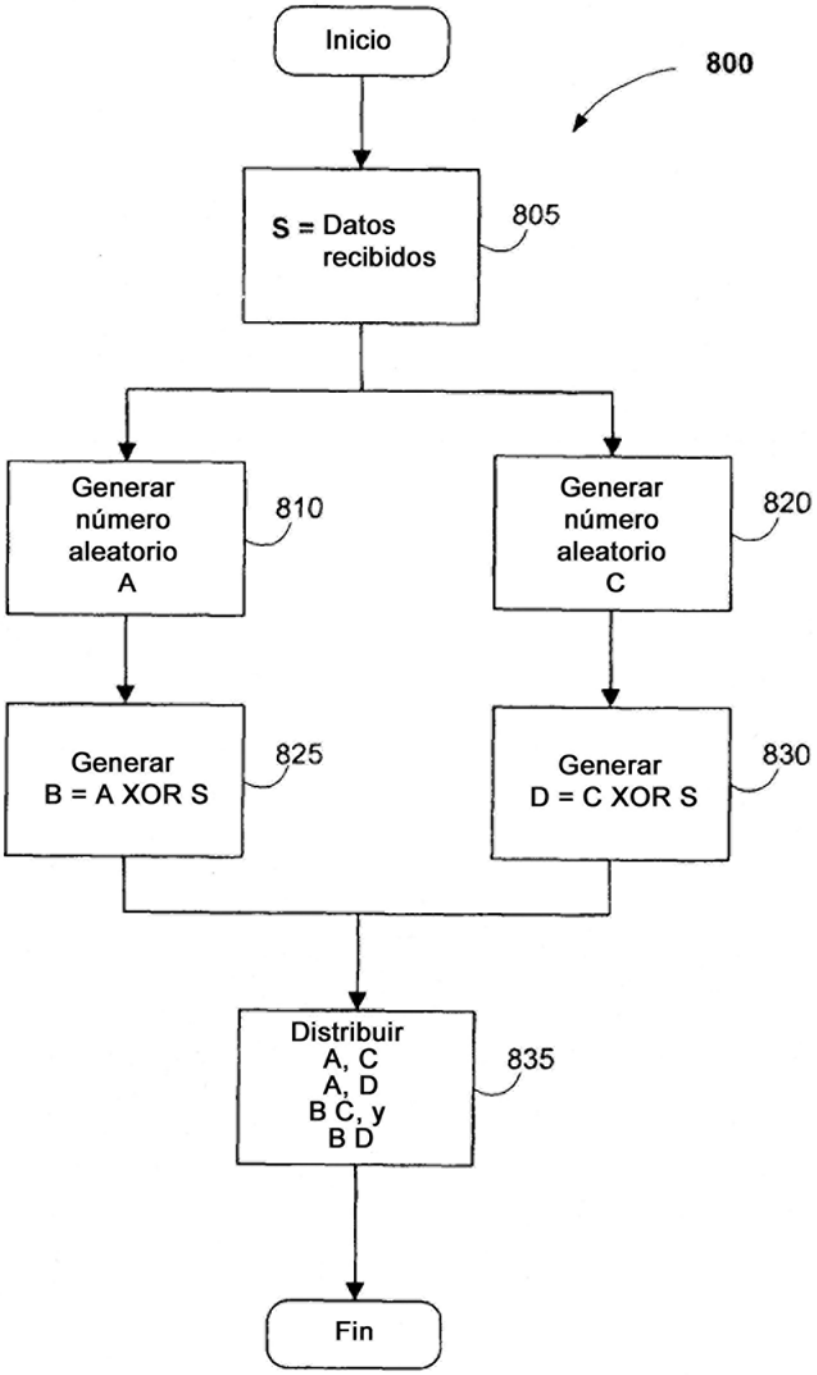
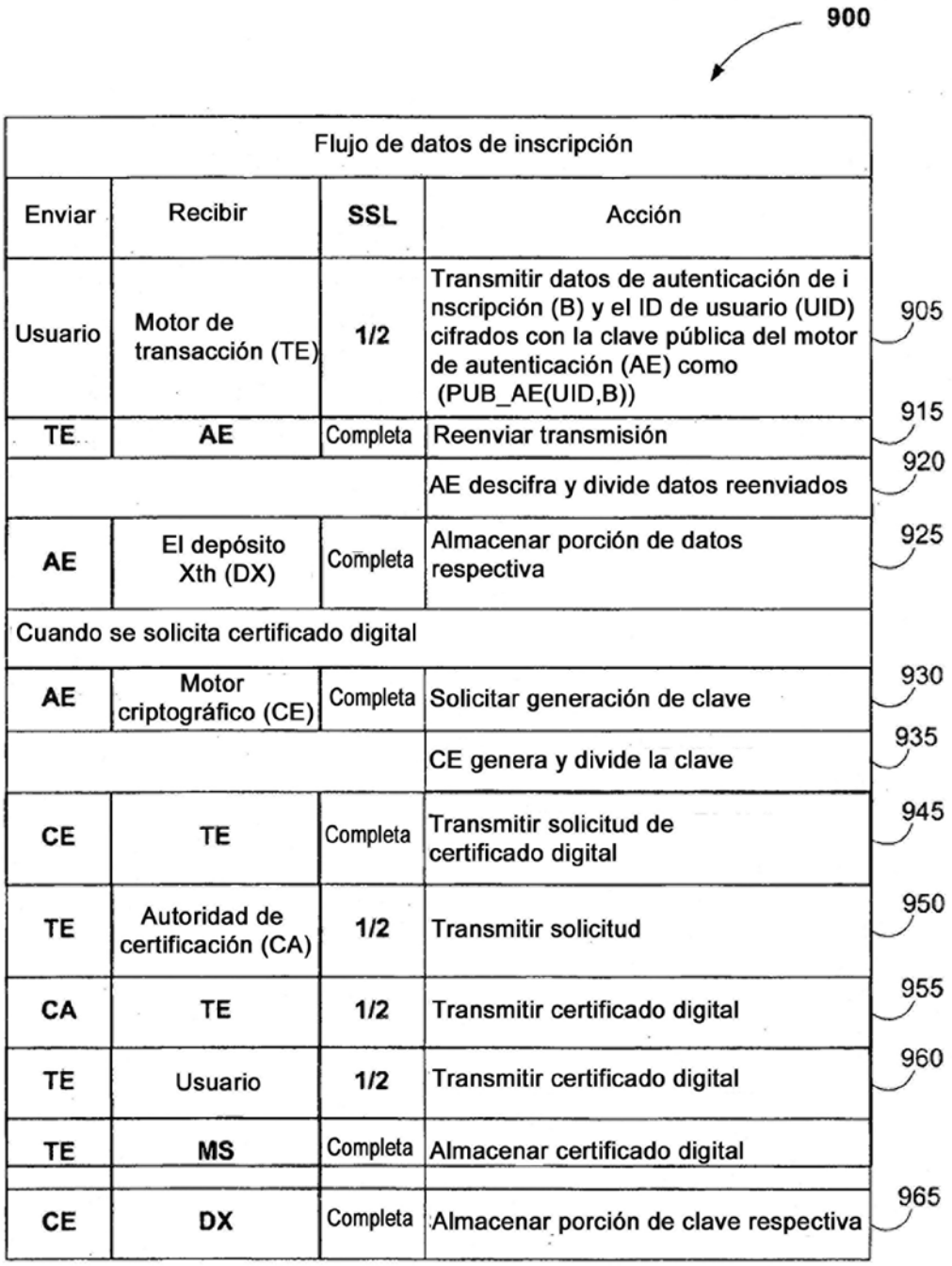

Inicio
800
S = Datos recibidos
805
Generar número aleatorio A
810
Generar número aleatorio C
820
Generar B = A XOR S
825
Generar D = C XOR S
830
Distribuir A, C A, D B C, y B D
835
Fin

FIG. 8



Flujo de datos de inscripción			
Enviar	Recibir	SSL	Acción
Usuario	Motor de transacción (TE)	1/2	Transmitir datos de autenticación de inscripción (B) y el ID de usuario (UID) cifrados con la clave pública del motor de autenticación (AE) como (PUB_AE(UID,B))
TE	AE	Completa	Reenviar transmisión
			AE descifra y divide datos reenviados
AE	El depósito Xth (DX)	Completa	Almacenar porción de datos respectiva
Cuando se solicita certificado digital			
AE	Motor criptográfico (CE)	Completa	Solicitar generación de clave
			CE genera y divide la clave
CE	TE	Completa	Transmitir solicitud de certificado digital
TE	Autoridad de certificación (CA)	1/2	Transmitir solicitud
CA	TE	1/2	Transmitir certificado digital
TE	Usuario	1/2	Transmitir certificado digital
TE	MS	Completa	Almacenar certificado digital
CE	DX	Completa	Almacenar porción de clave respectiva

FIG. 9, Panel A

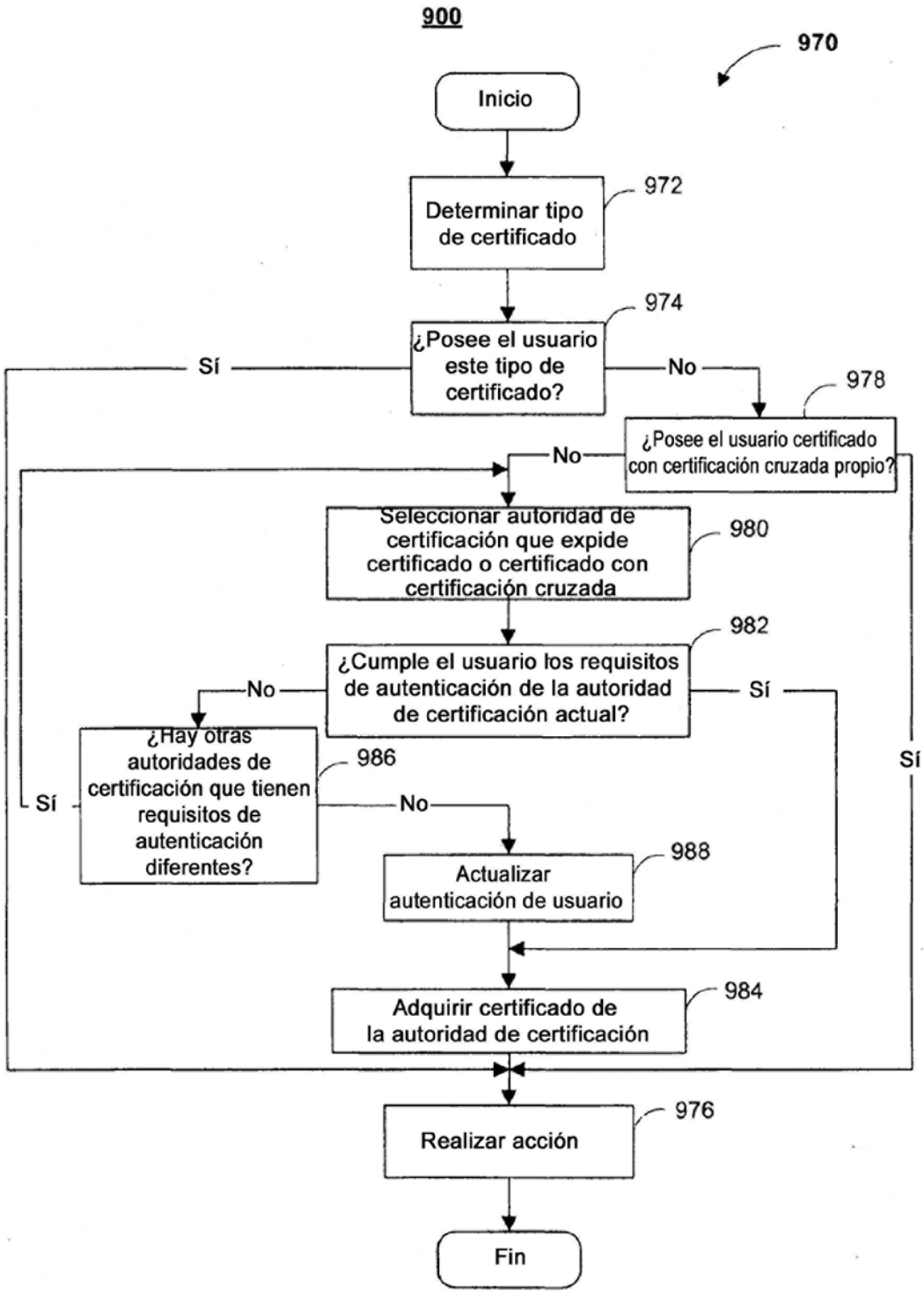

900
970
Inicio
Determinar tipo de certificado
972
¿Posee el usuario este tipo de certificado?
974
Sí
No
¿Posee el usuario certificado con certificación cruzada propio?
978
No
Sí
Seleccionar autoridad de certificación que expide certificado o certificado con certificación cruzada
980
¿Cumple el usuario los requisitos de autenticación de la autoridad de certificación actual?
982
No
Sí
¿Hay otras autoridades de certificación que tienen requisitos de autenticación diferentes?
986
Sí
No
Actualizar autenticación de usuario
988
Adquirir certificado de la autoridad de certificación
984
Realizar acción
976
Fin

FIG. 9, Panel B

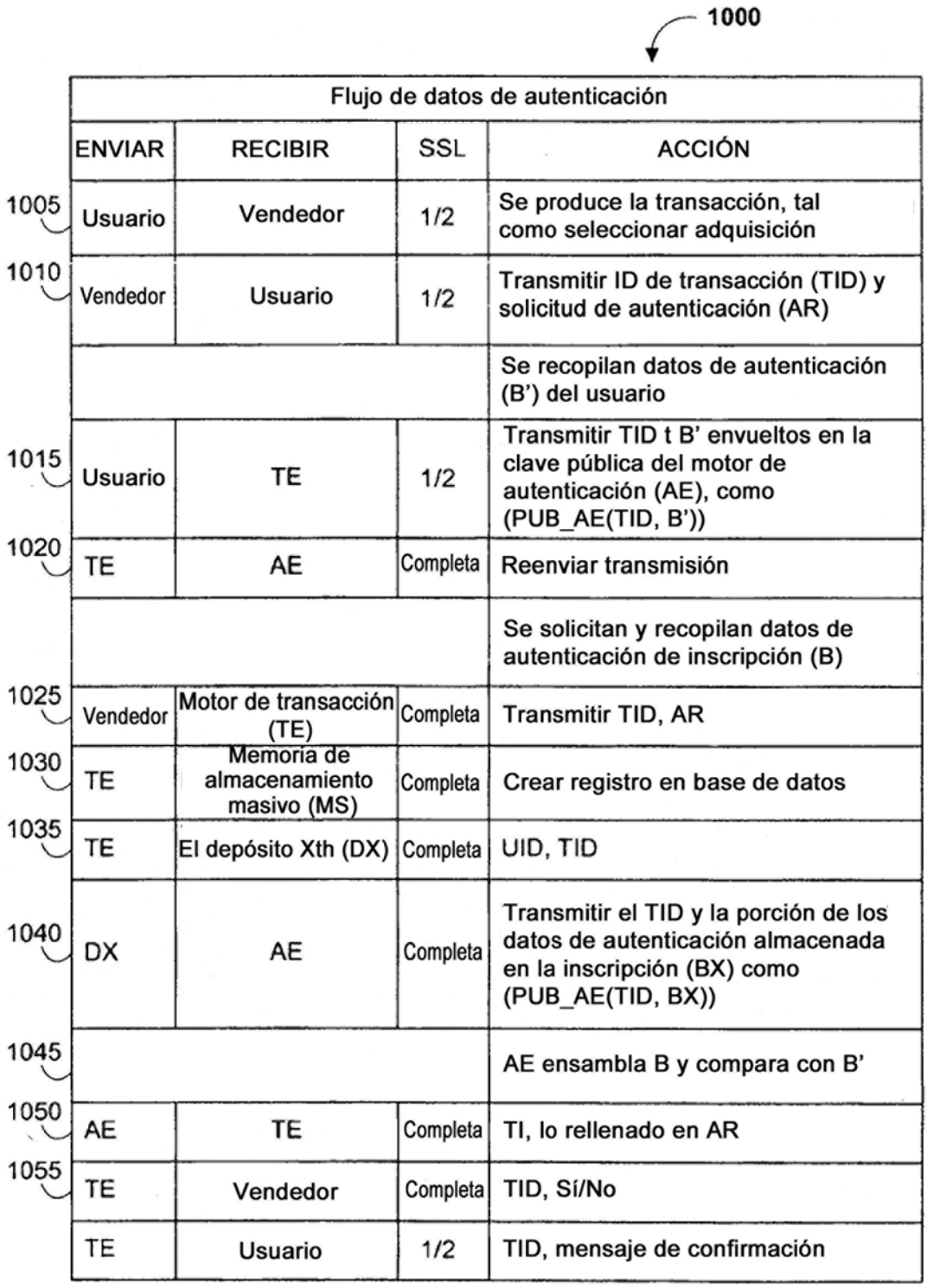

1000
Flujo de datos de autenticación
ENVIAR
RECIBIR
SSL
ACCIÓN
1005
Usuario
Vendedor
1/2
Se produce la transacción, tal como seleccionar adquisición
1010
Vendedor
Usuario
1/2
Transmitir ID de transacción (TID) y solicitud de autenticación (AR)
Se recopilan datos de autenticación (B') del usuario
1015
Usuario
TE
1/2
Transmitir TID t B' envueltos en la clave pública del motor de autenticación (AE), como (PUB_AE(TID, B'))
1020
TE
AE
Completa
Reenviar transmisión
Se solicitan y recopilan datos de autenticación de inscripción (B)
1025
Vendedor
Motor de transacción (TE)
Completa
Transmitir TID, AR
1030
TE
Memoria de almacenamiento masivo (MS)
Completa
Crear registro en base de datos
1035
TE
El depósito Xth (DX)
Completa
UID, TID
1040
DX
AE
Completa
Transmitir el TID y la porción de los datos de autenticación almacenada en la inscripción (BX) como (PUB_AE(TID, BX))
1045
AE ensambla B y compara con B'
1050
AE
TE
Completa
TI, lo rellenado en AR
1055
TE
Vendedor
Completa
TID, Sí/No
TE
Usuario
1/2
TID, mensaje de confirmación

FIG. 10

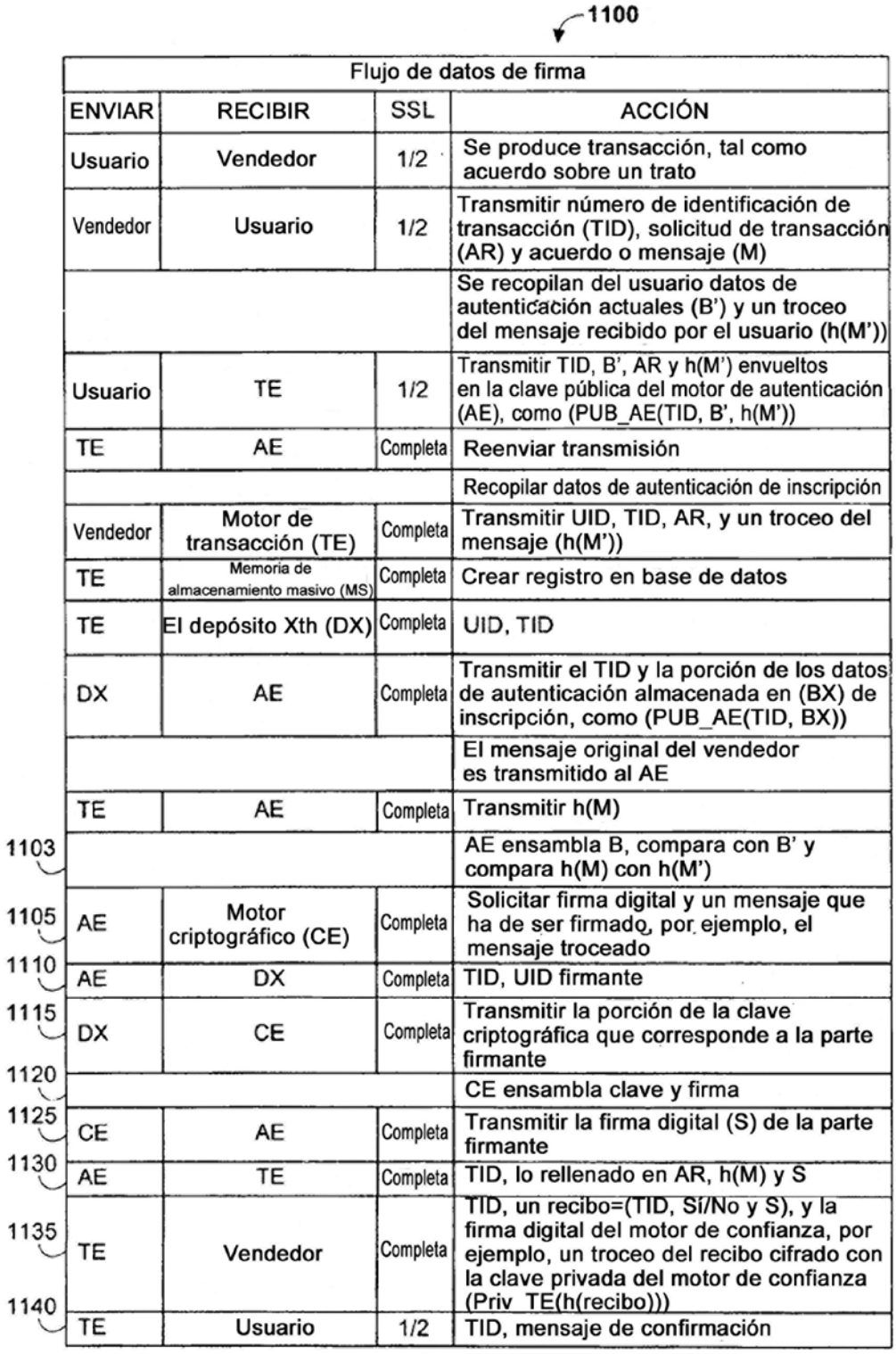

1100
Flujo de datos de firma
ENVIAR
RECIBIR
SSL
ACCIÓN
Usuario
Vendedor
1/2
Se produce transacción, tal como acuerdo sobre un trato
Vendedor
Usuario
1/2
Transmitir número de identificación de transacción (TID), solicitud de transacción (AR) y acuerdo o mensaje (M)
Se recopilan del usuario datos de autenticación actuales (B') y un troceo del mensaje recibido por el usuario (h(M'))
Usuario
TE
1/2
Transmitir TID, B', AR y h(M') envueltos en la clave pública del motor de autenticación (AE), como (PUB_AE(TID, B', h(M'))
TE
AE
Completa
Reenviar transmisión
Recopilar datos de autenticación de inscripción
Vendedor
Motor de transacción (TE)
Completa
Transmitir UID, TID, AR, y un troceo del mensaje (h(M'))
TE
Memoria de almacenamiento masivo (MS)
Completa
Crear registro en base de datos
TE
El depósito Xth (DX)
Completa
UID, TID
DX
AE
Completa
Transmitir el TID y la porción de los datos de autenticación almacenada en (BX) de inscripción, como (PUB_AE(TID, BX))
El mensaje original del vendedor es transmitido al AE
TE
AE
Completa
Transmitir h(M)
1103
AE ensambla B, compara con B' y compara h(M) con h(M')
1105
AE
Motor criptográfico (CE)
Completa
Solicitar firma digital y un mensaje que ha de ser firmado, por ejemplo, el mensaje troceado
1110
AE
DX
Completa
TID, UID firmante
1115
DX
CE
Completa
Transmitir la porción de la clave criptográfica que corresponde a la parte firmante
1120
CE ensambla clave y firma
1125
CE
AE
Completa
Transmitir la firma digital (S) de la parte firmante
1130
AE
TE
Completa
TID, lo rellenado en AR, h(M) y S
1135
TE
Vendedor
Completa
TID, un recibo=(TID, Sí/No y S), y la firma digital del motor de confianza, por ejemplo, un troceo del recibo cifrado con la clave privada del motor de confianza (Priv_TE(h(recibo)))
1140
TE
Usuario
1/2
TID, mensaje de confirmación

FIG. 11

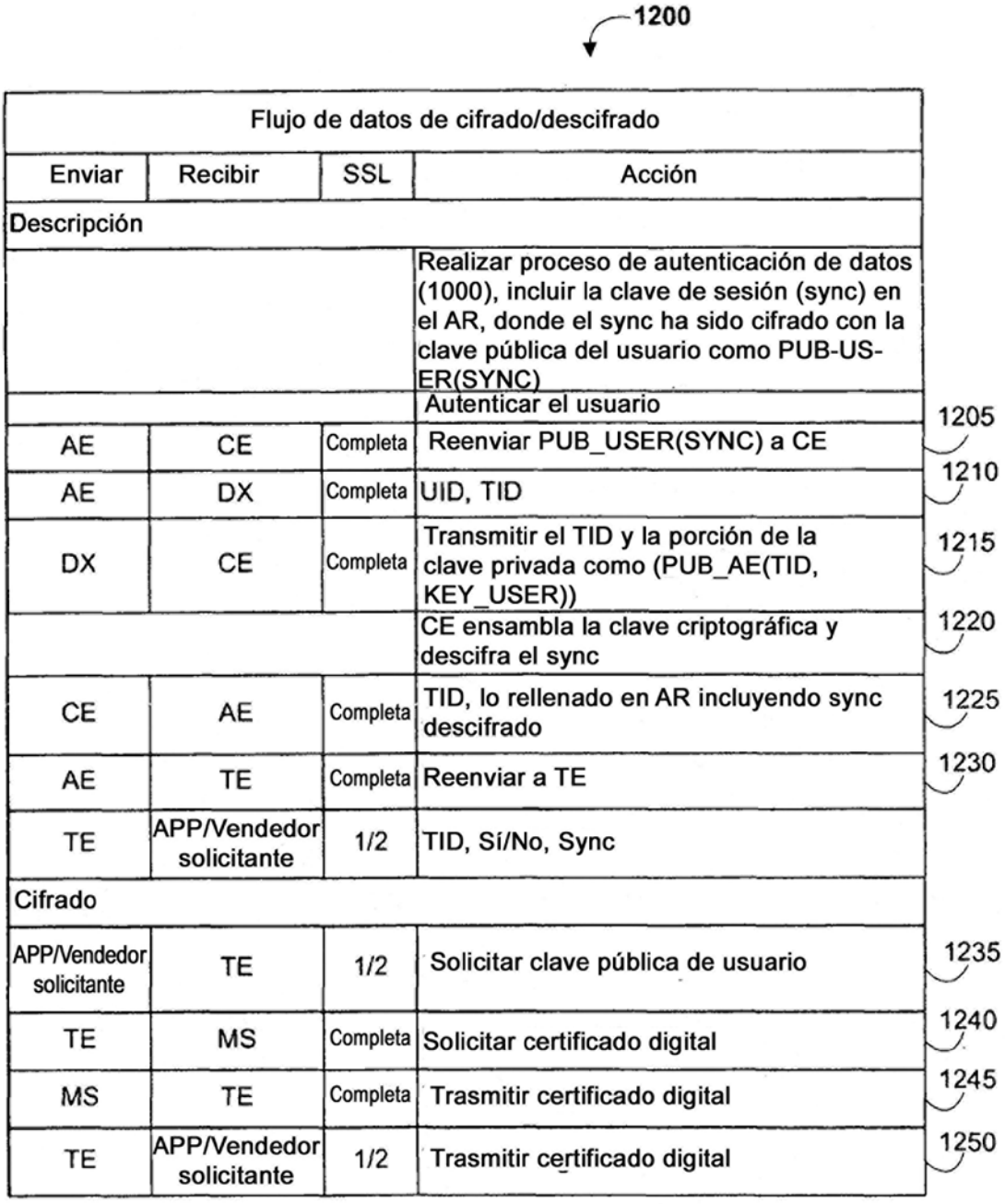

1200
Flujo de datos de cifrado/descifrado
Enviar
Recibir
SSL
Acción
Descripción
Realizar proceso de autenticación de datos (1000), incluir la clave de sesión (sync) en el AR, donde el sync ha sido cifrado con la clave pública del usuario como PUB-USER(SYNC)
Autenticar el usuario
AE
CE
Completa
Reenviar PUB_USER(SYNC) a CE
1205
AE
DX
Completa
UID, TID
1210
DX
CE
Completa
Transmitir el TID y la porción de la clave privada como (PUB_AE(TID, KEY_USER))
1215
CE ensambla la clave criptográfica y descifra el sync
1220
CE
AE
Completa
TID, lo rellenado en AR incluyendo sync descifrado
1225
AE
TE
Completa
Reenviar a TE
1230
TE
APP/Vendedor solicitante
1/2
TID, Sí/No, Sync
Cifrado
APP/Vendedor solicitante
TE
1/2
Solicitar clave pública de usuario
1235
TE
MS
Completa
Solicitar certificado digital
1240
MS
TE
Completa
Trasmitir certificado digital
1245
TE
APP/Vendedor solicitante
1/2
Trasmitir certificado digital
1250

FIG. 12

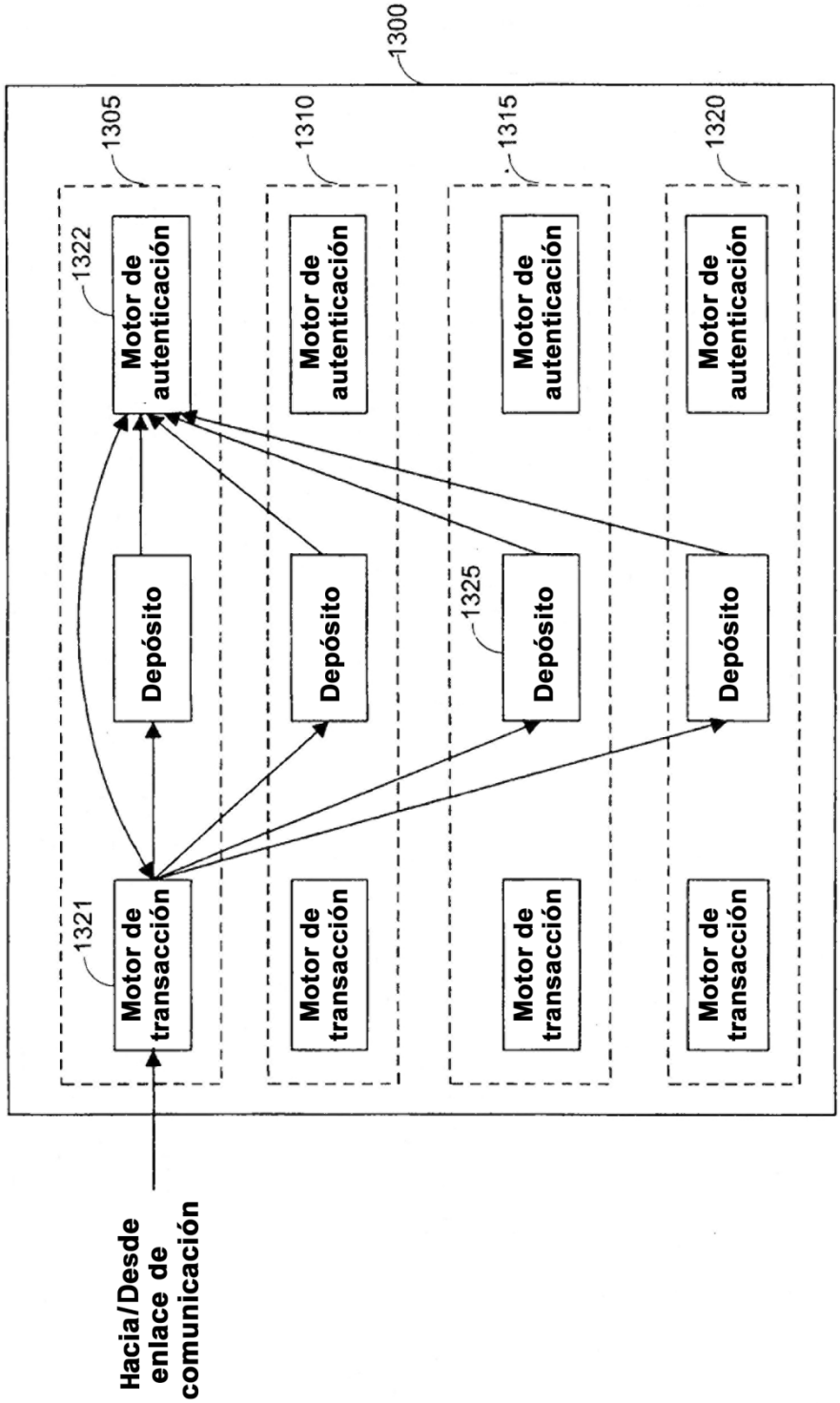

1300
1305
1310
1315
1320
1322
1321
1325
Motor de autenticación
Depósito
Motor de transacción
Hacia/Desde enlace de comunicación

FIG. 13

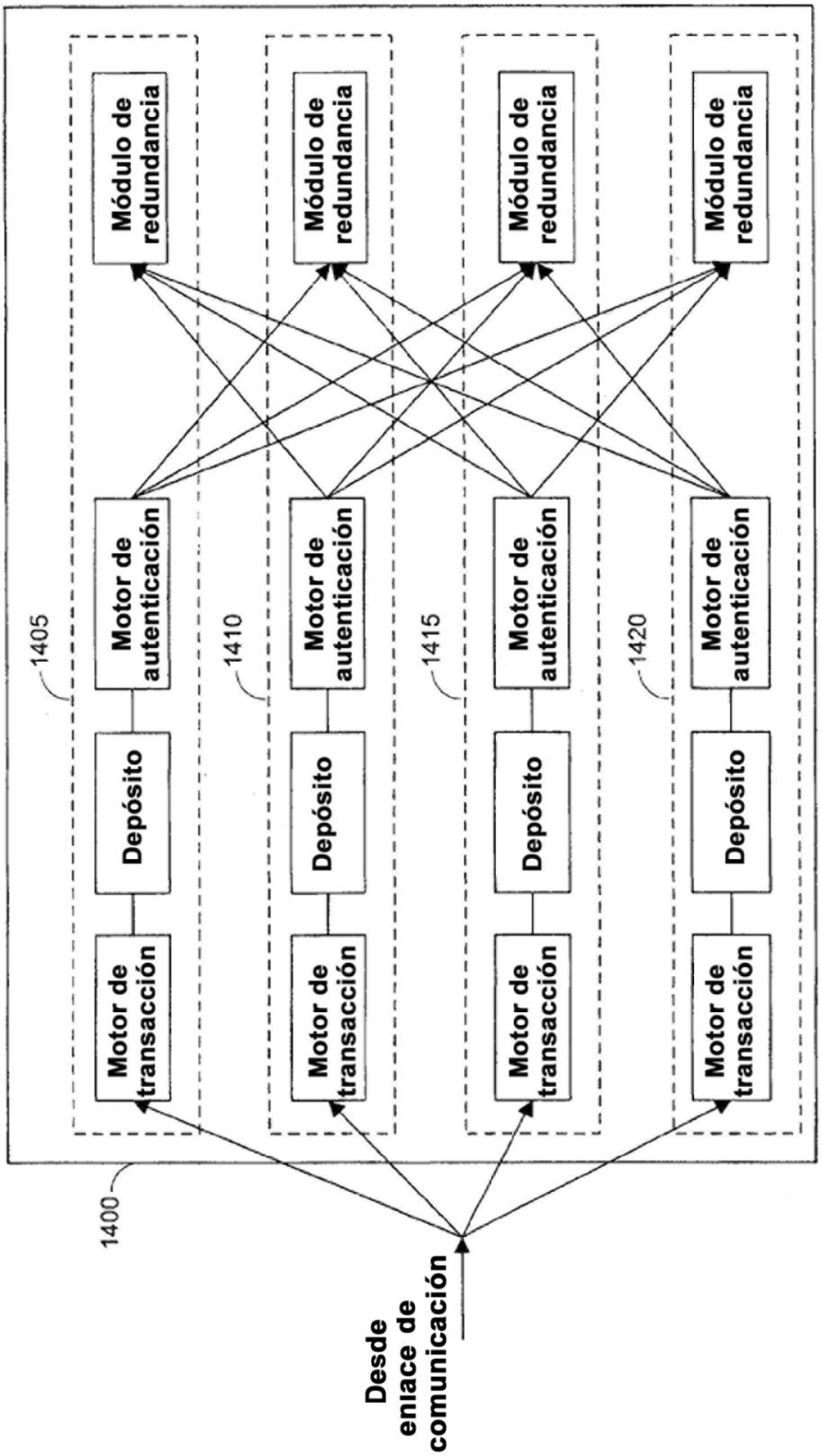

Desde enlace de comunicación
1400
1405
1410
1415
1420
Motor de transacción
Depósito
Motor de autenticación
Módulo de redundancia

FIG. 14

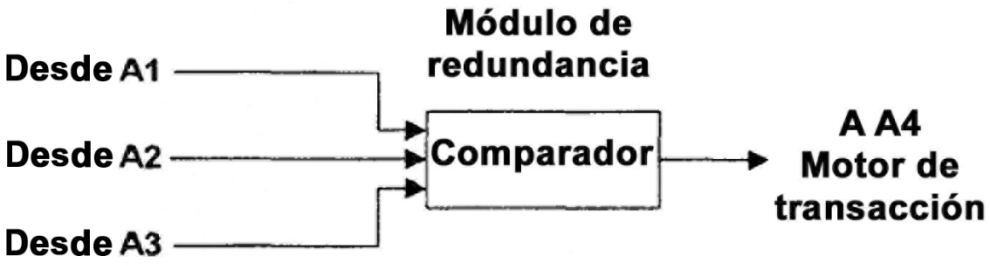

Módulo de redundancia
Desde A1
Desde A2
Desde A3
Comparador
A A4 Motor de transacción

FIG. 15

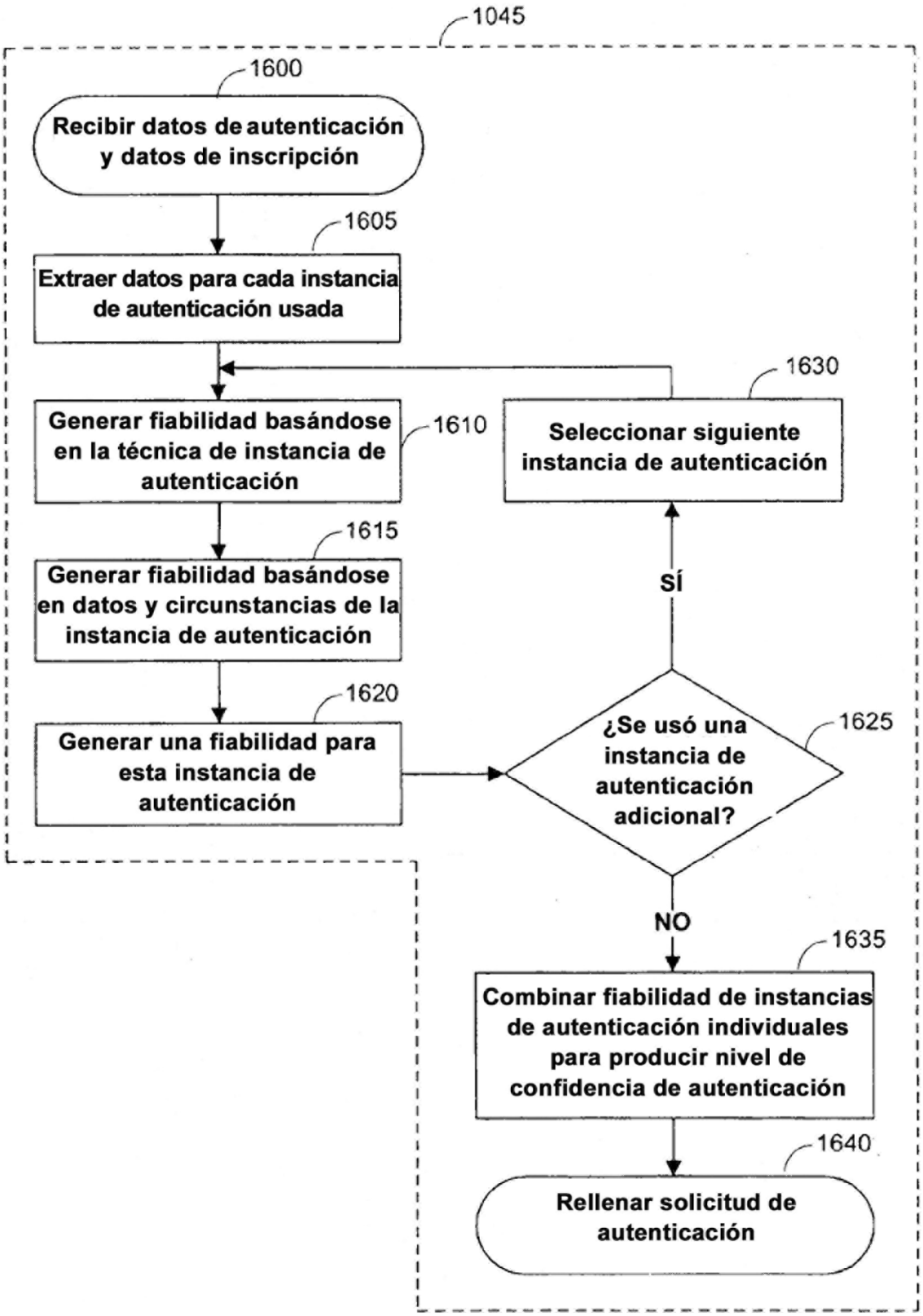

1045
1600
Recibir datos de autenticación y datos de inscripción
1605
Extraer datos para cada instancia de autenticación usada
1610
Generar fiabilidad basándose en la técnica de instancia de autenticación
1615
Generar fiabilidad basándose en datos y circunstancias de la instancia de autenticación
1620
Generar una fiabilidad para esta instancia de autenticación
1625
¿Se usó una instancia de autenticación adicional?
SÍ
1630
Seleccionar siguiente instancia de autenticación
NO
1635
Combinar fiabilidad de instancias de autenticación individuales para producir nivel de confidencia de autenticación
1640
Rellenar solicitud de autenticación

FIG. 16

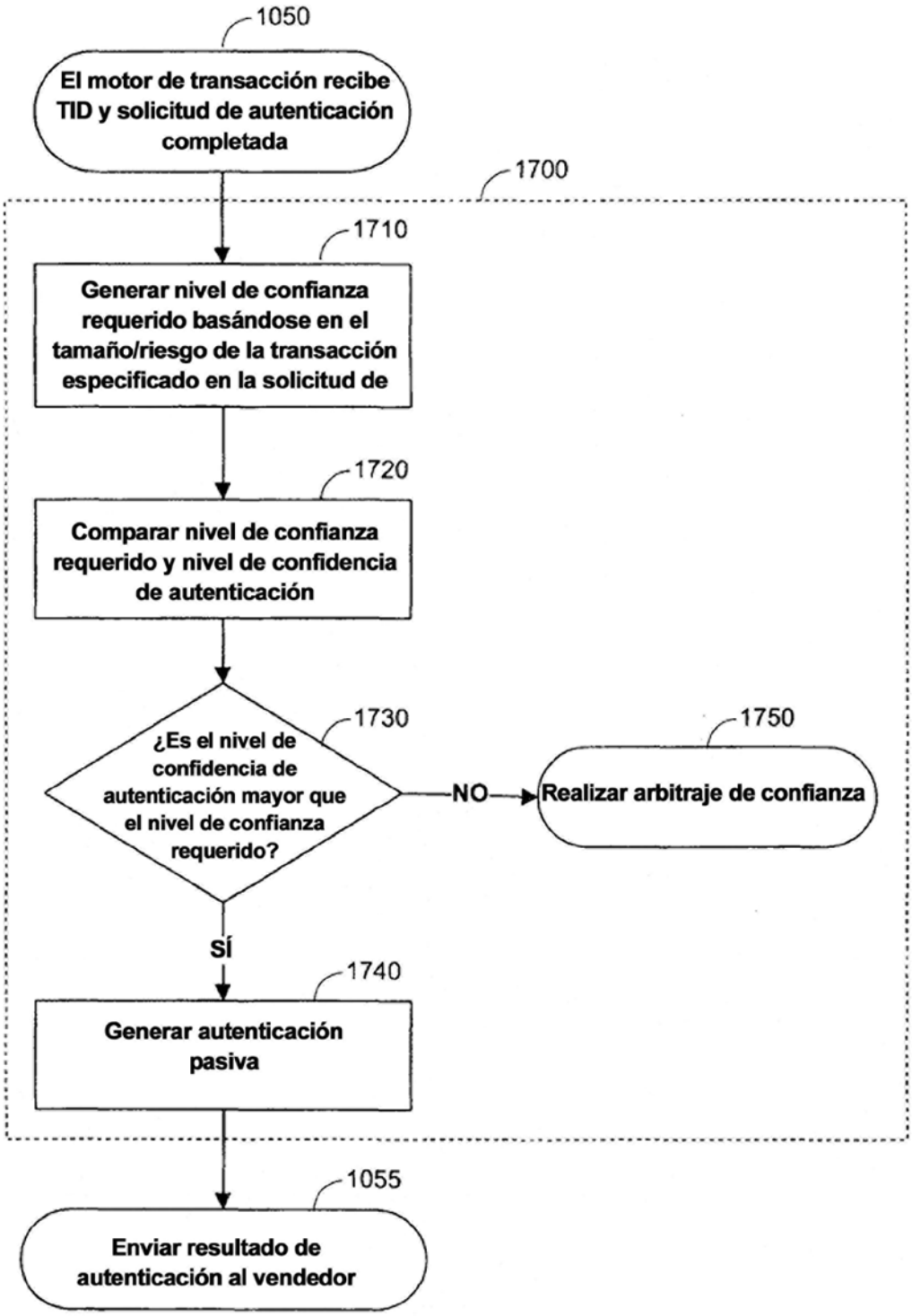

1050
El motor de transacción recibe TID y solicitud de autenticación completada
1700
1710
Generar nivel de confianza requerido basándose en el tamaño/riesgo de la transacción especificado en la solicitud de
1720
Comparar nivel de confianza requerido y nivel de confidencia de autenticación
1730
¿Es el nivel de confidencia de autenticación mayor que el nivel de confianza requerido?
NO
1750
Realizar arbitraje de confianza
SÍ
1740
Generar autenticación pasiva
1055
Enviar resultado de autenticación al vendedor

FIG. 17

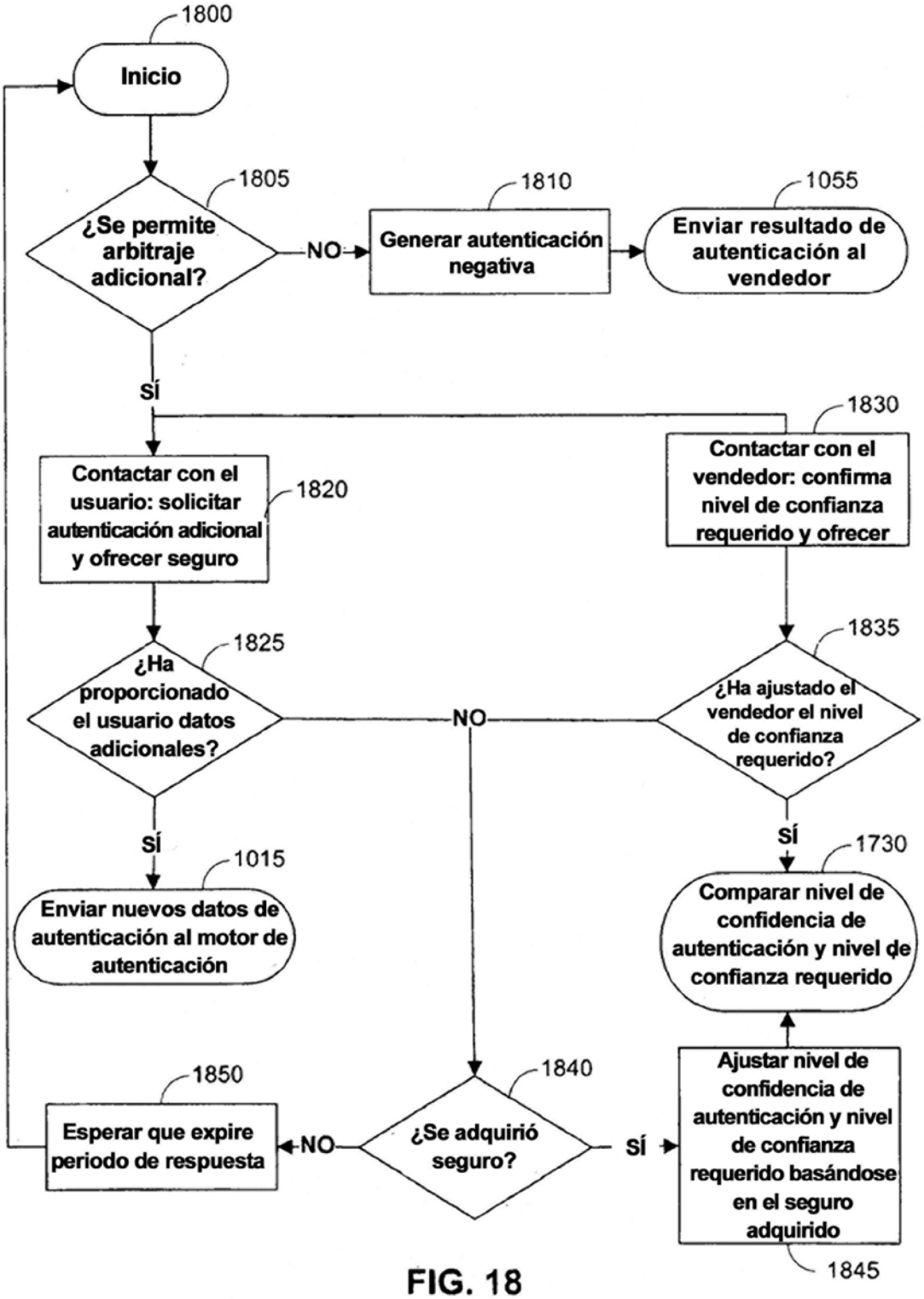

1800
Inicio
1805
¿Se permite arbitraje adicional?
NO
1810
Generar autenticación negativa
1055
Enviar resultado de autenticación al vendedor
SÍ
1830
Contactar con el vendedor: confirma nivel de confianza requerido y ofrecer
Contactar con el usuario: solicitar autenticación adicional y ofrecer seguro
1820
1825
¿Ha proporcionado el usuario datos adicionales?
NO
1835
¿Ha ajustado el vendedor el nivel de confianza requerido?
SÍ
1730
Comparar nivel de confidencia de autenticación y nivel de confianza requerido
SÍ
1015
Enviar nuevos datos de autenticación al motor de autenticación
1840
¿Se adquirió seguro?
NO
1850
Esperar que expire periodo de respuesta
SÍ
Ajustar nivel de confidencia de autenticación y nivel de confianza requerido basándose en el seguro adquirido
1845

FIG. 18

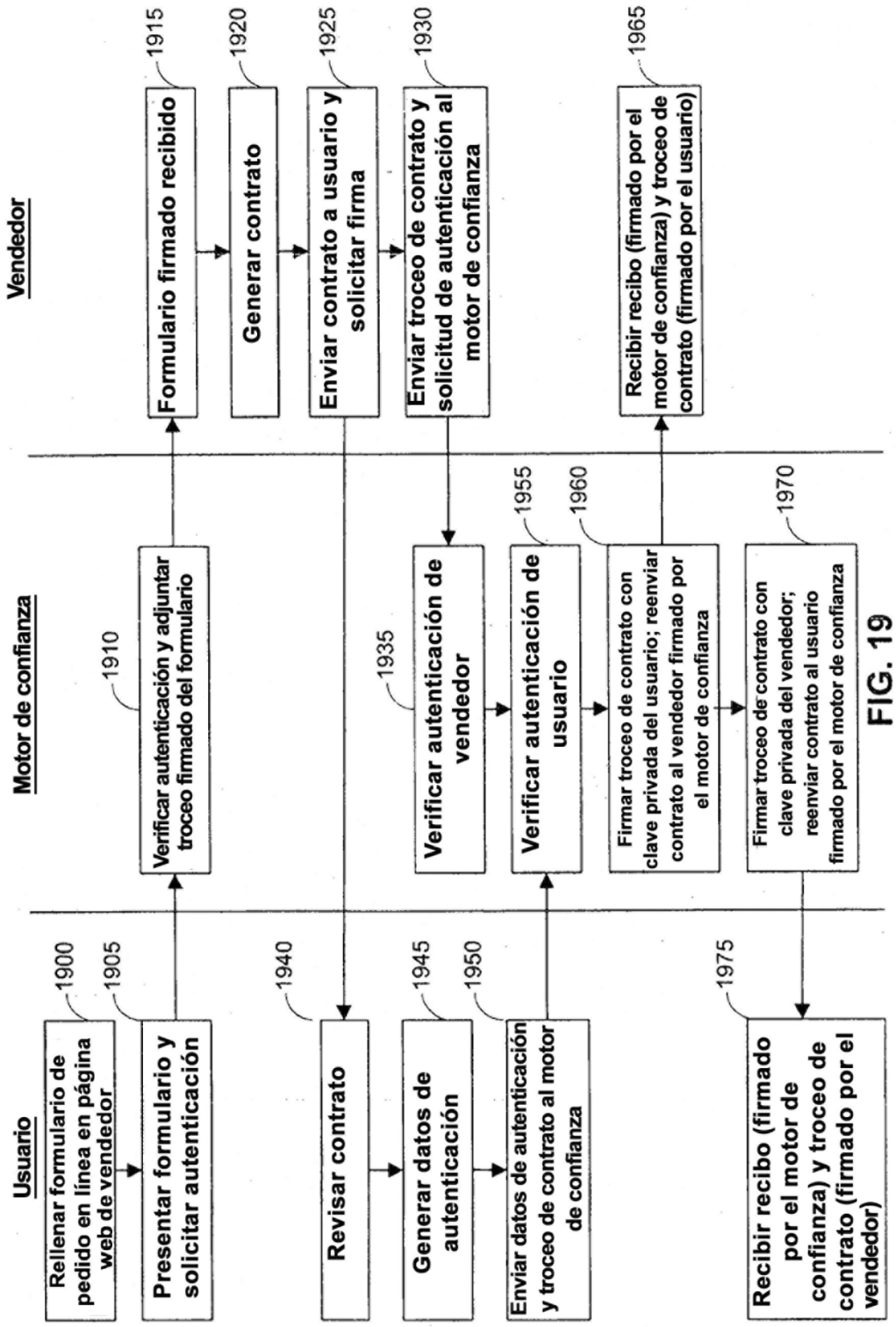

Usuario
Motor de confianza
Vendedor
Rellenar formulario de pedido en línea en página web de vendedor
1900
Presentar formulario y solicitar autenticación
1905
Verificar autenticación y adjuntar troceo firmado del formulario
1910
Formulario firmado recibido
1915
Generar contrato
1920
Enviar contrato a usuario y solicitar firma
1925
Enviar troceo de contrato y solicitud de autenticación al motor de confianza
1930
Verificar autenticación de vendedor
1935
Revisar contrato
1940
Generar datos de autenticación
1945
Enviar datos de autenticación y troceo de contrato al motor de confianza
1950
Verificar autenticación de usuario
1955
Firmar troceo de contrato con clave privada del usuario; reenviar contrato al vendedor firmado por el motor de confianza
1960
Recibir recibo (firmado por el motor de confianza) y troceo de contrato (firmado por el usuario)
1965
Firmar troceo de contrato con clave privada del vendedor; reenviar contrato al usuario firmado por el motor de confianza
1970
Recibir recibo (firmado por el motor de confianza) y troceo de contrato (firmado por el vendedor)
1975

FIG. 19

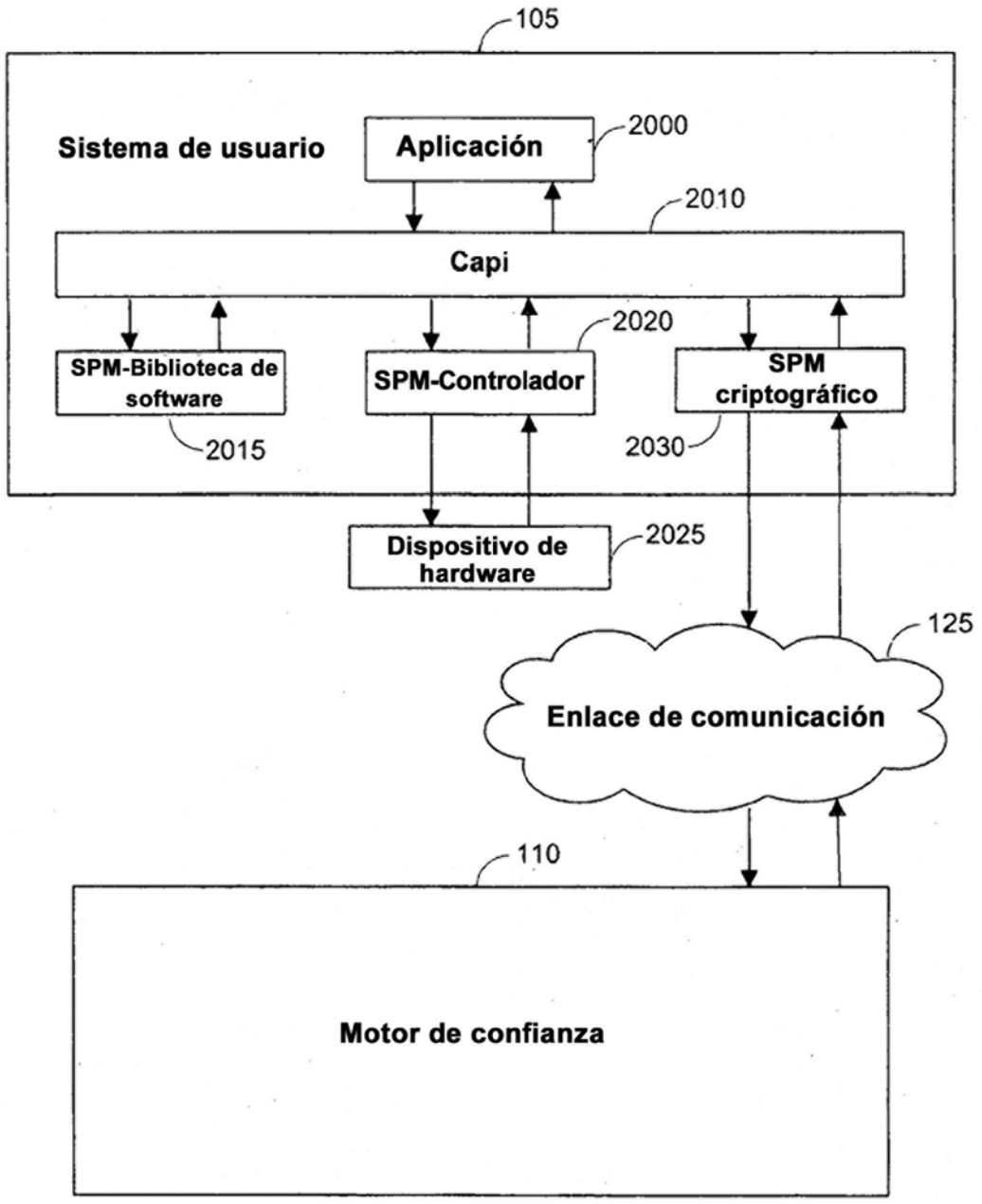

105
Sistema de usuario
Aplicación
2000
2010
Capi
2020
SPM-Biblioteca de software
SPM-Controlador
SPM criptográfico
2015
2030
Dispositivo de hardware
2025
125
Enlace de comunicación
110
Motor de confianza

FIG. 20

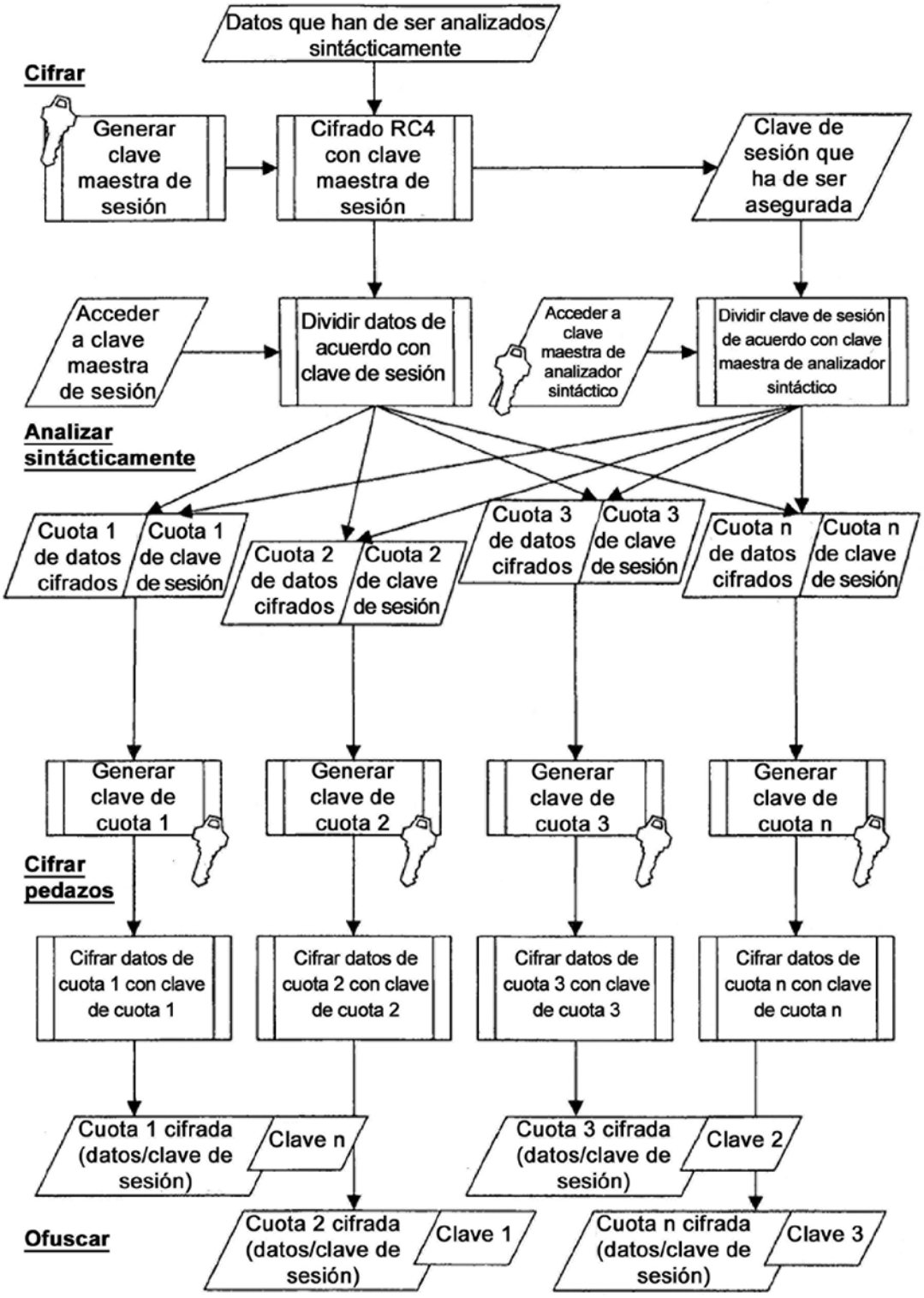

Datos que han de ser analizados sintácticamente
Cifrar
Generar clave maestra de sesión
Cifrado RC4 con clave maestra de sesión
Clave de sesión que ha de ser asegurada
Acceder a clave maestra de sesión
Dividir datos de acuerdo con clave de sesión
Acceder a clave maestra de analizador sintáctico
Dividir clave de sesión de acuerdo con clave maestra de analizador sintáctico
Analizar sintácticamente
Cuota 1 de datos cifrados
Cuota 1 de clave de sesión
Cuota 2 de datos cifrados
Cuota 2 de clave de sesión
Cuota 3 de datos cifrados
Cuota 3 de clave de sesión
Cuota n de datos cifrados
Cuota n de clave de sesión
Generar clave de cuota 1
Generar clave de cuota 2
Generar clave de cuota 3
Generar clave de cuota n
Cifrar pedazos
Cifrar datos de cuota 1 con clave de cuota 1
Cifrar datos de cuota 2 con clave de cuota 2
Cifrar datos de cuota 3 con clave de cuota 3
Cifrar datos de cuota n con clave de cuota n
Cuota 1 cifrada (datos/clave de sesión)
Clave n
Cuota 3 cifrada (datos/clave de sesión)
Clave 2
Ofuscar
Cuota 2 cifrada (datos/clave de sesión)
Clave 1
Cuota n cifrada (datos/clave de sesión)
Clave 3

FIG. 21

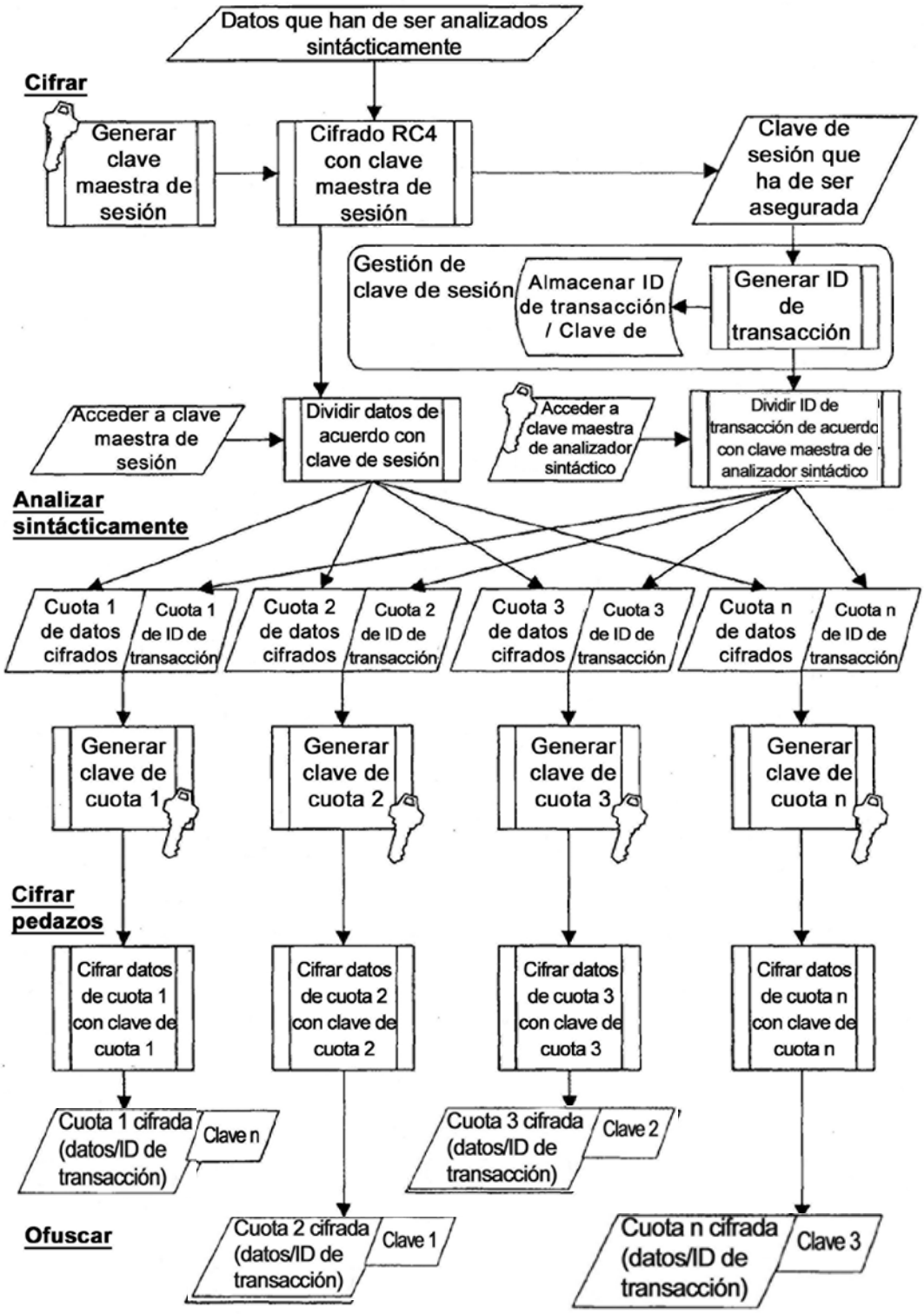

Datos que han de ser analizados sintácticamente
Cifrar
Generar clave maestra de sesión
Cifrado RC4 con clave maestra de sesión
Clave de sesión que ha de ser asegurada
Gestión de clave de sesión
Almacenar ID de transacción / Clave de
Generar ID de transacción
Acceder a clave maestra de sesión
Dividir datos de acuerdo con clave de sesión
Acceder a clave maestra de analizador sintáctico
Dividir ID de transacción de acuerdo con clave maestra de analizador sintáctico
Analizar sintácticamente
Cuota 1 de datos cifrados
Cuota 1 de ID de transacción
Cuota 2 de datos cifrados
Cuota 2 de ID de transacción
Cuota 3 de datos cifrados
Cuota 3 de ID de transacción
Cuota n de datos cifrados
Cuota n de ID de transacción
Generar clave de cuota 1
Generar clave de cuota 2
Generar clave de cuota 3
Generar clave de cuota n
Cifrar pedazos
Cifrar datos de cuota 1 con clave de cuota 1
Cifrar datos de cuota 2 con clave de cuota 2
Cifrar datos de cuota 3 con clave de cuota 3
Cifrar datos de cuota n con clave de cuota n
Cuota 1 cifrada (datos/ID de transacción)
Clave n
Cuota 3 cifrada (datos/ID de transacción)
Clave 2
Ofuscar
Cuota 2 cifrada (datos/ID de transacción)
Clave 1
Cuota n cifrada (datos/ID de transacción)
Clave 3

FIG. 22

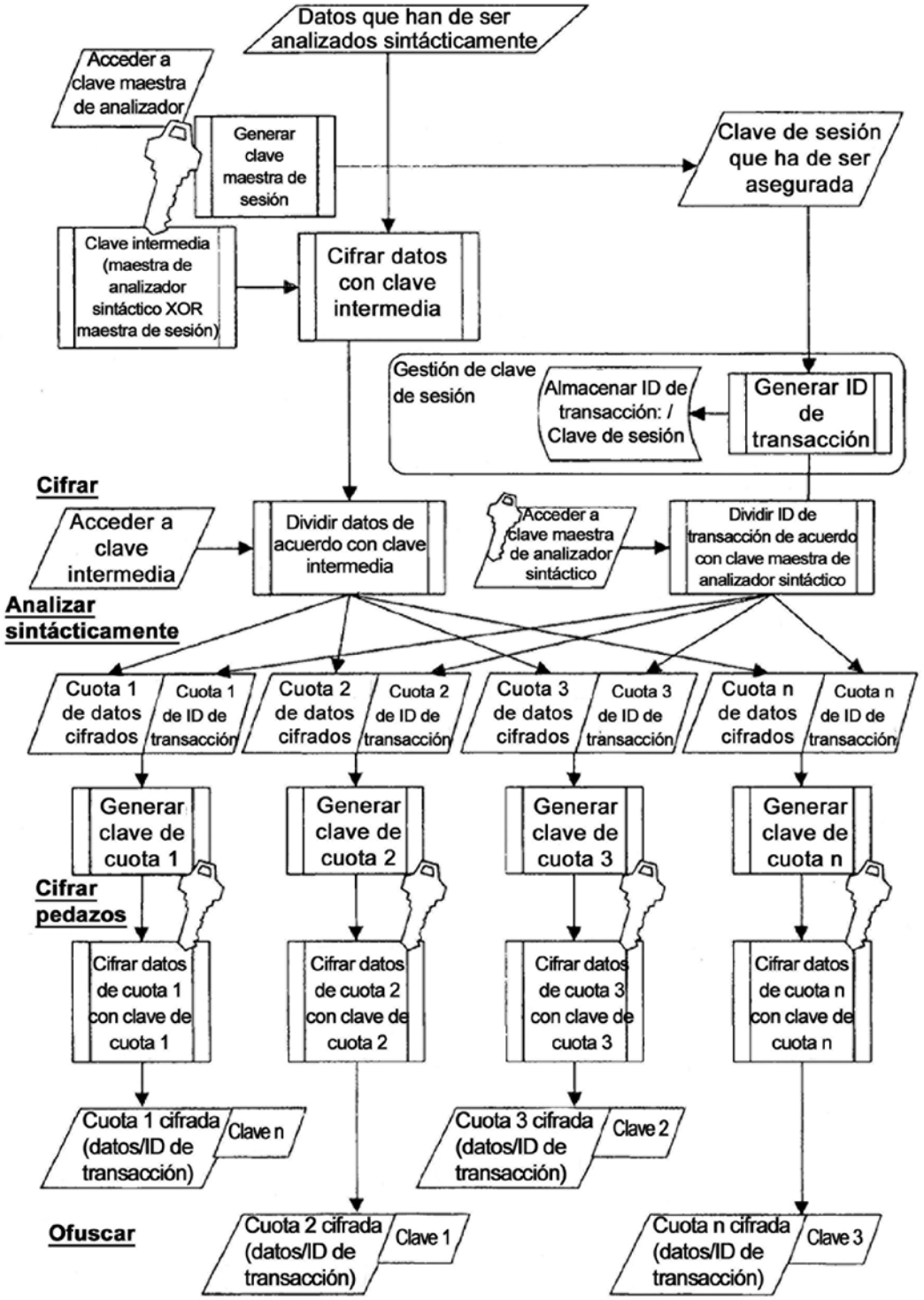

Datos que han de ser analizados sintácticamente
Acceder a clave maestra de analizador
Generar clave maestra de sesión
Clave de sesión que ha de ser asegurada
Clave intermedia (maestra de analizador sintáctico XOR maestra de sesión)
Cifrar datos con clave intermedia
Gestión de clave de sesión
Almacenar ID de transacción: / Clave de sesión
Generar ID de transacción
Cifrar
Acceder a clave intermedia
Dividir datos de acuerdo con clave intermedia
Acceder a clave maestra de analizador sintáctico
Dividir ID de transacción de acuerdo con clave maestra de analizador sintáctico
Analizar sintácticamente
Cuota 1 de datos cifrados
Cuota 1 de ID de transacción
Cuota 2 de datos cifrados
Cuota 2 de ID de transacción
Cuota 3 de datos cifrados
Cuota 3 de ID de transacción
Cuota n de datos cifrados
Cuota n de ID de transacción
Generar clave de cuota 1
Generar clave de cuota 2
Generar clave de cuota 3
Generar clave de cuota n
Cifrar pedazos
Cifrar datos de cuota 1 con clave de cuota 1
Cifrar datos de cuota 2 con clave de cuota 2
Cifrar datos de cuota 3 con clave de cuota 3
Cifrar datos de cuota n con clave de cuota n
Cuota 1 cifrada (datos/ID de transacción)
Clave n
Cuota 3 cifrada (datos/ID de transacción)
Clave 2
Ofuscar
Cuota 2 cifrada (datos/ID de transacción)
Clave 1
Cuota n cifrada (datos/ID de transacción)
Clave 3

FIG. 23

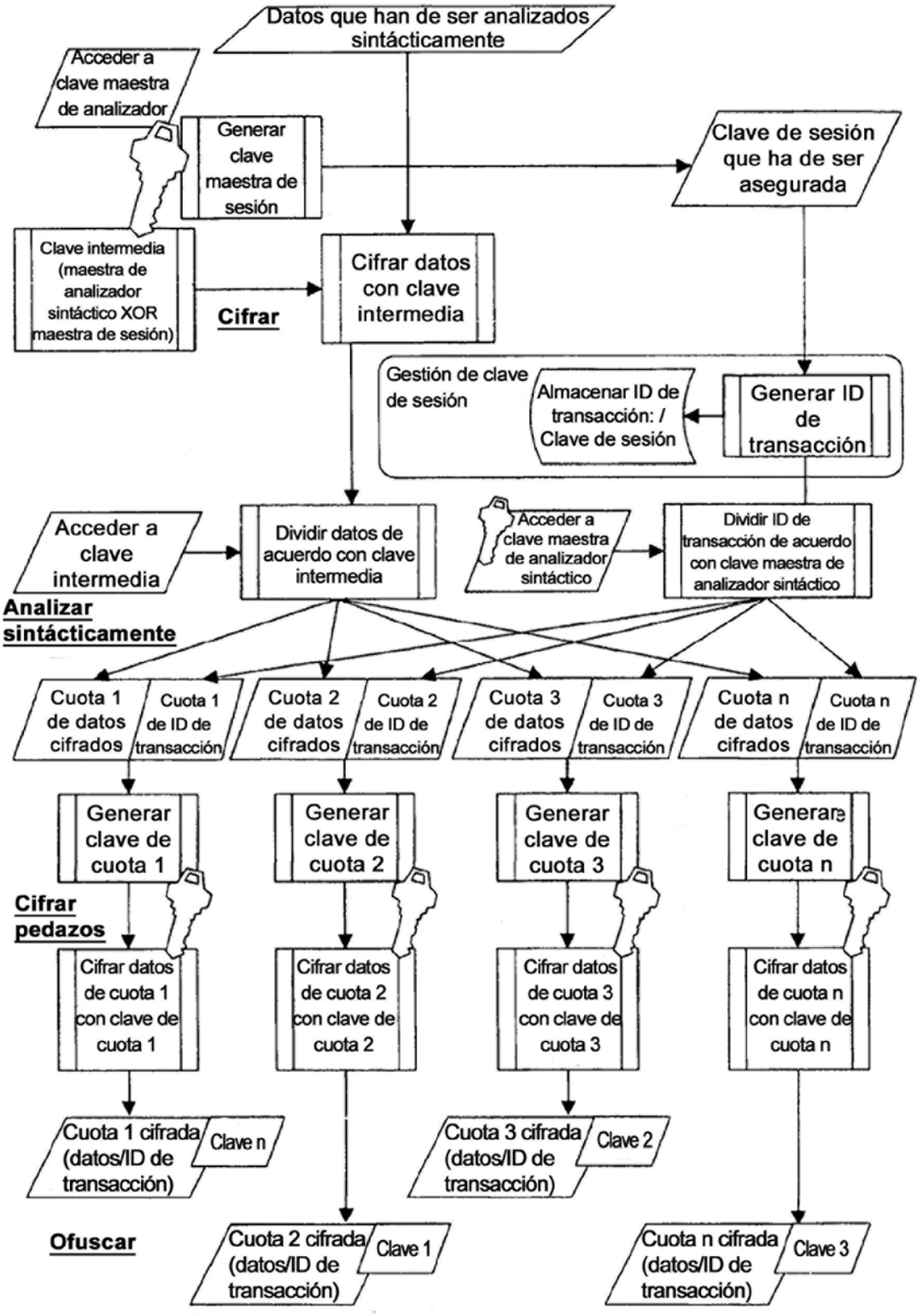

Datos que han de ser analizados sintácticamente
Acceder a clave maestra de analizador
Generar clave maestra de sesión
Clave de sesión que ha de ser asegurada
Clave intermedia (maestra de analizador sintáctico XOR maestra de sesión)
Cifrar
Cifrar datos con clave intermedia
Gestión de clave de sesión
Almacenar ID de transacción: / Clave de sesión
Generar ID de transacción
Acceder a clave intermedia
Analizar sintácticamente
Dividir datos de acuerdo con clave intermedia
Acceder a clave maestra de analizador sintáctico
Dividir ID de transacción de acuerdo con clave maestra de analizador sintáctico
Cuota 1 de datos cifrados
Cuota 1 de ID de transacción
Cuota 2 de datos cifrados
Cuota 2 de ID de transacción
Cuota 3 de datos cifrados
Cuota 3 de ID de transacción
Cuota n de datos cifrados
Cuota n de ID de transacción
Generar clave de cuota 1
Generar clave de cuota 2
Generar clave de cuota 3
Generare clave de cuota n
Cifrar pedazos
Cifrar datos de cuota 1 con clave de cuota 1
Cifrar datos de cuota 2 con clave de cuota 2
Cifrar datos de cuota 3 con clave de cuota 3
Cifrar datos de cuota n con clave de cuota n
Cuota 1 cifrada (datos/ID de transacción)
Clave n
Cuota 3 cifrada (datos/ID de transacción)
Clave 2
Ofuscar
Cuota 2 cifrada (datos/ID de transacción)
Clave 1
Cuota n cifrada (datos/ID de transacción)
Clave 3

FIG. 24

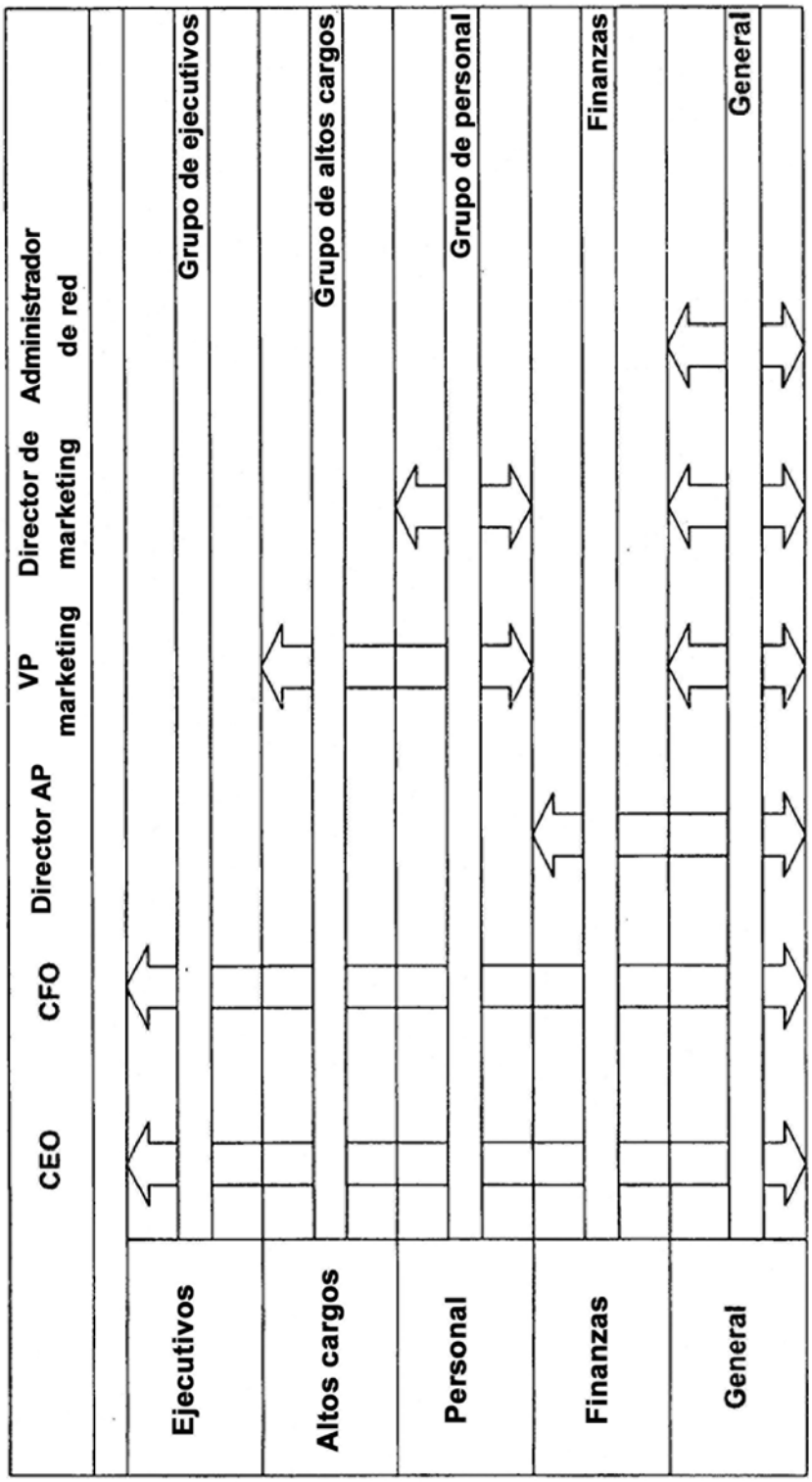

CEO
CFO
Director AP
VP marketing
Director de marketing
Administrador de red
Ejecutivos
Grupo de ejecutivos
Altos cargos
Grupo de altos cargos
Personal
Grupo de personal
Finanzas
Finanzas
General
General

FIG. 25

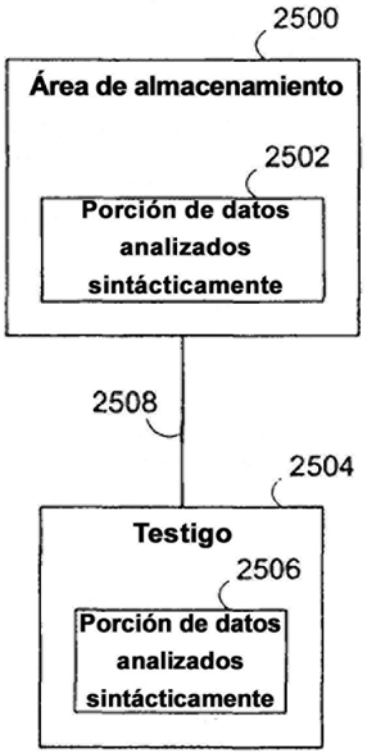

2500
Área de almacenamiento
2502
Porción de datos analizados sintácticamente
2508
2504
Testigo
2506
Porción de datos analizados sintácticamente

FIG. 26

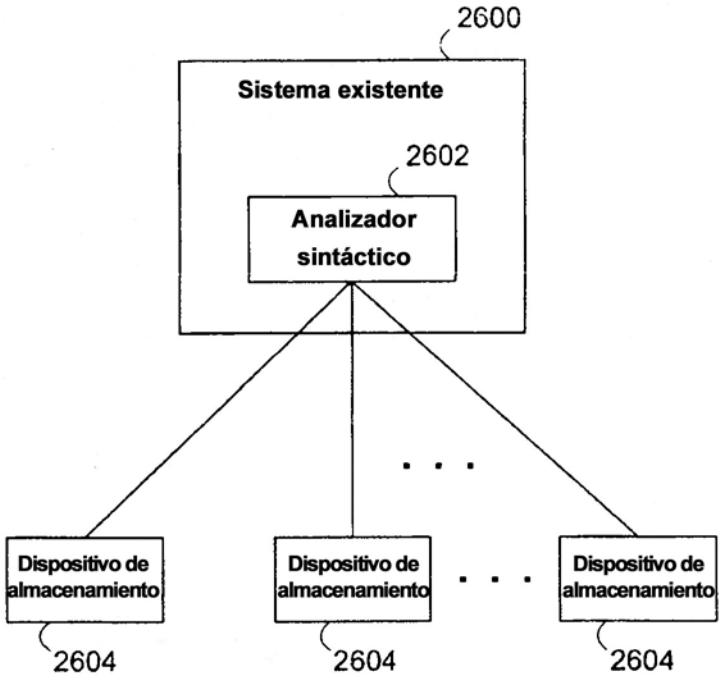

2600
Sistema existente
2602
Analizador sintáctico
Dispositivo de almacenamiento
2604
Dispositivo de almacenamiento
2604
Dispositivo de almacenamiento
2604

FIG. 27

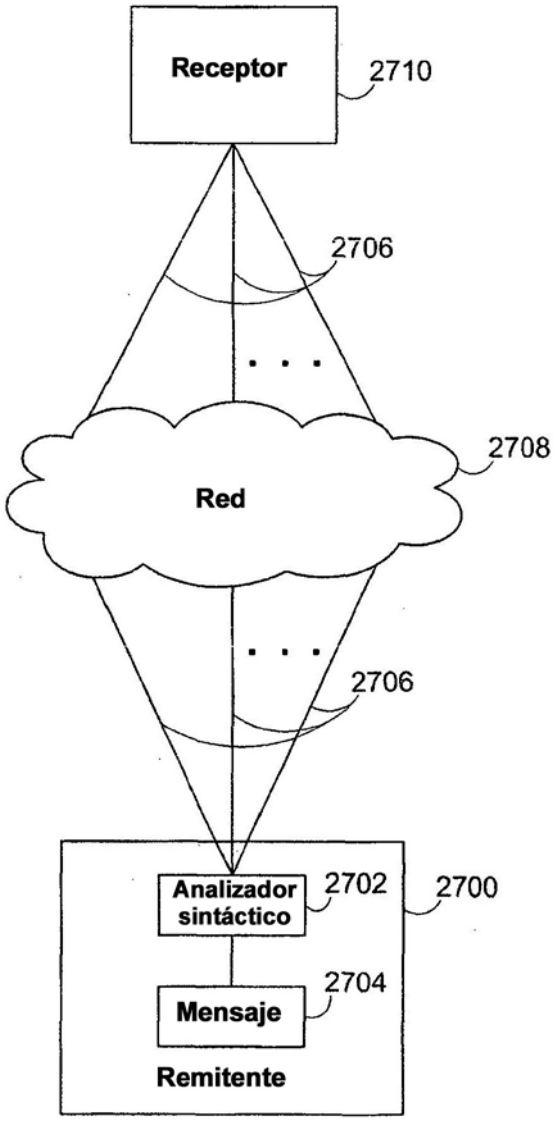

Receptor
2710
2706
2708
Red
2706
Analizador sintáctico
2702
2700
2704
Mensaje
Remitente

FIG. 28

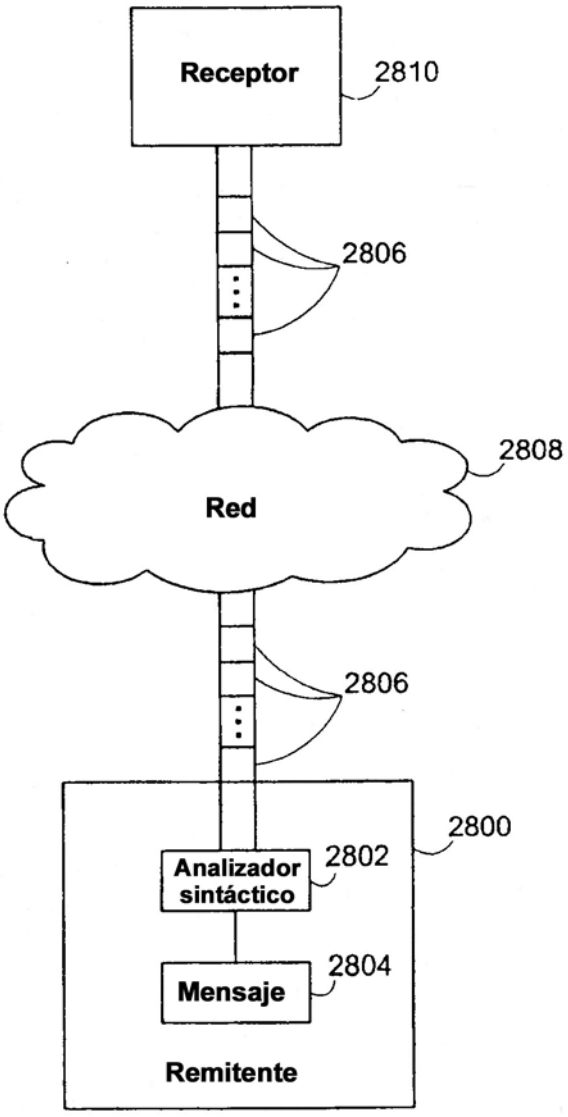

Receptor
2810
2806
2808
Red
2806
2800
Analizador sintáctico
2802
Mensaje
2804
Remitente

FIG. 29

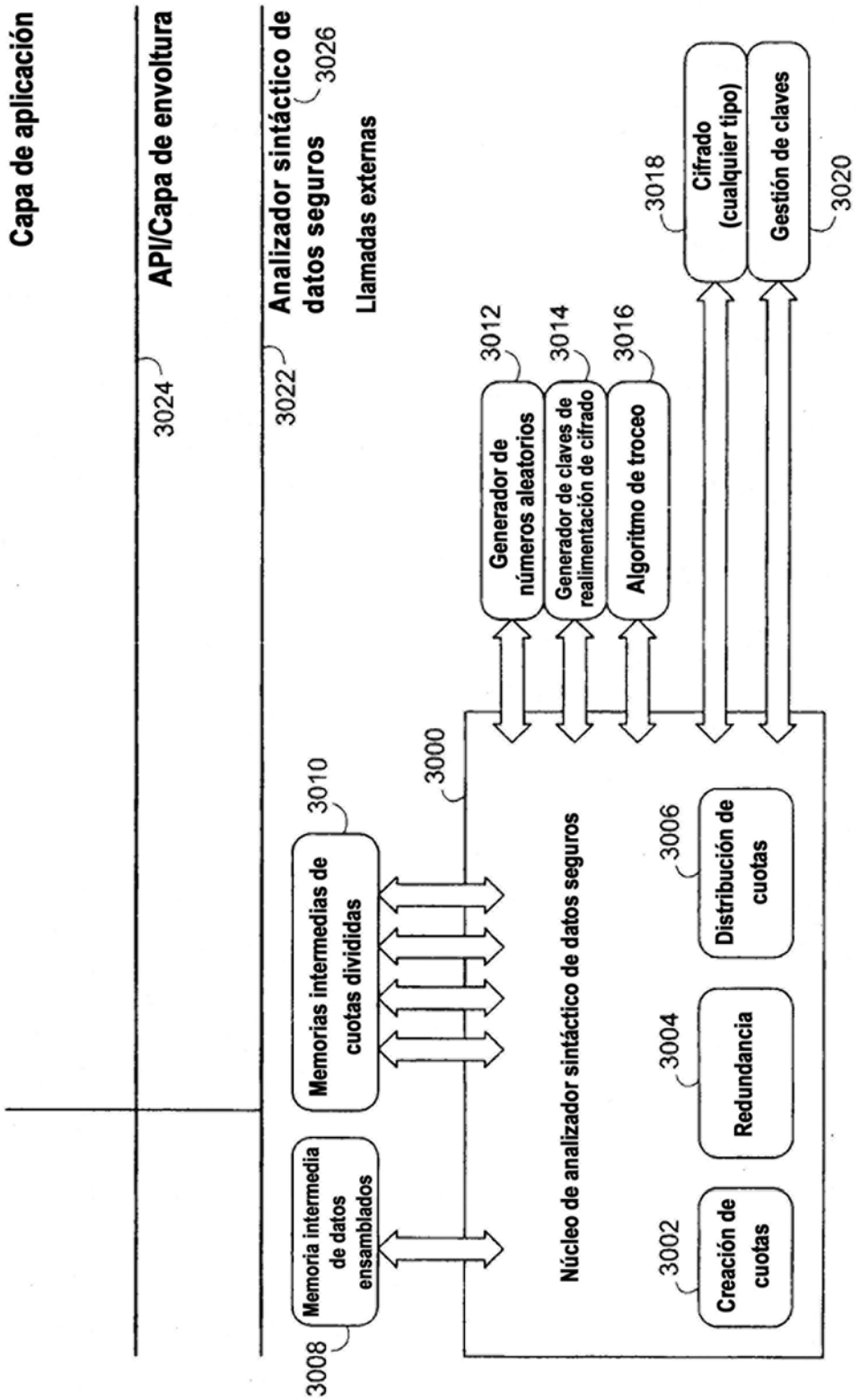

Capa de aplicación
API/Capa de envoltura
3024
3022
Analizador sintáctico de datos seguros
3026
Llamadas externas
3012
Generador de números aleatorios
3014
Generador de claves de realimentación de cifrado
3016
Algoritmo de troceo
3018
Cifrado (cualquier tipo)
Gestión de claves
3020
3000
3010
Memorias intermedias de cuotas divididas
Núcleo de analizador sintáctico de datos seguros
3006
Distribución de cuotas
3004
Redundancia
3002
Creación de cuotas
3008
Memoria intermedia de datos ensamblados

FIG. 30

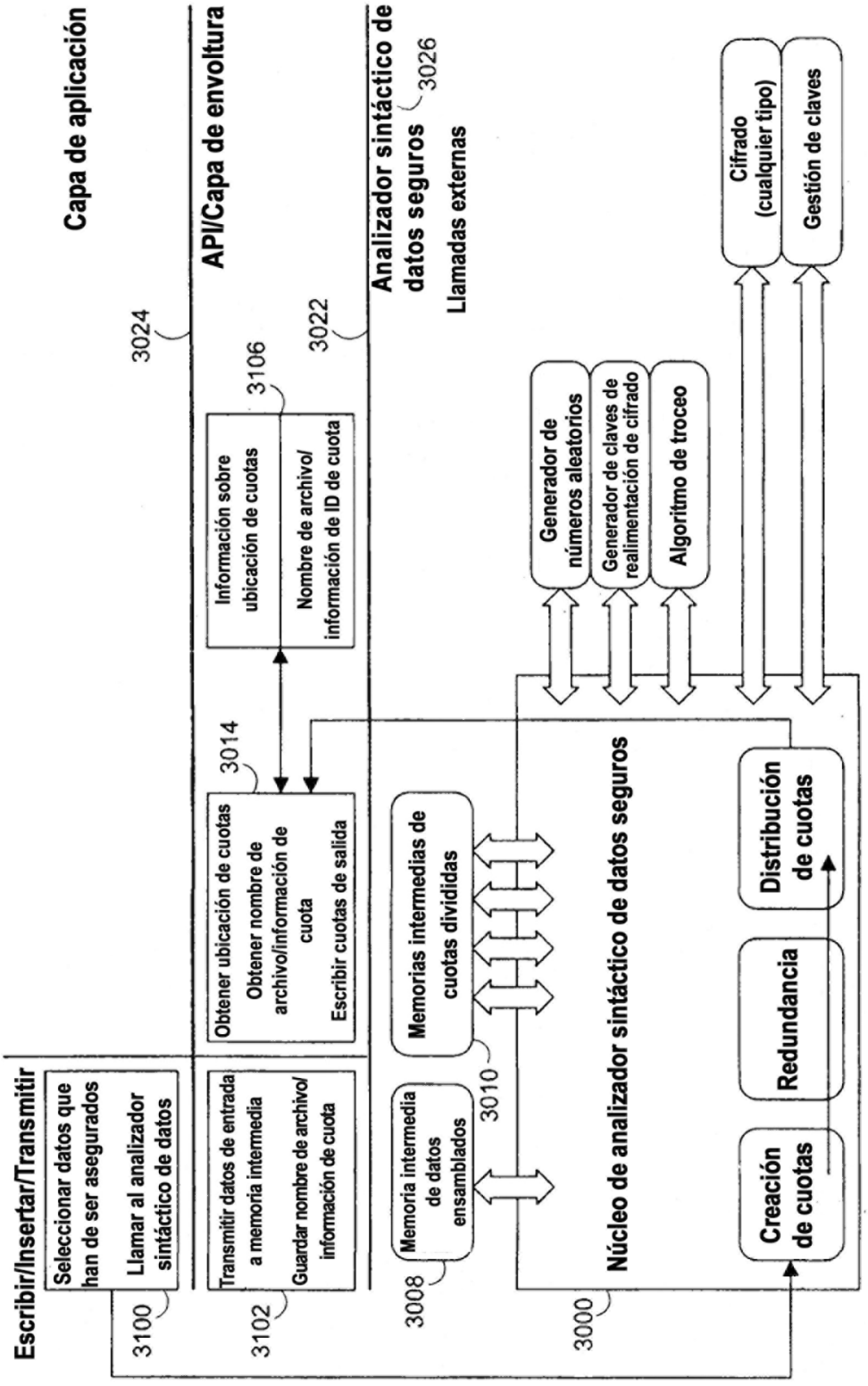

Capa de aplicación
API/Capa de envoltura
Analizador sintáctico de datos seguros
Llamadas externas
3024
3022
3026
3106
3014
3100
3102
3008
3010
3000
Escribir/Insertar/Transmitir
Seleccionar datos que han de ser asegurados
Llamar al analizador sintáctico de datos
Transmitir datos de entrada a memoria intermedia
Guardar nombre de archivo/ información de cuota
Obtener ubicación de cuotas
Obtener nombre de archivo/información de cuota
Escribir cuotas de salida
Información sobre ubicación de cuotas
Nombre de archivo/ información de ID de cuota
Memorias intermedias de cuotas divididas
Memoria intermedia de datos ensamblados
Núcleo de analizador sintáctico de datos seguros
Creación de cuotas
Redundancia
Distribución de cuotas
Generador de números aleatorios
Generador de claves de realimentación de cifrado
Algoritmo de troceo
Cifrado (cualquier tipo)
Gestión de claves

FIG. 31

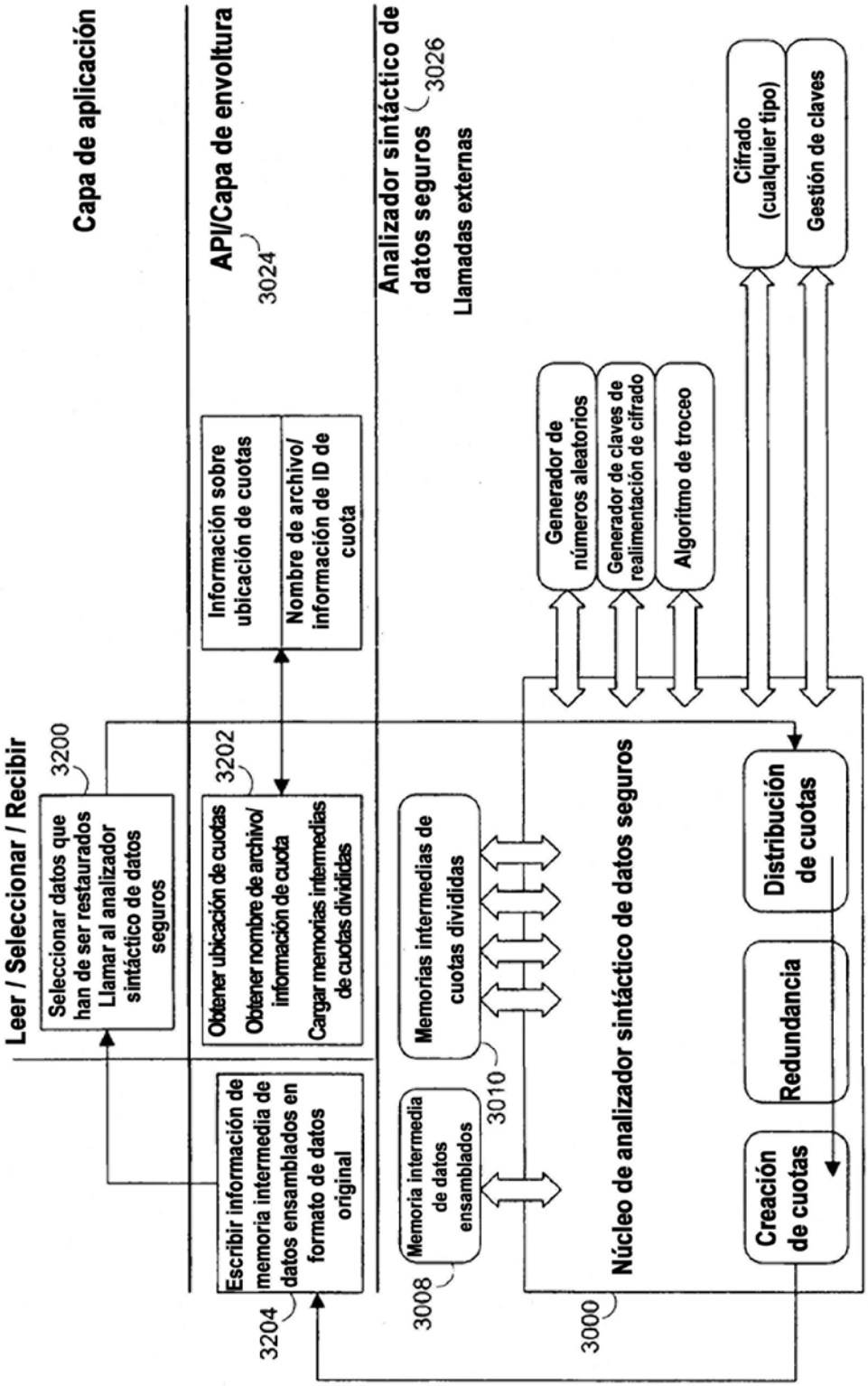

Capa de aplicación
API/Capa de envoltura
3024
Analizador sintáctico de datos seguros
3026
Llamadas externas
Leer / Seleccionar / Recibir
3200
Seleccionar datos que han de ser restaurados
Llamar al analizador sintáctico de datos seguros
3202
Obtener ubicación de cuotas
Obtener nombre de archivo/ información de cuota
Cargar memorias intermedias de cuotas divididas
Información sobre ubicación de cuotas
Nombre de archivo/ información de ID de cuota
Escribir información de memoria intermedia de datos ensamblados en formato de datos original
3204
Memoria intermedia de datos ensamblados
3008
Memorias intermedias de cuotas divididas
3010
Generador de números aleatorios
Generador de claves de realimentación de cifrado
Algoritmo de troceo
Cifrado (cualquier tipo)
Gestión de claves
Núcleo de analizador sintáctico de datos seguros
3000
Distribución de cuotas
Redundancia
Creación de cuotas

FIG. 32

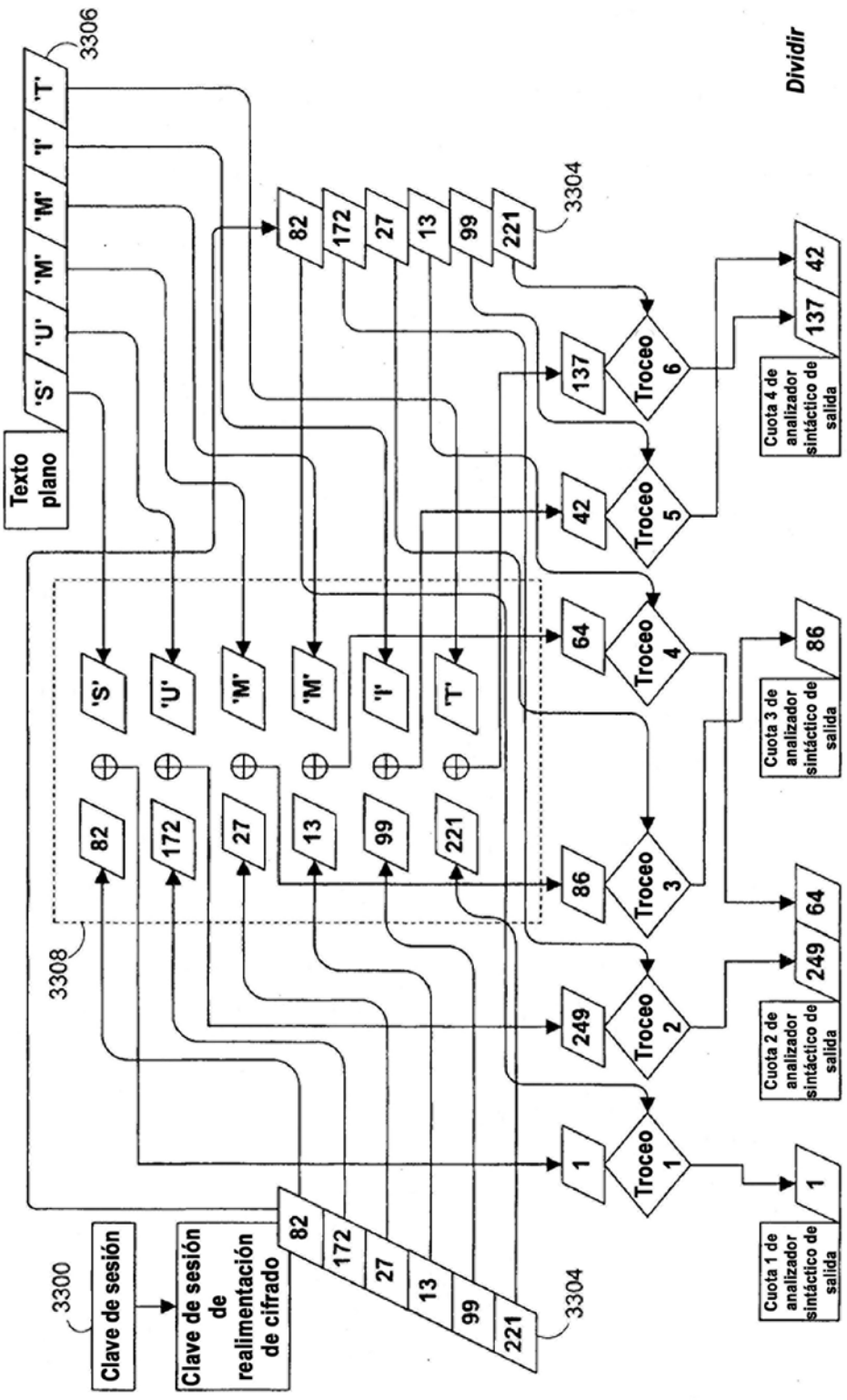

3306
Texto plano
'S' 'U' 'M' 'M' 'T' 'T'
3300
Clave de sesión
Clave de sesión de realimentación de cifrado
82 172 27 13 99 221
3304
3308
'S' 'U' 'M' 'M' 'I' 'T'
82 172 27 13 99 221
Dividir
Troceo 1
Troceo 2
Troceo 3
Troceo 4
Troceo 5
Troceo 6
1 249 86 64 42 137
Cuota 1 de analizador sintáctico de salida
Cuota 2 de analizador sintáctico de salida
Cuota 3 de analizador sintáctico de salida
Cuota 4 de analizador sintáctico de salida

FIG. 33

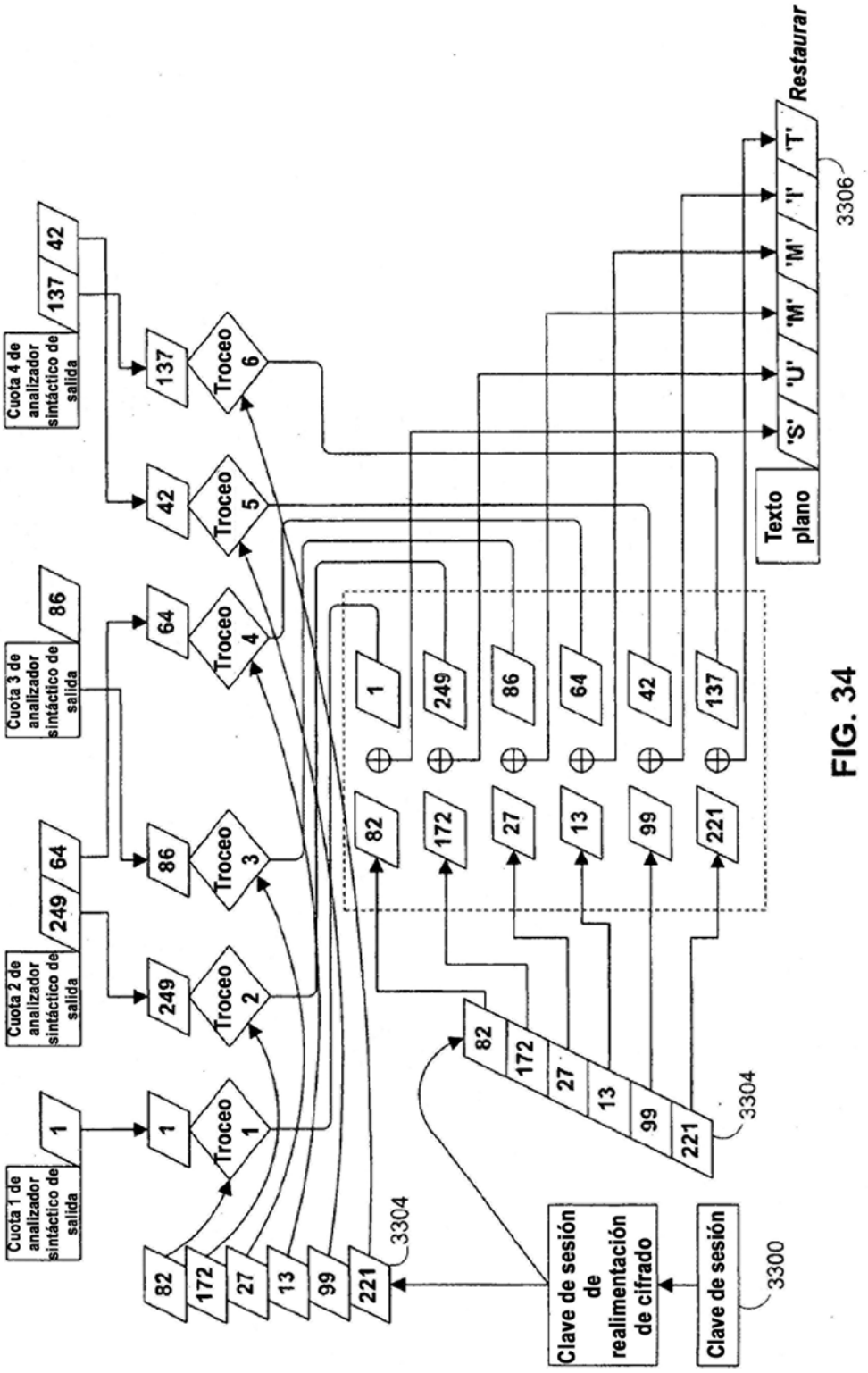

Cuota 1 de analizador sintáctico de salida
Cuota 2 de analizador sintáctico de salida
Cuota 3 de analizador sintáctico de salida
Cuota 4 de analizador sintáctico de salida
Troceo 1
Troceo 2
Troceo 3
Troceo 4
Troceo 5
Troceo 6
Clave de sesión de realimentación de cifrado
Clave de sesión
Texto plano
Restaurar
3300
3304
3306

FIG. 34

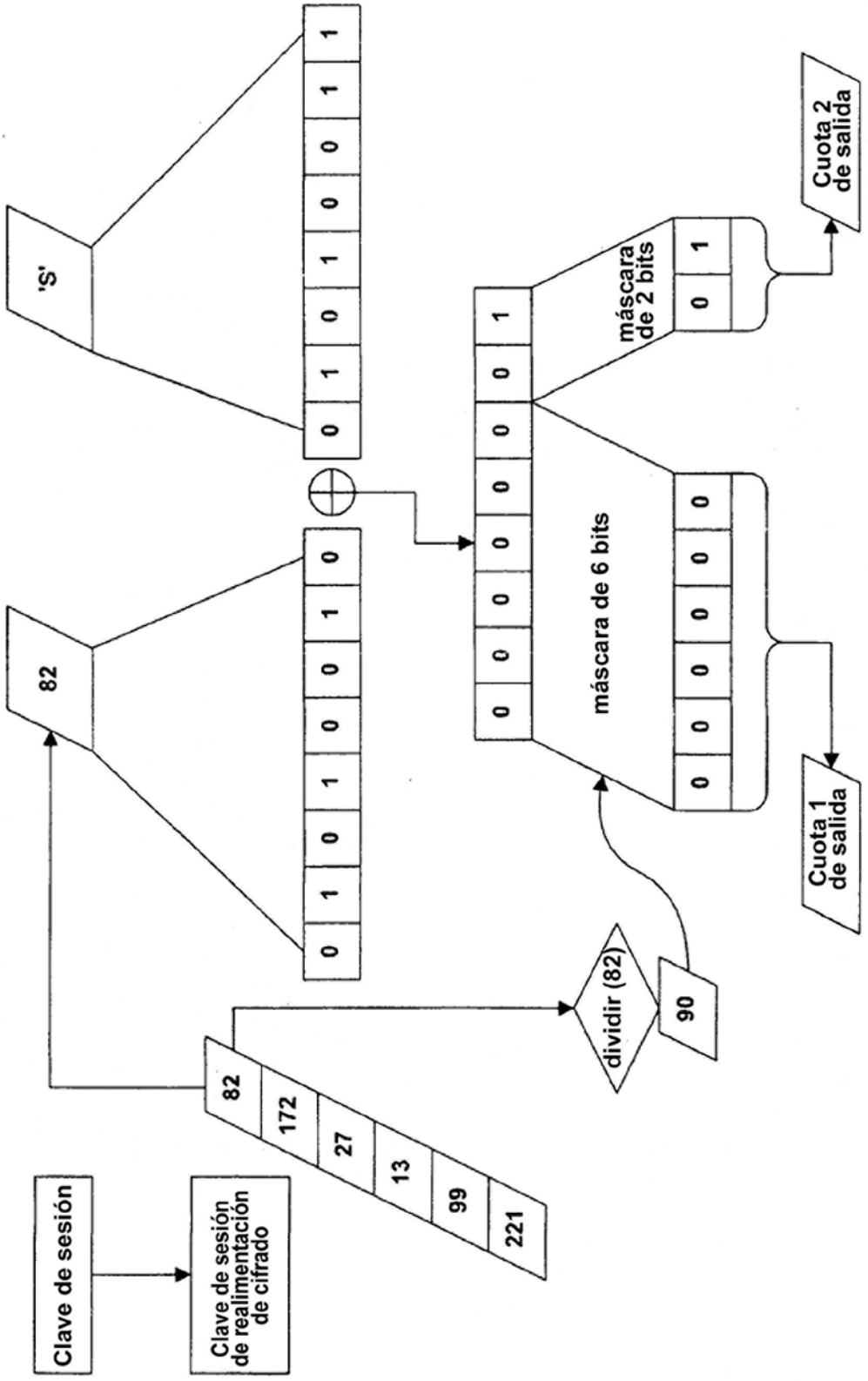

Clave de sesión
Clave de sesión de realimentación de cifrado
82
172
27
13
99
221
dividir (82)
90
82
'S'
máscara de 6 bits
máscara de 2 bits
Cuota 1 de salida
Cuota 2 de salida

FIG. 35

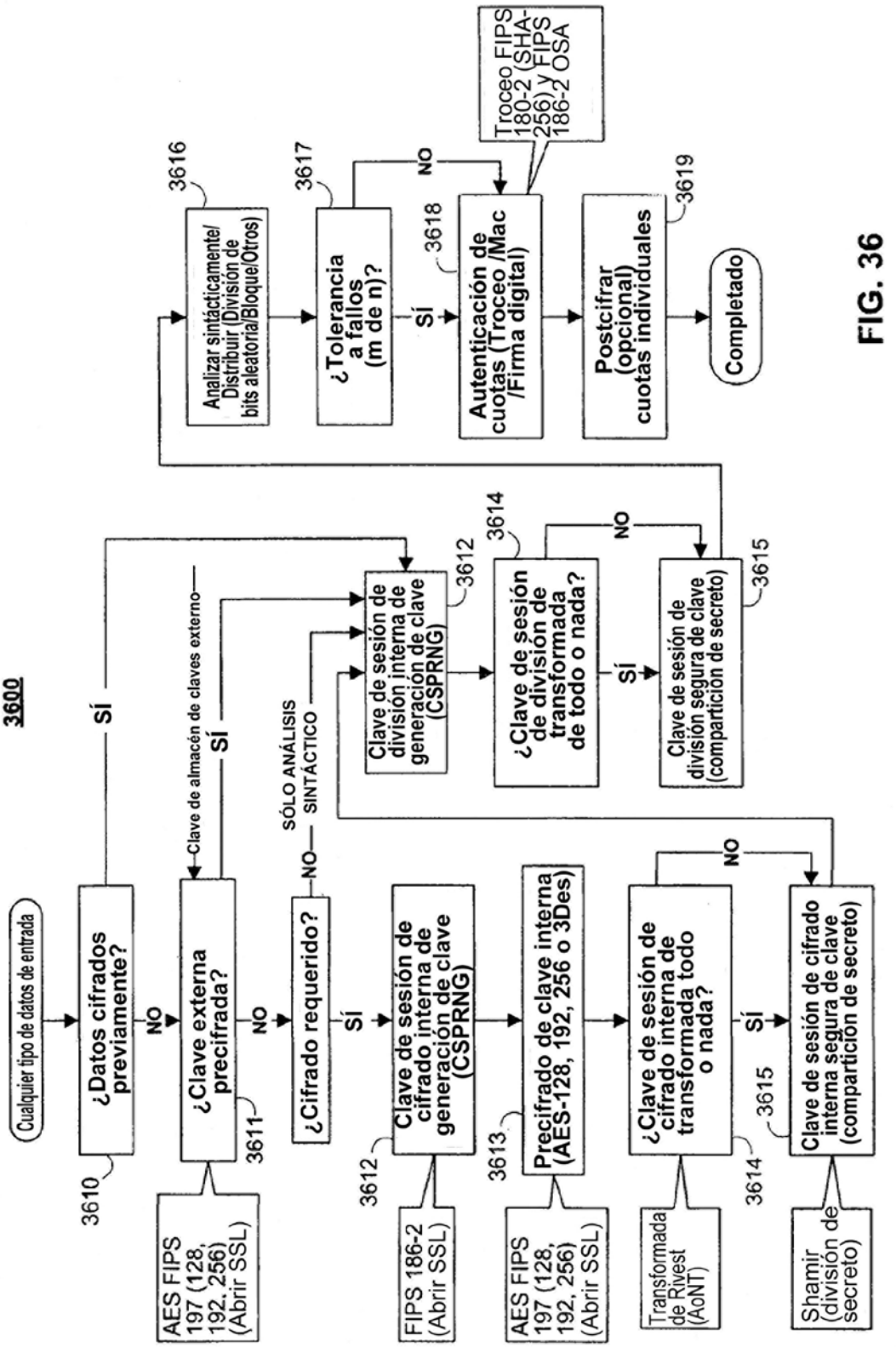

3600
Cualquier tipo de datos de entrada
¿Datos cifrados previamente?
SÍ
NO
3610
¿Clave externa precifrada?
Clave de almacén de claves externo
SÍ
NO
3611
AES FIPS 197 (128, 192, 256) (Abrir SSL)
¿Cifrado requerido?
SÓLO ANÁLISIS SINTÁCTICO
NO
SÍ
Clave de sesión de cifrado interna de generación de clave (CSPRNG)
3612
FIPS 186-2 (Abrir SSL)
Precifrado de clave interna (AES-128, 192, 256 o 3Des)
3613
AES FIPS 197 (128, 192, 256) (Abrir SSL)
¿Clave de sesión de cifrado interna transformada todo o nada?
NO
SÍ
3614
Transformada de Rivest (AoNT)
Clave de sesión de cifrado interna segura de clave (compartición de secreto)
3615
Shamir (división de secreto)
Clave de sesión de división interna de generación de clave (CSPRNG)
3612
¿Clave de sesión de división transformada de todo o nada?
3614
NO
SÍ
Clave de sesión de división segura de clave (compartición de secreto)
3615
Analizar sintácticamente/ Distribuir (División de bits aleatoria/Bloque/Otros)
3616
¿Tolerancia a fallos (m de n)?
3617
NO
SÍ
3618
Troceo FIPS 180-2 (SHA-256) y FIPS 186-2 OSA
Autenticación de cuotas (Troceo /Mac /Firma digital)
Postcifrar (opcional) cuotas individuales
3619
Completado

FIG. 36

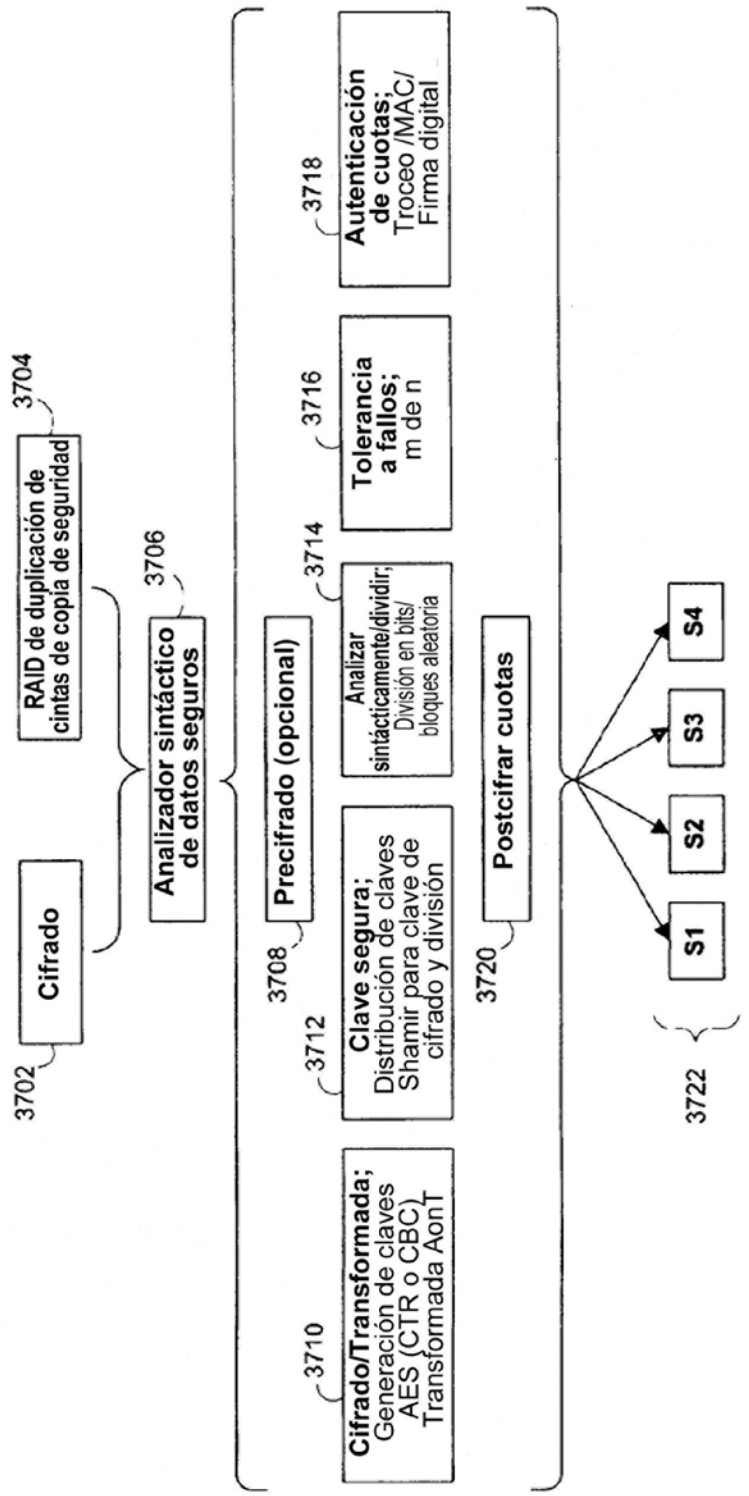

3700
Cifrado
3702
RAID de duplicación de cintas de copia de seguridad
3704
Analizador sintáctico de datos seguros
3706
Precifrado (opcional)
3708
Postcifrar cuotas
3720
Cifrado/Transformada; Generación de claves AES (CTR o CBC) Transformada AonT
3710
Clave segura; Distribución de claves Shamir para clave de cifrado y división
3712
Analizar sintácticamente/dividir; División en bits/ bloques aleatoria
3714
Tolerancia a fallos; m de n
3716
Autenticación de cuotas; Troceo /MAC/ Firma digital
3718
S1
S2
S3
S4
3722

FIG. 37

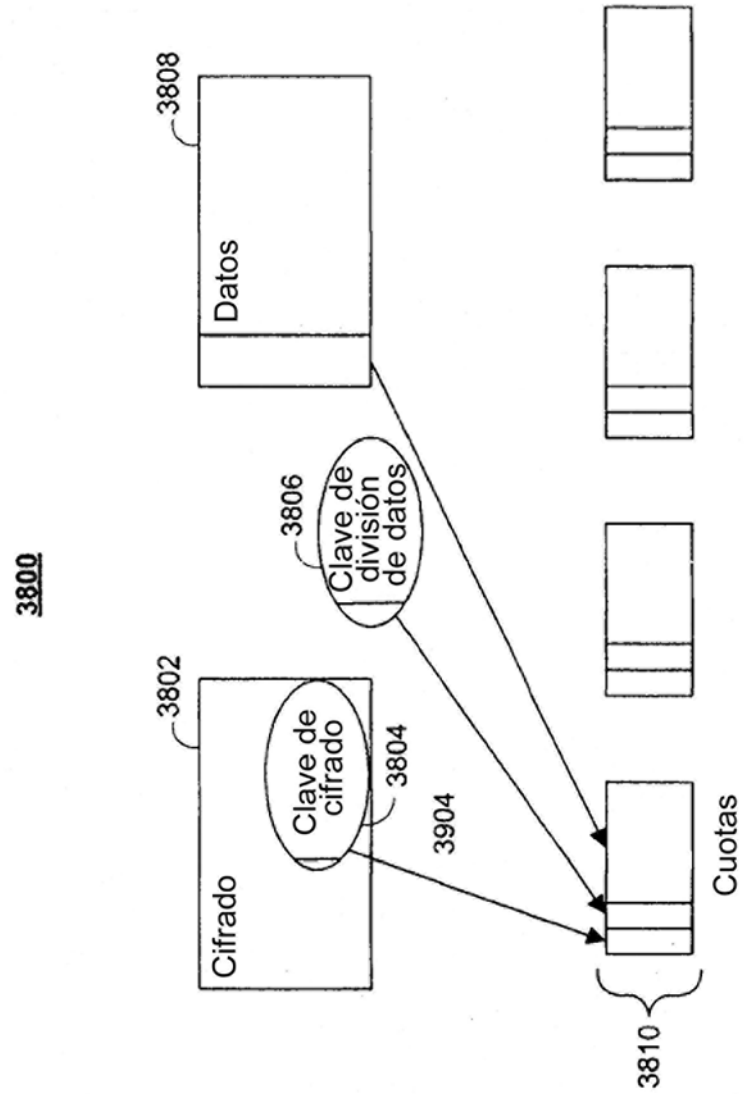

3800
3808
Datos
3806
Clave de división de datos
3802
Clave de cifrado
3804
Cifrado
3904
Cuotas
3810

FIG. 38

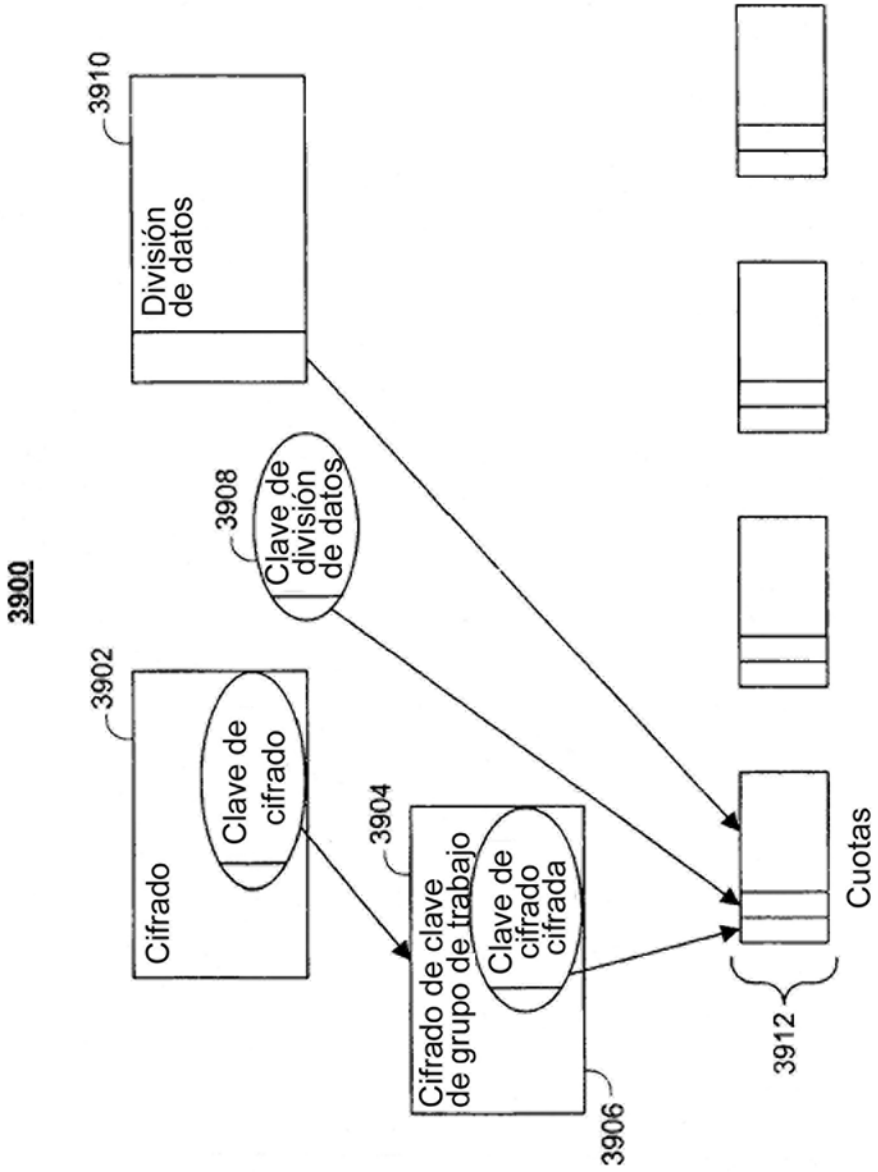

3900
3910
División de datos
3908
Clave de división de datos
3902
Cifrado
Clave de cifrado
3904
Cifrado de clave de grupo de trabajo
Clave de cifrado cifrada
3906
3912
Cuotas

FIG. 39

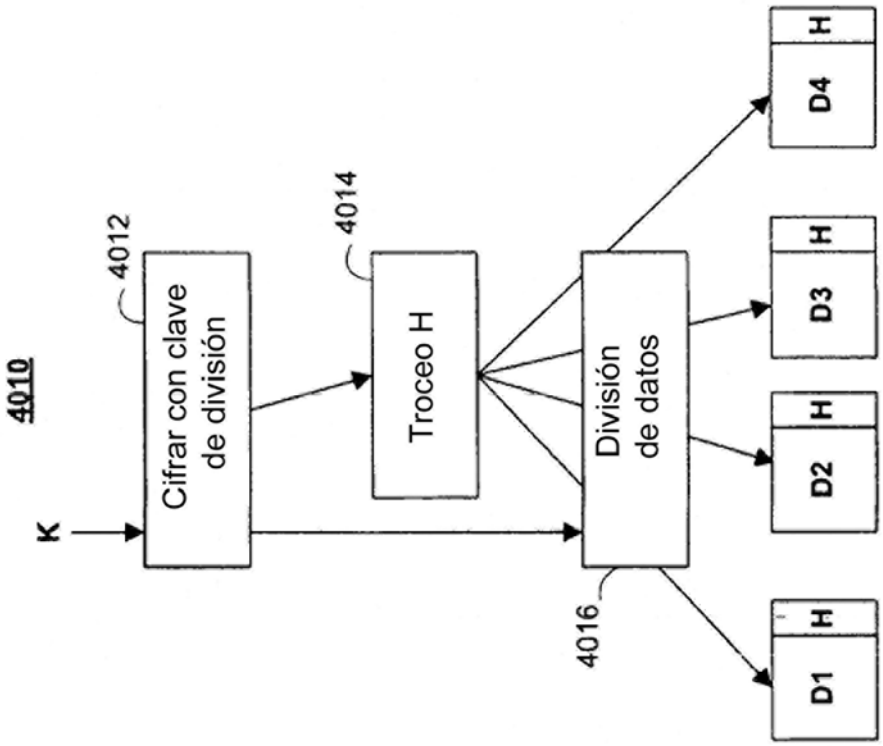


FIG. 40B

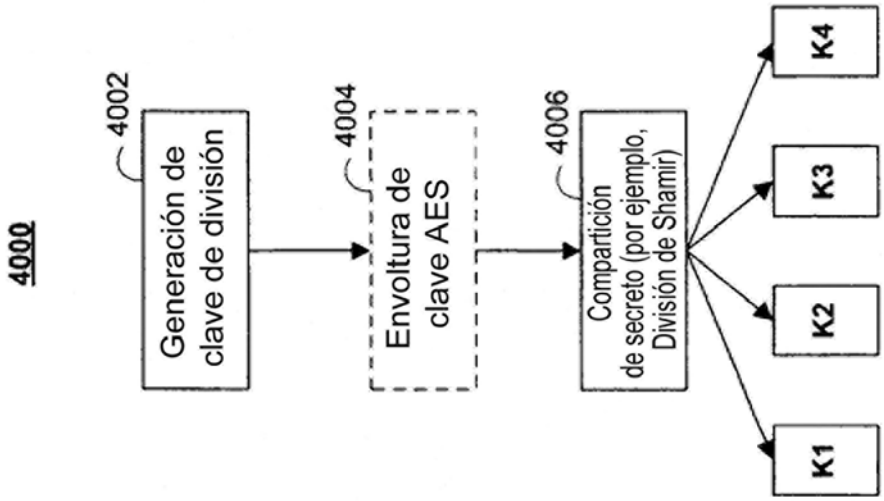


FIG. 40A

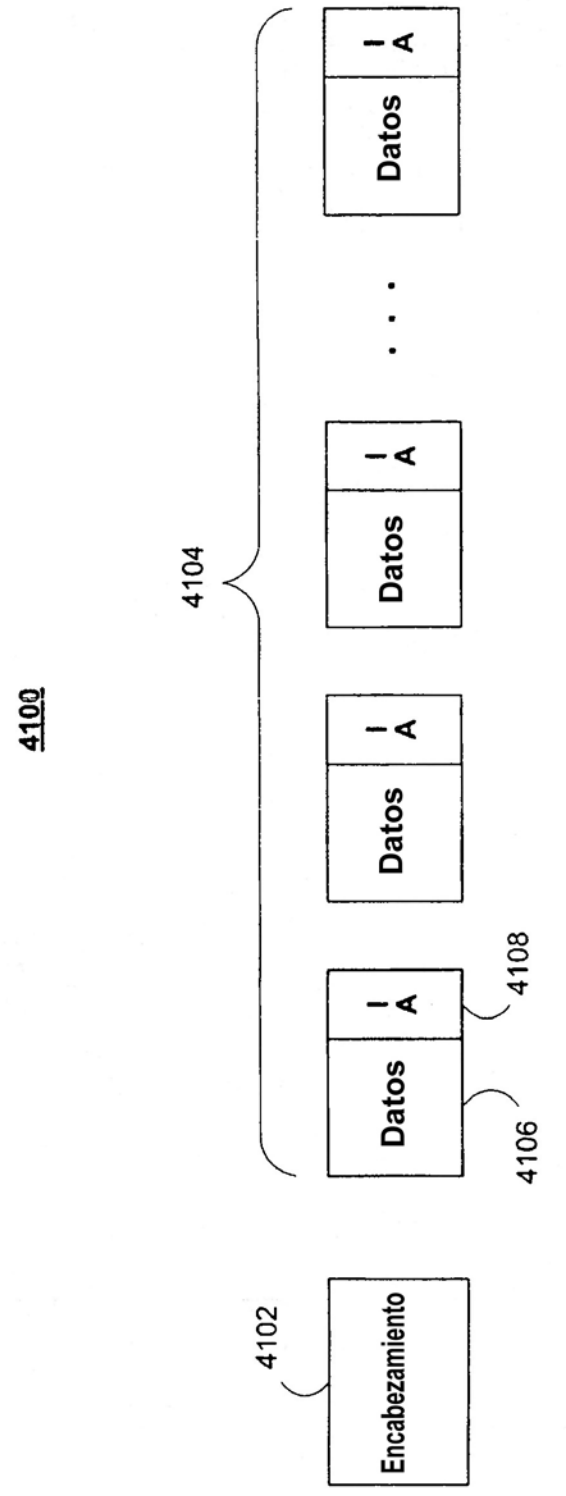


FIG. 41

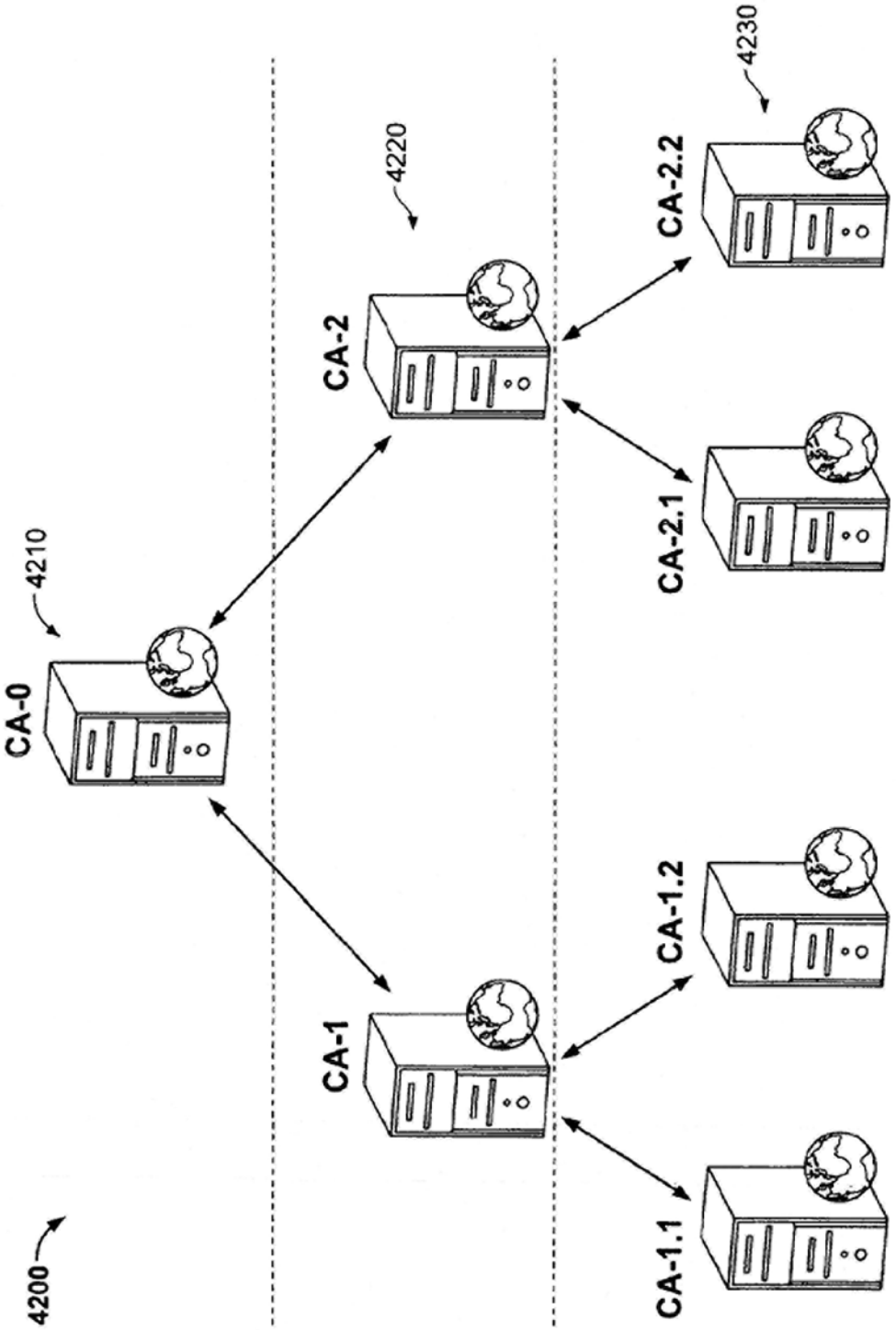


FIG. 42

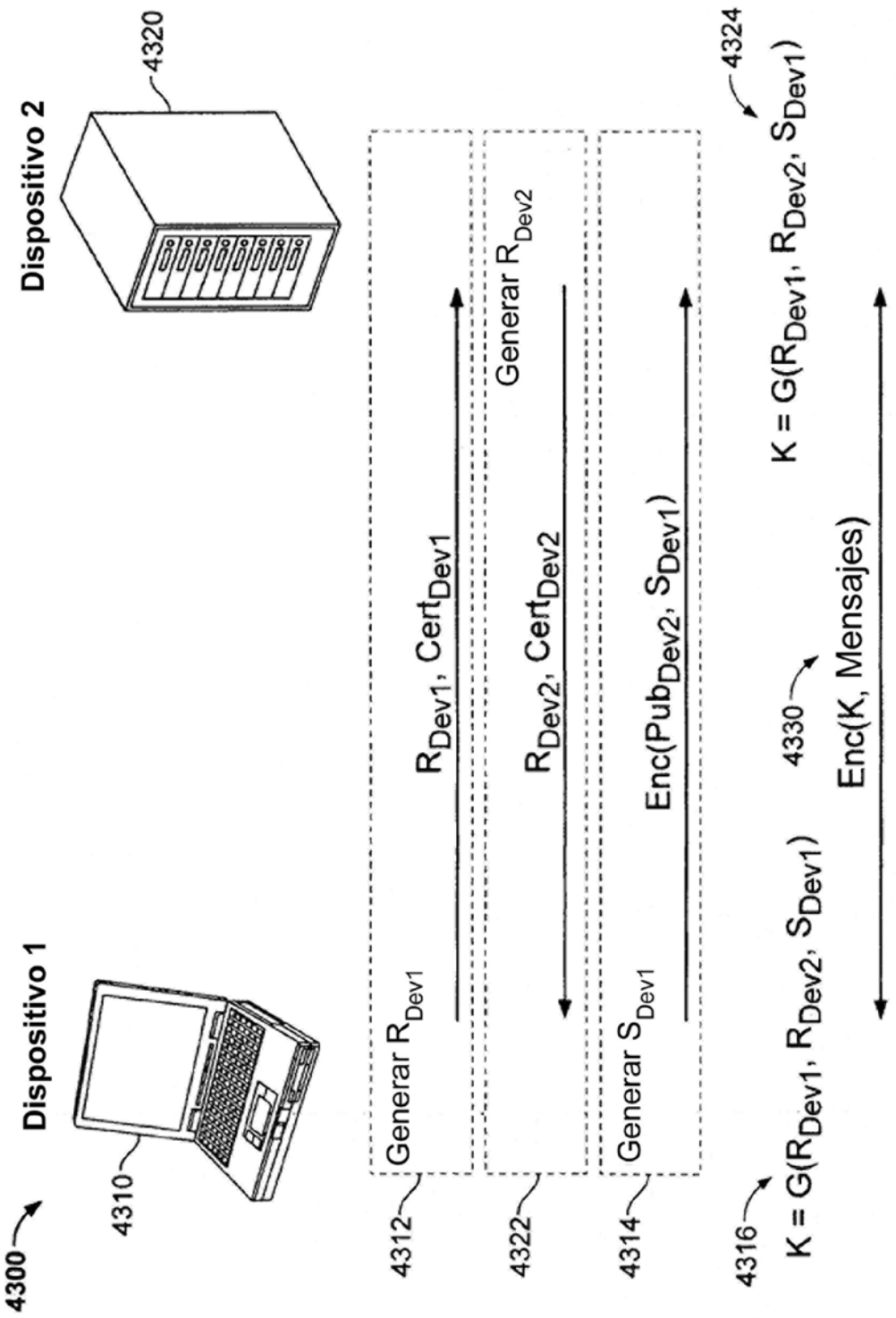

4300
Dispositivo 1
4310
Dispositivo 2
4320
Generar R_{Dev1}
R_{Dev1}, $Cert_{Dev1}$
4312
Generar R_{Dev2}
R_{Dev2}, $Cert_{Dev2}$
4322
Generar S_{Dev1}
$Enc(Pub_{Dev2}, S_{Dev1})$
4314
4324
$K = G(R_{Dev1}, R_{Dev2}, S_{Dev1})$
4316
$K = G(R_{Dev1}, R_{Dev2}, S_{Dev1})$
4330
Enc(K, Mensajes)

FIG. 43

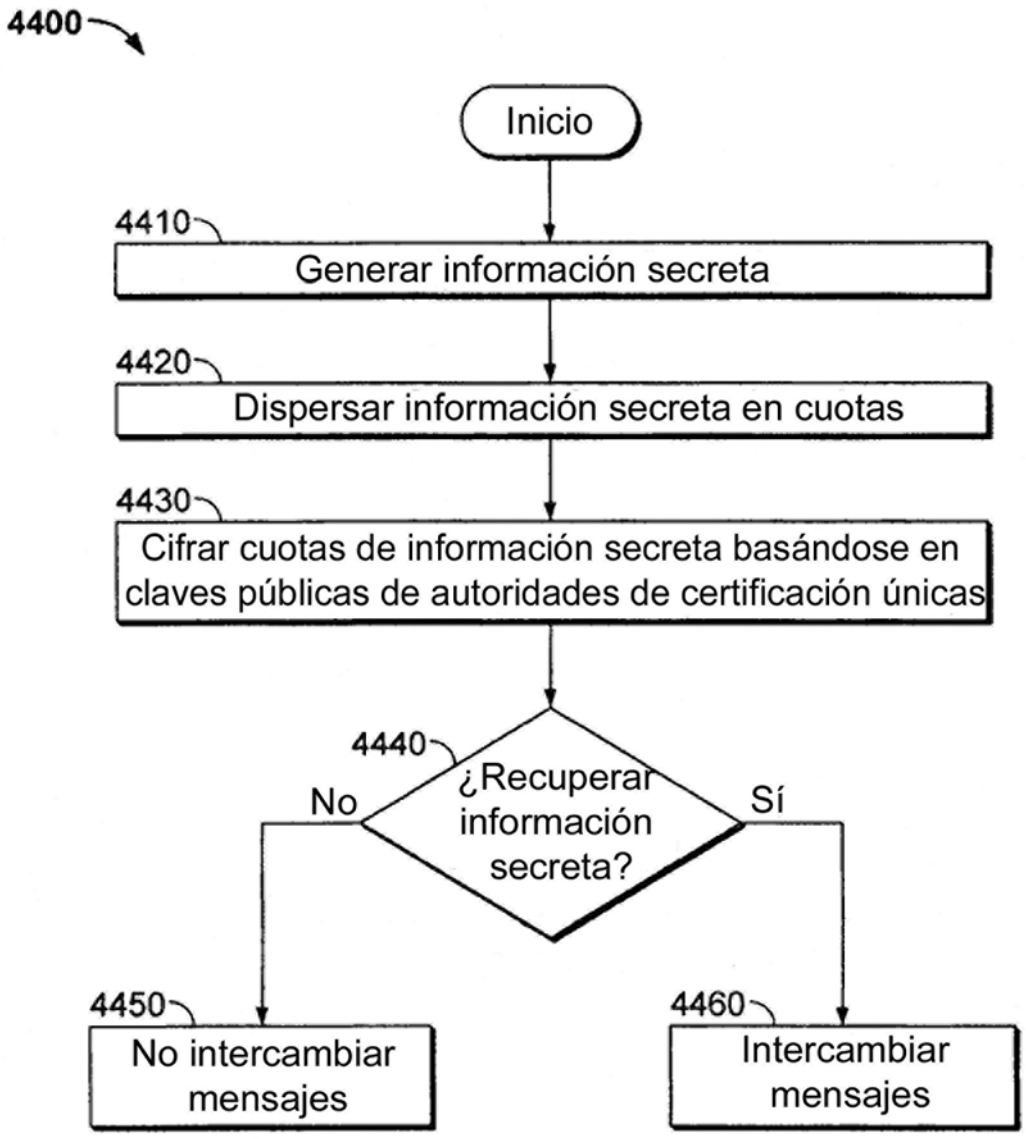

4400
Inicio
4410
Generar información secreta
4420
Dispersar información secreta en cuotas
4430
Cifrar cuotas de información secreta basándose en claves públicas de autoridades de certificación únicas
4440
¿Recuperar información secreta?
No
Sí
4450
No intercambiar mensajes
4460
Intercambiar mensajes

FIG. 44

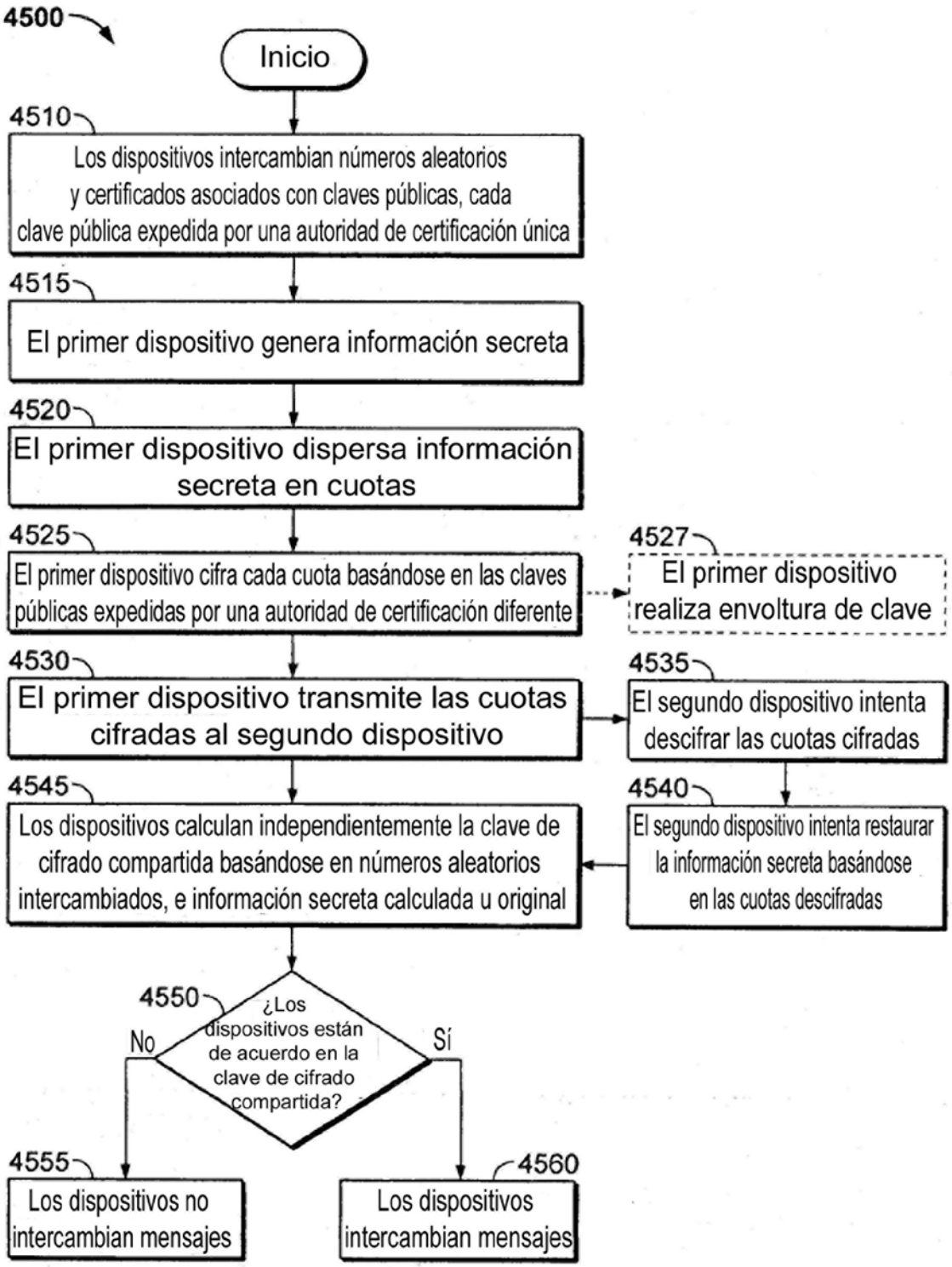

4500
Inicio
4510
Los dispositivos intercambian números aleatorios y certificados asociados con claves públicas, cada clave pública expedida por una autoridad de certificación única
4515
El primer dispositivo genera información secreta
4520
El primer dispositivo dispersa información secreta en cuotas
4525
El primer dispositivo cifra cada cuota basándose en las claves públicas expedidas por una autoridad de certificación diferente
4527
El primer dispositivo realiza envoltura de clave
4530
El primer dispositivo transmite las cuotas cifradas al segundo dispositivo
4535
El segundo dispositivo intenta descifrar las cuotas cifradas
4540
El segundo dispositivo intenta restaurar la información secreta basándose en las cuotas descifradas
4545
Los dispositivos calculan independientemente la clave de cifrado compartida basándose en números aleatorios intercambiados, e información secreta calculada u original
4550
¿Los dispositivos están de acuerdo en la clave de cifrado compartida?
No
Sí
4555
Los dispositivos no intercambian mensajes
4560
Los dispositivos intercambian mensajes

FIG. 45

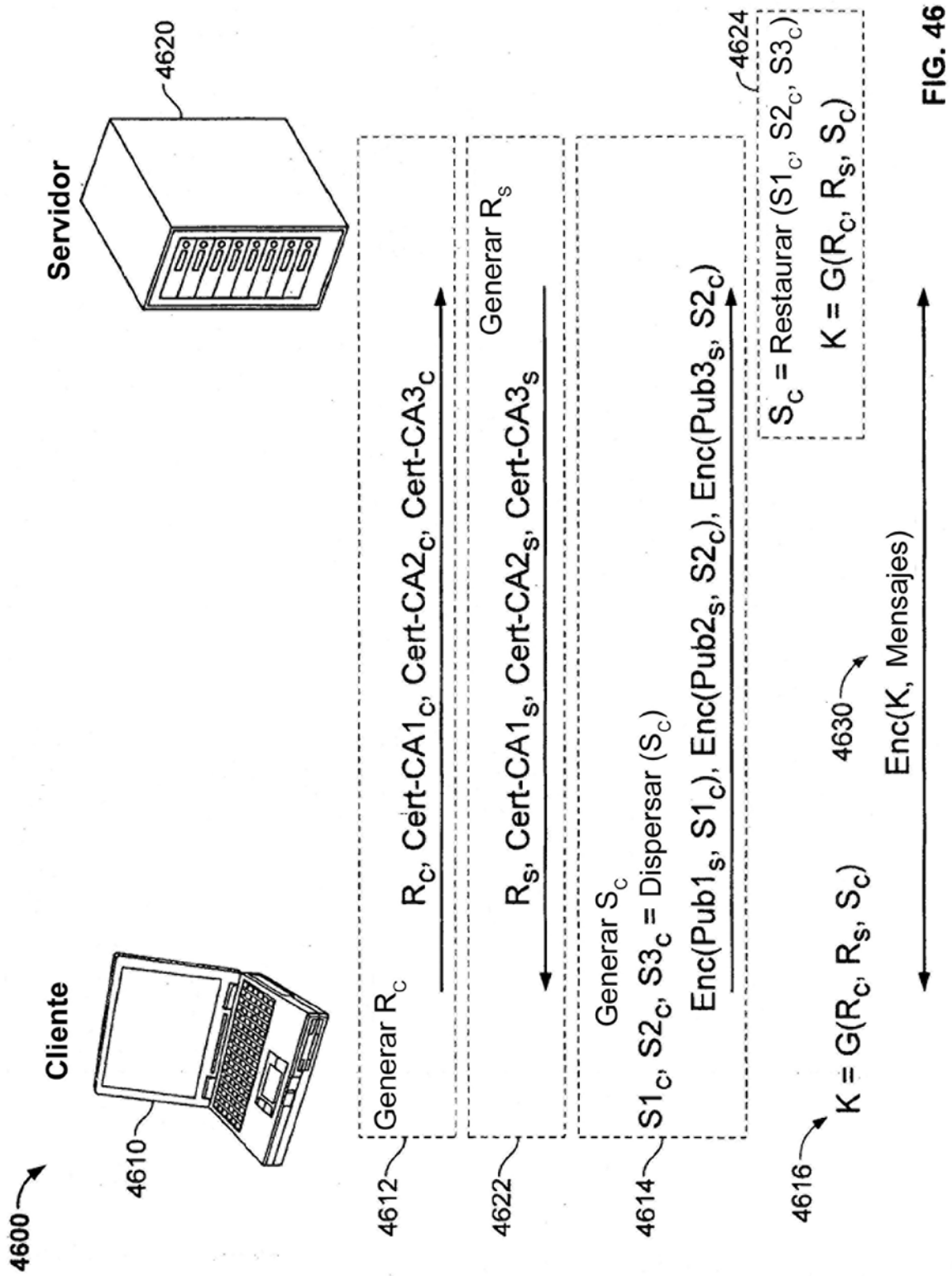

4600
Cliente
4610
Servidor
4620
4612
Generar R_C
R_C, Cert-$CA1_C$, Cert-$CA2_C$, Cert-$CA3_C$
4622
Generar R_S
R_S, Cert-$CA1_S$, Cert-$CA2_S$, Cert-$CA3_S$
4614
Generar S_C
$S1_C$, $S2_C$, $S3_C$ = Dispersar (S_C)
Enc($Pub1_S$, $S1_C$), Enc($Pub2_S$, $S2_C$), Enc($Pub3_S$, $S2_C$)
4624
S_C = Restaurar ($S1_C$, $S2_C$, $S3_C$)
$K = G(R_C, R_S, S_C)$
4616
$K = G(R_C, R_S, S_C)$
4630
Enc(K, Mensajes)

FIG. 46

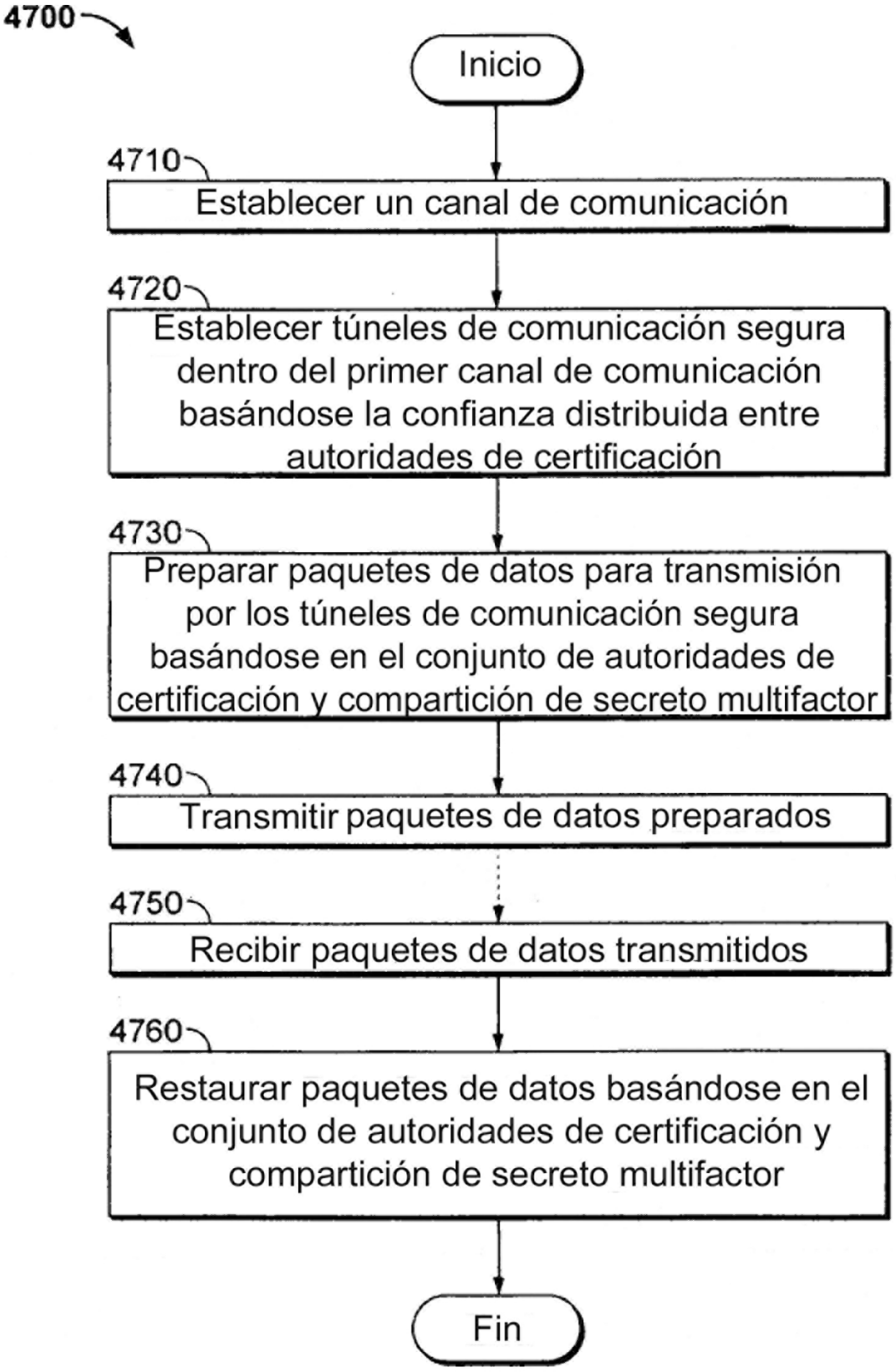

4700
Inicio
4710
Establecer un canal de comunicación
4720
Establecer túneles de comunicación segura dentro del primer canal de comunicación basándose la confianza distribuida entre autoridades de certificación
4730
Preparar paquetes de datos para transmisión por los túneles de comunicación segura basándose en el conjunto de autoridades de certificación y compartición de secreto multifactor
4740
Transmitir paquetes de datos preparados
4750
Recibir paquetes de datos transmitidos
4760
Restaurar paquetes de datos basándose en el conjunto de autoridades de certificación y compartición de secreto multifactor
Fin

FIG. 47

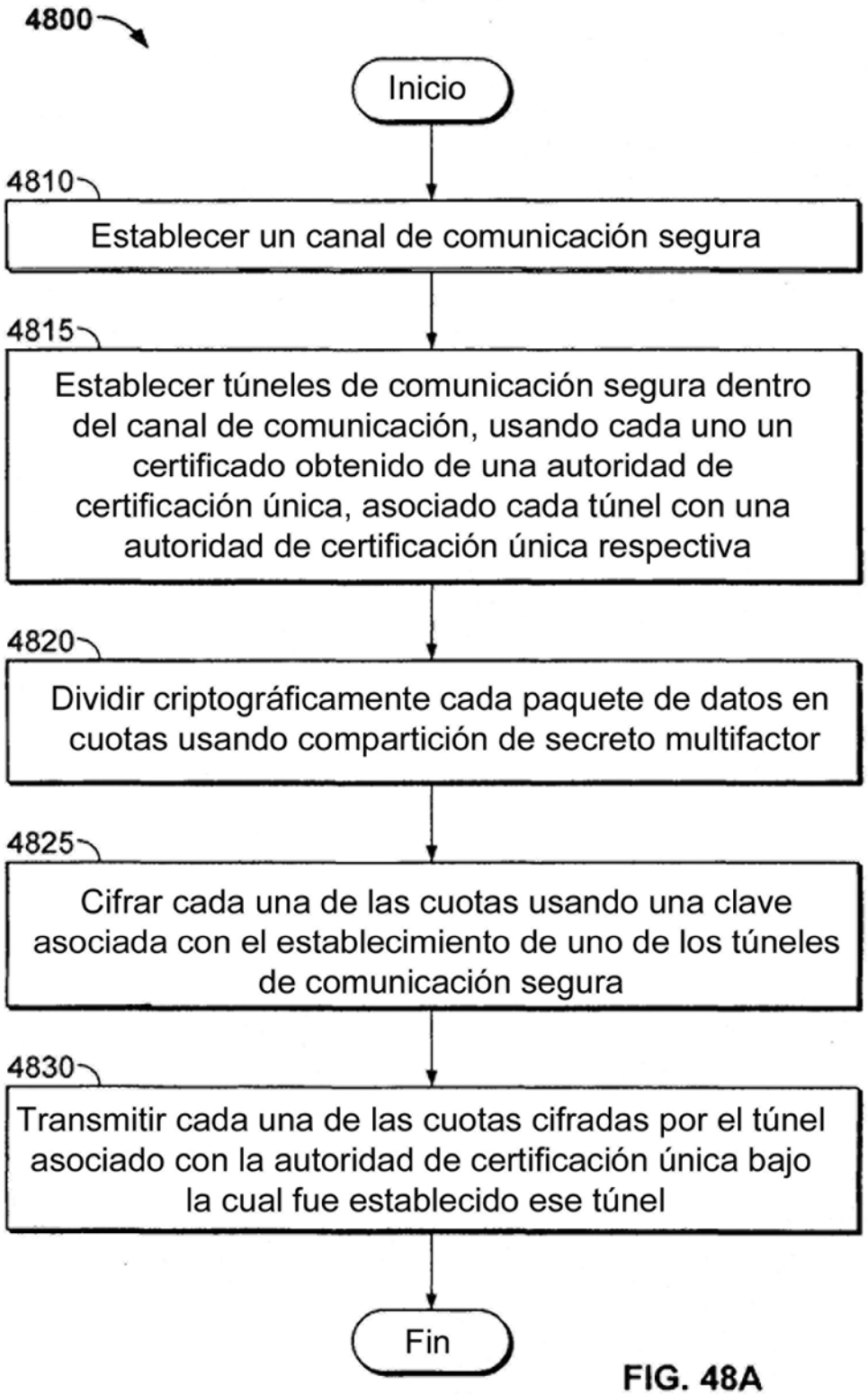

4800
Inicio
4810
Establecer un canal de comunicación segura
4815
Establecer túneles de comunicación segura dentro del canal de comunicación, usando cada uno un certificado obtenido de una autoridad de certificación única, asociado cada túnel con una autoridad de certificación única respectiva
4820
Dividir criptográficamente cada paquete de datos en cuotas usando compartición de secreto multifactor
4825
Cifrar cada una de las cuotas usando una clave asociada con el establecimiento de uno de los túneles de comunicación segura
4830
Transmitir cada una de las cuotas cifradas por el túnel asociado con la autoridad de certificación única bajo la cual fue establecido ese túnel
Fin

FIG. 48A

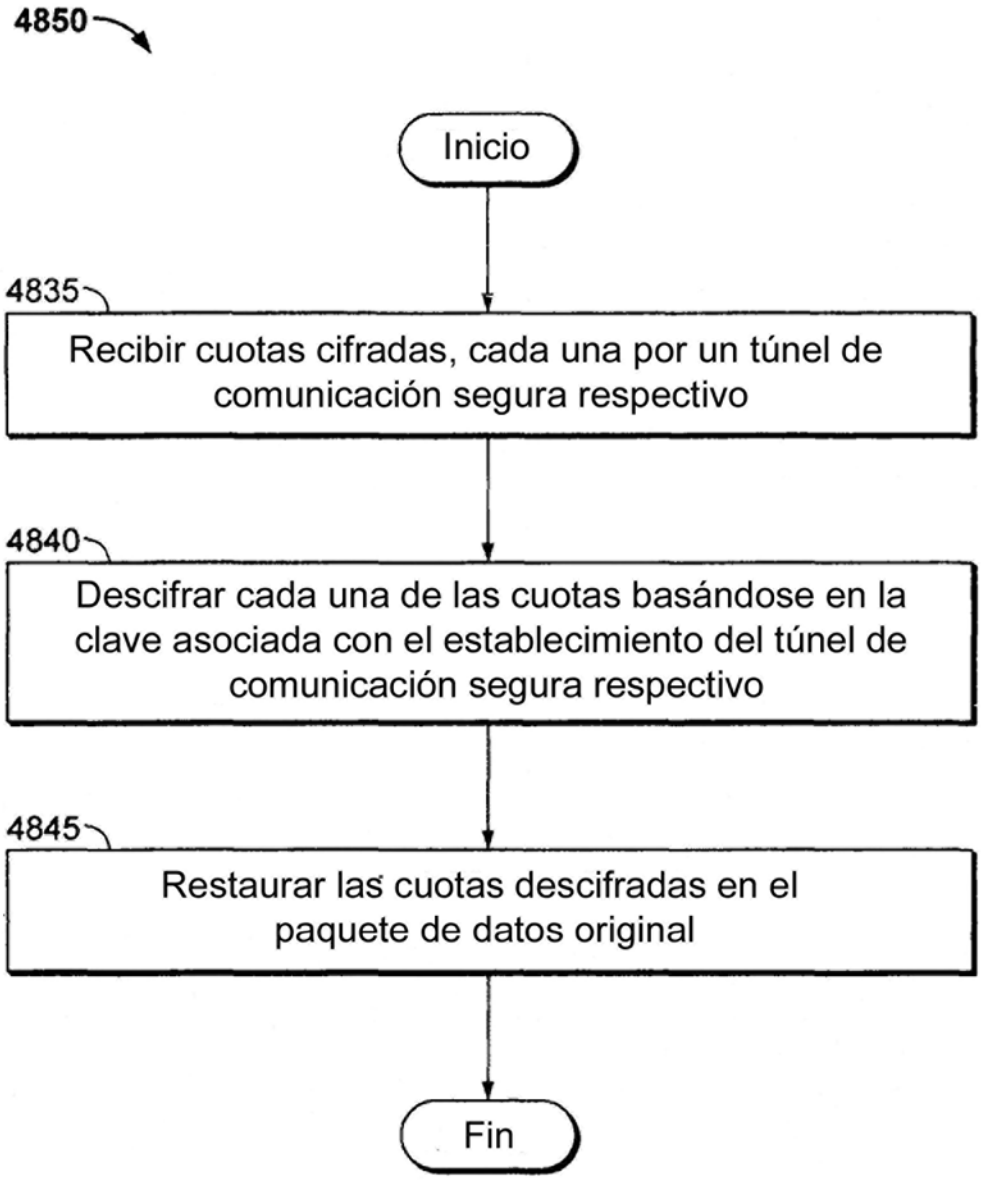

4850
Inicio
4835
Recibir cuotas cifradas, cada una por un túnel de comunicación segura respectivo
4840
Descifrar cada una de las cuotas basándose en la clave asociada con el establecimiento del túnel de comunicación segura respectivo
4845
Restaurar las cuotas descifradas en el paquete de datos original
Fin

FIG. 48B

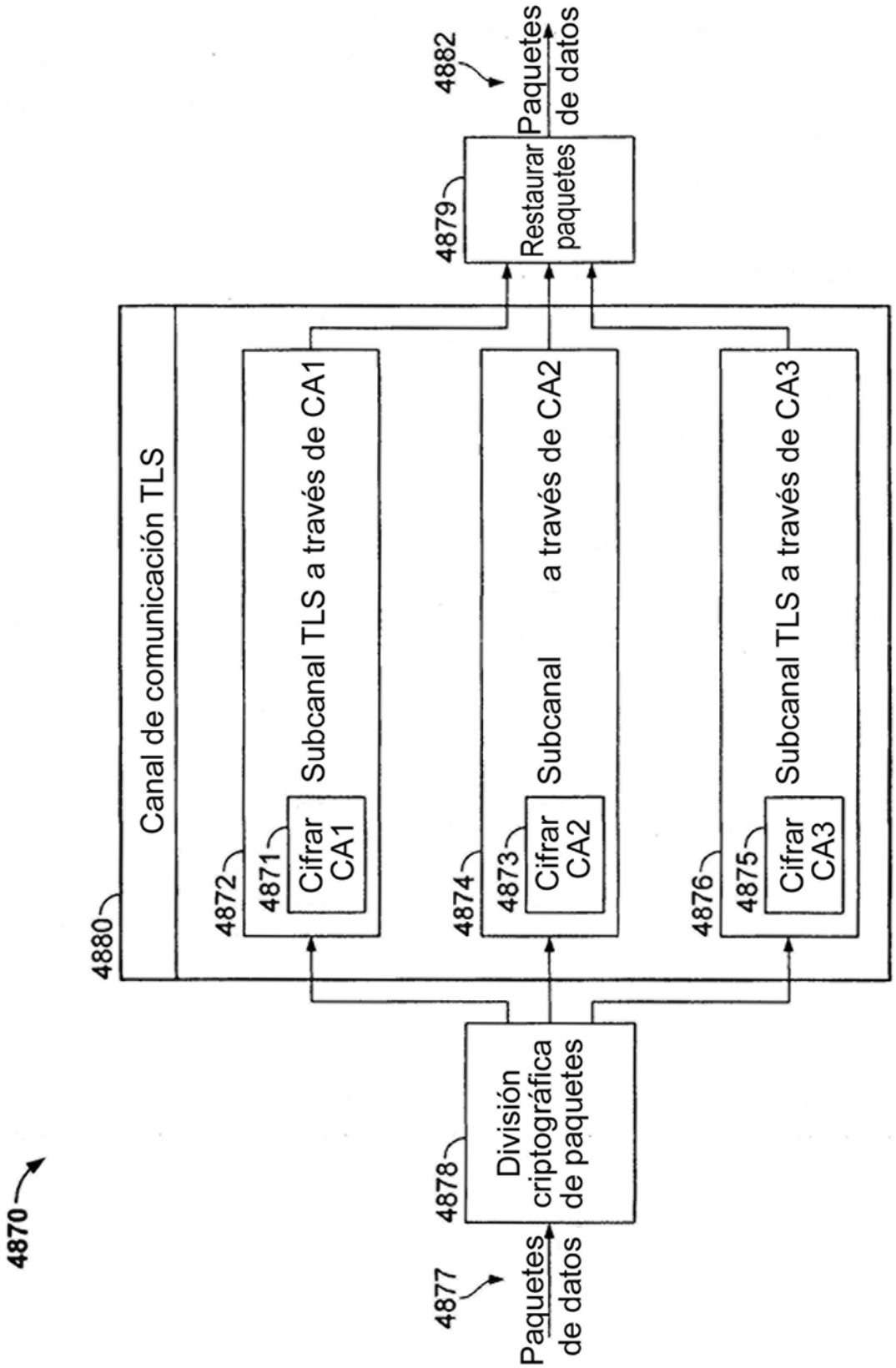

4870
4877
Paquetes de datos
4878
División criptográfica de paquetes
4880
Canal de comunicación TLS
4871
Cifrar CA1
4872
Subcanal TLS a través de CA1
4873
Cifrar CA2
4874
Subcanal a través de CA2
4875
Cifrar CA3
4876
Subcanal TLS a través de CA3
4879
Restaurar paquetes
4882
Paquetes de datos

FIG. 48C

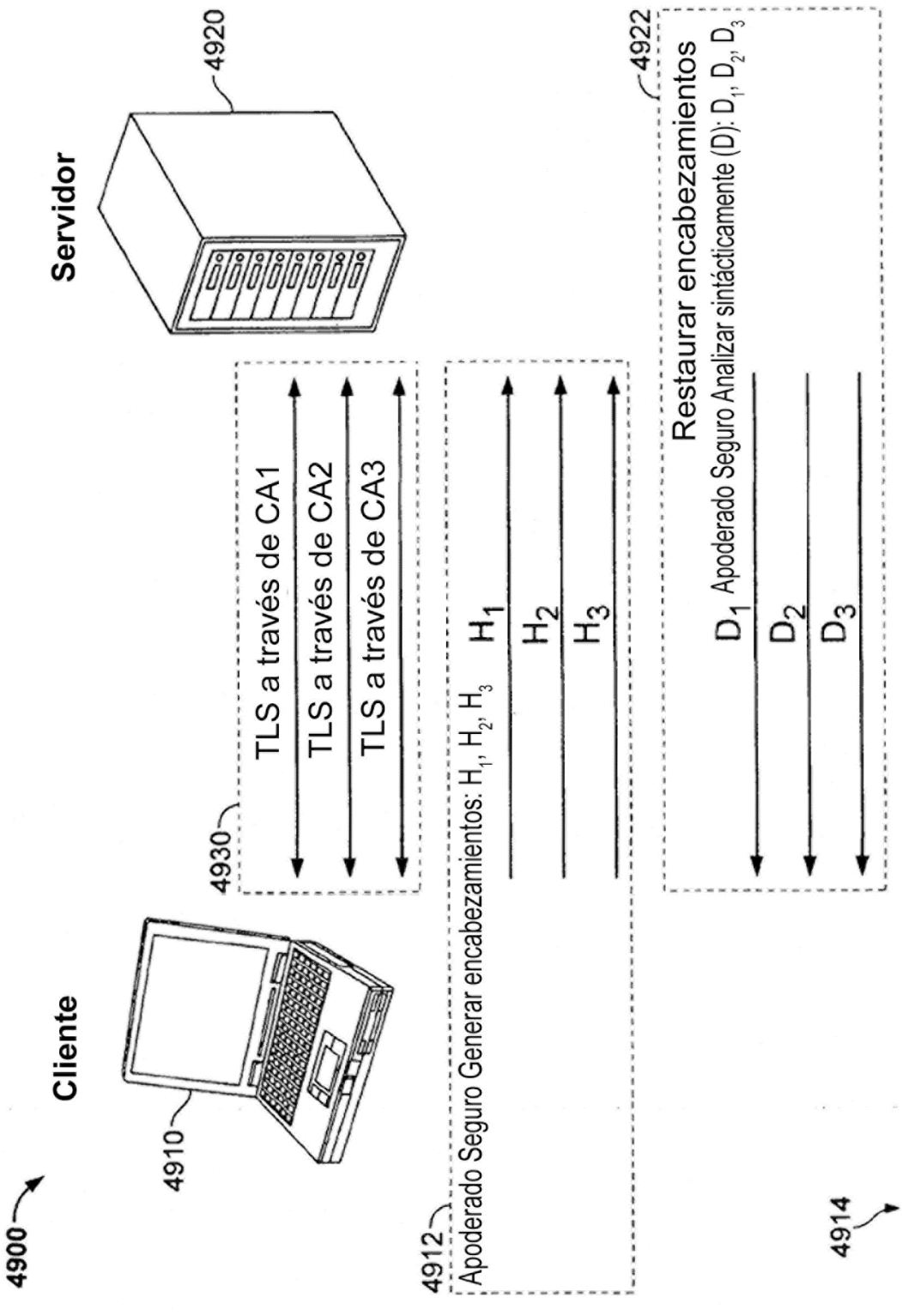

4900
Cliente
4910
Servidor
4920
4930
TLS a través de CA1
TLS a través de CA2
TLS a través de CA3
4912
Apoderado Seguro Generar encabezamientos: H_1, H_2, H_3
H_1
H_2
H_3
4922
Restaurar encabezamientos
D_1 Apoderado Seguro Analizar sintácticamente (D): D_1, D_2, D_3
D_1
D_2
D_3
4914
Apoderado Seguro Analizar sintácticamente (D): D_1, D_2, D_3

FIG. 49

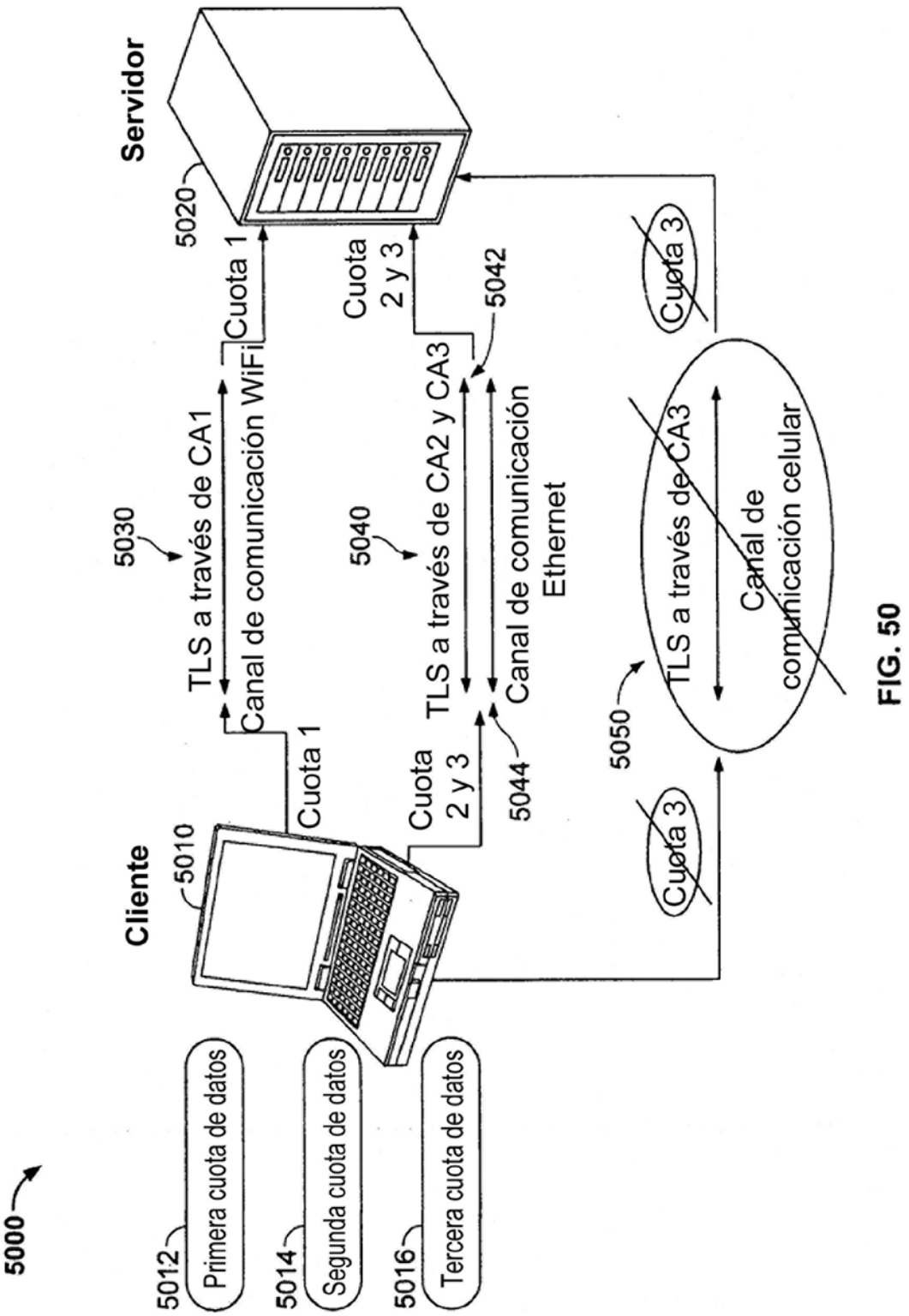

5000
Servidor
5020
Cliente
5010
Cuota 1
Cuota 2 y 3
5042
5030
TLS a través de CA1
Canal de comunicación WiFi
5040
TLS a través de CA2 y CA3
Canal de comunicación Ethernet
5044
5050
TLS a través de CA3
Canal de comunicación celular
Cuota 3
5012
Primera cuota de datos
5014
Segunda cuota de datos
5016
Tercera cuota de datos

FIG. 50