(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 581 548**

(51) Int. CI.:

G06F 21/53 (2013.01)
G06F 21/62 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **18.08.2011 E 11752394 (4)**

(97) Fecha y número de publicación de la concesión europea: **10.02.2016 EP 2606448**

(54) Título: **Sistemas y procedimientos para asegurar entornos informáticos de máquinas virtuales**

(30) Prioridad:

18.08.2010 US 374950 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
06.09.2016

(73) Titular/es:

SECURITY FIRST CORP. (100.0%)
29811 Santa Margarita Parkway, Suite 600
Rancho Santa Margarita, CA 92688, US

(72) Inventor/es:

STAKER, MATTHEW;
O'HARE, MARK S.;
MUMAUGH, JOHN ROBERT y
ORSINI, RICK L.

(74) Agente/Representante:

PONS ARIÑO, Ángel

DESCRIPCIÓN

Sistemas y procedimientos para asegurar entornos informáticos de máquinas virtuales.

Referencia a solicitudes relacionadas

La presente solicitud reivindica el beneficio de la solicitud de patente estadounidense provisional nº 61/374.950, presentada el 18 de agosto de 2010.

Campo de la invención

La presente invención se refiere, en general, a sistemas y procedimientos para asegurar entornos informáticos de máquinas virtuales. Los sistemas y procedimientos que se describen en este documento se pueden usar conjuntamente con otros sistemas y procedimientos que se describen en la patente estadounidense, de titularidad compartida, número 7.391.865 y en las solicitudes de patentes estadounidenses, de titularidad compartida, números 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; 12/783.276, presentada el 19 de mayo de 2010; 12/953.877, presentada el 24 de noviembre de 2010; 13/077.770, presentada el 31 de marzo de 2011; 13/077.802, presentada el 31 de marzo de 2011 y 13/117.791, presentada el 27 de mayo de 2011 y las solicitudes de patentes estadounidenses provisionales, números 61/436.991, presentada el 27 de enero de 2011; 61/264.464, presentada el 25 de noviembre de 2009; 61/319.658, presentada el 31 de marzo de 2010; 61/320.242, presentada el 1 de abril de 2010; 61/349.560, presentada el 28 de mayo de 2010; 61/373.187, presentada el 12 de agosto de 2010; 61/374.950, presentada el 18 de agosto de 2010; 61/384.583, presentada el 20 de septiembre de 2010.

Gracias al documento US2010/0058051 se conoce un procedimiento para asegurar la comunicación entre máquinas virtuales.

Resumen

Las realizaciones están dirigidas, por lo general, a sistemas y procedimientos para asegurar datos. Una realización se refiere, por lo general, a un procedimiento para asegurar datos en el que se recibe una petición de una operación de seguridad de una primera máquina virtual que funciona en un sistema operativo anfitrión de un primer dispositivo. En respuesta a la recepción de la petición, la operación de seguridad se ejecuta en un primer módulo de seguridad implementado en un núcleo del sistema operativo anfitrión y el resultado de la operación de seguridad se proporciona a la primera máquina virtual.

En algunas implementaciones, la petición de la primera máquina virtual es una petición de una aplicación que se ejecuta en la primera máquina virtual. En algunas implementaciones, la petición de la aplicación que se ejecuta en la primera máquina virtual es una petición de una operación de seguridad que ejecutará el primer módulo de seguridad. En algunas implementaciones, ejecutar la operación de seguridad en el primer módulo de seguridad incluye generar una pluralidad de porciones, donde cada una de la pluralidad de porciones contiene una distribución de datos de un conjunto de datos. Ejecutar la operación de seguridad en el primer módulo de seguridad puede incluir, además, cifrar el conjunto de datos. En algunas implementaciones, la petición de la operación de seguridad de la primera máquina virtual es una petición de una operación de seguridad que ejecutará un segundo módulo de seguridad implementado en un núcleo de un sistema operativo de la primera máquina virtual. Ejecutar la operación de seguridad en el primer módulo de seguridad puede incluir determinar que el segundo módulo de seguridad no puede ejecutar la operación de seguridad pedida. Ejecutar la operación de seguridad en el primer módulo de seguridad puede incluir, además, recibir en el primer módulo de seguridad una petición del segundo módulo de seguridad, para ejecutar la operación pedida. Ejecutar la operación de seguridad en el primer módulo de seguridad puede incluir determinar que el primer módulo de seguridad puede ejecutar la operación de seguridad pedida. En algunas implementaciones, la petición de la primera máquina virtual es una petición para asegurar una comunicación entre la primera máquina virtual y una segunda máquina virtual. La segunda máquina virtual puede funcionar en el sistema operativo anfitrión del primer dispositivo. En algunas implementaciones, ejecutar la operación de seguridad del primer módulo de seguridad incluye llamar a un acelerador de hardware desde el núcleo del sistema operativo anfitrión. En algunas implementaciones, el primer módulo de seguridad incluye un analizador sintáctico seguro.

Asimismo, se proporcionan sistemas para asegurar máquinas virtuales.

Breve descripción de los dibujos

A continuación, se describe la presente invención más detalladamente en relación con los dibujos adjuntos, cuya intención es ilustrar y no limitar la invención, y en los que:

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

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

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

la figura 4 ilustra un diagrama de bloques del 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 depósitos 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 registro 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 diagrama de flujo 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 motores 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 motores 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 que se muestra en la figura 16 de la invención;

la figura 18 ilustra un proceso para llevar a cabo un arbitraje de confianza en un aspecto de la invención que se muestra en la figura 17;

la figura 19 ilustra una transacción de muestra entre un usuario y un vendedor de acuerdo con aspectos de una realización de la invención, cuando un contacto inicial en la red lleva a un contrato de venta firmado por ambas partes;

la figura 20 ilustra un sistema de usuario de muestra con un módulo de proveedor de servicios criptográficos 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 almacenar 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 separada de los datos;

la figura 23 ilustra el proceso de clave intermedia para analizar sintácticamente, dividir y/o separar datos con cifrado y almacenar la clave maestra de cifrado con los datos;

la figura 24 ilustra el proceso de clave intermedia para analizar sintácticamente, dividir y/o separar datos con cifrado y almacenar la clave maestra de cifrado separada de los datos;

la figura 25 ilustra la utilización de los procedimientos y sistemas criptográficos de la presente invención con un grupo de trabajo reducido;

la figura 26 es un diagrama de bloques de un sistema de seguridad de testigos físicos ilustrativo que emplea el analizador sintáctico de datos seguro de acuerdo con una realización de la presente invención;

la figura 27 es un diagrama de bloques de una disposición ilustrativa en la que el analizador sintáctico de datos seguro 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 otro diagrama de bloques de un sistema de datos en movimiento ilustrativo de acuerdo con una realización de la presente invención;

las figuras 30 a 32 son diagramas de bloques de un sistema ilustrativo que tiene integrado el analizador sintáctico de datos seguro de acuerdo con una realización de la presente invención;

la figura 33 es un diagrama de flujo de procesos 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 procesos de un proceso ilustrativo para restablecer partes de datos a datos originales de acuerdo con una realización de la presente invención;

la figura 35 es un diagrama de flujo de procesos de un proceso ilustrativo para dividir datos a nivel de bits de acuerdo con una realización de la presente invención;

la figura 36 es un diagrama de flujo de procesos de etapas y características ilustrativas, que se puede usar en cualquier combinación adecuada, con cualquier incorporación, eliminación o modificación adecuada, de acuerdo con una realización de la presente invención;

la figura 37 es un diagrama de flujo de procesos de etapas y características ilustrativas, que se puede usar en cualquier combinación adecuada, con cualquier incorporación, eliminación o modificación adecuada, de acuerdo con una realización de la presente invención;

la figura 38 es un diagrama de bloques simplificado del almacenamiento de componentes de claves y datos dentro de porciones, que se puede usar en cualquier combinación adecuada, con cualquier incorporación, eliminación o

modificación adecuada, de acuerdo con una realización de la presente invención;

la figura 39 es un diagrama de bloques simplificado del almacenamiento de componentes de claves y datos dentro de porciones usando una clave de grupo de trabajo, que se puede usar en cualquier combinación adecuada, con cualquier incorporación, eliminación o modificación adecuada, de acuerdo con una realización de la presente invención;

las figuras 40A y 40B son diagramas de flujo de procesos ilustrativos y simplificados para generación de cabeceras y división de datos para datos en movimiento, que se pueden usar en cualquier combinación adecuada, con cualquier incorporación, eliminación o modificación adecuada, de acuerdo con una realización de la presente invención;

la figura 41 es un diagrama de bloques simplificado de un formato de porción ilustrativo, que se puede usar en cualquier combinación adecuada, con cualquier incorporación, eliminación o modificación adecuada, de acuerdo con una realización de la presente invención;

la figura 42 es un diagrama de bloques de una disposición ilustrativa en la que el analizador sintáctico de datos seguro está integrado en un sistema conectado a recursos informáticos en la nube de acuerdo con una realización de la presente invención;

la figura 43 es un diagrama de bloques de una disposición ilustrativa en la que el analizador sintáctico de datos seguro está integrado en un sistema para enviar datos a través de la nube de acuerdo con una realización de la presente invención;

la figura 44 es un diagrama de bloques de una disposición ilustrativa en la que el analizador sintáctico de datos seguro se usa para asegurar servicios de datos en la nube de acuerdo con una realización de la presente invención;

la figura 45 es un diagrama de bloques de una disposición ilustrativa en la que analizador sintáctico de datos seguro se usa para asegurar el almacenamiento de datos en la nube de acuerdo con una realización de la presente invención;

la figura 46 es un diagrama de bloques de una disposición ilustrativa en la que el analizador sintáctico de datos seguro se usa para asegurar el control de acceso a red de acuerdo con una realización de la presente invención;

la figura 47 es un diagrama de bloques de una disposición ilustrativa en la que el analizador sintáctico de datos seguro se usa para asegurar recursos informáticos de alto rendimiento de acuerdo con una realización de la presente invención;

la figura 48 es un diagrama de bloques de una disposición ilustrativa en la que el analizador sintáctico de datos seguro se usa para asegurar el acceso usando máquinas virtuales de acuerdo con una realización de la presente invención;

las figuras 49 y 50 muestran diagramas de bloques de disposiciones ilustrativas alternativas para asegurar el acceso usando máquinas virtuales de acuerdo con realizaciones de la presente invención;

la figura 51 es un diagrama de bloques de una disposición ilustrativa en la que el analizador sintáctico de datos seguro se usa para asegurar redes de multiplexación por división ortogonal de frecuencia (OFDM) de acuerdo con una realización de la presente invención;

la figura 52 es un diagrama de bloques de una disposición ilustrativa en la que el analizador sintáctico de datos seguro se usa para asegurar la red eléctrica de acuerdo con una realización de la presente invención;

la figura 53 es un diagrama de bloques de un entorno informático de máquina virtual

la figura 54 es un diagrama de flujo de un proceso para asegurar una máquina virtual y

la figura 55 es un diagrama de flujo de un entorno informático de máquina virtual seguro.

Descripción detallada de la invención

Un aspecto de la presente invención es proporcionar un sistema criptográfico donde uno o más servidores seguros, o un motor de confianza, almacenan claves criptográficas y datos de autenticación de usuarios. Los usuarios acceden a la funcionalidad de sistemas criptográficos tradicionales mediante acceso por red al motor de confianza, no obstante, el motor de confianza no autoriza claves reales ni otros datos de autenticación y, por lo tanto, las claves y los datos siguen seguros. Dicho almacenamiento en servidores de claves y datos de autenticación proporciona seguridad, portabilidad, disponibilidad y honestidad a cada usuario.

Dado que los usuarios pueden confiar en el sistema criptográfico para llevar a cabo la autenticación de documentos y usuarios y otras funciones criptográficas, se pueden incorporar en el sistema una gran variedad de funcionalidades. Por ejemplo, el proveedor de motores de confianza puede evitar la denuncia de un acuerdo, por ejemplo, autenticando a los participantes del acuerdo, firmando digitalmente el acuerdo en nombre de los participantes o por éstos y almacenando un registro del acuerdo firmado digitalmente por cada participante. Además, el sistema criptográfico puede supervisar acuerdos y determinar aplicar distintos grados de autenticación, por ejemplo, en función del precio, el usuario, el vendedor, la ubicación geográfica, el lugar de uso o similares.

Para facilitar el total entendimiento de la invención, en el resto de la descripción detallada se describe la invención haciendo referencia a las figuras, donde elementos similares están referenciados con números similares en toda la descripción.

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 universal convencional que tiene uno o más microprocesadores, tales como, por ejemplo, un procesador Intel. Además, el sistema de usuario (105) incluye un sistema operativo apropiado, tal 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). De manera ventajosa, el dispositivo biométrico (107) puede captar datos biométricos de un usuario y transferir los datos biométricos captados al motor de confianza (110). De acuerdo con una realización de la invención, de manera ventajosa, el dispositivo biométrico puede comprender un dispositivo que tiene atributos y características similares a los que se describen en la solicitud de patente estadounidense número 08/926.277, presentada el 5 de septiembre de 1997, titulada *"RELIEF OBJECT IMAGE GENERATOR";* en la solicitud de patente estadounidense número 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";* en la solicitud de patente estadounidense número 09/435.011, presentada el 5 de noviembre de 1999, titulada *"RELIEF OBJECT SENSOR ADAPTOR"* y en la solicitud de patente estadounidense número 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".*

Además, el sistema de usuario (105) puede estar conectado al enlace de comunicación (125) a través de un proveedor de servicios convencional, tal como, por ejemplo, una conexión por línea conmutada, una línea de abonado digital (DSL), un módem de cable, una conexión de fibra o similares. De acuerdo con otra realización, el sistema de usuario (105) está conectado al enlace de comunicación (125) a través de conectividad de red, tal como, por ejemplo, una red de área amplia o local. De acuerdo con una realización, el sistema operativo incluye una pila TCP/IP que maneja todo el tráfico de mensajes entrantes y salientes que pasan por el enlace de comunicación (125).

Si bien el sistema de usuario (105) se describe haciendo referencia a las realizaciones anteriores, con las mismas no se pretende limitar la invención. Por el contrario, un experto en la materia reconocerá en la descripción de este documento una serie de realizaciones alternativas del sistema de usuario (105), que incluyen prácticamente cualquier dispositivo informático capaz de enviar o recibir información desde otro sistema informático. Por ejemplo, el sistema de usuario (105) puede incluir, entre otros, una estación de trabajo informatizada, una televisión interactiva, un quiosco interactivo, un dispositivo informático móvil personal, tal como un asistente digital, un teléfono móvil, un portátil o similares, un dispositivo de comunicaciones inalámbricas, una tarjeta inteligente, un dispositivo informático embebido o similares, que pueden interactuar con el enlace de comunicación (125). En tales sistemas alternativos, los sistemas operativos posiblemente serán diferentes y estarán adaptados al dispositivo específico. No obstante, de acuerdo con una realización, de manera ventajosa, los sistemas operativos continúan proporcionando los protocolos de comunicación 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 confidencial y almacenarla, que puede ser cualquier tipo o forma de datos, tal como, entre otros, texto, audio, video, datos de autenticación de usuarios y claves criptográficas públicas y privadas. De acuerdo con una realización, los datos de autenticación incluyen datos diseñados para identificar exclusivamente a un usuario del sistema criptográfico (100). Por ejemplo, los datos de autenticación pueden incluir un número de identificación de usuario, uno o más datos biométricos, y una serie de preguntas y respuestas generadas por el motor de confianza (110) o el usuario, pero respondidas inicialmente por el usuario en el registro. Las preguntas anteriores pueden incluir datos demográficos, tales como lugar de nacimiento, dirección, aniversario o similares, datos personales, tales como apellido de soltera de la madre, helado favorito o similares u otros datos diseñados exclusivamente para identificar al usuario. El motor de confianza (110) compara los datos de autenticación de un usuario asociados a una transacción actual con los datos de autenticación proporcionados con anterioridad, tal como, por ejemplo, durante el registro. De manera ventajosa, el motor de confianza (110) puede requerir al usuario que produzca los datos de autenticación en el momento de cada transacción o, de manera ventajosa, el motor de confianza (110) puede, permitir que el usuario produzca periódicamente los datos de autenticación, tal como al iniciar una serie de transacciones o al entrar en un sitio web del vendedor específico.

De acuerdo con la realización en la que el usuario produce datos biométricos, el usuario proporciona una característica física, tal como, entre otras, escáner de cara, escáner de mano, escáner de oreja, escáner de iris, escáner de retina, patrón vascular, ADN, una huella dactilar, escritura o habla, al dispositivo biométrico (107). De manera ventajosa, el dispositivo biométrico produce un patrón electrónico, o biométrico, de las características físicas. El patrón electrónico se transfiere a través del sistema de usuario (105) al motor de confianza (110) a efectos de registro o de 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 del registro (datos de autenticación de registro), el motor de confianza (110) provee al usuario de una funcionalidad criptográfica completa. Por ejemplo, de manera ventajosa, el usuario debidamente autenticado puede emplear el motor de confianza (110) para llevar a cabo resúmenes (hashing), firma digital, cifrado y descifrado (con frecuencia denominados conjuntamente cifrado), crear o distribuir certificados digitales y similares. No obstante, las claves criptográficas privadas que se usan 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 a cada usuario. Además, cuando las claves criptográficas incluyen tecnología de clave pública, cada clave privada asociada a un usuario se genera dentro del motor de confianza (110) y no sale de éste. Por consiguiente, mientras el usuario tenga acceso al motor de confianza (110), el usuario puede llevar a cabo funciones criptográficas usando su clave privada o pública. De manera ventajosa, dicho acceso remoto, permite a los usuarios mantener una movilidad total y acceder a la funcionalidad criptográfica a través de prácticamente cualquier conexión a internet, tal como, teléfonos móviles y satélites, quioscos, portátiles, habitaciones de hotel y similares.

De acuerdo con otra realización, el motor de confianza (110) lleva a cabo 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) primero autentica al usuario y una vez que el usuario ha proporcionado debidamente datos de autenticación que coinciden con los datos de autenticación de registro, el motor de confianza (110) usa su propio par de claves criptográficas para llevar a cabo funciones criptográficas en nombre del usuario autenticado.

Un experto en la materia reconocerá en la descripción de este documento que las claves criptográficas pueden incluir, de manera ventajosa, algunas de entre claves simétricas, claves públicas y claves privadas o todas. Además, un experto en la materia reconocerá en la descripción de este documento que las claves anteriores se pueden implementar con un gran número de algoritmos disponibles en tecnologías comerciales, tales como, por ejemplo, RSA, ELGAMAL o similares.

La figura 1 también ilustra la autoridad de certificación (115). De acuerdo con una realización, de manera ventajosa, la autoridad de certificación (115) puede comprender una organización o empresa independiente de confianza que expide certificados digitales, tal como, por ejemplo, VeriSign, Baltimore, Entrust o similares. De manera ventajosa, el motor de confianza (110) puede transmitir peticiones de certificados digitales, a través de uno o más protocolos de

certificados digitales, tales 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 una serie de protocolos diferentes, tales como, por ejemplo, PKCS7. De acuerdo con una realización de la invención, el motor de confianza (110) pide certificados digitales a varias de las autoridades de certificación (115) destacadas o a todas, de manera que el motor de confianza (110) tenga acceso a un certificado digital correspondiente al estándar de certificado de cualquier peticionario.

De acuerdo con otra realización, el motor de confianza (110) expide certificados internamente. 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 se piden, tal como por ejemplo, en el momento de la generación de claves o en el estándar de certificado pedido en el momento de la petición. El motor de confianza (110) se describirá más detalladamente más adelante.

La figura 1 también ilustra el sistema de vendedor (120). De acuerdo con una realización, de manera ventajosa, el sistema de vendedor (120) comprende un servidor web. Por lo general, los servidores web típicos sirven contenido por internet usando uno o varios lenguajes de marcado de internet o estándares de formato de documentos, tales como el Lenguaje de Marcado de Hipertexto (HTML) o el Lenguaje de Marcado Extensible (XML). El servidor web acepta peticiones desde navegadores tales como Netscape e Internet Explorer y, posteriormente, devuelve los documentos electrónicos apropiados. Se pueden usar una serie de tecnologías desde el cliente o servidor para aumentar la potencia del servidor web más allá de su capacidad de entregar documentos electrónicos estándar. Por ejemplo, dichas tecnologías incluyen guiones de Interfaz de Acceso Común (CGI), seguridad de la Capa de Conexión Segura (SSL) y Páginas de Servidor Activas (ASPs). De manera ventajosa, el sistema de vendedor (120) puede proporcionar contenido electrónico relativo a transacciones comerciales, personales, educativas o de otro tipo.

Si bien el sistema de vendedor (120) se describe haciendo referencia a las realizaciones anteriores, con las mismas no se pretende limitar la invención. Por el contrario, un experto en la materia reconocerá en la descripción de este documento que, de manera ventajosa, el sistema de vendedor (120) puede comprender cualquiera de los dispositivos que se describen haciendo referencia al sistema de usuario (105) o una combinación 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 y como se usa en toda esta descripción, es una red mundial de ordenadores. La estructura de internet, que es muy conocida para las personas con conocimientos normales de la materia, incluye un núcleo central de redes con redes que se ramifican desde el núcleo central. Dichas ramificaciones, a su vez, tienen redes que se ramifican desde las mismas, etc. Enrutadores mueven paquetes de información entre niveles de red y, posteriormente, de red a red, hasta que el paquete llega a la zona 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 centros de encaminamiento de internet comprenden servidores de sistema de nombres de dominio (DNS) que usan un Protocolo de Control de Transmisión/ Protocolo de Internet (TCP/IP) como bien se conoce en la técnica. Los centros de encaminamiento conectan a uno o más centros de encaminamiento distintos a través de enlaces de comunicación de alta velocidad.

Una parte popular de internet es la Red Informática Mundial. La Red Informática Mundial contiene diferentes ordenadores que almacenan documentos capaces de visualizar información gráfica y de texto. Los ordenadores que proporcionan información en la Red Informática Mundial normalmente se denominan “sitios web”. Un sitio web está definido por una dirección de internet que tiene una página electrónica asociada. La página electrónica se puede identificar por medio de un Localizador Uniforme de Recursos (URL). Por lo general, una página electrónica es un documento que organiza la presentación de texto, imágenes gráficas, audio, video, etc.

Si bien el enlace de comunicación (125) se describe en términos de su realización preferente, alguien con conocimientos normales de la materia reconocerá en la descripción de este documento que el enlace de comunicación (125) puede incluir una amplia gama de enlaces de comunicación interactivos. Por ejemplo, el enlace de comunicación (125) puede incluir redes de televisiones interactivas, redes telefónicas, sistemas de transmisión inalámbrica de datos, sistemas de cables bidireccionales, redes informáticas públicas o privadas personalizadas, redes de quioscos interactivos, redes de cajeros automáticos, enlaces directos, redes satélites 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 transacciones (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 un dispositivo de almacenamiento masivo (225). Como se muestra además en la figura 2, el motor de transacciones (205) se comunica con el depósito (210), con el motor de autenticación (215) y con el motor criptográfico (220), además de con el dispositivo de almacenamiento masivo (225). Además, el depósito (210) se comunica con el motor de autenticación (215), con el motor criptográfico (220) y con el dispositivo de almacenamiento masivo (225). Además, el motor de autenticación (215) se comunica con el motor criptográfico (220). De acuerdo con una realización de la invención, de manera ventajosa, algunas de las comunicaciones anteriores o todas pueden comprender la trasmisión de documentos XML a direcciones IP que corresponden al dispositivo receptor. Como se ha mencionado anteriormente, de manera ventajosa los documentos XML permiten a los diseñadores crear sus propias etiquetas de documentos personalizadas, posibilitando la definición, transmisión, validación e interpretación de datos entre aplicaciones y entre organizaciones. Además, algunas de las comunicaciones anteriores o todas pueden incluir tecnologías SSL convencionales.

De acuerdo con una realización, el motor de transacciones (205) comprende un dispositivo de encaminamiento de datos, tal como un servidor web convencional comercializado por Netscape, Microsoft, Apache o similares. Por ejemplo, de manera ventajosa, el servidor web puede recibir datos entrantes desde el enlace de comunicación (125). De acuerdo con una realización de la invención, los datos entrantes se direccionan a un sistema frontal de seguridad del motor de confianza (110). Por ejemplo, de manera ventajosa, el sistema frontal de seguridad puede incluir un cortafuego, un sistema de detección de intrusiones que busca perfiles de ataque conocidos y/o un explorador de virus. Una vez vaciado el sistema frontal de seguridad, el motor de transacciones (205) recibe los datos y los encamina hacia uno de entre el depósito (210), el motor de autenticación (215), el motor criptográfico (220) y el dispositivo de almacenamiento masivo (225). Además, el motor de transacciones (205) supervisa los datos entrantes desde el motor de autenticación (215) y desde el motor criptográfico (220) y encamina los datos hacia sistemas específicos a través del enlace de comunicación (125). Por ejemplo, de manera ventajosa, el motor de transacciones (205) puede encaminar datos hacia el sistema de usuario (105), la autoridad de certificación (115) o el sistema de vendedor (120).

De acuerdo con una realización, los datos se encaminan usando técnicas de encaminamiento HTTP convencionales, tales como, por ejemplo, empleando URLs o Indicadores Uniformes de Recursos (URIs). Los URIs son similares a los URLs, no obstante, los URIs normalmente indican la fuente de los archivos o acciones, tales como, por ejemplo, ejecutables, guiones y similares. Por lo tanto, de acuerdo con una realización, de manera ventajosa, el sistema de usuario (105), la autoridad de certificación (115), el sistema de vendedor (120) y los componentes del motor de confianza (210) incluyen datos suficientes dentro de la comunicación URLs o URIs para que el motor de transacciones (205) encamine debidamente los datos por todo el sistema criptográfico.

Si bien el encaminamiento de datos se describe haciendo referencia a su realización preferente, un experto en la materia reconocerá un gran número de estrategias o soluciones posibles de encaminamiento de datos. Por ejemplo, de manera ventajosa, XML u otros paquetes de datos se pueden desenvolver y reconocer por su formato, contenido o similares, de manera que el motor de transacciones (205) pueda encaminar debidamente los datos por todo el motor de confianza (110). Además, un experto en la materia reconocerá que, de manera ventajosa, el encaminamiento de datos se puede adaptar a los protocolos de transferencia de datos que se ajusten a sistemas de redes específicos, tales como, por ejemplo, cuando el enlace de comunicación (125) comprende una red local.

De acuerdo con otra realización más de la invención, el motor de transacciones (205) incluye tecnologías de cifrado SSL convencionales, de manera que los sistemas anteriores se puedan autenticar y, viceversa, con el motor de transacciones (205) durante comunicaciones específicas. Tal y como se usará en esta descripción el término "½ SSL" se refiere a comunicaciones en las que un servidor, pero no necesariamente el cliente, está autenticado en SSL y el término "SSL COMPLETA" se refiere a comunicaciones en las que el cliente y el servidor están autenticados en SSL. Cuando en la presente descripción se usa el término "SSL", la comunicación puede comprender ½ SSL o SSL COMPLETA.

A medida que el motor de transacciones (205) encamina datos a los distintos componentes del sistema criptográfico (100), de manera ventajosa, el motor de transacciones (205) puede crear una pista de auditoría. De acuerdo con una realización, la pista de auditoría incluye un registro de al menos el tipo y el formato de los datos encaminados por el motor de transacciones (205) por todo el sistema criptográfico (100). De manera ventajosa, dichos datos de auditoría se pueden almacenar en el dispositivo de almacenamiento masivo (225).

La figura 2 también ilustra el depósito (210). De acuerdo con una realización, el depósito (210) comprende uno o más equipos de almacenamiento de datos, tal como, por ejemplo, un servidor de directorios, un servidor de bases de datos o similares. Como se muestra en la figura 2, el depósito (210) almacena claves criptográficas y datos de autenticación de registro. De manera ventajosa, las claves criptográficas pueden corresponder al motor de confianza (110) o a usuarios del sistema criptográfico (100), tales como el usuario o el vendedor. De manera ventajosa, los datos de autenticación de registro pueden incluir datos diseñados para identificar exclusivamente a un usuario, tales como, ID de usuario, contraseñas, respuesta a preguntas, datos biométricos o similares. De manera ventajosa, los datos de autenticación de registro se pueden obtener al registrarse un usuario o en otro momento posterior alternativo. Por ejemplo, el motor de confianza (110) puede incluir renovaciones o reexpediciones periódicas o de otro tipo de los datos de autenticación de registro.

De acuerdo con otra realización, la comunicación desde el motor de transacciones (205) hacia y desde el motor de autenticación (215) y el motor criptográfico (220) comprende una comunicación segura, tal como, por ejemplo, tecnología SSL convencional. Además, como se ha mencionado anteriormente, los datos de las comunicaciones hacia y desde el depósito (210) se pueden transferir usando documentos XML, HTTP, URIs o URLs, teniendo cualquiera de los anteriores, de manera ventajosa, peticiones de datos y formatos embebidos en los mismos.

Como se ha mencionado anteriormente, de manera ventajosa, el depósito (210) puede comprender una pluralidad de equipos de almacenamiento de datos seguros. En una realización de este tipo, los equipos de almacenamiento de datos seguros pueden estar configurados de manera que una puesta en peligro de la seguridad de un equipo de almacenamiento de datos individual no pondrá en peligro las claves criptográficas o los datos de autenticación almacenados en el mismo. Por ejemplo, de acuerdo con esta realización, las claves criptográficas y los datos de autenticación se operan matemáticamente a fin de aleatorizar sustancial y estadísticamente los datos almacenados en cada equipo de almacenamiento de datos. De acuerdo con una realización, la aleatorización de los datos de un equipo de almacenamiento de datos individual hace que esos datos resulten indescifrables. Por consiguiente, la puesta en peligro de un equipo de almacenamiento de datos individual sólo produce un número indescifrable aleatorio y no pone en peligro la seguridad de cualquier clave criptográfica o los datos de autenticación en su totalidad.

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 del motor de transacciones (205) con datos del depósito (210). Por ejemplo, durante la autenticación, un usuario suministra datos de autenticación actuales al motor de confianza (110) de manera que el motor de transacciones (205) reciba los datos de autenticación actuales. Como se ha mencionado anteriormente, el motor de transacciones (205) reconoce las peticiones de datos, preferentemente en el URL o URI, y encamina los datos de autenticación hacia el motor de autenticación (215). Además, previa petición, el depósito (210) remite, al motor de autenticación (215), datos de autenticación de registro correspondientes al usuario. Por consiguiente, el motor de autenticación (215) tiene tanto los datos de autenticación actuales como los datos de autenticación de registro para su comparación.

De acuerdo con una realización, las comunicaciones hacia el motor de autenticación comprenden comunicaciones seguras, tales como por ejemplo, tecnología SSL. Adicionalmente, se puede proporcionar seguridad dentro de los componentes del motor de confianza (110), tal como, por ejemplo, supercifrado usando tecnologías de claves públicas. 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 registro con la clave pública del motor de autenticación (215). De ese modo, sólo se puede usar 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, de manera ventajosa, proporcionar funciones criptográficas convencionales, tales como, por ejemplo, funcionalidad de infraestructura de clave pública (PKI). Por ejemplo, de manera ventajosa, el motor criptográfico (220) puede expedir claves públicas y privadas para usuarios del sistema criptográfico (100). De este modo, las claves criptográficas se generan en el motor criptográfico (220) y se remiten al depósito (210), de manera que al menos las claves criptográficas privadas no estén disponibles fuera del motor de confianza (110). De acuerdo con otra realización, el motor criptográfico (220) aleatoriza y divide al menos los datos de la clave criptográfica privada, almacenando de ese modo sólo los datos divididos y aleatorios. Similar a la división de los datos de autenticación de registro, el proceso de división garantiza que las claves almacenadas no estén disponibles fuera del motor criptográfico (220). De acuerdo con otra realización, las funciones del motor criptográfico se pueden combinar y llevar a cabo con el motor

de autenticación (215).

De acuerdo con otra realización, las comunicaciones hacia y desde el motor criptográfico incluyen comunicaciones seguras, tales como tecnología SSL. Además, de manera ventajosa, se pueden emplear documentos XML para transferir datos y/o hacer peticiones de funciones criptográficas.

La figura 2 también ilustra el motor de confianza (110) que tiene el dispositivo de almacenamiento masivo (225). Como se ha mencionado anteriormente, el motor de transacciones (205) mantiene datos correspondientes a una pista de auditoría y almacena dichos datos en el dispositivo de almacenamiento masivo (225). Asimismo, de acuerdo con una realización de la invención, el depósito (210) mantiene datos correspondientes a una pista de auditoría y almacena dichos datos en el dispositivo de almacenamiento masivo (225). Los datos de la pista de auditoría del depósito son similares a los del motor de transacciones (205) por el hecho de que los datos de la pista de auditoría comprenden un registro de las peticiones recibidas por el depósito (210) y la respuesta del mismo. Además, el dispositivo de almacenamiento masivo (225) se puede usar para almacenar certificados digitales que tienen la clave pública de un usuario contenida en los mismos.

Si bien el motor de confianza (110) se describe haciendo referencia a sus realizaciones preferentes y alternativas, con las mismas no se pretende limitar la invención. Por el contrario, 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, de manera ventajosa, el motor de confianza (110) puede llevar a cabo sólo la autenticación o, alternativamente, sólo algunas de las funciones criptográficas o todas, tales como cifrado y descifrado de datos. De acuerdo con dichas realizaciones, de manera ventajosa, se puede eliminar uno de entre el motor de autenticación (215) y el motor criptográfico (220), creando así un diseño más sencillo del motor de confianza (110). Además, el motor criptográfico (220) también se puede comunicar con una autoridad de certificación, de manera que la autoridad de certificación esté incorporada en el motor de confianza (110). De acuerdo con otra realización más, de manera ventajosa, el motor de confianza (110) puede llevar a cabo la autenticación y una o más funciones criptográficas, tales como, por ejemplo, firma digital.

La figura 3 ilustra un diagrama de bloques del motor de transacciones (205) de la figura 2 de acuerdo con aspectos de una realización de la invención. De acuerdo con esta realización, el motor de transacciones (205) comprende un sistema operativo (305) que tiene un hilo de tratamiento y un hilo de escucha. De manera ventajosa, el sistema operativo (305) puede ser similar a los que se encuentran en servidores de gran capacidad convencionales, tales como, por ejemplo, servidores web comercializados por Apache. El hilo de escucha supervisa la comunicación entrante desde uno de entre el enlace de comunicación (125), el motor de autenticación (215) y el motor criptográfico (220) para el flujo de datos entrantes. El hilo de tratamiento reconoce estructuras de datos específicas del flujo de datos entrantes, tales como, por ejemplo, las estructuras de datos anteriores, encaminando de ese modo los datos entrantes hacia uno de entre el enlace de comunicación (125), el depósito (210), el motor de autenticación (215), el motor criptográfico (220) o el dispositivo de almacenamiento masivo (225). Como se muestra en la figura 3, de manera ventajosa, los datos entrantes y salientes se pueden asegurar mediante, por ejemplo, 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). Una gran variedad de fabricantes, tales como Netscape, ISO y otros, comercializan servidores de directorios LDAP. La figura 4 también muestra que, preferentemente, el servidor de directorios almacena datos (405) correspondientes a las claves criptográficas y datos (410) correspondientes a los datos de autenticación de registro. De acuerdo con una realización, el depósito (210) comprende una estructura única de memoria lógica que indexa datos de autenticación y datos de claves criptográficas a una ID de usuario exclusiva. Preferentemente, la estructura única de memoria lógica incluye mecanismos para garantizar un alto grado de confianza o seguridad en los datos almacenados en la misma. Por ejemplo, de manera ventajosa, la ubicación física del depósito (210) puede incluir un gran número de medidas de seguridad convencionales, tales como, acceso limitado de los empleados, modernos sistemas de vigilancia y similares. Además de las seguridades físicas, o en lugar de éstas, de manera ventajosa, el servidor o sistema informático puede incluir soluciones de software para proteger los datos almacenados. Por ejemplo, de manera ventajosa, el depósito (210) puede crear y almacenar datos (415) correspondientes a una pista de auditoría de acciones emprendidas. Además, de manera ventajosa, las comunicaciones entrantes y salientes se pueden cifrar con cifrado de claves públicas unido a tecnologías SSL convencionales.

De acuerdo con otra realización, el depósito (210) puede comprender distintos equipos de almacenamiento de datos y físicamente separados, como se describe detalladamente haciendo 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. Similar al motor de transacciones (205) de la figura 3, el motor de autenticación (215) comprende un sistema operativo (505) que tiene al menos una escucha y un hilo de tratamiento de una versión modificada de un servidor web convencional, tal como, por ejemplo, servidores web comercializados por Apache. Como se muestra en la figura 5, el motor de autenticación (215) incluye acceso al menos a una clave privada (510). De manera ventajosa, la clave privada (510) se puede usar, por ejemplo, para descifrar datos del motor de transacciones (205) o del depósito (210) que se cifraron 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 preferente de la invención, el comparador (515) incluye tecnología capaz de comparar patrones potencialmente complejos relacionados con los datos biométricos de autenticación anteriores. La tecnología puede incluir hardware, software o soluciones combinadas para comparaciones de patrones, tales como, por ejemplo, las que representan patrones de huella dactilar o patrones de voz. Además, de acuerdo con una realización, de manera ventajosa, el comparador (515) del motor de autenticación (215) puede comparar resúmenes (hashes) convencionales de documentos a fin de dar un resultado de comparación. De acuerdo con una realización de la invención, el comparador (515) incluye la aplicación de heurística (530) para la comparación. De manera ventajosa, la heurística (530) puede tratar circunstancias relacionadas con un intento de autenticación, tales como, por ejemplo, la hora del día, dirección IP o enmascaramiento de subred, perfil de compra, dirección de correo electrónico, ID o número de serie del procesador o similares.

Además, la naturaleza de las comparaciones de datos biométricos puede tener como resultado que se produzcan varios grados de certidumbre a partir de la coincidencia de datos biométricos de autentificación actuales con datos de registro. Por ejemplo, a diferencia de la contraseña tradicional que sólo puede devolver una coincidencia positiva o negativa, se puede determinar que una huella dactilar sea una coincidencia parcial, por ejemplo, una coincidencia del 90%, una coincidencia del 75% o una coincidencia del 10%, en lugar de que simplemente sea correcta o incorrecta. Otros identificadores biométricos, tales como análisis de características de la voz o reconocimiento facial pueden compartir esta propiedad de autenticación probabilística, en lugar de autenticación absoluta.

Cuando se trabaja con dicha autenticación probabilística o en otros casos en los que una autenticación se considera menos que absolutamente fidedigna, es aconsejable aplicar la heurística (530) para determinar si el nivel de certidumbre de la autenticación proporcionada es lo suficientemente alto como para autenticar la transacción que se está realizando.

A veces se dará el caso de que la transacción en cuestión sea una transacción de valor relativamente bajo en la que es aceptable ser autenticado a un nivel inferior de certidumbre. Esto podría incluir una transacción que tiene un valor bajo en dólares asociado a la misma (por ejemplo, una compra de 10$) o una transacción con bajo riesgo (por ejemplo, admisión en un sitio web sólo para socios).

A la inversa, para autenticar otras transacciones puede ser aconsejable requerir un alto grado de certidumbre de la autenticación antes de permitir que la transacción continúe. Dichas transacciones pueden incluir transacciones de alto valor en dólares (por ejemplo, firmar un contrato de suministro de varios millones de dólares) o transacciones con un alto riesgo si tiene lugar una autenticación indebida (por ejemplo, entrar a distancia en un ordenador gubernamental).

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

De acuerdo con otra realización de la invención, de manera ventajosa, el comparador (515) puede hacer un seguimiento de los intentos de autenticación correspondientes a una transacción específica. Por ejemplo, cuando una transacción falla, el motor de confianza (110) puede pedir al usuario que vuelva a introducir sus datos de autenticación actuales. De manera ventajosa, el comparador (515) del motor de autenticación (215) puede emplear un limitador de intentos (535) para limitar el número de intentos de autenticación, prohibiendo de ese modo los intentos por la fuerza para imitar los datos de autenticación de un usuario. De acuerdo con una realización, el limitador de intentos (535) comprende un módulo de software que supervisa las transacciones en busca de repetidos intentos de autenticación y, por ejemplo, que limita a tres los intentos de autenticación para una transacción

determinada. Por consiguiente, el limitador de intentos (535) limitará un intento automático para imitar los datos de autenticación de un individuo, por ejemplo, a simplemente tres “oportunidades”. Tras tres intentos fallidos, de manera ventajosa, el limitador de intentos (535) puede denegar intentos de autenticación adicionales. De manera ventajosa, dicha denegación se puede implementar, por ejemplo, mediante la devolución por parte del comparador (515) de un resultado negativo independientemente de que se transmitan los datos de autenticación actuales. Por otro lado, de manera ventajosa, el motor de transacciones (205) puede bloquear cualquier intento de autenticación adicional relacionado con una transacción en la que los tres intentos anteriores fueron fallidos.

El motor de autenticación (215) también incluye el módulo de división de datos (520) y el módulo de ensamblaje de datos (525). De manera ventajosa, el módulo de división de datos (520) comprende un módulo de software, de hardware o combinado que tiene la capacidad de operar matemáticamente sobre varios datos a fin de aleatorizar sustancialmente y dividir los datos en partes. De acuerdo con una realización, los datos originales no se pueden recrear a partir de una parte individual. De manera ventajosa, el módulo de ensamblaje de datos (525) comprende un módulo de software, de hardware o combinado configurado para operar matemáticamente sobre las partes anteriores sustancialmente aleatorias, de manera que la combinación de las mismas proporciona los datos originales descifrados. 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 registro en partes y emplea el módulo de ensamblaje de datos (525) para reensamblar las partes en datos de autenticación de registro 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. Similar al motor de transacciones (205) de la figura 3, el motor criptográfico (220) comprende un sistema operativo (605) que tiene al menos una escucha y un hilo de tratamiento de una versión modificada de un servidor web convencional, tal como, por ejemplo, servidores web comercializados 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. No obstante, de acuerdo con una realización, el módulo de división de datos (610) y el módulo de ensamblaje de datos (620) procesan datos de claves criptográficas, en contraposición a los datos de autenticación de registro anteriores. No obstante, un experto en la materia reconocerá en la descripción de este documento que el módulo de división de datos (910) y el módulo de división de datos (620) se pueden combinar con los del motor de autenticación (215).

El motor criptográfico (220) también comprende un módulo de tratamiento criptográfico (625) configurado para llevar a cabo una o alguna de un gran número de funciones criptográficas o todas. De acuerdo con una realización, el módulo de tratamiento criptográfico (625) puede comprender módulos de software o programas, hardware o ambos. De acuerdo con otra realización, el módulo de tratamiento criptográfico (625) puede llevar a cabo comparaciones de datos, análisis sintáctico de datos, división de datos, separación de datos, resúmenes de datos, cifrado o descifrado de datos, creación o verificación de firmas digitales, generación de certificados digitales, almacenamiento o peticiones, generación de claves criptográficas o similares. Además, un experto en la materia reconocerá en la descripción de este documento que, de manera ventajosa, el módulo de tratamiento criptográfico (825) puede comprender una 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 llevar a cabo 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 módulos o programas informáticos, hardware o ambos para implementar funciones continuas, transparentes y de interoperabilidad.

Un experto en la materia también reconocerá en la descripción de este documento que la funcionalidad criptográfica puede incluir un gran número o variedad de funciones, por lo general, relacionadas 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, de manera ventajosa, el sistema de depósito (700) comprende múltiples equipos de almacenamiento de datos, por ejemplo, equipos de almacenamiento de datos (D1), (D2), (D3) y (D4). No obstante, alguien con conocimientos normales de la materia entenderá fácilmente que el sistema de depósito puede tener sólo un equipo de almacenamiento de datos. De acuerdo con una realización de la invención, de manera ventajosa, cada uno de los equipos de almacenamiento de datos (D1 a D4) puede comprender algunos de los elementos que se describen haciendo referencia al depósito (210) de la figura 4 o todos. Similar al depósito (210), los equipos de almacenamiento de datos (D1 a D4) se comunican con el motor de transacciones (205), con el motor de autenticación (215) y con el motor criptográfico (220), preferentemente, mediante SSL convencional. Enlaces de comunicación que transfieren, por ejemplo, documentos XML. De manera ventajosa, las

comunicaciones desde el motor de transacciones (205) pueden incluir peticiones de datos, donde la petición se difunde, de manera ventajosa, a la dirección IP de cada equipo de almacenamiento de datos (D1 a D4). Por otro lado, el motor de transacciones (205) puede difundir peticiones a equipos de almacenamiento de datos específicos en función de un gran número de criterios, tales como, por ejemplo, tiempo de respuesta, cargas de servidor, calendarios de mantenimiento o similares.

En respuesta a peticiones de datos del motor de transacciones (205), de manera ventajosa, el sistema de depósito (700) remite datos almacenados al motor de autenticación (215) y al motor criptográfico (220). Los respectivos módulos de ensamblaje de datos reciben los datos remitidos y ensamblan los datos en formatos utilizables. Por otro lado, las comunicaciones desde el motor de autenticación (215) y el motor criptográfico (220) hacia los equipos de almacenamiento de datos (D1 a D4) pueden incluir la transmisión de los datos confidenciales que se almacenarán. Por ejemplo, de acuerdo con una realización, de manera ventajosa el motor de autenticación (215) y el motor criptográfico (220) pueden emplear sus módulos respectivos de división de datos para dividir datos confidenciales en partes indescifrables y, posteriormente, transmitir una o más partes indescifrables de los datos confidenciales a un equipo de almacenamiento de datos específico.

De acuerdo con una realización, cada equipo de almacenamiento de datos, (D1 a D4), comprende un sistema de almacenamiento separado e independiente, tal como, por ejemplo, un servidor de directorios. 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 confidenciales en equipos de almacenamientos distintos e independientes (D1 a D4), de los que algunos o todos pueden estar, de manera ventajosa, separados geográficamente, el sistema de depósito (700) proporciona redundancia junto con medidas de seguridad adicionales. Por ejemplo, de acuerdo con una realización, sólo se necesitan datos de dos de los múltiples equipos de almacenamiento de datos, (D1 a D4), para descifrar y reensamblar los datos confidenciales. Por consiguiente, hasta dos de los cuatro equipos de almacenamiento de datos (D1 a D4) pueden no funcionar debido a mantenimiento, fallo del sistema, corte en el suministro eléctrico o similar, sin que afecte a la funcionalidad del motor de confianza (110). Además, dado que, de acuerdo con una realización, los datos almacenados en cada equipo de almacenamiento de datos son aleatorios e indescifrables, la puesta en peligro de cualquier equipo de almacenamiento de datos individual no necesariamente pone en peligro los datos confidenciales. Además, en la realización que tiene separación geográfica de los equipos de almacenamiento de datos, una puesta en peligro de múltiples equipos remotos geográficamente resulta cada vez más difícil. De hecho, incluso para un empleado deshonesto será un gran reto trastocar los múltiples equipos de almacenamiento de datos remotos geográficamente e independientes necesarios.

Se bien el sistema de depósito (700) se describe haciendo referencia a sus realizaciones alternativas y preferentes, con las mismas no se pretende limitar la invención. Por el contrario, un experto en la materia reconocerá en 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 uno, dos o más equipos de almacenamiento de datos. Además, los datos confidenciales se pueden operar matemáticamente de manera que se necesiten partes de dos o más equipos de almacenamiento de datos para reensamblar y descifrar los datos confidenciales.

Como se ha mencionado anteriormente, 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 confidenciales, tales como, por ejemplo, texto, audio, video, los datos de autenticación y los datos de claves criptográficas. La figura 8 ilustra un diagrama de flujo de un proceso de división de datos (800) que lleva a cabo 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 el módulo de división de datos del motor de autenticación (215) o del motor criptográfico (220) recibe datos confidenciales “S”. Preferentemente, en la etapa (810), el módulo de división de datos genera un número, valor o cadena o conjunto de bits sustancialmente aleatorio, “A”. Por ejemplo, el número aleatorio (A) se puede generar en un gran número de diversas técnicas convencionales disponibles para alguien con conocimientos normales de la materia, para producir números aleatorios de gran calidad adecuados para uso en aplicaciones criptográficas. Además, de acuerdo con una realización, el número aleatorio (A) comprende una longitud de bit que puede ser cualquier longitud adecuada, tal como más corta, más larga o igual que la longitud de bits de los datos confidenciales, (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 manera ventajosa, la generación de números estadísticamente aleatorios (A) y (C) se puede hacer en paralelo. El módulo de división de datos combina los números (A) y (C) con los datos confidenciales (S), de manera que se generen 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 función “or exclusiva”, es muy conocida para alguien con conocimientos normales de la materia. Preferentemente, las combinaciones anteriores tienen lugar en las etapas (825) y (830), respectivamente, y de acuerdo con una realización, las combinaciones anteriores también tienen lugar en paralelo. A continuación, el proceso de división de datos (800) pasa a la etapa (835) en la que los números aleatorios (A) y (C) y los números (B) y (D) se emparejan, de manera que ninguna de las parejas contenga datos suficientes, por sí misma, para reorganizar y descifrar los datos confidenciales originales (S). Por ejemplo, los números se pueden emparejar como sigue: AC, AD, BC y BD. De acuerdo con una realización, cada una de las parejas anteriores se distribuye a uno de los depósitos (D1 a D4) de la figura 7. De acuerdo con otra realización, cada una de las parejas anteriores se distribuye aleatoriamente a uno de los depósitos (D1 a D4). Por ejemplo, durante un primer proceso de división de datos (800), la pareja AC se puede enviar al depósito (D2), por ejemplo, mediante una selección aleatoria de la dirección IP de (D2). Posteriormente, durante un segundo proceso de división de datos (800) la pareja AC se puede enviar al depósito (D4), por ejemplo, mediante una selección aleatoria de la dirección IP de (D4). Además, todas las parejas se pueden almacenar en un depósito y se pueden almacenar en ubicaciones independientes de dicho depósito.

En función de lo anterior, de manera ventajosa, el proceso de división de datos (800) coloca partes de los datos confidenciales en cada uno de los cuatro equipos de almacenamiento de datos (D1 a D4), de manera que ningún equipo de almacenamiento de datos (D1 a D4) incluya datos cifrados suficientes para recrear los datos confidenciales originales (S). Como se ha mencionado anteriormente, dicha aleatorización de los datos en partes cifradas inutilizables por separado aumenta la seguridad y proporciona una confianza continua en los datos incluso si se pone en peligro uno de los equipos de almacenamiento de datos, (D1 a D4).

Si bien el proceso de división de datos (800) se describe haciendo referencia a su realización preferente, con la misma no se pretende limitar la invención. Por el contrario, un experto en la materia reconocerá en la descripción de este documento, un gran número de alternativas para el proceso de división de datos (800). Por ejemplo, de manera ventajosa, el proceso de división de datos puede dividir los datos en dos números, por ejemplo, el número aleatorio (A) y el número (B) y distribuir aleatoriamente (A) y (B) a través de dos equipos de almacenamiento de datos. Además, de manera ventajosa, el proceso de división de datos (800) puede dividir los datos entre un gran número de equipos de almacenamiento de datos mediante la generación de números aleatorios adicionales. Los datos se pueden dividir en cualquier unidad de tamaño deseada, seleccionada, predeterminada o asignada aleatoriamente, que incluye, entre otras, un bit, bits, bytes, kilobytes, megabytes o mayor o cualquier combinación o secuencia de tamaños. Además, variar los tamaños de unidad de datos que resultan del proceso de división puede hacer que resulte más difícil restablecer los datos a una forma utilizable, aumentando de ese modo la seguridad de los datos confidenciales. Resultará evidente para alguien con conocimientos normales de la materia que los tamaños de unidad de datos divididos pueden ser una gran variedad de tamaños de unidad de datos, patrones de tamaños o combinaciones de tamaños. Por ejemplo, los tamaños de unidad de datos se pueden seleccionar o predeterminar para que todos sean del mismo tamaño, un conjunto fijo de tamaños diferentes, una combinación de tamaños o tamaños generados aleatoriamente. Asimismo, las unidades de datos se pueden distribuir en una o más porciones 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 porción.

Como se ha mencionado anteriormente, a fin de recrear los datos confidenciales (S), es necesario eliminar la aleatoriedad de las partes de datos y reorganizarlas. De manera ventajosa, este proceso puede tener lugar en los módulos de ensamblaje de datos, (525) y (620), del motor de autenticación (215) y del motor criptográfico (220), respectivamente. El módulo de ensamblaje de datos, por ejemplo, módulo de ensamblaje de datos (525), recibe partes de datos de los equipos de almacenamiento de datos (D1 a D4) y reensambla los datos en forma utilizable. Por ejemplo, de acuerdo con una realización en la que el módulo de división de datos (520) empleó el proceso de división de datos (800) de la figura 8, el módulo de ensamblaje de datos (525) usa partes de datos de al menos dos de los equipos de almacenamiento de datos (D1 a D4) para recrear los datos confidenciales (S). Por ejemplo, las parejas de AC, AD, BC y BD, se distribuyeron de manera que dos cualquiera proporcionen uno de entre (A) y (B) ó (C) y (D). Cabe señalar que S = A XOR B o S = C XOR D indica que cuando el módulo de ensamblaje de datos recibe uno de entre (A) y (B) o (C) y (D), de manera ventajosa, el módulo de ensamblaje de datos (525) puede reensamblar los datos confidenciales (S). Por consiguiente, el módulo de ensamblaje de datos (525) puede ensamblar los datos confidenciales (S) cuando, por ejemplo, recibe partes de datos de al menos los dos primeros de los equipos de almacenamiento de datos (D1 a D4) para responder a una petición de ensamblaje por parte del motor de confianza (110).

En función de los procesos de división y ensamblaje de datos anteriores, los datos confidenciales (S) existen en

formato utilizable sólo en un área limitada del motor de confianza (110). Por ejemplo, cuando los datos confidenciales (S) incluyen datos de autenticación de registro, los datos de autenticación de registro utilizables y no aleatorios sólo están disponibles en el motor de autenticación (215). Del mismo modo, cuando los datos confidenciales (S) incluyen datos de claves criptográficas privadas, los datos de claves criptográficas privadas utilizables y no aleatorios sólo están disponibles en el motor criptográfico (220).

Si bien los procesos de división y ensamblaje de datos se describen haciendo referencia a sus realizaciones preferentes, con las mismas no se pretende limitar la invención. Por el contrario, un experto en la materia reconocerá en la descripción de este documento, un gran número de alterativas para dividir y reensamblar los datos confidenciales (S). Por ejemplo, se puede usar cifrado de claves públicas para asegurar aún más los datos en los equipos de almacenamiento de datos (D1 a D4). Además, resultará fácilmente evidente para alguien con conocimientos normales de la materia que el módulo de división de datos que se describe en este documento también es un realización distinta e independiente de la presente invención que se puede incorporar en sistemas informáticos, paquetes de software, bases de datos o combinaciones de los mismos preexistentes, se puede combinar con éstos o puede formar parte de los mismos u otras realizaciones de la presente invención, tales como el motor de confianza, el motor de autenticación y el motor de transacciones que se describen en este documento.

La figura 9A ilustra un flujo de datos de un proceso de registro (900) de acuerdo con aspectos de una realización de la invención. Como se muestra en la figura 9A, el proceso de registro (900) comienza en la etapa (905) cuando un usuario desea registrarse con el motor de confianza (110) del sistema criptográfico (100). De acuerdo con esta realización, de manera ventajosa, el sistema de usuario (105) incluye una miniaplicación de cliente, tal como una basada en Java, que solicita al usuario que introduzca datos de registro, tales como datos demográficos y datos de autenticación de registro. De acuerdo con una realización, los datos de autenticación de registro incluyen, ID de usuario, contraseñas, datos biométricos o similares. De acuerdo con una realización, durante el proceso de solicitud, preferentemente, la miniaplicación de cliente se comunica con el motor de confianza (110) para garantizar que una ID de usuario elegida es exclusiva. Cuando la ID de usuario no es exclusiva, de manera ventajosa, el motor de confianza (110) puede sugerir una ID de usuario exclusiva. La miniaplicación de cliente reúne los datos de registro y transmite los datos de registro, por ejemplo, mediante un documento XML, al motor de confianza (110) y, en particular, al motor de transacciones (205). De acuerdo con una realización, la transmisión se codifica con la clave pública del motor de autenticación (215).

De acuerdo con una realización, el usuario lleva a cabo un único registro durante la etapa (905) del proceso de registro (900). Por ejemplo, el usuario se registra como una persona específica, tal como Usuario Joe. Cuando Usuario Joe desea registrarse como Usuario Joe, Presidente de Mega Corp., de acuerdo con esta realización, Usuario Joe se registra una segunda vez, recibe una segunda ID de usuario exclusiva y el motor de confianza (110) no asocia las dos identidades. De acuerdo con otra realización de la invención, el proceso de registro (900) prevé múltiples identidades de usuario para una única ID de usuario. Por consiguiente, en el ejemplo anterior, de manera ventajosa, el motor de confianza (110) asociará las dos identidades del Usuario Joe. Como entenderá un experto en la materia, gracias a la descripción de este documento, un usuario puede tener muchas identidades, por ejemplo, Usuario Joe el cabeza de familia, Usuario Joe el miembro de las Fundaciones de Beneficencia y similares. A pesar de que el usuario puede tener múltiples identidades, de acuerdo con esta realización, preferentemente, el motor de confianza (110) sólo almacena un conjunto de datos de registro. Además, de manera ventajosa, los usuarios pueden añadir, editar/actualizar o borrar identidades según se necesiten.

Si bien el proceso de registro (900) se describe haciendo referencia a su realización preferente, con la misma no se pretende limitar la invención. Por el contrario, un experto en la materia reconocerá en la descripción de este documento, un gran número de alternativas para recopilar datos de registro y, en particular, datos de autenticación de registro. Por ejemplo, la miniaplicación puede ser una miniaplicación basada en modelo común de objetos (COM) o similar.

Por otro lado, el proceso de registro puede incluir registro escalonado. Por ejemplo, a un nivel más bajo de registro, el usuario puede registrarse a través del enlace de comunicación (125) sin producir documentación relativa a su identidad. De acuerdo con un nivel mayor de registro, el usuario se registra usando un tercero de confianza, tal como un notario digital. Por ejemplo, el usuario puede comparecer ante el tercero de confianza, producir credenciales, tales como un certificado de nacimiento, un carné de conducir, una ID militar o similares y, de manera ventajosa, el tercero de confianza puede incluir, por ejemplo, su firma digital en la presentación del registro. El tercero de confianza puede incluir un notario propiamente dicho, un organismo gubernamental, tal como la Oficina de Correos o la Dirección General de Tráfico, una persona de recursos humanos de una empresa grande que registra a un empleado o similar. Un experto en la materia entenderá, gracias a la descripción de este documento, que durante el

proceso de registro (900) pueden tener lugar un gran número de niveles distintos de registro.

Tras recibir los datos de autenticación de registro, en la etapa (915), el motor de transacciones (205), usando tecnología SSL COMPLETA convencional, remite los datos de autenticación de registro al motor de autenticación (215). En la etapa (920), el motor de autenticación (215) descifra los datos de autenticación de registro 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 registro, a fin de dividir los datos en al menos dos números aleatorios e indescifrables por separado. Como se ha mencionado anteriormente, al menos dos números pueden comprender un número estadísticamente aleatorio y un número binario en el que se ha llevado a cabo la función XOR. En la etapa (925), el motor de autenticación (215) remite cada parte de los números aleatorios a uno de los equipos de almacenamiento de datos (D1 a D4). Como se ha mencionado anteriormente, de manera ventajosa, el motor de autenticación (215) también puede aleatorizar qué partes se transfieren a qué depósitos.

A menudo durante el proceso de registro (900), el usuario también deseará que se le expida un certificado digital, de manera que pueda recibir documentos cifrados de otros externos al sistema criptográfico (100). Como se ha mencionado anteriormente, la autoridad de certificación (115), por lo general, expide certificados digitales de acuerdo con uno o más de varios estándares convencionales. Por lo general, el certificado digital incluye una clave pública del usuario o sistema, que conoce todo el mundo.

Si el usuario pide un certificado digital durante el registro, o en otro momento, la petición se transfiere a través del motor de confianza (110) al motor de autenticación (215). De acuerdo con una realización, la petición incluye un documento XML que tiene, por ejemplo, el nombre apropiado del usuario. De acuerdo con la etapa (935), el motor de autenticación (215) transfiere la petición al motor criptográfico (220) dando órdenes al motor criptográfico (220) para que genere un par de claves o clave criptográfica.

Previa petición, 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, en las que una se usa como una clave privada y una se usa una 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 petición de un certificado digital al motor de transacciones (205). De acuerdo con una realización, de manera ventajosa, la petición incluye una petición normalizada, tal como PKCS10, embebida, por ejemplo, en un documento XML. De manera ventajosa, la petición de un certificado digital puede corresponder a una o más autoridades de certificación y al uno o más formatos estándar que requieren las autoridades de certificación.

En la etapa (950), el motor de transacciones (205) remite la petición a la autoridad de certificación (115), quien, en la etapa (955), devuelve un certificado digital. De manera ventajosa, el certificado digital devuelto puede tener un formato normalizado, tal como PKCS7, o un formato patentado de una o más de las autoridades de certificación (115). En la etapa (960), el motor de transacciones (205) recibe el certificado digital y se remite una copia al usuario y una copia se almacena en el motor de confianza (110). El motor de confianza (110) almacena una copia del certificado digital de manera que el motor de confianza (110) no necesitará 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 petición del certificado digital normalmente se envía a la autoridad de certificación (115). No obstante, si la autoridad de certificación (115) está realizando un mantenimiento, tiene una avería o es victima de una puesta en peligro de la seguridad, puede que el certificado digital no esté disponible.

En cualquier momento tras expedir las claves criptográficas, de manera ventajosa, el motor criptográfico (220) puede emplear el proceso de división de datos (800), que se ha descrito anteriormente, de manera que las claves criptográficas se dividan en números aleatorios e indescifrables por separado. Similar a los datos de autenticación, en la etapa (965) el motor criptográfico (220) transfiere los números aleatorios a los equipos de almacenamiento de datos (D1 a D4).

Un experto en la materia reconocerá en la descripción de este documento que el usuario puede pedir un certificado digital en cualquier momento tras el registro. Además, de manera ventajosa, las comunicaciones entre sistemas pueden incluir tecnologías de cifrado de claves públicas o de SSL COMPLETA. Además, el proceso de registro puede expedir múltiples certificados digitales desde múltiples autoridades de certificación, que incluyen una o más autoridades de certificación patentadas internas o externas al motor de confianza (110).

Como se describe en las etapas (935 a 960), una realización de la invención incluye la petición de un certificado que

finalmente se almacena en el motor de confianza (110). Dado que, de acuerdo con una realización, el módulo de tratamiento criptográfico (625) expide las claves que usa el motor de confianza (110), cada certificado corresponde a una clave privada. Por lo tanto, de manera ventajosa, el motor de confianza (110) puede proporcionar interoperabilidad mediante la supervisión de los certificados que posee un usuario o asociados a éste. Por ejemplo, cuando el motor criptográfico (220) recibe una petición de una función criptográfica, el módulo de tratamiento criptográfico (625) puede investigar los certificados que posee el usuario peticionario para determinar si el usuario posee una clave privada que coincide con los atributos de la petición. Cuando existe un certificado de este tipo, el módulo de tratamiento criptográfico (625) puede usar el certificado o las claves públicas o privadas asociadas al mismo para llevar a cabo la función pedida. Cuando no existe un certificado de este tipo, de manera ventajosa y clara, el módulo de tratamiento criptográfico (625) puede llevar a cabo una serie de 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 garantizar que el módulo de tratamiento criptográfico (625) lleva a cabo 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, de manera ventajosa, el tipo de certificado se puede especificar en la petición de funciones criptográficas u otros datos proporcionados por el peticionario. De acuerdo con otra realización, el tipo de certificado se puede establecer por el formato de datos de la petición. Por ejemplo, de manera ventajosa, el módulo de tratamiento criptográfico (925) puede reconocer que la petición corresponde a un tipo específico.

De acuerdo con una realización, el tipo de certificado puede incluir uno o más estándares de algoritmos, por ejemplo, RSA, ELGAMAL o similares. Además, el tipo de certificado puede incluir uno o más tipos de claves, tales como claves simétricas claves públicas, claves de cifrado robustas, tales como claves de 256 bits, claves menos seguras o similares. Además, el tipo de certificado puede incluir mejoras o sustituciones de uno o más de los estándares de algoritmos o claves anteriores, uno o más formatos de datos o mensajes, uno o más esquemas de codificación o encapsulación de datos, tales como Base 32 o Base 64. El tipo de certificado también puede incluir compatibilidad con una o más interfaces o aplicaciones criptográficas de terceros, uno o más protocolos de comunicación o uno o más protocolos o estándares de certificados. Un experto en la materia reconocerá en la descripción de este documento que pueden existir otras diferencias en los tipos de certificados y se pueden implementar traslaciones hacia esas diferencias y desde las mismas 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 coincide con el tipo determinado en la etapa (974). Cuando el usuario posee un certificado coincidente, el motor de confianza (110) tiene acceso al certificado coincidente, por ejemplo, mediante previo almacenamiento del mismo, el módulo de tratamiento criptográfico (825) conoce que una clave privada coincidente también está almacenada dentro del motor de confianza (110). Por ejemplo, la clave privada coincidente puede estar almacenada dentro del depósito (210) o del sistema de depósito (700). De manera ventajosa, el módulo de tratamiento criptográfico (625) puede pedir que la clave privada coincidente se ensamble desde, por ejemplo, el depósito (210) y, posteriormente, en la etapa (976), usar la clave privada coincidente para llevar a cabo funciones o acciones criptográficas. Por ejemplo, como se ha mencionado anteriormente, de manera ventajosa, el módulo de tratamiento criptográfico (625) puede llevar a cabo resúmenes, comparación de resúmenes, cifrado o descifrado de datos, creación o verificación de firmas digitales, o similares.

Cuando el usuario no posee un certificado coincidente, el proceso de interoperabilidad (970) pasa a la etapa (978) en la que el módulo de tratamiento criptográfico (625) determina si los usuarios poseen un certificado de certificación cruzada. De acuerdo con una realización, la certificación cruzada entre autoridades de certificación tiene lugar cuando una primera autoridad de certificación determina confiar en certificados de una segunda autoridad de certificación. Es decir, la primera autoridad de certificación determina qué certificados de la segunda autoridad de certificación cumplen determinados estándares de calidad y, por lo tanto, se pueden “certificar” como equivalentes a los certificados propios de la primera autoridad de certificación. La certificación cruzada resulta 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 específico, normalmente en función del grado de fiabilidad en el proceso de registro, mientras que la segunda autoridad de certificación puede proporcionar siete niveles de confianza. De manera ventajosa, la certificación cruzada puede hacer un seguimiento de qué niveles y qué certificados de la segunda autoridad de certificación se pueden sustituir por qué niveles y qué certificados de la primera. Cuando la certificación cruzada anterior se hace de

manera oficial y pública entre dos autoridades de certificación, la correlación de certificados y niveles entre sí a menudo se denomina “encadenamiento”.

De acuerdo con otra realización de la invención, de manera ventajosa, el módulo de tratamiento criptográfico (625) puede desarrollar certificaciones cruzadas distintas 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 la primera autoridad de certificación, o a otra declaración de política publicada, y usar, por ejemplo, los testigos de autenticación requeridos por niveles de confianza específicos, para 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 de certificación cruzada, el proceso de interoperabilidad (970) pasa a la etapa (976) y lleva a cabo la función o acción criptográfica usando la clave pública, clave privada de certificación cruzada o ambas. Alternativamente, cuando el módulo de tratamiento criptográfico (625) determina que los usuarios no poseen un certificado de certificación cruzada, el proceso de interoperabilidad (970) pasa a la etapa (980), en la que el módulo de tratamiento criptográfico (625) selecciona una autoridad de certificación que expide el tipo de certificado pedido o un certificado con certificación cruzada para el mismo. En la etapa (982), el módulo de tratamiento criptográfico (625) determina si los datos de autenticación de registro del usuario, que se han analizado anteriormente, cumplen los requisitos de autenticación de la autoridad de certificación elegida. Por ejemplo, si el usuario se registró a través de una red, por ejemplo, contestando a preguntas demográficas y de otro tipo, los datos de autenticación proporcionados pueden establecer un nivel más bajo de confianza que un usuario que proporciona datos biométricos y comparece ante un tercero, tal como, por ejemplo, un notario. De acuerdo con una realización, de manera ventajosa, los requisitos de autenticación anteriores se pueden proporcionara en la CPS de la autoridad de certificación elegida.

Cuando el usuario ha provisto al motor de confianza (110) de datos de autenticación de registro que cumplen los requisitos de la autoridad de certificación elegida, el proceso de interoperabilidad (970) pasa a la etapa (984), en la que el módulo de tratamiento criptográfico (825) obtiene el certificado de la autoridad de certificación elegida. De acuerdo con una realización, el módulo de tratamiento criptográfico (625) obtiene el certificado siguiendo las etapas (945 a 960) del proceso de registro (900). Por ejemplo, de manera ventajosa, el módulo de tratamiento criptográfico (625) puede emplear una o más claves públicas, de uno o más de los pares de claves ya disponibles para el motor criptográfico (220), para pedir el certificado de la autoridad de certificación. De acuerdo con otra realización, de manera ventajosa, el módulo de tratamiento criptográfico (625) puede generar uno o más pares de claves nuevos y usar las claves públicas correspondientes a los mismos para pedir el certificado de la autoridad de certificación.

De acuerdo con otra realización, de manera ventajosa, el motor de confianza (110) puede incluir uno o más módulos de expedición de certificados capaces de expedir uno o más tipos de certificados. De acuerdo con esta realización, el módulo de expedición de certificados puede proporcionar el certificado anterior. Cuando el módulo de tratamiento criptográfico (625) obtiene el certificado, el proceso de interoperabilidad (970) pasa a la etapa (976) y lleva a cabo la función o acción criptográfica usando la clave pública, la clave privada o ambas correspondiente al certificado obtenido.

Cuando, en la etapa (982), el usuario no ha provisto al motor de confianza (110) de datos de autenticación de registro que cumplen los requisitos de la autoridad de certificación elegida, en la etapa (986), el módulo de tratamiento criptográfico (625) determina si hay otras autoridades de certificación que tienen requisitos de autenticación diferentes. Por ejemplo, el módulo de tratamiento criptográfico (625) puede buscar autoridades de certificación que tengan menos requisitos de autenticación, pero que sigan expidiendo los certificados elegidos o certificaciones cruzadas de los mismos.

Cuando la autoridad de certificación anterior que tiene menos requisitos existe, el proceso de interoperabilidad (970) pasa a la etapa (980) y elige esa autoridad de certificación. Alternativamente, cuando no existe tal autoridad de certificación, en la etapa (988), el motor de confianza (110) puede pedir testigos de autenticación adicionales al usuario. Por ejemplo, el motor de confianza (110) puede pedir nuevos datos de autenticación de registro que comprendan, por ejemplo, datos biométricos. Asimismo, el motor de confianza (110) puede pedir que el usuario comparezca ante un tercero de confianza y proporcione documentos de autenticación apropiados, tal como, por ejemplo, comparecer ante un notario con un carné de conducir, una tarjeta de la seguridad social, una tarjeta bancaria, un certificado de nacimiento, una ID miliar o similares. Cuando el motor de confianza (110) recibe datos de autenticación actualizados, el proceso de interoperabilidad (970) pasa a la etapa (984) y obtiene el certificado elegido anterior.

Mediante el proceso de interoperabilidad (970) anterior, de manera ventajosa, el módulo de tratamiento criptográfico (625) proporciona traslaciones y conversiones claras y continuas entre distintos sistemas criptográficos. Un experto en la materia reconocerá en la descripción de este documento, un gran número de ventajas e implementaciones del sistema interoperable anterior. Por ejemplo, de manera ventajosa, la etapa anterior (986) del proceso de interoperabilidad (970) puede incluir aspectos de arbitraje de confianza, que se analizan más detalladamente más adelante, en los que la autoridad de certificación puede en circunstancias especiales aceptar niveles inferiores de certificación cruzada. Además, el proceso de interoperabilidad (970) puede incluir garantizar la interoperabilidad entre revocaciones de certificados estándar y el empleo de las mismas, tal como emplear 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 de un usuario y compararlos con los datos de autenticación de registro del usuario. Por ejemplo, el proceso de autenticación (1000) comienza en la etapa (1005) cuando un usuario desea llevar a cabo una transacción, por ejemplo, con un vendedor. Dichas transacciones pueden incluir, por ejemplo, seleccionar una opción de compra, pedir acceso a un área restringida o dispositivo del sistema de vendedor (120) o similares. En la etapa (1010), un vendedor provee al usuario de una ID de transacción y de una petición de autenticación. De manera ventajosa, la ID de transacción puede incluir una cantidad de 192 bits que tiene un sello de tiempo de 32 bits concatenado con una cantidad aleatoria de 128 bits, o un "número único" (nonce), concatenada con una constante específica de vendedor de 32 bits. Una ID de transacción de este tipo identifica exclusivamente a la transacción, de manera que el motor de confianza (110) pueda rechazar transacciones imitadas.

De manera ventajosa, la petición de autenticación puede incluir qué nivel de autenticación se necesita para una transacción específica. Por ejemplo, el vendedor puede especificar un nivel específico de certidumbre que se requiere para la transacción en cuestión. Si la autenticación no se puede realizar a este nivel de certidumbre, como se analizará más adelante, la transacción no tendrá lugar sin una autenticación adicional por parte del usuario para elevar el nivel de certidumbre o un cambio en cuanto a la autenticación entre el vendedor y el servidor. Esto se analiza de manera más completa más adelante.

De acuerdo con una realización, de manera ventajosa, una miniaplicación de vendedor u otro programa puede generar la ID de transacción y la petición de autenticación. Además, la transmisión de la ID de transacción y de los datos de autenticación puede incluir uno o más documentos XML cifrados mediante el uso de tecnología SSL convencional, tal como, por ejemplo, ½ SSL o, dicho de otra forma, SSL autenticada por el vendedor.

Tras recibir el sistema de usuario (105) la ID de transacción y la petición de autenticación, el sistema de usuario (105) recopila los datos de autenticación actuales del usuario, que posiblemente incluyan información biométrica actual. En la etapa (1015), el sistema de usuario (105) 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 esos datos al motor de confianza (110). Preferentemente, la transmisión comprende documentos XML encriptados con al menos tecnología ½ SSL convencional. En la etapa (1020), el motor de transacciones (205) recibe la transmisión, preferentemente reconoce el formato de datos o petición en el URL o URI y remite la transmisión al motor de autenticación (215).

Durante las etapas (1015) y (1020), el sistema de vendedor (120), en la etapa (1025), remite la ID de transacción y la petición de autenticación al motor de confianza (110) usando la tecnología SSL COMPLETA preferente. Esta comunicación también puede incluir una ID de vendedor, si bien la identificación de vendedor también se puede comunicar a través de una parte no aleatoria de la ID de transacción. En las etapas (1030) y (1035), el motor de transacciones (205) recibe la comunicación, crea un registro en la pista de auditoría y genera una petición para que los datos de autenticación de registro del usuario se ensamblen desde los equipos de almacenamiento de datos (D1 a D4). En la etapa (1040), el sistema de depósito (700) transfiere al motor de autenticación (215) las partes de los datos de autenticación de registro correspondientes al usuario. En la etapa (1045), el motor de autenticación (215) descifra la transmisión usando su clave privada y compara los datos de autenticación de registro con los datos de autenticación actuales proporcionados por el usuario.

De manera ventajosa, la comparación de la etapa (1045) puede aplicar autenticación heurística dependiente del contexto, a la que se ha hecho referencia anteriormente y que se analiza detalladamente más adelante. Por ejemplo, si la información biométrica recibida no coincide perfectamente, resulta una coincidencia de certidumbre inferior. En realizaciones específicas, el nivel de certidumbre de la autenticación se sopesa con la naturaleza de la transacción y con los deseos del usuario y del vendedor. Nuevamente, esto se analizará más detalladamente más adelante.

En la etapa (1050), el motor de autenticación (215) cumplimenta la petición de autenticación con el resultado de la comparación de la etapa (1045). De acuerdo con una realización de la invención, la petición de autenticación se cumplimenta con el resultado SÍ/NO o VERADADERO/FALSO del proceso de autenticación (1000). En la etapa (1055), la petición de autenticación cumplimentada se devuelve al vendedor para que el vendedor actúe en consecuencia, por ejemplo, permitiendo que el usuario concluya la transacción que inició la petición de autenticación. De acuerdo con una realización, se pasa un mensaje de confirmación al usuario.

En función de lo anterior, de manera ventajosa, el proceso de autenticación (1000) mantiene seguros los datos confidenciales y produce resultados configurados para mantener la integridad de los datos confidenciales. Por ejemplo, los datos confidenciales sólo se ensamblan dentro del motor de autenticación (215). Por ejemplo, los datos de autenticación de registro son indescifrables hasta que se ensamblan en el motor de autenticación (215) por medio del módulo de ensamblaje de datos y los datos de autenticación actuales son indescifrables hasta que se desenvuelven con la tecnología SSL convencional y la clave privada del motor de autenticación (215). Además, el resultado de la autenticación que se transmite al vendedor no incluye los datos confidenciales y el usuario puede incluso no saber si produjo datos de autenticación válidos.

Si bien el proceso de autenticación (1000) se describe haciendo referencia a sus realizaciones preferentes y alternativas, con las mismas no se pretende limitar la invención. Por el contrario, un experto en la materia reconocerá en la descripción de este documento, un gran número de alternativas para el proceso de autenticación (1000). Por ejemplo, de manera ventajosa, el vendedor se puede sustituir por casi cualquier aplicación peticionaria, incluso las que residen en el sistema de usuario (105). Por ejemplo, una aplicación de cliente, tal como Microsoft Word, puede usar una interfaz de programación de aplicaciones (API) o una API criptográfica (CAPI) para pedir autenticación antes de desbloquear un documento. Alternativamente, un servidor de correo, una red, un teléfono móvil, un dispositivo informatizado personal o móvil, una estación de trabajo, o similares, todos pueden hacer peticiones de autenticación que se pueden cumplimentar con el proceso de autenticación (1000). De hecho, tras proporcionar el proceso de autenticación de confianza (1000) anterior, la aplicación o dispositivo peticionario puede proporcionar acceso a un gran número de sistemas o dispositivos informáticos o electrónicos o usar los mismos.

Además, el proceso de autenticación (1000) puede emplear un gran número de procedimientos alternativos en caso de error de autenticación. Por ejemplo, el error de autenticación puede mantener la misma ID de transacción y pedir al usuario que vuelva a introducir sus datos de autenticación actuales. Como se ha mencionado anteriormente, el uso de la misma ID de transacción permite al comparador del motor de autenticación (215) supervisar y limitar el número de intentos de autenticación para una transacción específica, creando de ese modo un sistema criptográfico (100) más seguro.

Además, de manera ventajosa, el proceso de autenticación (1000) se puede emplear para desarrollar soluciones elegantes de inicio de sesión único, tales como, desbloquear un depósito de seguridad de datos confidenciales. Por ejemplo, una autenticación satisfactoria 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 contraseña, conexión, credenciales financieras o similares, asociadas a múltiples vendedores en línea, una red de área local, varios dispositivos informatizados personales, proveedores de servicios de internet, proveedores de subastas, corredores de inversiones o similares. Empleando un depósito de seguridad de datos confidenciales, los usuarios pueden elegir contraseñas aleatorias y muy largas porque ya no necesitan recordarlas mediante asociación. Por el contrario, el proceso de autenticación (1000) proporciona acceso a las mismas. Por ejemplo, un usuario puede elegir una cadena alfanumérica aleatoria que tenga una longitud de más de veinte dígitos en lugar de algo asociado a una fecha memorable, nombre, etc.

De acuerdo con una realización, de manera ventajosa, un depósito de seguridad de datos confidenciales con un usuario determinado puede estar almacenado en los equipos de almacenamiento de datos del depósito (210) o dividido y almacenado en el sistema de depósito (700). De acuerdo con esta realización, tras la autenticación de usuario positiva, el motor de confianza (110) entrega los datos confidenciales pedidos, tal como, por ejemplo, a la contraseña apropiada para la aplicación peticionaria. De acuerdo con otra realización, el motor de confianza (110) puede incluir un sistema independiente para almacenar el depósito de seguridad de datos confidenciales. Por ejemplo, el motor de confianza (110) puede incluir un motor de software autónomo que implementa la funcionalidad de depósito de seguridad de datos y que, de manera figurada, reside “detrás del” sistema de seguridad frontal anterior del motor de confianza (110). De acuerdo con esta realización, el motor de software entrega los datos confidenciales pedidos una vez que el motor de software recibe del motor de confianza (110) una señal que indica una autenticación de usuario positiva.

En otra realización más, el depósito de seguridad de datos se puede implementar por medio de un sistema de terceros. Similar a la realización del motor de software, de manera ventajosa, el sistema de terceros puede entregar los datos confidenciales pedidos una vez que el sistema de terceros recibe desde el motor de confianza (110) una señal que indica una autenticación de usuario positiva. De acuerdo con otra realización más, el depósito de seguridad de datos se puede implementar en el sistema de usuario (105). De manera ventajosa, un motor de software de usuario puede entregar los datos anteriores tras recibir desde motor de confianza (110) una señal que indica una autenticación de usuario positiva.

Si bien los depósitos de seguridad de datos anteriores se describen haciendo referencia a realizaciones alternativas, un experto en la materia reconocerá en la descripción de este documento, un gran número de implementaciones adicionales de los mismos. Por ejemplo, un depósito de seguridad de datos específico puede incluir aspectos de algunas de las realizaciones anteriores o de todas. Además, cualquiera de los depósitos de seguridad de datos anteriores puede emplear una o más peticiones de autenticación en distintos momentos. Por ejemplo, cualquiera de los depósitos de seguridad 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 específicos distintos, 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) que se ha descrito anteriormente haciendo referencia a la figura 10. De acuerdo con una realización de la invención, el proceso de firma (1100) primero autentica al usuario y, posteriormente, lleva a cabo una o más de varias funciones de firma digital como se analizará más detalladamente más adelante. De acuerdo con otra realización, de manera ventajosa, el proceso de firma (1100) puede almacenar datos relacionados con el mismo, tales como resúmenes de mensajes o documentos o similares. De manera ventajosa, estos datos se pueden usar en una auditoría o en cualquier otro evento, tal como, por ejemplo, cuando una parte participante intenta denunciar una transacción.

Como se muestra en la figura 11, durante las etapas de autenticación, de manera ventajosa, el usuario y el vendedor pueden ponerse de acuerdo en un mensaje, tal como, por ejemplo, un contrato. Durante la firma, de manera ventajosa, el proceso de firma (1100) garantiza 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 resumen de sus respectivas copias del mensaje o contrato, en los datos transmitidos al motor de autenticación (215). Empleando sólo un resumen de un mensaje o contrato, de manera ventajosa, el motor de confianza (110) puede almacenar una cantidad considerablemente reducida de datos, proporcionando un sistema criptográfico más eficiente y rentable. Además, de manera ventajosa, el resumen almacenado se puede comparar con un resumen 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 a uno relacionado con una transacción proporciona pruebas adicionales que se pueden usar frente a una reclamación de denuncia por una parte de una transacción.

En la etapa (1103), el motor de autenticación (215) ensambla los datos de autenticación de registro 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 registro coinciden con los datos de autenticación actuales, el comparador del motor de autenticación (215) también compara el resumen del mensaje suministrado por el vendedor con el resumen del mensaje suministrado por el usuario. Por consiguiente, de manera ventajosa, el motor de autenticación (215) garantiza 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 petición de firma digital al motor criptográfico (220). De acuerdo con una realización de la invención, la petición incluye un resumen del mensaje o contrato. No obstante, un experto en la materia reconocerá en la descripción de este documento que el motor criptográfico (220) puede cifrar prácticamente cualquier tipo de datos, que incluyen, entre otros, video, audio, biométricos, imágenes o texto para formar la firma digital deseada. Volviendo a la etapa (1105), preferentemente, la petición de firma digital comprende un documento XML comunicado mediante tecnologías SSL convencionales.

En la etapa (1110), el motor de autenticación (215) transmite una petición a cada uno de los equipos de almacenamiento de datos (D1 a D4), de manera que cada uno de los equipos de almacenamiento de datos (D1 a D4) transmita su parte respectiva de la clave o claves criptográficas correspondiente a una parte firmante. De

acuerdo con otra realización, el motor criptográfico (220) emplea algunas de las etapas del proceso de interoperabilidad (970) que se ha analizado anteriormente o todas, de manera que el motor criptográfico (220) determine primero la clave o claves apropiadas de la parte firmante para pedirlas al depósito (210) o al sistema de depósito (700) y tome medidas para proporcionar claves coincidentes apropiadas. De acuerdo con otra realización más, de manera ventajosa, el motor de autenticación (215) o el motor criptográfico (220) pueden pedir una o más de las claves asociadas a la parte firmante y almacenadas en el depósito (210) o sistema de depósito (700).

De acuerdo con una realización, la parte firmante incluye uno o ambos del usuario y el vendedor. En tal caso, de manera ventajosa el motor de autenticación (215) pide las claves criptográficas correspondientes al usuario y/o al 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 debidamente al usuario, al vendedor o a ambos. Por lo tanto, el motor de autenticación (215) pide la clave criptográfica del motor de confianza (110), tal como, por ejemplo, la clave que pertenece al motor criptográfico (220), para llevar a cabo la firma digital. De acuerdo con otra realización, el motor de confianza (110) lleva a cabo una función de tipo notario digital. En esta realización, la parte firmante incluye el usuario, el vendedor o ambos, junto con el motor de confianza (110). Por consiguiente, el motor de confianza (110) proporciona la firma digital del usuario y/o vendedor y, posteriormente, indica con su propia firma digital que el usuario y/o el vendedor se identificaron debidamente. En esta realización, de manera ventajosa, el motor de autenticación (215) puede pedir el ensamblaje de las claves criptográficas correspondientes al usuario, al vendedor o a ambos. De acuerdo con otra realización, de manera ventajosa, el motor de autenticación (215) puede pedir el ensamblaje de las claves criptográficas correspondientes al motor de confianza (110).

De acuerdo con otra realización, el motor de confianza (110) lleva a cabo funciones de tipo poder de representación. 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) pide las claves criptográficas asociadas al tercero. De acuerdo con esta realización, de manera ventajosa, el proceso de firma (1100) puede incluir autenticación del tercero antes de permitir funciones de tipo poder de representación. Además, el proceso de autenticación (1000) puede incluir una comprobación de restricciones del tercero, tales como, por ejemplo, lógica empresarial o similar, que dicten cuándo y en qué circunstancias se puede usar la firma de un tercero específico.

En función de lo anterior, en la etapa (1110), el motor de autenticación pidió las claves criptográficas a los equipos de almacenamiento de datos (D1 a D4) correspondientes a la parte firmante. En la etapa (1115), los equipos de almacenamiento de datos (D1 a D4) transmiten al motor criptográfico (220) sus partes respectivas de la clave criptográfica correspondiente a la parte firmante. De acuerdo con una realización, las transmisiones anteriores incluyen tecnologías SSL. De acuerdo con otra realización, de manera ventajosa, las transmisiones anteriores se pueden supercifrar 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 firma digital. En la etapa (1125) del proceso de firma (1100), el motor criptográfico (220) transmite la firma digital al motor de autenticación (215). En la etapa (1130), el motor de autenticación (215) transmite la petición de autenticación cumplimentada junto con una copia del mensaje resumido y la firma digital al motor de transacciones (205). En la etapa (1135), el motor de transacciones (205) transmite al vendedor un recibo que comprende la ID de transacción, una indicación de si la autenticación fue satisfactoria y la firma digital. De acuerdo con una realización, de manera ventajosa, la transmisión anterior incluye la firma digital del motor de confianza (110). Por ejemplo, el motor de confianza (110) puede cifrar el resumen del recibo con su clave privada, formando de ese modo una firma digital que se adjuntará a la transmisión al vendedor.

De acuerdo con una realización, el motor de transacciones (205) también transmite un mensaje de confirmación al usuario. Si bien el proceso de firma (1100) se describe haciendo referencia a sus realizaciones preferentes y alternativas, con las mismas no se pretende limitar la invención. Por el contrario, un experto en la materia reconocerá en la descripción de este documento, un gran número de alternativas para el proceso de firma (1100). Por ejemplo, el vendedor se puede sustituir por una aplicación de usuario, tal como una aplicación de correo electrónico. Por ejemplo, el usuario puede querer firmar digitalmente un correo electrónico específico con su firma digital. En una realización de este tipo, de manera ventajosa, la transmisión en todo el proceso de firma (1100) puede incluir sólo una copia de un resumen del mensaje. Además, un experto en la materia reconocerá en la descripción de este documento que un gran número de aplicaciones de cliente pueden pedir firmas digitales. Por ejemplo, las aplicaciones de cliente pueden comprender procesadores de texto, hojas de cálculo, correos electrónicos, correos de voz, acceso a áreas restringidas del sistema o similares.

Además, un experto en la materia reconocerá en la descripción de este documento que, de manera ventajosa, las etapas (1105 a 1120) del proceso de firma (1100) pueden emplear algunas de las etapas del proceso de interoperabilidad (970) de la figura 9B o todas, proporcionando de ese modo interoperabilidad entre distintos sistemas criptográficos que, por ejemplo, pueden necesitar procesar la firma digital con distintos 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 cifrado (1200) comienza autenticando al usuario usando el proceso de autenticación (1000). De acuerdo con una realización, el proceso de autenticación (1000) incluye en la petición de autenticación, una clave de sesión síncrona. Por ejemplo, en tecnologías PKI convencionales, los expertos en la materia entienden que cifrar o descifrar datos, usando claves públicas y privadas, es matemáticamente intensivo y puede requerir considerables recursos de sistema. No obstante, en sistemas criptográficos de claves simétricas o sistemas en los que el remitente y el destinatario de un mensaje comparten una clave única común que se usa para cifrar y descifrar un mensaje, las operaciones matemáticas son considerablemente más sencillas y rápidas. Por consiguiente, en las tecnologías PKI convencionales, el remitente de un mensaje generará claves de sesión síncronas y cifrará el mensaje usando el sistema de claves simétricas más sencillo y rápido. Posteriormente, el remitente cifrará la clave de sesión con la clave pública del destinatario. La clave de sesión cifrada se adjuntará al mensaje cifrado síncronamente y ambos datos se envían al destinatario. El destinatario usa su clave privada para descifrar la clave de sesión y, posteriormente, usa la clave de sesión para descifrar el mensaje. En función de lo anterior, el sistema de claves simétricas más sencillo y rápido se usa para la mayoría de los procesos de cifrado/descifrado. Por consiguiente, en el proceso de descifrado (1200), de manera ventajosa, el descifrado asume que una clave síncrona se ha cifrado con la clave pública del usuario. Por consiguiente, como se ha mencionado anteriormente, la clave de sesión cifrada está incluida en la petición de autenticación.

Volviendo al proceso de descifrado (1200), una vez autenticado el usuario en la etapa (1205), el motor de autenticación (215) remite la clave de sesión cifrada al motor criptográfico (220). En la etapa (1210), el motor de autenticación (215) remite una petición a cada uno de los equipos de almacenamiento de datos (D1 a D4), pidiendo los datos de clave criptográfica del usuario. En la etapa (1215), cada equipo de almacenamiento de datos, (D1 a D4), transmite su parte respectiva de la clave criptográfica al motor criptográfico (220). De acuerdo con una realización, la transmisión anterior se cifra 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 remite la clave de sesión al motor de autenticación (215). En la etapa (1227), el motor de autenticación (215) cumplimenta la petición de autenticación incluyendo la clave de sesión descifrada y transmite la petición de autenticación cumplimentada al motor de transacciones (205). En la etapa (1230), el motor de transacciones (205) remite la petición de autenticación junto con la clave de sesión al vendedor o aplicación peticionarios. Posteriormente, de acuerdo con una realización, el vendedor o aplicación peticionarios usan la clave de sesión para descifrar el mensaje cifrado.

Si bien el proceso de descifrado (1200) se describe haciendo referencia a sus realizaciones preferentes y alternativas, un experto en la materia reconocerá en la descripción de este documento, un gran número de alternativas para el proceso de cifrado (1200). Por ejemplo, el proceso de descifrado (1200) puede preceder al cifrado de la clave síncrona y basarse en tecnología de clave pública completa. En una realización de este tipo, la aplicación peticionaria puede transmitir todo el mensaje al motor criptográfico (220) o puede emplear algún tipo de compresión o resumen reversible a fin de transmitir el mensaje al motor criptográfico (220). Un experto en la materia también reconocerá en la descripción de este documento que, de manera ventajosa, las comunicaciones anteriores pueden incluir documentos XML envueltos en tecnología SSL.

El proceso de cifrado/descifrado (1200) también prevé el cifrado de documentos u otros datos. Por consiguiente, en la etapa (1235), de manera ventajosa, un vendedor o aplicación peticionarios pueden transmitir al motor de transacciones (205) del motor de confianza (110), una petición de la clave pública del usuario. El vendedor o aplicación peticionarios realizan dicha petición porque el vendedor o aplicación peticionarios usan la clave pública del usuario, por ejemplo, para cifrar la clave de sesión que se usará para cifrar el documento o mensaje. Como se ha mencionado en el proceso de registro (900), el motor de transacciones (205) almacena una copia del certificado digital del usuario, por ejemplo, en el dispositivo de almacenamiento masivo (225). Por consiguiente, en la etapa (1240) del proceso de cifrado (1200), el motor de transacciones (205) pide el certificado digital del usuario al dispositivo de almacenamiento masivo (225). En la etapa (1245), el dispositivo de almacenamiento masivo (225) transmite el certificado digital correspondiente al usuario al motor de transacciones (205). En la etapa (1250), el motor de transacciones (205) transmite el certificado digital al vendedor o aplicación peticionarios. De acuerdo con

una realización, la parte de cifrado del proceso de cifrado (1200) no incluye la autenticación de un usuario. Esto se debe a que el vendedor peticionario sólo necesita la clave pública del usuario y no está pidiendo datos confidenciales.

Un experto en la materia reconocerá en la descripción de este documento que si un usuario específico no tiene un certificado digital, el motor de confianza (110) puede emplear algo del proceso de registro (900) o todo a fin de generar un certificado digital para ese usuario específico. Posteriormente, 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 en la descripción de este documento que, de manera ventajosa, las etapas (1220) y (1235 a 1250) del proceso de cifrado/descifrado (1200) pueden emplear algunas de las etapas del proceso de interoperabilidad de la figura 9B o todas, proporcionando, de ese modo, interoperabilidad entre distintos sistemas criptográficos que, por ejemplo, pueden necesitar procesar el cifrado.

La figura 13 ilustra un diagrama de bloques simplificado de un sistema de motores de confianza (1300) de acuerdo con aspectos de otra realización más de la invención. Como se muestra en la figura 13, el sistema de motores de confianza (1300) comprende una pluralidad de motores de confianza diferentes (1305), (1310), (1315) y (1320), respectivamente. Para facilitar un entendimiento más completo de la invención, la figura 13 ilustra cada motor de confianza (1305), (1310), (1315) y (1320) como que tiene un motor de transacciones, un depósito y un motor de autenticación. No obstante, un experto en la materia reconocerá que, de manera ventajosa, cada motor de transacciones puede comprender algunos de los elementos y canales de comunicación que se describen haciendo referencia a las figuras 1 a 8, una combinación de los mismos o todos. Por ejemplo, de manera ventajosa, una realización puede incluir motores de confianza que tienen uno o más motores de transacciones, 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) está separado geográficamente, tal como, 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. De manera ventajosa, la separación geográfica anterior reduce el tiempo de respuesta del sistema a la vez que aumenta la seguridad de todo el sistema de motores de confianza (1300).

Por ejemplo, cuando un usuario entra al sistema criptográfico (100), el usuario puede estar más cerca de la primera ubicación y puede desear ser autenticado. Como se ha descrito haciendo referencia a la figura 10, para ser autenticado, el usuario proporciona datos de autenticación actuales, tales como un dato biométrico o similar y los datos de autenticación actuales se comparan con los datos de autenticación de registro de ese usuario. Por lo tanto, de acuerdo con un ejemplo, de manera ventajosa, el usuario proporciona datos de autenticación actuales al motor de confianza más cercano geográficamente (1305). El motor de transacciones (1321) del motor de confianza (1305) remite 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 transacciones (1321) remite 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 transacciones (1321) también pide a los depósitos, por ejemplo, de cada uno de los motores de confianza, (1305 a 1320) el ensamblaje de los datos de autenticación de registro. De acuerdo con esta realización, cada depósito proporciona su parte de los datos de autenticación de registro al motor de autenticación (1322) del motor de confianza (1305). Posteriormente, el motor de autenticación (1322) emplea las partes de datos encriptados, por ejemplo, de los dos primeros depósitos para responder y ensambla los datos de autenticación de registro en forma descifrada. El motor de autenticación (1322) compara los datos de autenticación de registro con los datos de autenticación actuales y devuelve un resultado de autenticación al motor de transacciones (1321) del motor de confianza (1305).

En función de lo anterior, el sistema de motores de confianza (1300) emplea el más cercano de una pluralidad de motores de confianza separados geográficamente (1305 a 1320) para llevar a cabo el proceso de autenticación. De acuerdo con una realización de la invención, de manera ventajosa, el encaminamiento de información al motor de transacciones más cercano se puede llevar a cabo en miniaplicaciones de cliente que se ejecutan en uno o más de entre el sistema de usuario (105), el sistema de vendedor (120) o la autoridad de certificación (115). De acuerdo con una realización alternativa, se puede emplear un proceso de decisión mas sofisticado para seleccionar de entre los motores de confianza (1305 a 1320). Por ejemplo, la decisión se puede basar 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 determinado.

De este modo, el sistema de motores de confianza (1300) reduce su tiempo de respuesta mientras mantiene las ventajas de seguridad asociadas a equipos de almacenamiento de datos remotos geográficamente, tales como los que se han analizado haciendo referencia a la figura 7, en los que cada equipo de almacenamiento de datos almacena partes aleatorias de datos confidenciales. Por ejemplo, una puesta en peligro de la seguridad del depósito (1325) del motor de confianza (1315) no necesariamente pone en peligro los datos confidenciales del sistema de motores de confianza (1300). Esto se debe a que el depósito (1325) sólo contiene datos aleatorios no descifrables que, sin más, son totalmente inútiles.

De acuerdo con otra realización, de manera ventajosa, el sistema de motores de confianza (1300) puede incluir múltiples motores criptográficos dispuestos de manera similar a los motores de autenticación. De manera ventajosa, los motores criptográficos pueden llevar a cabo funciones criptográficas, tales como las que se han descrito haciendo referencia a las figuras 1 a 8. De acuerdo con otra realización más, de manera ventajosa, el sistema de motores de confianza (1300) puede sustituir los múltiples motores de autenticación por múltiples motores criptográficos, llevando a cabo, de ese modo, funciones criptográficas tales como las que se han descrito haciendo referencia a las figuras 1 a 8. De acuerdo con otra realización más de la invención, el sistema de motores de confianza (1300) puede sustituir cada múltiple motor de autenticación por un motor que tiene alguna de la funcionalidad de los motores de autenticación, los motores criptográficos o ambos o toda, como se ha descrito anteriormente.

Si bien el sistema de motores de confianza (1300) se describe haciendo referencia a sus realizaciones preferentes y alternativas, un experto en la materia reconocerá que el sistema de motores de confianza (1300) puede comprender partes de motores de confianza (1305 a 1320). Por ejemplo, el sistema de motores de confianza (1300) puede incluir uno o más motores de transacciones, 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 motores de confianza (1400) de acuerdo con aspectos de otra realización más de la invención. Como se muestra en la figura 14, el sistema de motores 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 alguno de los elementos del motor de confianza (110) que se han descrito haciendo referencia a las figuras 1 a 8 o todos. De acuerdo con esta realización, cuando las miniaplicaciones de cliente del sistema de usuario (105), del sistema de vendedor (120) o de la autoridad de certificación (115), se comunica con el sistema de motores de confianza (1400), esas comunicaciones se envían a la dirección IP de cada uno de los motores de confianza (1405 a 1420). Además, cada motor de transacciones de cada uno de los motores de confianza (1405), (1410), (1415) y (1420) se comporta de manera similar al motor de transacciones (1321) del motor de confianza (1305) que se ha descrito haciendo referencia a la figura 13. Por ejemplo, durante un proceso de autenticación, cada motor de transacciones de cada uno de los motores de confianza (1405), (1410), (1415) y (1420) transmite los datos de autenticación actuales a sus respectivos motores de autenticación y transmite una petición para ensamblar los datos aleatorios 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 dicha ilustración sería demasiado compleja. Continuando con el proceso de autenticación, cada uno de los depósitos comunica su parte de los datos aleatorios 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 registro 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 medio de cada uno de los motores de autenticación se transmite a un módulo de redundancia de los otros tres motores de confianza. Por ejemplo, el resultado del motor de autenticación del motor de confianza (1405) se transmite a los módulos de redundancia de los motores de confianza (1410), (1415) y (1420). Por consiguiente, el módulo de redundancia del motor de confianza (1405) recibe asimismo el resultado de los motores de autenticación 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 de tres motores de autenticación y transmitir ese resultado al motor de transacciones del cuarto motor de confianza. El comparador compara el resultado de autenticación 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. Posteriormente, este resultado se vuelve a transmitir al motor de transacciones correspondiente al motor de confianza no asociado a los tres motores de autenticación.

En función de lo anterior, el módulo de redundancia determina un resultado de autenticación a partir de datos recibidos de motores de autenticación que, preferentemente, están apartados geográficamente del motor de confianza de ese módulo de redundancia. Proporcionando tal funcionalidad de redundancia, el sistema de motores de confianza (1400) garantiza que una puesta en peligro del motor de autenticación de uno de los motores de confianza (1405 a 1420) es insuficiente para poner en peligro el resultado de autenticación del módulo de redundancia de ese motor de confianza específico. Un experto en la materia reconocerá que la funcionalidad del módulo de redundancia del sistema de motores de confianza (1400) también se puede aplicar al motor criptográfico de cada uno de los motores de confianza (1405 a 1420). No obstante, dicha comunicación del motor criptográfico no se mostró en la figura 14 para evitar complejidad. Además, un experto en la materia reconocerá que un gran número de algoritmos alternativos de resolución de conflictos de resultados de autenticación para el comparador de la figura 15 son adecuados para uso en la presente invención.

De acuerdo con otra realización más de la invención, de manera ventajosa, el sistema de motores de confianza (1400) puede emplear el módulo de redundancia durante las etapas de comparación criptográfica. Por ejemplo, de manera ventajosa, alguna de las descripciones anteriores del módulo de redundancia haciendo referencia a las figuras 14 y 15 o todas se pueden implementar durante una comparación de resúmenes de documentos proporcionados por una o más partes durante una transacción específica.

Si bien la invención anterior se ha descrito en función de determinadas realizaciones preferentes y alternativas, otras realizaciones resultarán evidentes para alguien con conocimientos normales de la materia gracias a la descripción de este documento. Por ejemplo, el motor de confianza (110) puede expedir certificados a corto plazo, en los que la clave criptográfica autoriza al usuario por un periodo de tiempo predeterminado. Por ejemplo, estándares de certificado actuales incluyen un campo de validez que se puede establecer para que se anule después de un tiempo predeterminado. Por consiguiente, el motor de confianza (110) puede autorizar una clave privada a un usuario en la que la clave privada sería válida, por ejemplo, durante 24 horas. De acuerdo con una realización de este tipo, de manera ventajosa, el motor de confianza (110) puede expedir un nuevo par de claves criptográficas para asociarlas a un usuario específico y, posteriormente, autorizar la clave privada del nuevo par de claves criptográficas. Posteriormente, una vez que se autoriza la clave criptográfica privada, el motor de confianza (110) anula inmediatamente cualquier uso interno válido de dicha clave privada, ya que el motor de confianza (110) ya no la puede asegurar.

Si bien la invención anterior se ha descrito en función de determinadas realizaciones preferentes y alternativas, otras realizaciones resultarán evidentes para alguien con conocimientos normales de la materia gracias a la descripción de este documento. Por ejemplo, el motor de confianza (110) puede expedir certificados a corto plazo, en los que la clave criptográfica autoriza al usuario por un periodo de tiempo predeterminado. Por ejemplo, estándares de certificado actuales incluyen un campo de validez que se puede establecer para que se anule después de un tiempo predeterminado. Por consiguiente, el motor de confianza (110) puede autorizar una clave privada a un usuario en la que la clave privada sería válida, por ejemplo, durante 24 horas. De acuerdo con una realización de este tipo, de manera ventajosa, el motor de confianza (110) puede expedir un nuevo par de claves criptográficas para asociarlas a un usuario específico y, posteriormente, autorizar la clave privada del nuevo par de claves criptográficas. Posteriormente, una vez que se autoriza la clave criptográfica privada, el motor de confianza (110) anula inmediatamente cualquier uso interno válido de dicha clave privada, ya que el motor de confianza (110) ya no la puede asegurar.

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 dispositivos, tales como, entre otros, un portátil, un teléfono móvil, una red, un dispositivo biométrico o similar. De acuerdo con una realización, dicho reconocimiento puede venir de datos suministrados en la petición de un servicio específico, tal como, una petición de autenticación que da lugar a acceso o uso, una petición de funcionalidad criptográfica o similar. De acuerdo con una realización, la petición anterior puede incluir una identificación exclusiva de dispositivos, tal como, por ejemplo, una ID de procesadores. Alternativamente, la petición puede incluir datos en un formato de datos reconocible específico. Por ejemplo, los teléfonos móviles y satélite a menudo no incluyen la potencia de procesamiento para certificados completos de cifrado pesado X509.v3 y, por lo tanto, no los piden. De acuerdo con esta realización, el motor de confianza (110) puede reconocer el tipo de formato de datos presentado y responder sólo de la misma manera.

Como se ha analizado anteriormente, la autenticación es el proceso de probar que un usuario es quien dice ser. Por lo general, la autenticación requiere demostrar algún hecho a una autoridad de autenticación. El motor de confianza (110) de la presente invención representa la autoridad a la que un usuario se debe identificar. El usuario debe

demostrar al motor de confianza (110) que es quien dice ser: conociendo algo que sólo el usuario debería conocer (autenticación basada en conocimientos), teniendo algo que sólo el usuario debería tener (autenticación basada en testigos) o siendo algo que sólo el usuario debería ser (autenticación basada en biometría).

Ejemplos de autenticación basada en conocimientos incluyen, entre otros, una contraseña, número PIN o combinación de bloqueo. Ejemplos de autenticación basada en testigos incluyen, entre otros, una llave de casa, una tarjeta de crédito física, un carnet de conducir o un número de teléfono específico. Ejemplos de autenticación basada en biometría incluyen, entre otros, una huella dactilar, un análisis de escritura, un escáner de cara, un escáner de mano, un escáner de oreja, un escáner de iris, un patrón vascular, ADN, un análisis de voz o un escáner de retina.

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

Tal y como se usa en este documento, "autenticación" se referirá, en líneas generales, al proceso global de verificar la identidad de alguien para que sea quien dice ser. Una "técnica de autenticación" se referirá a un tipo específico de autenticación basado en un conocimiento específico, testigo físico o lectura biométrica. "Datos de autenticación" se refiere a información que se envía o se demuestra de otro modo a una autoridad de autenticación a fin de establecer la identidad. "Datos de registro" se referirá a los datos que se presentan inicialmente a una autoridad de autenticación a fin de establecer valores iniciales de comparación con datos de autenticación. Una "instancia de autenticación" se referirá a los datos asociados a un intento de autenticar mediante una técnica de autenticación.

Las comunicaciones y protocolos internos que participan en el proceso de autenticación de un usuario se describen haciendo referencia a la figura 10 anterior. La parte de este proceso dentro de la cual tiene lugar la autenticación dependiente del contexto se produce en la etapa de comparación que se muestra como etapa (1045) de la figura 10. Esta etapa tiene lugar dentro del motor de autenticación (215) y conlleva ensamblar los datos de registro (410) recuperados del depósito (210) y comparar los datos de autenticación proporcionados por el usuario con éstos. Una realización específica 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 registro recuperados del depósito (210) se reciben por medio del motor de autenticación (215) en la etapa (1600) de la figura 16. Ambos de estos conjuntos de datos pueden contener datos que están relacionados con técnicas independientes de autenticación. El motor de autenticación (215) separa los datos de autenticación asociados a cada instancia de autenticación individual, en la etapa (1605). Esto es necesario para que los datos de autenticación se comparen con el subconjunto apropiado de los datos de registro correspondientes al usuario (por ejemplo, datos de autenticación de huella dactilar se deberían comparar con datos de registro de huella dactilar, en lugar de con datos de de registro de contraseña).

Por lo general, autenticar a un usuario conlleva una o más instancias de autenticación individuales, dependiendo de qué técnicas de autenticación disponga el usuario. Estos procedimientos están limitados por los datos de registro que proporcionó el usuario durante su proceso de registro (si el usuario no proporcionó un escáner de retina cuando se registró, no podrá autenticarse usando un escáner de retina), así como por los medios de que puede disponer actualmente el usuario (por ejemplo, si el usuario no tiene un lector de huellas dactilares en su ubicación actual, la autenticación de huella dactilar no será factible). En algunos casos, una única instancia de autenticación puede ser suficiente para autenticar a un usuario. No obstante, en determinadas circunstancias, se puede usar una combinación de múltiples instancias de autenticación a fin de autenticar con mayor certidumbre a un usuario para una transacción específica.

Cada instancia de autenticación consiste en datos relativos a una técnica de autenticación específica (por ejemplo, huella dactilar, contraseña, tarjeta inteligente, etc.) y las circunstancias relacionadas con la captación y entrega de los datos para esa técnica específica. Por ejemplo, una instancia específica de intentar autenticar a través de contraseña generará no sólo los datos relativos a la contraseña propiamente dicha, sino también datos circunstanciales, conocidos como "metadatos", relativos a ese intento de contraseña. Dichos datos circunstanciales incluyen información tal como: el momento en que tuvo lugar la instancia de autenticación específica, la dirección de red desde la que se entregó la información de autenticación, así como cualquier otra información que conozcan los expertos en la materia que se pueda determinar sobre el origen de los datos de autenticación (el tipo de conexión, el número de serie del procesador, etc.).

En muchos casos, sólo estará disponible una pequeña cantidad de metadatos circunstanciales. Por ejemplo, si el usuario está ubicado en una red que usa proxies, traslación de dirección de red u otra técnica que oculta la dirección del ordenador de origen, sólo se puede determinar la dirección del proxy o enrutador. Asimismo, en muchos casos información tal como el número de serie del procesador no estará disponible debido a limitaciones del hardware o sistema operativo, a desactivación de tales características por el operador del sistema o a 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 en la etapa (1605) se han extraído y separado las instancias de autenticación individuales representadas dentro de los datos de autenticación, el motor de autenticación (215) evalúa la fiabilidad de cada instancia al indicar que el usuario es quien reivindica ser. La fiabilidad de una única instancia de autenticación, por lo general, se determinará en función de varios factores. Los mismos se pueden agrupar como factores relativos a la fiabilidad asociada a la técnica de autenticación, que se evalúan en la etapa (1610), y factores relativos a la fiabilidad de los datos de autenticación específicos proporcionados, que se evalúan en la etapa (1815). El primer grupo incluye, a título enunciativo, la fiabilidad inherente de la técnica de autenticación que se está usando y la fiabilidad de los datos de registro que se están usando con ese procedimiento. El segundo grupo incluye, a título enunciativo, el grado de coincidencia entre los datos de registro y los datos proporcionados con la instancia de autenticación y los metadatos asociados a esa instancia de autenticación. Cada uno de estos factores puede variar independientemente del resto.

La fiabilidad inherente de una técnica de autenticación se basa en cuánta dificultad tiene un impostor para proporcionar datos correctos de otra persona, así como en las probabilidades globales de error de la técnica de autenticación. Para los procedimientos de autenticación basada en conocimientos y contraseñas, a menudo dicha fiabilidad es bastante baja porque no hay nada que evite que alguien revele su contraseña a otra persona y que esa segunda persona use esa contraseña. Incluso un sistema basado en conocimientos más complejo puede tener sólo fiabilidad moderada, dado que los conocimientos se pueden transferir de persona a persona bastante fácilmente. La autenticación basada en testigos, tal como tener una tarjeta inteligente apropiada u usar un terminal específico para llevar a cabo la autenticación, es igualmente de baja fiabilidad usada por sí misma, dado que no hay garantía de que la persona adecuada esté en posesión del testigo apropiado.

No obstante, las técnicas biométricas son intrínsecamente más fidedignas porque, por lo general, es difícil proveer a otra persona de la capacidad de usar sus huellas digitales de manera adecuada, incluso intencionadamente. Dado que trastocar técnicas de autenticación biométrica es más difícil, la fiabilidad inherente de los procedimientos biométricos, por lo general, es mayor que la de las técnicas de autenticación basadas meramente en conocimientos o testigos. No obstante, incluso las técnicas biométricas pueden tener ocasiones en las que se genera una aceptación falsa o un rechazo falso. Estas incidencias se pueden reflejar mediante distintas fiabilidades para diferentes implementaciones de la misma técnica biométrica. Por ejemplo, un sistema de coincidencia de huella dactilar proporcionado por una empresa puede proporcionar una mayor fiabilidad que uno proporcionado por una empresa diferente, porque uno usa óptica de mayor calidad, una resolución de escaneo mejor o alguna otra mejora que reduce la incidencia de aceptaciones falsas o rechazos falsos.

Cabe señalar que dicha fiabilidad se puede expresar de maneras diferentes. De manera aconsejable, la fiabilidad se expresa en alguna métrica que puedan usar la heurística (530) y los algoritmos del motor de autenticación (215) para calcular el nivel de certidumbre de cada autenticación. Un modo preferente de expresar dichas fiabilidades es un porcentaje o fracción. Por ejemplo, se podría asignar a las huellas dactilares una fiabilidad inherente del 97%, mientras que a las contraseñas se podría asignar sólo una fiabilidad inherente del 50%. Los expertos en la materia reconocerán que estos valores específicos son sólo de ejemplo y pueden variar entre implementaciones específicas.

El segundo factor para el que se debe valorar la fiabilidad es la fiabilidad del registro. Esto forma parte del proceso de "registro escalonado" al que se ha hecho referencia anteriormente. Este factor de fiabilidad refleja la fiabilidad de la identificación proporcionada durante el proceso de registro inicial. Por ejemplo, si el individuo se registra inicialmente de una manera en la que produce físicamente pruebas de su identidad a un notario u otro funcionario y los datos de registro se registran en ese momento y se autentican notarialmente, los datos serán más fidedignos que datos que se proporcionan a través de una red durante el registro y sólo se da fe mediante una firma digital u otra información que no está realmente relacionada con el individuo.

Otras técnicas de registro con distintos niveles de fiabilidad incluyen, a título enunciativo: registro en una oficina física del operador del motor de confianza (110); registro en el lugar de trabajo de un usuario; registro en una oficina de correos u organismo que expide pasaportes; registro a través de una filial o parte de confianza del operador del

motor de confianza (110); registro anónimo o bajo seudónimo en el que la identidad registrada aún no está identificada con un individuo real específico, así como tantos otros medios como se conozcan en la técnica.

Estos factores reflejan la confianza entre el motor de confianza (110) y la fuente de identificación proporcionada durante el proceso de registro. Por ejemplo, si el registro se lleva a cabo en asociación con un empleador durante el proceso inicial de proporcionar pruebas de identidad, esta información se puede considerar extremadamente fidedigna a efectos dentro la empresa, pero un organismo gubernamental o un competidor pueden confiar en la misma en menor grado. Por lo tanto, motores de confianza operados por cada una de estas otras organizaciones pueden asignar diferentes niveles de fiabilidad a este registro.

Asimismo, datos adicionales que se presentan a través de una red, pero que están autenticados por otros datos de confianza proporcionados durante un registro previo con el mismo motor de confianza (110) se pueden considerar tan fidedignos como lo eran los datos de registro originales, aunque éstos se presentaran a través de una red abierta. En tales circunstancias, una autenticación notarial posterior aumentará de manera eficaz el nivel de fiabilidad asociado a los datos de registro originales. De este modo, por ejemplo, un registro anónimo o bajo seudónimo se puede elevar a un registro completo demostrando a algún funcionario de registro que la identidad del individuo coincide con los datos registrados.

Los factores de fiabilidad que se han analizado anteriormente, por lo general, son valores que se pueden determinar con anterioridad a cualquier instancia de autenticación específica. Esto se debe a que se basan en el registro y en la técnica, en lugar de en la autenticación propiamente dicha. En una realización, la etapa de generar fiabilidad basada en estos factores conlleva buscar valores previamente determinados para esta técnica de autenticación específica y los datos de registro del usuario. En otro aspecto de una realización ventajosa de la presente invención, dichas fiabilidades se pueden incluir con los propios datos de registro. De este modo, estos factores se entregan automáticamente al motor de autenticación (215) junto con los datos de registro enviados desde el depósito (210).

Aunque, por lo general, estos factores se pueden determinar con anterioridad a cualquier instancia de autenticación individual, siguen afectando a cada instancia de autenticación que usa esa técnica de autenticación específica para ese usuario. Además, aunque los valores pueden cambiar con el tiempo (por ejemplo, si el usuario se vuelve a registrar de una manera más fidedigna), no dependen de los propios datos de identificación. Por el contrario, los factores de fiabilidad asociados a datos de una única instancia específica pueden variar en cada ocasión. Estos factores, como se analiza más adelante, se deben evaluar para cada nueva identificación a 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 específica y los datos proporcionados durante el registro de autenticación. Esta es la cuestión fundamental de si los datos de autenticación coinciden con los datos de registro correspondientes al individuo que el usuario reivindica ser. Normalmente, cuando los datos no coinciden, se considera que el usuario no se ha autenticado satisfactoriamente y la autenticación fracasa. La manera en que se evalúa esto puede cambiar dependiendo de la técnica de autenticación que se use. La comparación de dichos datos se lleva a cabo con la función del comparador (515) del motor de autenticación (215), como se muestra en la figura 5.

Por ejemplo, por lo general, las coincidencias de contraseñas se evalúan de manera binaria. Es decir, una contraseña es una coincidencia perfecta o una coincidencia fallida. Normalmente, no es aconsejable aceptar como exacta una coincidencia parcial con una contraseña que se acerca a la contraseña correcta si no es exactamente correcta. Por lo tanto, al evaluar una autenticación de contraseña, la fiabilidad de la autenticación que devuelve el comparador (515) es, normalmente, del 100% (correcta) o del 0% (incorrecta), sin posibilidad de valores intermedios.

Reglas similares a las de las contraseñas se aplican, por lo general, a los procedimientos de autenticación basada en testigos, tales como tarjetas inteligentes. Esto se debe a que tener una tarjeta inteligente que tiene un identificador similar o que es similar a la correcta, es tan incorrecto como tener cualquier otro testigo inadecuado. Por lo tanto, los testigos suelen ser también autenticadores binarios: un usuario tiene el testigo correcto o no.

No obstante, determinados tipos de datos de autenticación, tales como cuestionarios y biometría, por lo general no son autenticadores binarios. Por ejemplo, una huella dactilar puede coincidir con una huella dactilar de referencia en distintos grados. Hasta cierto punto, esto se puede deber a variaciones en la calidad de los datos captados durante el registro inicial o en autenticaciones posteriores. (Una huella dactilar puede estar difuminada o una persona puede tener una quemadura o una cicatriz sin regenerar en un dedo específico). En otros casos, los datos pueden coincidir menos que perfectamente porque la propia información es algo variable y se basa en coincidencia de patrones. (Un

análisis de voz puede parecer cercano pero no totalmente adecuado por el ruido de fondo o la acústica del entorno en el que se registra la voz o porque la persona está resfriada). Por último, en situaciones en las que se están comparando grandes cantidades de datos, simplemente se puede dar el caso de que muchos de los datos coincidan perfectamente, pero otros no. (Un cuestionario de diez preguntas puede haber tenido como resultado ocho respuestas correctas a preguntas personales, pero dos respuestas incorrectas). Por cualquiera de estos motivos, puede ser aconsejable que el comparador (515) asigne a la coincidencia entre los datos de registro y los datos de una instancia de autenticación específica un valor de coincidencia parcial. De este modo, se podría decir, por ejemplo, que la huella dactilar es una coincidencia del 85%, las características de la voz una coincidencia del 65% y el cuestionario una coincidencia del 80%.

Esta medición (grado de coincidencia) que produce el comparador (515) es el factor que representa la cuestión básica de si una autenticación es correcta o no. No obstante, como se ha analizado anteriormente, este es sólo uno de los factores que se puede usar para determinar la fiabilidad de una instancia de autenticación determinada. Cabe señalar también que aunque se puede determinar una coincidencia en cierto grado parcial, a la larga, puede ser aconsejable proporcionar un resultado binario basado en una coincidencia parcial. En un modo de funcionamiento alternativo, las coincidencias parciales también se pueden tratar como binarias, es decir, coincidencias perfectas (100%) o fallidas (0%), basado en si el grado de coincidencia supera o no un nivel umbral específico de coincidencia. Un proceso de este tipo se puede usar para proporcionar un nivel simple de superación/fracaso de coincidencia para sistemas que de lo contrario producirían coincidencias parciales.

Otro factor que se debe considerar al evaluar la fiabilidad de una instancia de autenticación determinada concierne a las circunstancias en las que se proporcionan los datos de autenticación para esta instancia específica. Como se ha analizado anteriormente, las circunstancias se refieren a los metadatos asociados a una instancia de autenticación específica. Esto puede incluir, a título enunciativo, información tal como: la dirección de red del autenticador, en la medida en que se pueda determinar; 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 se pueden usar para producir un perfil del tipo de autenticación que normalmente pide el usuario. Posteriormente, esta información se puede usar para valorar la fiabilidad al menos de dos formas. Una forma es considerar si el usuario está pidiendo autenticación de una forma que es coherente con el perfil de autenticación de ese usuario. Si el usuario normalmente hace peticiones de autenticación desde una dirección de red durante días laborables (cuando está en el trabajo) y desde una dirección de red diferente por las tardes o durante los fines de semana (cuando está en casa), una autenticación que tiene lugar desde la dirección particular durante el día laborable es menos fidedigna, porque está fuera del perfil normal de autenticación. Asimismo, si el usuario normalmente se autentica usando una biometría de huella dactilar y por las tardes, una autenticación que se origine durante el día usando sólo una contraseña es menos fidedigna.

Un modo adicional en que se pueden usar los metadatos circunstanciales para evaluar la fiabilidad de una instancia de autenticación es determinar cuánta corroboración proporciona la circunstancia de que el autenticador es quien reivindica ser. Por ejemplo, si la autenticación viene de un sistema con un número de serie que se conoce que está asociado al usuario, es un buen indicador circunstancial de que el usuario es el individuo que reivindica ser. Por el contrario, si la autenticación viene de una dirección de red que se conoce que está en Los Ángeles cuando el usuario reside en Londres, es una indicación de que esta autenticación es menos fidedigna basándose en sus circunstancias.

También es posible colocar una cookie u otros datos electrónicos en el sistema que está usando un usuario cuando interactúa con un sistema de vendedor o con el motor de confianza (110). Estos datos se escriben en el dispositivo de almacenamiento del sistema del usuario y pueden contener una identificación que se puede leer con un navegador de red u otro software del sistema de usuario. Si se permite que estos datos residan en el sistema de usuario entre sesiones (una "cookie persistente") se pueden enviar con los datos de autenticación como prueba adicional del uso anterior de este sistema durante la autenticación de un usuario específico. De hecho, los metadatos de una instancia determinada, en particular, una cookie persistente, pueden formar por sí mismos una especie de autenticador basado en testigos.

Una vez que se generan los factores de fiabilidad apropiados en función de la técnica y los datos de la instancia de autenticación, como se ha descrito 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 para hacer esto es simplemente expresar cada fiabilidad como un porcentaje y, posteriormente, multiplicarlas entre sí.

Por ejemplo, supongamos que los datos de autenticación se están enviando desde una dirección de red que se conoce que es el ordenador particular del usuario, completamente de acuerdo con el perfil anterior de autenticación del usuario (100%), y la técnica que se está usando es identificación de huella dactilar (97%) y los datos iniciales de huella dactilar se desplazaron de un lado a otro a través del empleador del usuario con el motor de confianza (110) (90%) y la coincidencia entre los datos de autenticación y la plantilla original de huella dactilar de los datos de registro es muy buena (99%). La fiabilidad global de esta instancia de autenticación se podría calcular como el producto de estas fiabilidades: fiabilidad 100% * 97% * 90% * 99% - 86,4%.

Esta fiabilidad calculada representa la fiabilidad de una única instancia de autenticación. La fiabilidad global de una única instancia de autenticación también se puede calcular usando técnicas que tratan los diferentes factores de fiabilidad de manera diferente, por ejemplo, usando fórmulas en las que se asignan diferentes ponderaciones a cada factor de fiabilidad. Además, los expertos en la materia reconocerán que los valores propiamente dichos que se usan pueden representar valores distintos a porcentajes y pueden usar sistemas no aritméticos. Una realización puede incluir un módulo que usa un peticionario de autenticación para establecer las ponderaciones de cada factor y los algoritmos que se usan 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 única instancia de autenticación, que se indica como etapa (1620). No obstante, puede ser útil, en muchas situaciones de autenticación, proporcionar múltiples instancias de autenticación a la vez. Por ejemplo, mientras intenta autenticarse usando el sistema de la presente invención, un usuario puede proporcionar datos de autenticación de huella dactilar de identificación del usuario, una tarjeta inteligente y una contraseña. En tal caso, se proporcionan al motor de confianza (110) tres instancias de autenticación independientes para 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, a su vez se seleccionará cada instancia, como se muestra en la etapa (1630), y se evaluará como se ha descrito anteriormente en las etapas (1610), (1615) y (1620).

Cabe señalar que muchos de los factores de fiabilidad que se analizan pueden variar de una de estas instancias a otra. Por ejemplo, es probable que la fiabilidad inherente de estas técnicas, así como el grado de coincidencia proporcionado entre los datos de autenticación y los datos de registro sean diferentes. Además, el usuario puede haber proporcionado datos de registro en diferentes momentos y en diferentes circunstancias para cada una de estas técnicas, lo que proporciona, asimismo, diferentes fiabilidades de registro para cada una de estas instancias. Por último, aunque las circunstancias en las que se están presentando los datos para cada una de estas instancias sean las mismas, el uso de cada una de dichas técnicas puede ajustarse al perfil del usuario de manera diferente y se pueden asignar diferentes fiabilidades circunstanciales. (Por ejemplo, el usuario puede normalmente usar su contraseña y huella dactilar, pero no su tarjeta inteligente).

Por consiguiente, la fiabilidad definitiva para cada una de estas instancias de autenticación puede ser diferente. No obstante, usando múltiples instancias juntas, el nivel global de certidumbre de la autenticación tenderá a aumentar.

Una vez que el motor de autenticación ha llevado a cabo 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 global de certidumbre de la autenticación. Este proceso de combinar las fiabilidades de instancias de autenticación individuales en el nivel de certidumbre de la autenticación, se puede modelar con varios procedimientos relacionados con las fiabilidades individuales producidas y también puede tratar la interacción específica entre algunas de estas técnicas de autenticación. (Por ejemplo, múltiples sistemas basados en conocimientos, tales como contraseñas, pueden producir menos certidumbre que una única contraseña e incluso que datos biométricos poco convincentes, tales como un análisis básico de voz).

Un medio en el que el motor de autenticación (215) puede combinar las fiabilidades de múltiples instancias de autenticación concurrentes para generar un nivel de certidumbre definitivo es multiplicar la falta de fiabilidad de cada instancia para llegar a una falta de fiabilidad total. Por lo general, la falta de fiabilidad es el porcentaje complementario de la fiabilidad. Por ejemplo, una técnica que es fidedigna al 84% no es fidedigna al 16%. Las tres instancias de autenticación que se han descrito anteriormente (huella dactilar, tarjeta inteligente, contraseña) que producen fiabilidades del 86%, 75% y 72% tendría faltas de fiabilidad correspondientes del (100-86) %, (100-75) % y (100-72) % ó 14%, 25% y 28%, respectivamente. Multiplicando, estas faltas de fiabilidad, se obtiene una falta de fiabilidad acumulada del 14% * 25% * 28% - 0,98%, que corresponde a una fiabilidad del 99,02%.

En un modo adicional de funcionamiento, se pueden aplicar factores adicionales y heurística (530) dentro del motor de autenticación (215) para explicar la interdependencia de varias técnicas de autenticación. Por ejemplo, si alguien

tiene acceso no autorizado a un ordenador particular específico, probablemente también tendrá acceso a la línea telefónica de esa dirección. Por lo tanto, autenticar en función de un número de teléfono de origen, así como del número de serie del sistema de autenticación, no añade mucho más a la certidumbre global de la autenticación. No obstante, la autenticación basada en conocimientos es en gran parte independiente de la autenticación basada en testigos (es decir, si alguien le roba el teléfono móvil o las llaves, no tiene más probabilidades de conocer su PIN o contraseña que si no lo hubiera robado).

Además, diferentes vendedores u otros peticionarios de autenticación pueden querer ponderar diferentes aspectos de autenticación de manera diferente. Esto puede incluir el uso de algoritmos o factores de ponderación independientes que se usan al calcular la fiabilidad de instancias individuales, así como el uso de diferentes medios para evaluar eventos de autenticación con múltiples instancias.

Por ejemplo, vendedores de determinados tipos de transacciones, por ejemplo, sistemas de correo electrónico corporativo, pueden desear autenticar principalmente en función de la heurística y otros datos circunstanciales por defecto. Por lo tanto, pueden aplicar ponderaciones altas a factores relativos a los metadatos y otros perfiles relativos a información asociada a las circunstancias relacionadas con los eventos de autenticación. Esta disposición se podría usar para aligerar la carga a los usuarios durante horas de funcionamiento normales, siendo el único requisito que el usuario entre a la máquina correcta durante las horas laborables. No obstante, otro vendedor puede ponderar las autenticaciones que vienen de una técnica específica de manera más exigente, por ejemplo, coincidencia de huella dactilar, debido a una decisión de política de que una técnica de este tipo se adapta más a la autenticación, a efectos del vendedor específico.

El peticionario de autenticación puede definir dichas distintas ponderaciones al generar la petición de autenticación y enviarlas al motor de confianza (110) con la petición de autenticación en un modo de funcionamiento. Dichas opciones también se podrían establecer como preferencias durante un proceso de registro inicial correspondiente al peticionario de autenticación y almacenar dentro del motor de autenticación, en otro modo de funcionamiento.

Una vez que el motor de autenticación (215) produce un nivel de certidumbre de la autenticación para los datos de autenticación proporcionados, dicho nivel de certidumbre se usa para rellenar la petición de autenticación en la etapa (1640) y esta información se remite desde el motor de autenticación (215) al motor de transacciones (205) para inclusión en un mensaje al peticionario de autenticación.

El proceso que se ha descrito anteriormente es únicamente de ejemplo y los expertos en la materia reconocerán que no es necesario llevar a cabo las etapas en el orden que se muestra o que sólo se desea llevar a cabo determinadas etapas o que se puede desear una variedad de combinaciones de etapas. Además, determinadas etapas, tales como la evaluación de la fiabilidad de cada instancia de autenticación proporcionada, se puede realizar en paralelo con otra si las circunstancias lo permiten.

En un aspecto adicional de esta invención, se proporciona un procedimiento para satisfacer condiciones, cuando el nivel de certidumbre de la autenticación que produce el proceso que se ha descrito anteriormente no cumple el nivel de confianza requerido del vendedor u otras partes que requieran la autenticación. En circunstancias como estas en las que existe una brecha entre el nivel de certidumbre proporcionado y el nivel de confianza deseado, el operador del motor de confianza 110 está en posición de dar oportunidades para que una o ambas partes proporcionen datos alternativos o requisitos a fin de cerrar esta brecha de confianza. En este documento este proceso se denominará "arbitraje de confianza".

El arbitraje de confianza puede tener lugar dentro de una estructura de autenticación criptográfica, como se ha descrito anteriormente haciendo referencia a las figuras 10 y 11. Como se muestra en las mismas, un vendedor u otra parte pedirán la autenticación de un usuario específico en asociación con una transacción específica. En una circunstancia, el vendedor simplemente pide una autenticación, positiva o negativa, y tras recibir los datos adecuados del usuario, el motor de confianza (110) proporcionará una autenticación binaria de este tipo. En tales circunstancias, el grado de certidumbre requerido para asegura una autenticación positiva se determina en función de preferencias establecidas dentro del motor de confianza (110).

No obstante, también es posible que el vendedor pueda pedir un nivel específico de confianza a fin de concluir una transacción específica. Este nivel requerido se puede incluir con la petición de autenticación (por ejemplo, autenticar a este usuario con una certidumbre del 98%) o se puede determinar por medio del motor de confianza (110) en función de otros factores asociados a la transacción (es decir, autenticar a este usuario como adecuado para esta transacción). Un factor de este tipo podría ser el valor económico de la transacción. Para transacciones que tienen

mayor valor económico, se puede requerir un grado de confianza superior. Asimismo, para transacciones con altos grados de riesgo se puede requerir un alto grado de confianza. Por el contrario, para transacciones que son de bajo riesgo o de poco valor, el vendedor u otro peticionario de autenticación puede requerir niveles de confianza inferiores.

El proceso de arbitraje de confianza tiene lugar 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 da lugar a la evaluación de niveles de confianza y el posible arbitraje de confianza tiene lugar como se muestra en la figura 17. En circunstancias en las que se lleva a cabo una autenticación binaria sencilla, el proceso que se muestra en la figura 17 reduce que el motor de transacciones (205) tenga que comparar directamente los datos de autenticación proporcionados con los datos de registro del usuario identificado, como se ha analizado anteriormente haciendo referencia a la figura 10, marcando cualquier diferencia como autenticación negativa.

Como se muestra en la figura 17, la primera etapa tras recibir los datos en la etapa (1050) es para que el motor de transacciones (205) determine el nivel de confianza que se refiere para una autenticación positiva, para esta transacción específica, en la etapa (1710). Esta etapa se puede llevar a cabo con uno de varios procedimientos diferentes. El peticionario de autenticación puede especificar al motor de confianza (110) el nivel de confianza requerido en el momento en que se hace la petición de autenticación. El peticionario de autenticación también puede establecer con antelación una preferencia que se almacena dentro del depósito (210) u otro dispositivo de almacenamiento al que pueda acceder el motor de transacciones (205). Posteriormente, esta preferencia se puede leer y usar cada vez que este peticionario de autenticación haga una petición de autenticación. La preferencia también puede estar asociada a un usuario específico como medida de seguridad, de manera que siempre se requiera un nivel específico de confianza a fin de autenticar a ese usuario, almacenándose la preferencia de usuario en el depósito (210) u otros medios de almacenamiento a los que pueda acceder el motor de transacciones (205). El motor de transacciones (205) o el motor de autenticación (215) también pueden obtener el nivel requerido en función de la información proporcionada en la petición de autenticación, tal como el valor y nivel de riesgo de la transacción que se va a autenticar.

En un modo de funcionamiento, un módulo de gestión de políticas u otro software que se usa al generar la petición de autenticación se usa para especificar el grado requerido de confianza para la autenticación de la transacción. Esto se puede usar para proporcionar una serie de reglas que se deben seguir al asignar el nivel de confianza requerido en función de las políticas que se especifican dentro del módulo de gestión de políticas. Un modo ventajoso de funcionamiento es que un módulo de este tipo tenga incorporado el servidor web de un vendedor a fin de determinar adecuadamente el nivel de confianza requerido para transacciones iniciadas con el servidor web del vendedor. De este modo, se puede asignar a las peticiones de transacciones de usuarios un nivel de confianza requerido de acuerdo con las políticas del vendedor y dicha información se puede remitir al motor de confianza (110) junto con la petición de autenticación.

El nivel de confianza requerido está correlacionado con el grado de certeza que el vendedor quiere tener respecto a que el individuo que se autentica es de hecho como quien se identifica. Por ejemplo, si la transacción es una en la que el vendedor quiere un grado justo de certeza porque los productos cambian de manos, el vendedor puede requerir un nivel de confianza del 85%. Para situaciones en las que el vendedor está autenticando al usuario únicamente para dejarle ver contenido sólo para miembros o ejercer privilegios en una sala de tertulias, el riesgo a la baja puede ser lo suficientemente bajo como para que el vendedor requiera sólo un nivel de confianza del 60%. No obstante, para celebrar un contrato de producción con un valor de decenas de miles de dólares, el vendedor puede requerir un nivel de confianza del 99% o superior.

Este nivel de confianza requerido representa una métrica a la que el usuario se debe autentificar a fin de concluir la transacción. Si el nivel de confianza requerido es, por ejemplo, el 85%, el usuario debe proporcionara autenticación al motor de confianza (110) suficiente para que el motor de confianza (110) diga con una certidumbre del 85% que el usuario es quien dice ser. Es el equilibrio entre este nivel de confianza requerido y el nivel de certidumbre de la autenticación lo que produce una autenticación positiva (a satisfacción del vendedor) o una posibilidad de arbitraje de confianza.

Como se muestra en la figura 17, una vez que el motor de transacciones (205) recibe el nivel de confianza requerido, en la etapa (1720) compara el nivel de confianza requerido con el nivel de certidumbre de la autenticación que calculó el motor de autenticación (215) para la autenticación actual (como se ha analizado haciendo referencia a la figura 16). Si el nivel de certidumbre de la autenticación es superior al nivel de confianza requerido para la

transacción en la etapa (1730), entonces el proceso se desplaza a la etapa (1740) en la que el motor de transacciones (205) produce una autenticación positiva para esta transacción. Un mensaje a tal efecto se insertará en los resultados de autenticación y se devolverá al vendedor por medio del motor de transacciones (205) como se muestra en la etapa (1055) (véase la figura 10).

No obstante, si el nivel de certidumbre de la autenticación no cumple el nivel de confianza requerido en la etapa (1730), existe una brecha de certidumbre para la autenticación actual y, en la etapa (1750), se realiza un arbitraje de confianza. El arbitraje de confianza se describe de manera más completa haciendo referencia a la figura 18 más adelante. Este proceso, como se describe más adelante, tiene lugar dentro del motor de transacciones (205) del motor de confianza (110). Dado que no se necesita autenticación ni otras operaciones criptográficas para ejecutar el arbitraje de confianza (distintas de las requeridas para la comunicación SSL entre el motor de transacciones (205) y otros componentes), el proceso se puede llevar a cabo fuera del motor de autenticación (215). No obstante, como se analizará más adelante, cualquier nueva evaluación de los datos de autenticación u otros eventos criptográficos o de autenticación requerirá que el motor de transacciones (205) vuelva a presentar los datos adecuados al motor de autenticación (215). Los expertos en la materia reconocerán que el proceso de arbitraje de confianza podría, alternativamente, estar estructurado para que tuviera lugar parcial o totalmente dentro del propio motor de autenticación (215).

Como se ha mencionado 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, si procede. Como se muestra en el etapa (1805), el motor de transacciones (205) determina primero si la situación actual es o no adecuada para el arbitraje de confianza. Esto se puede determinar en función de las circunstancias de la autenticación, por ejemplo, si esta autenticación ya ha pasado por múltiples ciclos de arbitraje, así como en función de las preferencias del vendedor o el usuario, como se analizará detenidamente más adelante.

En circunstancias en las que el arbitraje no es posible, el proceso pasa a la etapa (1810) en la que el motor de transacciones (205) genera una autenticación negativa y la inserta en los resultados de autenticación que se envían al vendedor en la etapa (1055) (véase la figura 10). Un límite que se puede usar, de manera ventajosa, para evitar que las autenticaciones estén pendientes indefinidamente es establecer un período de espera desde la petición de autenticación inicial. De este modo, en cualquier transacción que no se autentique positivamente dentro del límite de tiempo se deniega un arbitraje adicional y se autentica negativamente. Los expertos en la materia reconocerán que un tiempo límite de este tipo puede variar dependiendo de las circunstancias de la transacción y de los deseos del usuario y el vendedor. También se pueden poner limitaciones en el número de intentos que se pueden hacer para proporcionar una autenticación satisfactoria. Dichas limitaciones se pueden tratar por medio de 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 transacciones (205) iniciará la negociación con una o ambas de las partes de la transacción. El motor de transacciones (205) puede enviar un mensaje al usuario pidiendo alguna forma de autenticación adicional a fin de aumentar el nivel de certidumbre de la autenticación producido como se muestra en la etapa (1820). En la forma más sencilla, esto puede simplemente indicar que la autenticación era insuficiente. También se puede enviar una petición para producir una o más instancias de autenticación adicionales para mejorar el nivel de certidumbre global de la autenticación.

Si en la etapa (1825) el usuario proporciona algunas instancias de autenticación adicionales, el motor de transacciones (205) añade estas instancias de autenticación a los datos de autenticación correspondiente a la transacción y los remite al motor de autenticación (215) como se muestra en la etapa (1015) (véase la figura 10) y se vuelve a evaluar la autenticación en función tanto de las instancias de autenticación preexistentes para esta transacción como de las instancias de autenticación recién proporcionadas.

Un tipo adicional de autenticación puede ser una petición del motor de confianza (110) para hacer alguna forma de contacto persona a persona entre el operador del motor de confianza (110) (o un adjunto de confianza) y el usuario, por ejemplo, mediante llamada telefónica. Esta llamada telefónica u otra autenticación sin ordenador se puede usar para proporcionar contacto personal con el individuo y también para realizara alguna forma de autenticación basada en cuestionarios. Esto también puede dar la oportunidad de verificar un número de teléfono de origen y, potencialmente, un análisis de voz del usuario cuando llama. Aunque no se puedan proporcionar datos adicionales de autenticación, el contexto adicional asociado al número de teléfono del usuario puede mejorar la fiabilidad del contexto de autenticación. Cualquier circunstancia o dato revisado en función de esta llamada telefónica se alimenta al motor de confianza (110) para uso en la consideración de la petición de autenticación.

Adicionalmente, en la etapa (1820) el motor de confianza (110) puede dar una oportunidad para que el usuario adquiera un seguro, comprando de manera eficaz una autenticación de mayor certidumbre. El operador del motor de confianza (110) puede querer, a veces, poner a disposición esa opción sólo si el nivel de certidumbre de la autenticación es superior a determinado umbral con el que empezar. De hecho, este seguro de usuario es una manera de que el motor de confianza (110) responda del usuario cuando la autenticación cumple el nivel normal requerido de confianza del motor de confianza (110) para la autenticación, pero no cumple el nivel de confianza requerido del vendedor para esta transacción. De este modo, el usuario todavía se puede autenticar satisfactoriamente a un nivel muy alto que pueda requerir el vendedor, aun cuando sólo tiene instancias de autenticación que producen certidumbre suficiente para el motor de confianza (110).

Esta función del motor de confianza (110) permite al motor de confianza (110) responder de alguien que se autentica a satisfacción del motor de confianza (110), pero no del vendedor. Esto es análogo a la función que lleva a cabo un notario al añadir su firma a un documento a fin de indicar a alguien que lee el documento posteriormente que la persona cuya firma aparece en el documento es en realidad la persona que lo firmó. La firma del notario es prueba fehaciente del acto de firma por parte del usuario. Del mismo modo, el motor de confianza proporciona una indicación de que la persona que está llevando a cabo las transacciones es quien dice ser.

No obstante, dado que el motor de confianza (110) está aumentando artificialmente el nivel de certidumbre proporcionado por el usuario, existe mayor riesgo para el operador del motor de confianza (110), puesto que el usuario no está cumpliendo en realidad el nivel de confianza requerido del vendedor. El coste del seguro está diseñado para compensar el riesgo de una autenticación positiva falsa para el motor de confianza (110) (que puede de manera eficaz autenticar notarialmente las autenticaciones del usuario). El usuario paga al operador del motor de confianza (110) para que asuma el riesgo de autenticar a un nivel superior de certidumbre del que en realidad se ha proporcionado.

Dado que un sistema de seguro de este tipo permite a alguien comprar de manera eficaz una clasificación de certidumbre superior del motor de confianza (110), tanto vendedores como usuarios pueden querer evitar el uso del seguro de usuario en determinadas transacciones. Los vendedores pueden querer limitar las autenticaciones positivas a circunstancias en las que conocen que los datos de autenticación reales confirman el grado de certidumbre que requieren y pueden indicar al motor de confianza (110) que no se permita el seguro de usuario. Asimismo, para proteger su identidad en línea, un usuario puede querer evitar el uso del seguro de usuario por su cuenta o puede querer limitar su uso a situaciones en las que el nivel de certidumbre de la autenticación sin el seguro es superior a un límite determinado. Esto se puede usar como medida de seguridad para evitar que alguien oiga por casualidad una contraseña o robe una tarjeta inteligente y las use para autenticarse falsamente a un nivel bajo de certidumbre y, posteriormente, adquiera un seguro para producir un nivel muy alto de certidumbre (falsa). Estos factores se pueden evaluar al determinar si se permite el seguro de usuario.

Si en la etapa (1840) el usuario adquiere un seguro, en la etapa (1845), se ajusta el nivel de certidumbre de la autenticación en función el seguro adquirido y el nivel de certidumbre de la autenticación y el nivel de confianza requerido se vuelven a comparar en la etapa (1730) (véase la figura 17). El proceso continúa a partir de ahí y puede dar lugar a una autenticación positiva en la etapa (1740) (véase la figura 17) o volver al proceso de arbitraje de confianza en la etapa (1750) para un arbitraje adicional (si está permitido) o una autenticación negativa en la etapa (1810), si está prohibido un arbitraje adicional.

Además de enviar un mensaje al usuario en la etapa (1820), el motor de transacciones (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 al vendedor varias opciones sobre cómo seguir. Una de estas opciones es simplemente informar al vendedor de cuál es el nivel de certidumbre de la autenticación actual y preguntar si el vendedor quiere mantener sin cumplir su nivel de confianza requerido. Esto puede ser beneficioso porque, en algunos casos, el vendedor puede tener medios independientes para autenticar la transacción o puede haber estado usando un conjunto de requisitos por defecto que, por lo general, tienen como resultado haber especificado inicialmente un nivel requerido superior al que en realidad se necesita para la transacción específica en cuestión.

Por ejemplo, puede ser práctica normal esperar que todas las transacciones de orden de compra entrantes con el vendedor cumplan un nivel de confianza del 98%. No obstante, si el vendedor y un antiguo cliente hablaron recientemente por teléfono de una orden y justo después se autentica la transacción, pero sólo a un nivel de certidumbre del 93%, el vendedor puede querer simplemente bajar el umbral de aceptación para esta transacción, porque realmente la llamada telefónica proporciona autenticación adicional al vendedor. En determinadas

circunstancias, el vendedor puede estar dispuesto a bajar su nivel de confianza requerido, pero no hasta el nivel de la certidumbre de autenticación actual. Por ejemplo, el vendedor del ejemplo anterior podría considerar que la llamada telefónica anterior a la orden podría merecer una reducción del 4% del grado de confianza necesario. No obstante, sigue siendo superior a la certidumbre del 93% producida por el usuario.

Si en la etapa (1835) el vendedor ajusta su nivel de confianza requerido, en la etapa (1730) se compara el nivel de certidumbre de autenticación producido por la autenticación y el nivel de confianza requerido (véase la figura 17). Si ahora el nivel de certidumbre supera el nivel de confianza requerido, en la etapa (1740) se puede generar una autenticación positiva en el motor de transacciones (205) (véase la figura 17). Si no, se puede intentar un arbitraje adicional, como se ha analizado anteriormente, si está permitido.

Además de pedir un ajuste al nivel de confianza requerido, el motor de transacciones (205) también puede ofrecer un seguro de vendedor al vendedor que pide la autenticación. Este seguro tiene un propósito similar al que se ha descrito anteriormente en relación con el seguro de usuario. No obstante, en este caso, en lugar de que el motor de confianza (110) asuma el coste correspondiente al riesgo al autenticar por encima del nivel de certidumbre de la autenticación real, el coste del seguro corresponde al riesgo que asume el vendedor al aceptar un nivel de confianza inferior de la autenticación.

En lugar de simplemente bajar su nivel de confianza requerido real, el vendedor tiene la opción de adquirir un seguro para protegerse del riesgo adicional asociado a un nivel de confianza inferior de la autenticación del usuario. Como se ha descrito anteriormente, puede ser ventajoso que el vendedor sólo considere adquirir dicho seguro para cubrir la brecha de confianza en condiciones en las que la autenticación existente ya está por encima de determinado umbral.

La disponibilidad de dicho seguro de vendedor permite al vendedor la opción de: bajar su requisito de confianza directamente sin coste adicional para él, asumir el riesgo de una autenticación falsa (en función del nivel inferior de confianza requerido) o comprar un seguro para la brecha de confianza entre el nivel de certidumbre de la autenticación y su requisito, asumiendo el operador del motor de confianza (110) el riesgo del nivel inferior de certidumbre que se ha proporcionado. Adquiriendo el seguro, el vendedor mantiene de manera eficaz su requisito de alto nivel de confianza, porque el riesgo de una autenticación falsa se traspasa al operador del motor de confianza (110).

Si en la etapa (1840) el vendedor adquiere un seguro, en la etapa (1730) se compara el nivel de certidumbre de la autenticación y los niveles requeridos de confianza (véase la figura 17) y el proceso continúa como se ha descrito anteriormente.

Cabe señalar que también es posible que tanto el usuario como el vendedor respondan a mensajes del motor de confianza (110). Los expertos en la materia reconocerán que existen múltiples formas de tratar dichas situaciones. Una forma ventajosa de tratar la posibilidad de múltiples respuestas es simplemente tratar las respuestas de manera primero en llegar, primero en ser atendido. Por ejemplo, si el vendedor responde con un nivel de confianza baja requerido y justo después el usuario también adquiere un seguro para subir su nivel de autenticación, la autenticación se vuelve a evaluar primero en función del requisito del vendedor de confianza baja. Si ahora la autenticación es positiva, se ignora la adquisición de seguro del usuario. En otro modo ventajoso de funcionamiento, se podría cargar al usuario sólo el nivel del seguro requerido para cumplir el nuevo requisito del vendedor de confianza baja (si quedara una brecha de confianza incluso con el requisito del vendedor de confianza baja).

Si, en la etapa (1850), no se recibe respuesta de ninguna de las partes durante el proceso de arbitraje de confianza en el límite de tiempo fijado para la autenticación, en la etapa (1805) se vuelve a evaluar el arbitraje. Esto en realidad vuelve a empezar el proceso de arbitraje. Si el límite de tiempo era definitivo u otras circunstancias evitan un arbitraje adicional en la etapa (1805), en la etapa (1810) el motor de transacciones (205) genera una autenticación negativa y la devuelve al vendedor en la etapa (1055) (véase la figura 10). Si no, se puede enviar un nuevo mensaje al usuario y al vendedor y se puede repetir el proceso según se desee.

Cabe señalar que para determinados tipos de transacciones, por ejemplo, firmar digitalmente documentos que no forman parte de una transacción, no necesariamente tiene que ser un vendedor u otro tercero. Por lo tanto, la transacción es principalmente entre el usuario y el motor de confianza (110). En circunstancias como estas, el motor de confianza (110) tendrá su propio nivel de confianza requerido que se debe satisfacer a fin de generar una autenticación positiva. No obstante, en tales circunstancias, a menudo no será aconsejable que el motor de confianza (110) ofrezca un seguro al usuario para que éste suba la certidumbre de su propia firma.

El proceso que se ha descrito anteriormente y que se muestra en las figuras 16 a 18 se puede realizar usando varios modos de comunicaciones, como se ha descrito anteriormente haciendo referencia al motor de confianza (110). Por ejemplo, los mensajes pueden ser en red y se pueden enviar usando conexiones SSL entre el motor de confianza (110) y miniaplicaciones descargadas en tiempo real a navegadores que se ejecutan en los sistemas de usuario o vendedor. En un modo alternativo de funcionamiento, determinadas aplicaciones dedicadas las pueden usar el usuario y el vendedor, lo que facilita dichas transacciones de seguro y arbitraje. En otro modo alternativo de funcionamiento, se pueden usar operaciones de correo electrónico seguro para mediar el arbitraje que se ha descrito anteriormente, permitiendo de ese modo evaluaciones aplazadas y procesamiento por lotes de las autenticaciones. Los expertos en la materia reconocerán que se pueden usar diferentes modos de comunicaciones que sean adecuados a las circunstancias y a los requisitos de autenticación del vendedor.

En la siguiente descripción, haciendo referencia a la figura 19, se describe una transacción de muestra que integra los distintos aspectos de la presente invención que se han descrito anteriormente. Este ejemplo ilustra el proceso global entre un usuario y un vendedor mediado por el motor de confianza (110). Aunque se pueden usar las distintas etapas y componentes que se han descrito anteriormente para realizar la siguiente transacción, el proceso que se ilustra se centra en la interacción entre el motor de confianza (110), el usuario y el vendedor.

La transacción empieza en la etapa (1900), cuando el usuario, mientras ve páginas web en línea, cumplimenta una nota de pedido en el sitio web del vendedor. El usuario quiere presentar su nota de pedido al vendedor, firmada con su firma digital. Para hacer esto, en la etapa (1905), el usuario presenta la nota de pedido con su petición de una firma al motor de confianza (110). El usuario también proporcionará datos de autenticación que se usarán, como se ha descrito anteriormente, para autenticar su identidad.

En la etapa (1910), el motor de confianza (110) compara los datos de autenticación con los datos de registro, como se ha analizado anteriormente, y si se produce una autenticación positiva, el resumen de la nota de compra, firmado con la clave privada del usuario, se remite al vendedor junto con la nota de compra propiamente dicha.

En la etapa (1915), el vendedor recibe la nota firmada y, a continuación, el vendedor generará una factura u otro contrato relativo a la adquisición que se va a realizar en la etapa (1920). En la etapa (1925), dicho contrato se envía de vuelta al usuario con una petición de firma. En la etapa (1930), el vendedor también envía una petición de autenticación para esta transacción contractual al motor de confianza (110) que incluye un resumen del contrato que firmarán ambas partes. Para permitir que ambas partes firmen el contrato digitalmente, el vendedor también incluye sus propios datos de autenticación para que, posteriormente, si es necesario, se pueda verificar la firma del vendedor que figura en el contrato.

Como se ha analizado anteriormente, el motor de confianza (110) verifica los datos de autenticación proporcionados por el vendedor para confirmar la identidad del vendedor y si en la etapa (1935) los datos producen una autenticación positiva, continua con la etapa (1955) cuando se reciben los datos del usuario. Si los datos de autenticación del vendedor no coinciden con los datos de registro del vendedor en la medida deseada, se devuelve un mensaje al vendedor solicitando autenticación adicional. En este caso, se puede llevar a cabo el arbitraje de confianza si es necesario, como se ha descrito anteriormente, a fin de que el vendedor se pueda autentificar satisfactoriamente al motor de confianza (110).

Cuando en la etapa (1940) el usuario recibe el contrato, lo revisa, en la etapa (1945) genera datos de autenticación para firmarlo si es aceptable y en la etapa (1950) envía un resumen del contrato y sus datos de autenticación al motor de confianza (110). En la etapa (1955), el motor de confianza (110) verifica los datos de autenticación y si la autenticación es buena pasa a procesar el contrato como se describe más adelante. Como se ha analizado anteriormente haciendo referencia a las figuras 17 y 18, se puede llevar a un cabo un arbitraje de confianza, si procede, para cerrar cualquier brecha de confianza que exista entre el nivel de certidumbre de la autenticación y el nivel requerido de autenticación para la transacción.

El motor de confianza (110) firma el resumen del contrato con la clave privada del usuario, y envía el resumen firmado al vendedor en la etapa (1960), firmando todo el mensaje en su nombre, es decir, incluyendo un resumen de todo el mensaje (incluida la firma del usuario) cifrado con la clave privada (510) del motor de confianza (110). En la etapa (1965), el vendedor recibe este mensaje. El mensaje representa un contrato firmado (resumen del contrato cifrado usando la clave privada del usuario) y un recibo del motor de confianza (110) (el resumen del mensaje que incluye el contrato firmado, cifrado usando la clave privada del motor de confianza (110)).

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

Además de lo anterior, un aspecto adicional de la invención proporciona un Módulo de Proveedor de Servicios (SPM) criptográfico que puede estar disponible para una aplicación de cliente como medio para acceder a funciones proporcionadas por el motor de confianza (110) que se han descrito anteriormente. Un modo ventajoso de proporcionar un servicio de este tipo es que el SPM criptográfico medie en las comunicaciones entre una Interfaz de Programación de Aplicaciones (API) de terceros y un motor de confianza (110) que es accesible a través de una red u otra conexión remota. Más adelante se describe un SPM criptográfico de muestra haciendo referencia a la figura 20.

Por ejemplo, en un sistema típico, una serie de APIs están a disposición de los programadores. Cada API proporciona un conjunto de llamadas de función que se pueden hacer por medio de una aplicación (2000) que se ejecuta en el sistema. Ejemplos de APIs que proporcionan interfaces de programación adecuadas para funciones criptográficas, funciones de autenticación y otras funciones de seguridad incluyen la API criptográfica (CAPI) (2010) que Microsoft proporciona con sus sistemas operativos Windows y la Arquitectura de Seguridad de Datos Comunes (CDSA), patrocinada por IBM, Intel y otros miembros del Open Group. La CAPI se usará como API de seguridad de ejemplo en el análisis que viene a continuación. No obstante, el SPM criptográfico que se describe se podría usar con CDSA u otras APIs de seguridad que se conozcan en la técnica.

Un sistema de usuario (105) o un sistema de vendedor (120) usa esta API cuando hace una llamada para una función criptográfica. Entre estas funciones pueden estar incluidas peticiones asociadas a llevar a cabo distintas operaciones criptográficas, tales como, cifrar un documento con una clave específica, firmar un documento, pedir un certificado digital, verificar una firma de un documento firmado y otras funciones criptográficas que se describen en este documento o conocidas para los expertos en la materia.

Dichas funciones criptográficas normalmente se llevan a cabo localmente respecto al sistema en el que está ubicada la CAPI (2010). Esto se debe a que, por lo general, las funciones llamadas requieren el uso de recursos del sistema de usuario local (105), tal como un lector de huellas dactilares, o funciones de software que se programan usando bibliotecas que se ejecutan en la máquina local. Normalmente, el acceso a estos recursos locales se proporciona por medio de uno o más Módulos de Proveedor de Servicios (SPMs) (2015), (2020), como se ha denominado anteriormente, que proporcionan recursos con los que se realizan las funciones criptográficas. Dichos SPMs pueden incluir bibliotecas de software (2015) para llevar a cabo operaciones de cifrado o descifrado o controladores y aplicaciones (2020) que son capaces de acceder a hardware especializado (2025), tal como dispositivos de escaneo biométrico. Del mismo modo que la CAPI (2010) proporciona funciones que puede usar una aplicación (2000) del sistema (105), los SPMs (2015), (2020) proveen a la CAPI de acceso a los recursos y funciones de nivel inferior asociados a los servicios disponibles en el sistema.

De acuerdo con la invención, se puede proporcionar un SPM criptográfico (2030) que sea capaz de acceder a las funciones criptográficas que proporciona el motor de confianza (110) y poner dichas funciones a disposición de una aplicación (2000) a través de la CAPI (2010). A diferencia de las realizaciones en las que la CAPI (2010) sólo puede acceder a recursos que están disponibles localmente a través de SPMs (2015), (2020), un SPM criptográfico (2030), como se describe en esta invención, podría presentar peticiones de operaciones criptográficas a un motor de confianza (110) de ubicación remota y accesible por red a fin de llevar a cabo las operaciones deseadas.

Por ejemplo, si una aplicación (2000) tiene necesidad de una operación criptográfica, tal como firmar un documento, la aplicación (2000) hace una llamada de función a la función de la CAPI (2010) adecuada. A su vez, la CAPI (2010) ejecutará esta función haciendo uso de los recursos que han puesto a su disposición los SPMs (2015), (2020) y el SPM criptográfico (2030). En el caso de una función de firma digital, el SPM criptográfico (2030) generará una petición adecuada que se enviará al motor de confianza (110) a través del enlace de comunicación (125).

Las operaciones que tienen lugar 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). No obstante, estas funciones se ponen realmente a disposición de un sistema de usuario (105) a través de la CAPI (2010) de manera que parezcan estar disponibles localmente en el propio sistema de usuario (105). No obstante, a diferencia de los SMPS (2015), (2020) normales, las funciones se realizan en el motor de confianza (110) remoto y los resultados se transmiten al SPM criptográfico (2030) en respuesta a peticiones adecuadas a través del enlace de comunicación

(125).

El SPM criptográfico (230) pone una serie de operaciones a disposición del sistema de usuario (105) o de un sistema de vendedor (120) que de lo contrario no estarían disponibles. Estas funciones incluyen, a título enunciativo: cifrado y descifrado de documentos; expedición de certificados digitales; firma digital de documentos; verificación de firmas digitales y otras operaciones que resultarán evidentes para los expertos en la materia.

En una realización independiente, la presente invención comprende un sistema completo para llevar a cabo los procedimientos para asegurar datos de la presente invención en cualquier conjunto de datos. El sistema informático de esta realización comprende un módulo de división de datos que comprende la funcionalidad que se muestra en la figura 8 y que se describe 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 seguro, comprende un paquete de software o programa de analizador sintáctico que comprende funcionalidad de división de datos, cifrado y descifrado, reconstitución o reensamblaje. Esta realización puede comprender además un equipo de almacenamiento de datos o múltiples equipos de almacenamiento de datos. El módulo de división de datos, o analizador sintáctico de datos seguro, comprende un paquete de módulos de software de plataforma cruzada que se integra dentro de una infraestructura electrónica o como complemento de cualquier aplicación que requiere la seguridad máxima de sus elementos de datos. Este proceso de análisis sintáctico funciona en cualquier tipo de conjunto de datos y en todos y cada uno de los tipos de archivos o en una base de datos en cualquier fila columna o celda de datos de esa base de datos.

El proceso de análisis sintáctico de la presente invención puede, en una realización, estar diseñado en 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, entre otros, 1) dividir criptográficamente, dispersar y almacenar de manera segura en múltiples ubicaciones; 2) cifrar, dividir criptográficamente, dispersar y almacenar de manera segura en múltiples ubicaciones; 3) cifrar, dividir criptográficamente, cifrar cada porción, a continuación dispersar y almacenar de manera segura en múltiples ubicaciones y 4) cifrar, dividir criptográficamente, cifrar cada porción con un tipo de cifrado diferente al que se usó en la primera etapa, a continuación, dispersar y almacenar de manera segura en múltiples ubicaciones.

En una realización, el proceso comprende dividir los datos de acuerdo con el contenido de un número aleatorio generado, o clave, y llevar a cabo la misma división criptográfica de la clave que se usa en el cifrado de división de los datos para asegurarla en una o más partes, o porciones, de datos analizados sintácticamente y divididos y, en una realización, preferentemente, en cuatro o más partes de datos analizados sintácticamente y divididos, cifrar todas las partes, a continuación, esparcir y almacenar estas partes nuevamente en la base de datos o reubicarlas en cualquier dispositivo convenido, fijo o extraíble, dependiendo de la necesidad de privacidad y seguridad del peticionario. Alternativamente, en otra realización, el cifrado puede tener lugar antes de la división del conjunto de datos con el módulo de división o analizador sintáctico de datos seguro. Los datos originales procesados como se describe en esta realización se cifran y se hacen ininteligibles y se aseguran. La dispersión de los elementos cifrados, si se desea, puede ser prácticamente en cualquier sitio, entre otros, un único dispositivo de almacenamiento de datos o servidor o entre dispositivos o equipos de almacenamiento de datos independientes. En una realización, la gestión de claves de cifrado puede estar incluida en el paquete de software o, en otra realización, puede estar integrada en una infraestructura existente o en cualquier otra ubicación deseada.

Una división criptográfica (criptodivisión) particiona los datos en un número N de porciones. La partición puede ser en cualquier unidad de tamaño de datos, que incluye un bit individual, bits, kilobytes, megabytes o unidades mayores, así como en cualquier patrón o combinación de tamaños de unidades de datos ya sean predeterminados o generados aleatoriamente. Las unidades también pueden ser de diferente tamaño, en función de un conjunto de valores aleatorios o predeterminados. Esto significa que los datos se pueden ver como una secuencia de estas unidades. De este modo, el tamaño de las propias unidades de datos puede hacer los datos más seguros, por ejemplo, usando uno más patrones, secuencias o combinaciones de tamaños de unidades de datos predeterminados o generados aleatoriamente. Las unidades se distribuyen (de manera aleatoria o por un conjunto de valores predeterminado) en las N porciones. Esta distribución también podría conllevar una reorganización del orden de las unidades en las porciones. Resulta fácilmente evidente para los expertos en la materia que la distribución de las unidades de datos en las porciones se puede llevar a cabo de acuerdo con una gran variedad de selecciones posibles, que incluyen, entre otras, tamaño fijo, tamaños predeterminados o una o más combinaciones, patrones o secuencias de tamaños de unidades de datos predeterminados o que se generan aleatoriamente.

Un ejemplo de este proceso de división criptográfica, o criptodivisión, sería considerar que los datos tienen un

tamaño de 23 bytes, siendo el tamaño de unidades de datos elegido un byte y seleccionando 4 como el número de porciones. Cada byte se distribuiría en una de las 4 porciones. Suponiendo una distribución aleatoria, se obtendría una clave para crear una secuencia de 23 números aleatorios (r1, r2, r3 hasta r23), cada uno con valor entre 1 y 4 correspondiente a las cuatro porciones. Cada una de las unidades de datos (en este ejemplo 23 bytes individuales de datos) está asociada a uno de los 23 números aleatorios correspondientes a una de las cuatro porciones. La distribución de los bytes de los datos en cuatro porciones tendría lugar colocando el primer byte de los datos en el número de porción r1, el segundo byte en la porción r2, el tercer byte en la porción r3 hasta el 23º byte de los datos en la porción r23. Resulta fácilmente evidente para los expertos en la materia que en el proceso de criptodivisión de la presente invención se pueden usar una gran variedad de otras etapas o combinaciones o secuencias de etapas posibles, que incluyen el tamaño de las unidades de datos, y que el ejemplo anterior es una descripción no limitante de un proceso para criptodividir datos. Para recrear los datos originales, se llevaría a cabo la operación inversa.

En otra realización del proceso de criptodivisión de la presente invención, una opción para el proceso de criptodivisión es proporcionar redundancia suficiente en las porciones de manera que sólo se necesite un subconjunto de las porciones para reensamblar o restablecer los datos a su forma original o utilizable. Como ejemplo no limitante, la criptodivisión se puede hacer como criptodivisión de "3 de 4", de manera que sólo se necesiten tres de las cuatro porciones para reensamblar o restablecer los datos a su forma original o utilizable. Esto también se denomina una "criptodivisión de M de N", donde N es el número total de porciones y M es al menos uno menos que N. Resulta fácilmente evidente para alguien con conocimientos normales de 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 se almacena en dos porciones, la porción principal y la porción de reserva. Usando el proceso de criptodivisión de "3 de 4", que se ha descrito anteriormente, puede faltar cualquier porción, y esto es suficiente para reensamblar o restablecer los datos originales sin que falten unidades de datos, dado que sólo se requieren tres de las cuatro. Como se describe en este documento, se genera un número aleatorio que corresponde a una de las porciones. El número aleatorio se asocia a una unidad de datos y se almacena en la porción correspondiente, en función de una clave. En esta realización, se usa una clave para generar el número aleatorio de porción principal y de reserva. Como se describe en este documento respecto al proceso de criptodivisión de la presente invención, se genera un conjunto de números aleatorios (también denominados números de porción principal), de 0 a 3, igual al número de unidades de datos. A continuación, se genera otro conjunto de números aleatorios (también denominado números de porción de reserva), del 1 al 3, igual al número de unidades de datos. A continuación, cada unidad de datos se asocia a un número de porción principal y a un número de porción de reserva. Alternativamente, se puede generar un conjunto de números aleatorios que sea menor que el número de unidades de datos y repetir el conjunto de números aleatorios, pero esto puede reducir la seguridad de los datos confidenciales. El número de porción principal se usa para determinar en qué porción se almacena la unidad de datos. El número de porción de reserva se combina con el número de porción principal para crear un tercer número de porción entre 0 y 3 y este número se usa para determinar en qué porción se almacena la unidad de datos. En este ejemplo, la ecuación para determinar el tercer número de porción es:

(número de porción principal + número de porción de reserva) MOD 4 = tercer número de porción.

En la realización que se ha descrito anteriormente, en la que el número de porción principal es entre 0 y 3 y el número de porción de reserva es entre 1 y 3 garantiza que el tercer número de porción sea diferente al número de porción principal. Esto tiene como resultado que la unidad de datos se almacene en dos porciones diferentes. Resulta fácilmente evidente para alguien con conocimientos normales de la materia que existen muchas formas de llevar a cabo criptodivisión redundante y criptodivisión no redundante además de las realizaciones que se describen en este documento. Por ejemplo, las unidades de datos de cada porción se podrían reorganizar utilizando un algoritmo diferente. Dicha reorganización de unidades de datos se puede llevar a cabo, por ejemplo, cuando los datos originales se dividen en las unidades de datos, una vez que las unidades están colocadas en las porciones o una vez que la porción está llena.

Los distintos procesos de criptodivisión y procesos de reorganización de datos que se describen en este documento y el resto de realizaciones de los procedimientos de criptodivisión y reorganización de datos de la presente invención se pueden llevar a cabo en unidades de datos de cualquier tamaño, entre otros, tan pequeño como un bit individual, bits, bytes, kilobytes, megabytes o mayores.

Un ejemplo de una realización de código fuente que llevaría a cabo el proceso de criptodivisión que se describe en este documento es:

```
DATA [1:24] – conjunto de bytes con los datos que se van a dividir
SHARES [0:3; 1:24] – conjunto bidimensional, cada fila representa una de las porciones
RANDOM [1:24] – números aleatorios del conjunto 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,S2] = 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 llevaría a cabo el proceso RAID de criptodivisión que se describe en este documento es:

Generar dos conjuntos de números, Porción Principal es 0 a 3, Porción de Reserva es 1 a 3. A continuación, poner cada unidad de datos en porción[porciónprincipal[1]] y porción[(porciónprincipal[1]+porcióndereserva[1]) mod 4, con el mismo proceso que en la criptodivisión que se ha descrito anteriormente. Este procedimiento será escalable a cualquier N de tamaño, si sólo son necesarias N-1 porciones para restablecer los datos.

La recuperación, recombinación, reensamblaje o reconstitución de los elementos de datos cifrados puede utilizar cualquier número de técnicas de autenticación, entre otras, biometría, tal como reconocimiento de huella dactilar, escáner de cara, 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 análisis sintáctico de la presente invención se pueden integrar en una gran variedad de aplicaciones o productos de infraestructura, según se desee.

Tecnologías de cifrado tradicionales que se conocen en la técnica se basan en el uso de una o más claves para cifrar los datos y hacer que resulten inservibles sin la clave. No obstante, los datos se mantienen intactos y sujetos a ataque. En una realización, el analizador sintáctico de datos seguro de la presente invención soluciona este problema llevando a cabo un análisis sintáctico criptográfico y división del archivo cifrado en dos o más partes o porciones y, en otra realización, preferentemente, cuatro o más porciones, añadiendo otra capa de cifrado a cada porción de los datos, a continuación, almacenando las porciones en diferentes ubicaciones lógicas y/o físicas. Cuando una o más porciones de datos se extraen físicamente del sistema, usando un dispositivo extraíble, tal como un dispositivo de almacenamiento de datos, o colocando la porción bajo el control de un tercero, se elimina de manera eficaz cualquier posibilidad de poner en peligro los datos asegurados.

Un ejemplo de una realización del analizador sintáctico de datos seguro de la presente invención y un ejemplo de cómo se puede utilizar se muestran en la figura 21 y se describen más adelante. No obstante, resulta fácilmente evidente para alguien con conocimientos normales de la materia que el analizador sintáctico de datos seguro de la presente invención se puede utilizar de muchas formas además del ejemplo no limitante que se indica más adelante. Como opción de despliegue, y en una realización, el analizador sintáctico de datos seguro se puede implementar

con gestión externa de claves de sesión o almacenamiento seguro interno de claves de sesión. Tras la implementación, se generará una Clave Maestra de Analizador Sintáctico que se usará para asegurar la aplicación y a efectos de cifrado. También cabría señalar que la incorporación de la Clave Maestra de Analizador Sintáctico en los datos asegurados resultantes permite una flexibilidad de compartición de datos seguros por individuos de un grupo de trabajo, empresa o público en general.

Como se muestra en la figura 21, esta realización de la presente invención muestra las etapas del proceso que lleva a cabo el analizador sintáctico de datos seguro, en 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 de flujo RS1.

2. Separar los datos cifrados resultantes en cuatro porciones o partes 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 se almacenará junto con las porciones 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 los datos cifrados analizados sintácticamente.

4. Las cuatro porciones de datos resultantes contendrán partes cifradas de los datos originales y partes de la clave maestra de sesión. Generar una clave de cifrado de flujo para cada una de las cuatro porciones de datos.

5. Cifrar cada porción, a continuación, almacenar las claves de cifrado en diferentes ubicaciones de las partes o porciones de datos cifradas: Porción 1 obtiene Clave 4, Porción 2 obtiene Clave 1, Porción 3 obtiene Clave 2, Porción 4 obtiene Clave 3.

Para restablecer el formato de datos original se invierten las etapas.

Resulta fácilmente evidente para alguien con conocimientos normales de la materia que determinadas etapas de los procedimientos que se describen en este documento se pueden llevar a cabo en un orden diferente o repetir múltiples veces, según se desee. También resulta fácilmente evidente para los expertos en la materia que cada parte de los datos se puede tratar de manera diferente. Por ejemplo, se pueden llevar a cabo múltiples etapas de análisis sintáctico en sólo una parte de los datos analizados sintácticamente. Cada parte de los datos analizados sintácticamente se puede asegurar de manera exclusiva de cualquier forma aconsejable, siempre que los datos se puedan reensamblar, reconstituir, reformar, descifrar o restablecer 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 que lleva a cabo el analizador sintáctico de datos seguro, en los datos, para almacenar la clave maestra de sesión en una o más tablas independientes de gestión de claves:

1. Generar una clave maestra de sesión y cifrar los datos usando cifrado de flujo RS1.

2. Separar los datos cifrados resultantes en cuatro porciones o partes 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 se almacenará en una tabla independiente de gestión de claves de un depósito de datos. Generar una ID de transacción exclusiva para esta transacción. Almacenar la ID de transacción y la clave maestra de sesión en una tabla independiente de gestión de claves. Separar la ID de transacción de acuerdo con el patrón de la Clave Maestra de Analizador Sintáctico y adjuntar los datos a los datos cifrados separados o analizados sintácticamente.

4. Las cuatro porciones de datos resultantes contendrán partes cifradas de los datos originales y partes de la ID de transacción.

5. Generar una clave de cifrado de flujo para cada una de las cuatro porciones de datos.

6. Cifrar cada porción, a continuación, almacenar las claves de cifrado en diferentes ubicaciones de las partes o porciones de datos cifradas: Porción 1 obtiene Clave 4, Porción 2 obtiene Clave 1, Porción 3 obtiene Clave 2, Porción 4 obtiene Clave 3.

Para restablecer el formato de datos original se invierten las etapas.

Resulta fácilmente evidente para alguien con conocimientos normales de la materia que determinadas etapas de los procedimientos que se describen en este documento se pueden llevar a cabo en un orden diferente o repetir múltiples veces, según se desee. También resulta fácilmente evidente para los expertos en la materia que cada parte de los datos se puede tratar de manera diferente. Por ejemplo, se pueden llevar a cabo múltiples etapas de análisis sintáctico o separación en sólo una parte de los datos analizados sintácticamente. Cada parte de los datos analizados sintácticamente se puede asegurar de manera exclusiva de cualquier forma aconsejable, siempre que los datos se puedan reensamblar, reconstituir, reformar, descifrar o restablecer 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 que lleva a cabo el analizador de datos seguros, en los datos, para almacenar la clave maestra de sesión con los datos analizados sintácticamente:

1. Acceder a la clave maestra de analizador sintáctico asociada al usuario autenticado.

2. Generar una clave Maestra de Sesión exclusiva.

3. Obtener 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 nuevo o existente puesto en clave con la Clave Intermedia.

5. Separar los datos opcionalmente cifrados resultantes en cuatro porciones o partes de datos analizados sintácticamente de acuerdo con el patrón de la Clave Intermedia.

6. En esta realización del procedimiento, la clave maestra de sesión se almacenará junto con las porciones 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 porciones de datos opcionalmente cifrados analizados sintácticamente.

7. Las múltiples porciones de datos resultantes contendrán partes opcionalmente cifradas de los datos originales y partes de la clave maestra de sesión.

8. Opcionalmente, generar una clave de cifrado para cada una de las cuatro porciones de datos.

9. Opcionalmente, cifrar cada porción con un algoritmo de cifrado nuevo o existente, a continuación, almacenar las claves de cifrado en diferentes ubicaciones de las partes o porciones de datos cifradas: por ejemplo, Porción 1 obtiene Clave 4, Porción 2 obtiene Clave 1, Porción 3 obtiene Clave 2, Porción 4 obtiene Clave 3.

Para restablecer el formato de datos original se invierten las etapas.

Resulta fácilmente evidente para alguien con conocimientos normales de la materia que determinadas etapas de los procedimientos que se describen en este documento se pueden llevar a cabo en un orden diferente o repetir múltiples veces, según se desee. También resulta fácilmente evidente para los expertos en la materia que cada parte de los datos se puede tratar de manera diferente. Por ejemplo, se pueden llevar a cabo múltiples etapas de análisis sintáctico en sólo una parte de los datos analizados sintácticamente. Cada parte de los datos analizados sintácticamente se puede asegurar de manera exclusiva de cualquier forma aconsejable, siempre que los datos se puedan reensamblar, reconstituir, reformar, descifrar o restablecer 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 que lleva a cabo el analizador sintáctico de datos seguro, en los datos, para almacenar los datos de clave maestra de sesión en una o más tablas independientes de gestión de claves:

1. Acceder a la Clave Maestra de Analizador Sintáctico asociada al usuario autenticado.

2. Generar una Clave Maestra de Sesión exclusiva.

3. Obtener una Clave Intermedia a partir de una función OR exclusiva de la Clave Maestra de Analizador Sintáctico y la Clave Maestra de Sesión.

4. Opcionalmente, cifrar los datos usando un algoritmo de cifrado nuevo o existente puesto en clave con la Clave Intermedia.

5. Separar los datos opcionalmente cifrados resultantes en cuatro porciones o partes 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 se almacenará en una tabla independiente de gestión de claves de un depósito de datos. Generar una ID de transacción exclusiva para esta transacción. Almacenar la ID de transacción y la clave maestra de sesión en una tabla independiente de gestión de claves o pasar la Clave Maestra de Sesión y la ID de transacción nuevamente al programa de llamada 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 opcionalmente cifrados separados o analizados sintácticamente.

7. Las cuatro porciones de datos resultantes contendrán partes opcionalmente cifradas de los datos originales y partes de la ID de transacción.

8. Opcionalmente, generar una clave de cifrado para cada una de las cuatro porciones de datos.

9. Opcionalmente, cifrar cada porción, a continuación, almacenar las claves de cifrado en diferentes ubicaciones de las partes o porciones de datos cifradas: por ejemplo, Porción 1 obtiene Clave 4, Porción 2 obtiene Clave 1, Porción 3 obtiene Clave 2, Porción 4 obtiene Clave 3.

Para restablecer el formato de datos original se invierten las etapas.

Resulta fácilmente evidente para alguien con conocimientos normales de la materia que determinadas etapas de los procedimientos que se describen en este documento se pueden llevar a cabo en un orden diferente o repetir múltiples veces, según se desee. También resulta fácilmente evidente para los expertos en la materia que cada parte de los datos se puede tratar de manera diferente. Por ejemplo, se pueden llevar a cabo múltiples etapas de análisis sintáctico o separación en sólo una parte de los datos analizados sintácticamente. Cada parte de los datos analizados sintácticamente se puede asegurar de manera exclusiva de cualquier forma aconsejable, siempre que los datos se puedan reensamblar, reconstituir, reformar, descifrar o restablecer a su forma original u otra forma utilizable.

Una gran variedad de metodologías de cifrado son adecuadas para uso en los procedimientos de la presente invención, como resulta fácilmente evidente para los expertos en la materia. El algoritmo 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 Libreta de un Solo Uso requiere que se genere una clave tan larga como los datos que se van a asegurar. El uso de este procedimiento puede ser menos aconsejable en determinadas circunstancias, tales como las que tienen como resultado la generación y gestión de claves muy largas debido al tamaño del conjunto de datos que se va a asegurar. En el algoritmo Libreta de un Solo Uso (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 bit a bit de x e y.

A nivel de bits 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

se va a dividir. El proceso generará un valor aleatorio de n-bytes, a, y, a continuación, establece:

b = a XOR s

Cabe señalar que se puede obtener "s" por medio de la ecuación:

s = a XOR b

Los valores a y b se denominan porciones o partes y se colocan en depósitos independientes. Una vez que el secreto s está dividido en dos o más porciones, se descarta de manera segura.

El analizador sintáctico de datos seguro de la presente invención puede utilizar esta función llevando a cabo múltiples funciones XOR que incorporan múltiples valores de clave secreta distintos: K1, K2, K3, Kn, K5. Al principio de la operación, los datos que se van a asegurar se someten a la primera operación de cifrado, datos seguros = datos XOR clave secreta 5:

S = D XOR K5

A fin de almacenar de manera segura los datos cifrados resultantes, por ejemplo, en cuatro porciones, S1, S2, S3, Sn, los datos se analizan sintácticamente y se dividen en "n" segmentos o porciones, de acuerdo con el valor de K5. Esta operación tiene como resultado "n" porciones seudoaleatorias de los datos originales cifrados. Funciones XOR subsiguientes se pueden llevar a cabo en cada porción con los valores de clave secreta restantes, por ejemplo: Segmento de datos seguros 1 = porción 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, se puede no desear que cualquier depósito contenga información suficiente para descifrar la información que tiene, por lo tanto, la clave requerida para descifrar la porción se almacena en un depósito de datos diferente.

Depósito 1: SD1, Kn

Depósito 2: SD2, K1

Depósito 3: SD3, K2

Depósito n: SDn, K3

Adicionalmente, adjunta a cada porción puede estar la información requerida para recuperar la clave original de cifrado de sesión, K5. Por lo tanto, en el ejemplo de gestión de claves que se describe en este documento, la clave maestra de sesión original está referenciada por una ID de transacción dividida en "n" porciones 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 sesión de clave incorporada que se describe en este documento, la clave maestra de sesión se divide en "n" porciones de acuerdo con el contenido de la Clave Maestra de Analizador Sintáctico dependiente de la

instalación (SK1, 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 se recuperen las cuatro porciones, no se pueden reensamblar los datos de acuerdo con este ejemplo. Aunque se consigan las cuatro porciones, no hay posibilidad de reensamblar o restablecer la información original sin acceder a la clave maestra de sesión y a la Clave Maestra de Analizador Sintáctico.

En este ejemplo se ha descrito una realización del procedimiento de la presente invención y, en otra realización, también se describe el algoritmo que se usa para colocar porciones en depósitos, de manera que se puedan combinar porciones de todos los depósitos para formar el material de autenticación secreto. Los cálculos necesarios son muy simples y rápidos. No obstante, con el algoritmo Libreta de un solo Uso (OTP) puede haber circunstancias que hagan que sea menos aconsejable, tales como un conjunto de datos grande que se va a asegurar, porque el tamaño de clave tiene el mismo tamaño que los datos que se van a almacenar. Por lo tanto, sería necesario almacenar y transmitir aproximadamente el doble de la cantidad de datos originales, lo que puede ser menos aconsejable en determinadas circunstancias.

Cifrado de flujo RS1

La técnica de división por cifrado de flujo RS1 es muy similar a la técnica de división por OTP que se describe en este documento. En lugar de un valor aleatorio de n-bytes, se genera un valor aleatorio n' = min(n, 16)-bytes y se usa para poner en clave el algoritmo de Cifrado de Flujo RS1. La ventaja del algoritmo de Cifrado de Flujo RS1 es que se genera una clave seudoaleatoria a partir de un número esencial más pequeño. La velocidad de ejecución del cifrado por Cifrado de Flujo RS1 también se considera, aproximadamente, 10 veces la velocidad del cifrado Triple DES muy conocido en la técnica. El algoritmo de Cifrado de Flujo RS1 es muy conocido en la técnica y se puede usar para generar las claves que se usan en la función XOR. El algoritmo de Cifrado de Flujo RS1 es interoperable con otros algoritmos de cifrado de flujo disponibles en el mercado, tales como el algoritmo de cifrado de 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 son ahora 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 de Flujo RS1 puesto en clave con K1 a Kn. Ahora, las porciones están colocadas en depósitos de datos, como se describe en este documento.

En este algoritmo de cifrado de flujo RS1, los cálculos requeridos necesarios son casi tan simples y rápidos como el algoritmo OTP. La ventaja en este ejemplo que usa el Cifrado de Flujo RS1 es que el sistema necesita almacenar y transmitir una media de, aproximadamente, sólo 16 bytes más que el tamaño de los datos originales que se van a asegurar por porción. Cuando el tamaño de los datos originales es superior a 16 bytes, el algoritmo RS1 es más eficaz que el algoritmo OTP porque simplemente es más corto. Resulta fácilmente evidente para alguien con conocimientos normales de la materia que una gran variedad de algoritmos o procedimientos de cifrado son adecuados para uso en la presente invención, que incluyen, entre otros, RS1, OTP, RC4™, Triple DES y AES.

Los sistemas informáticos y procedimientos de seguridad de datos de la presente invención proporcionan ventajas muy importantes frente a los procedimientos de cifrado tradicionales. Una ventaja es la seguridad que se obtiene al mover porciones de los datos a diferentes ubicaciones en uno o más dispositivos de almacenamiento o depósitos de

datos, que pueden estar en diferentes ubicaciones lógicas, física o geográficas. Cuando las porciones de datos se dividen físicamente y bajo el control, por ejemplo, de personal diferente, se reduce considerablemente la posibilidad de poner en peligro los datos.

Otra ventaja que proporcionan los procedimientos y sistema de la presente invención es la combinación de las etapas del procedimiento de la presente invención para asegurar datos, para proporcionar un proceso exhaustivo de mantenimiento de la seguridad de datos confidenciales. Los datos se cifran con una clave segura y se dividen en una o más porciones y, en una realización, en cuatro porciones, de acuerdo con la clave segura. La clave segura se almacena sin peligro con un indicador de referencia que está asegurado en cuatro porciones de acuerdo con una calve segura. A continuación, las porciones de datos se cifran individualmente y las claves se almacenan sin peligro con diferentes porciones cifradas. Cuando se combina, todo el proceso para asegurar datos, de acuerdo con los procedimientos que se describen en este documento, se convierte en un paquete exhaustivo de seguridad de datos.

Los datos asegurados de acuerdo con los procedimientos de la presente invención se pueden recuperar fácilmente y restablecer, reconstituir, reensamblar, descifrar o devolver de otro modo a su forma original u otra forma adecuada para uso. A fin de restablecer los datos originales, se puede utilizar lo siguiente:

1. Todas las porciones o partes del conjunto de datos

2. Conocimiento y capacidad de reproducir el flujo de procesos del procedimiento que se usa para asegurar los datos.

3. Acceso a la clave maestra de sesión

4. Acceso a la Clave Maestra de Analizador Sintáctico

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

La protección frente a una aplicación deshonesta, que invoca la aplicación de procedimientos para asegurar datos, se puede imponer mediante el uso de la Clave Maestra de Analizador Sintáctico. Esta realización de la presente invención puede requerir un protocolo de intercambio de autenticación mutua entre el analizador sintáctico de datos seguro y la aplicación antes de iniciar cualquier acción.

La seguridad del sistema dicta que no existen procedimientos "encubiertos" para recreación de los datos originales. Para instalaciones en las que puedan surgir problemas de recuperación de datos, el analizador sintáctico de datos seguro se puede mejorar para proporcionar una réplica de las cuatros porciones y depósitos de clave maestra de sesión. Opciones de hardware, tales como RAID (conjunto redundante de discos independientes, que se usa para propagar información por varios discos), y opciones de software, tales como la reiteración, también pueden ayudar a los planes de recuperación de datos.

Gestión de claves

En una realización de la presente invención, el procedimiento para asegurar datos usa tres conjuntos de clave para una operación de cifrado. Cada conjunto de claves puede tener opciones individuales de almacenamiento, recuperación, seguridad y restablecimiento de claves, en función de la instalación. Las claves que se pueden usar incluyen, entre otras:

La Clave Maestra de Analizador Sintáctico

Esta clave es una clave individual asociada a la instalación del analizador sintáctico de datos seguro. Está instalada en el servidor en el que se ha desplegado el analizador sintáctico de datos seguro. Hay una variedad de opciones adecuadas para asegurar esta clave, que incluyen, entre otras, una tarjeta inteligente, almacén independiente de claves de hardware, almacenes de claves estándar, almacenes de claves de cliente o, por ejemplo, dentro de una tabla de base de datos asegurada.

La Clave Maestra de Sesión

Se puede generar una Clave Maestra de Sesión cada vez que se aseguran datos. La Clave Maestra de Sesión se usa para cifrar los datos antes de las operaciones de análisis sintáctico y división. También se puede incorporar (si la Clave Maestra de Sesión no está integrada en los datos analizados sintácticamente) como medio de análisis sintáctico de los datos cifrados. La Clave Maestra de Sesión se puede asegurar de varias maneras que incluyen, entre otras, un almacén de claves estándar, almacén de claves de cliente, tabla independiente de base de datos o, por ejemplo, asegurada dentro de las porciones cifradas.

Las Claves de Cifrado de Porciones

Para cada porción o parte de un conjunto de datos que se crea, se puede generar una Clave de Cifrado de Porciones para cifrar aun más las porciones. Las Claves de Cifrado de Porciones se pueden almacenar en porciones diferentes a la porción que se cifró.

Resulta fácilmente evidente para alguien con conocimientos normales de la materia que los sistemas informáticos y procedimientos para asegurar datos de la presente invención son comúnmente aplicables a cualquier tipo de datos de cualquier marco o entorno. Además de aplicaciones comerciales realizadas en internet o entre clientes y vendedores, los sistemas informáticos y procedimientos para asegurar datos de la presente invención son muy aplicables en marcos o entornos privados o no comerciales. Cualquier conjunto de datos que se desee proteger de usuarios no autorizados se puede asegurar usando los sistemas y procedimientos que se describen en este documento. Por ejemplo, el acceso a una base de datos específica de una empresa u organización se puede restringir, de manera ventajosa, sólo a usuarios seleccionados empleando los sistemas y procedimientos de la presente invención para asegurar datos. Otro ejemplo es la generación o modificación de documentos, o acceso a los mismos, donde se desea restringir el acceso o evitar la divulgación o el acceso no autorizado o fortuito fuera de un grupo de individuos, ordenadores o estaciones de trabajo seleccionados. Estos y otros ejemplos de las formas en que los sistemas y procedimientos para asegurar datos de la presente invención son aplicables a cualquier marco o entorno comercial o no comercial de cualquier marco, incluyen, entre otros, cualquier organización, organismo gubernamental o corporación.

En otra realización de la presente invención, el procedimiento para asegurar datos usa tres conjuntos de claves para una operación de cifrado. Cada conjunto de claves puede tener opciones individuales de almacenamiento, recuperación, seguridad y restablecimiento de claves, en función de la instalación. Las claves que se pueden usar, incluyen, entre otras:

La Clave Maestra de Analizador Sintáctico

Esta clave es una clave individual asociada a la instalación del analizador sintáctico de datos seguro. Está instalada en el servidor en el que se ha desplegado el analizador sintáctico de datos seguro. Hay una variedad de opciones adecuadas para asegurar esta clave, que incluyen, entre otras, una tarjeta inteligente, almacén independiente de claves de hardware, almacenes de claves estándar, almacenes de claves de cliente o, por ejemplo, dentro de una tabla de base de datos asegurada.

La Clave Maestra de Sesión

Se puede generar una Clave Maestra de Sesión cada vez que se aseguran datos. La Clave Maestra de Sesión se usa conjuntamente con la Clave Maestra de Analizador Sintáctico para obtener la Clave Intermedia. La Clave Maestra de Sesión se puede asegurar de varias maneras que incluyen, entre otras, un almacén de claves estándar, almacén de claves de cliente, tabla independiente de base de datos o, por ejemplo, asegurada dentro de las porciones cifradas.

La Clave Intermedia

Se puede generar una Clave Intermedia cada vez que se aseguran datos. La Clave Intermedia se usa para cifrar los datos antes de las operaciones de análisis sintáctico y división. También se puede incorporar como medio de análisis sintáctico de los datos cifrados.

Las Claves de Cifrado de Porciones

Para cada porción o parte de un conjunto de datos que se crea, se puede generar una Clave de Cifrado de Porciones para cifrar aun más las porciones. Las Claves de Cifrado de Porciones se pueden almacenar en porciones

diferentes a la porción que se cifró.

Resulta fácilmente evidente para alguien con conocimientos normales de la materia que los sistemas informáticos y procedimientos para asegurar datos de la presente invención son comúnmente aplicables a cualquier tipo de datos de cualquier marco o entorno. Además de aplicaciones comerciales realizadas en internet o entre clientes y vendedores, los sistemas informáticos y procedimientos para asegurar datos de la presente invención son muy aplicables en marcos o entornos privados o no comerciales. Cualquier conjunto de datos que se desee proteger de usuarios no autorizados se puede asegurar usando los sistemas y procedimientos que se describen en este documento. Por ejemplo, el acceso a una base de datos específica de una empresa u organización se puede restringir, de manera ventajosa, a sólo usuarios seleccionados empleando los sistemas y procedimientos de la presente invención para asegurar datos. Otro ejemplo es la generación o modificación de documentos, o acceso a los mismos, donde se desea restringir el acceso o evitar la divulgación o el acceso no autorizado o fortuito fuera de un grupo de individuos, ordenadores o estaciones de trabajo seleccionados. Estos y otros ejemplos de las formas en que los sistemas y procedimientos para asegurar datos de la presente invención son aplicables a cualquier marco o entorno comercial o no comercial de cualquier marco, incluyen, entre otros, cualquier organización, organismo gubernamental o corporación.

Seguridad de Datos de Grupos de Trabajo, Proyectos, Portátiles/PCs Individuales o Plataformas Cruzadas

Los sistemas informáticos y procedimientos para asegurar datos de la presente invención también son útiles al asegurar datos por grupo de trabajo, proyecto, portátil/PC individual y cualquier otra plataforma que esté en uso, por ejemplo, en empresas, oficinas, organismos gubernamentales o cualquier marco en el que se creen, manejen o almacenen datos confidenciales. La presente invención proporciona sistemas informáticos y procedimientos para asegurar datos que se conoce que buscan las organizaciones, tales como el Gobierno de los EEUU, para implementación en toda la organización gubernamental o entre gobiernos a nivel estatal o federal.

Los sistemas informáticos y procedimientos para asegurar datos de la presente invención proporcionan la capacidad de no sólo analizar sintácticamente y dividir archivos planos, sino también tablas, conjuntos y/o campos de datos de cualquier tipo. Adicionalmente, con este proceso se pueden asegurar todas las formas de datos, que incluyen, entre otras, texto, video, imágenes, datos biométricos y datos de voz. La escalabilidad, la velocidad y el rendimiento de los datos de los procedimientos para asegurar datos de la presente invención sólo se limitan al hardware de que disponga el usuario.

En una realización de la presente invención, los procedimientos para asegurar 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 para asegurar 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 comparta datos seguros. El procedimiento de la presente invención tiene la capacidad de asegurar datos para una empresa, grupo de trabajo o usuario individual, dependiendo de cómo se desplegó la Clave Maestra de Analizador Sintáctico.

En una realización, se pueden proporcionar programas adicionales de gestión de grupo/usuario y gestión de claves, que permiten la implementación de grupos de trabajo a gran escala con un único punto de administración y gestión de claves. El único programa de mantenimiento se encarga de la generación, gestión y revocación de claves, que son especialmente importantes a medida que aumenta el número de usuarios. En otra realización, la gestión de claves también se puede organizar en uno o más administradores de sistemas diferentes, que pueden no permitir a alguna persona o grupo controlar los datos según los necesiten. Esto permite que la gestión de datos asegurados se obtenga por funciones, responsabilidades, pertenencia, derechos, etc., de acuerdo con lo definido por una organización, y el acceso a datos asegurados se puede limitar simplemente a quien tiene permiso para tener acceso o requieren tener acceso sólo a la parte con la que está trabajando, mientras que otros, tales como directores o altos cargos, pueden tener acceso a todos los datos asegurados. Esta realización permite compartir datos asegurados entre diferentes grupos de una empresa u organización, mientras que a la vez sólo permite a determinados individuos seleccionados, tales como los que tienen funciones y responsabilidades autorizadas y predeterminadas, observar los datos en su totalidad. Además, esta realización de los sistemas y procedimientos de la presente invención también permite compartir datos entre, por ejemplo, empresas independientes o divisiones o departamentos independientes de empresas o departamentos, grupos, organismos u oficinas de organizaciones independientes o similares de cualquier organización o gobierno o de cualquier tipo, en las que se requiere compartir algo, pero ninguna parte puede tener permiso para acceder a todos los datos. Ejemplos especialmente evidentes de

la necesidad y utilidad de un sistema y procedimiento de la presente invención de este tipo son permitir compartir, pero mantener la seguridad, por ejemplo, entre áreas, organismos u oficinas gubernamentales y entre diferentes divisiones, departamos u oficinas de una empresa grande o cualquier otra organización.

Un ejemplo de la aplicabilidad de los procedimientos de la presente invención a menor escala es como sigue. Se usa una Clave Maestra de Analizador Sintáctico como serialización o marca del analizador sintáctico de datos seguro para una organización. A medida que se reduce la escala de uso de la Clave Maestra de Analizador Sintáctico, de toda la empresa a un grupo de trabajo más pequeño, los procedimientos para asegurar datos que se describen en este documento se usan para compartir archivos en grupos de usuarios.

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

Al configurar el analizador sintáctico de datos seguro para uso en este ejemplo, el administrador de sistemas accede a la información del usuario y del grupo desde el sistema operativo por medio de un programa de mantenimiento. Este programa de mantenimiento genera y asigna a los usuarios Claves Maestras de Grupo de Analizador Sintáctico en función de su pertenencia a los grupos.

En este ejemplo, hay tres miembros en el grupo de Personal con Cargo de Responsabilidad. Par este grupo, las acciones serían:

1. Acceder a Clave Maestra de Grupo de Analizador Sintáctico para el grupo de Personal con Cargo de Responsabilidad (generar una clave si no está disponible);

2. Generar un certificado digital que asocie Presidente al grupo de Personal con Cargo de Responsabilidad;

3. Generar un certificado digital que asocie Director Financiero al grupo de Personal con Cargo de Responsabilidad

4. Generar un certificado digital que asocie Vicepresidente, Marketing al grupo de Personal con Cargo de Responsabilidad.

El mismo conjunto de acciones se podrían realizar para cada grupo y cada miembro de cada grupo. Cuando concluye el programa de mantenimiento, la Clave Maestra de Grupo de Analizador Sintáctico es una credencial compartida por cada miembro del grupo. La revocación del certificado digital asignado se puede realizar automáticamente cuando el programa de mantenimiento extrae a un usuario de un grupo, sin que afecte al resto de miembros del grupo.

Una vez que se han definido las credenciales compartidas, el proceso de división y análisis sintáctico sigue siendo el mismo. Cuando se va a asegurar un archivo, documento o elemento de datos, se induce al usuario a usar el grupo de referencia cuando asegure los datos. Sólo otros miembros del grupo de referencia pueden acceder a los datos asegurados resultantes. Esta funcionalidad de los sistemas y procedimientos de la presente invención se puede usar con cualquier otra plataforma de software o sistema informático, por ejemplo, puede ser cualquiera integrado en programas de aplicaciones existentes o que se use de manera autónoma para seguridad de archivos.

Resulta evidente para alguien con conocimientos normales de la materia que cualquier algoritmo de cifrado o combinación de los mismos son adecuados para uso en los sistemas y procedimientos de la presente invención. Por ejemplo, en una realización, las etapas de cifrado se pueden repetir para producir un esquema de cifrado de múltiples capas. Además, se puede usar un algoritmo de cifrado diferente, o combinación de algoritmos de cifrado, para repetir etapas de cifrado de manera que se apliquen algoritmos de cifrado diferentes a las diferentes capas del esquema de cifrado de múltiples capas. Como tal, el propio esquema de cifrado puede ser un componente de los procedimientos de la presente invención para asegurar datos sensibles frente al acceso o uso no autorizado.

El analizador sintáctico de datos seguro puede incluir, como componente interno, como componente externo o como ambos, un componente de comprobación de errores. Por ejemplo, en una solución adecuada, a medida que se crean partes de datos usando el analizador sintáctico de datos seguro, de acuerdo con la presente invención, para asegurar la integridad de los datos dentro de una parte, se toma un valor resumen a intervalos preestablecidos dentro de la parte y se adjunta al final del intervalo. El valor resumen es una representación numérica previsible y

reproducible de los datos. Si dentro de los datos cambiara algún bit, el valor resumen sería diferente. Un módulo de escaneo (como componente autónomo externo al analizador sintáctico de datos seguro o como componente interno) puede escanear las partes de datos generadas por el analizador sintáctico de datos seguros. Cada parte de datos (o alternativamente, menos que el total de partes de datos de acuerdo con algún intervalo o por un muestreo aleatorio o seudoaleatorio) se compara con el valor o valores resumen adjuntos y se puede iniciar una acción. Dicha acción puede incluir un informe de valores que coinciden y no coinciden, una alerta para valores que no coinciden o invocación de algún programa externo o interno para provocar una recuperación de los datos. Por ejemplo, la recuperación de los datos se podría llevar a cabo invocando un módulo de recuperación en función del concepto de que se pueden necesitar menos que el total de partes para generar datos originales de acuerdo con la presente invención.

Se puede implementar cualquier otra comprobación de integridad adecuada usando cualquier información de integridad adjunta a cualquier sitio de todas las partes de datos o a un subconjunto de las mismas. La información de integridad puede incluir cualquier información adecuada que se pueda usar para determinar la integridad de partes de datos. Ejemplos de información de integridad pueden incluir valores resumen calculados en función de cualquier parámetro adecuado (por ejemplo, en función de respectivas partes de datos), información de firma digital, información de código de autenticación de mensaje (MAC), cualquier otra información adecuada o cualquier combinación de las mismas.

El analizador sintáctico de datos seguro de la presente invención se puede usar en cualquier aplicación adecuada. Concretamente, el analizador sintáctico de datos seguro que se describe en este documento tiene una variedad de aplicaciones en diferentes áreas de la informática y la tecnología. Varias de dichas áreas se analizan más adelante. Se entenderá que las mismas son sólo de carácter ilustrativo y que otra aplicación adecuada puede hacer uso del analizador sintáctico de datos seguro. Se entenderá además que los ejemplos que se describen son sólo realizaciones ilustrativas que se pueden modificar de cualquier forma adecuada a fin de satisfacer cualquier deseo adecuado. Por ejemplo, el análisis sintáctico y la división se pueden basar 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 seguro de la presente invención se puede usar para implementar testigos físicos seguros, con lo que se pueden requerir datos almacenados en un testigo físico para acceder a datos adicionales almacenados en otra área de almacenamiento. En una solución adecuada, un testigo físico, tal como una memoria USB compacta, un disquete, un disco óptico, una tarjeta inteligente o cualquier otro testigo físico adecuado, se puede usar para almacenar una de al menos dos partes de datos analizados sintácticamente de acuerdo con la presente invención. A fin de acceder a los datos originales, sería necesario acceder a la memoria USB. Por consiguiente, un ordenador personal que tiene una parte de datos analizados sintácticamente necesitaría tener acoplada la memoria USB, que tiene la otra parte de datos analizados sintácticamente, antes de que se pueda acceder a los datos originales. La figura 26 ilustra esta aplicación. El área de almacenamiento (2500) incluye una parte de datos analizados sintácticamente (2502). A fin de acceder a los datos originales, sería necesario acoplar el testigo físico (2504), que tiene una parte de datos analizados sintácticamente (2506), al área de almacenamiento (2500) usando cualquier interfaz de comunicaciones adecuada (2508) (por ejemplo, USB, en serie, paralela, Bluetooth, IR, IEEE 1394, Ethernet o cualquier otra interfaz de comunicaciones adecuada). Esto es útil, por ejemplo, en una situación en la que datos confidenciales contenidos en un ordenador se dejan desatendidos y sujetos a intentos de acceso no autorizado. Extrayendo el testigo físico (por ejemplo, la memoria USB), los datos confidenciales son inaccesibles. Se entenderá que se puede usar cualquier otra solución adecuada para usar testigos físicos.

El analizador sintáctico de datos seguro de la presente invención se puede usar para implementar un sistema de autenticación seguro con el que los datos de registro del usuario (por ejemplo, contraseñas, claves privadas de cifrado, plantillas de huellas dactilares, datos biométricos u otros datos de registro del usuario adecuados) se dividen y analizan sintácticamente usando el analizador sintáctico de datos seguro. Los datos de registro del usuario se pueden dividir y analizar sintácticamente, con lo que una o más partes se almacenan en una tarjeta inteligente, una Tarjeta de Acceso Común del gobierno, cualquier dispositivo físico de almacenamiento adecuado (por ejemplo, disco magnético u óptico, memoria USB, etc.) o cualquier otro dispositivo adecuado. Una o más de otras partes de los datos de registro del usuario analizados sintácticamente se pueden almacenar en el sistema que lleva a cabo la autenticación. Esto proporciona un nivel añadido de seguridad al proceso de autenticación (por ejemplo, además de la información de autenticación biométrica obtenida de la fuente biométrica, los datos de registro del usuario también se deben obtener a través de la parte apropiada de datos divididos y analizados sintácticamente).

El analizador sintáctico de datos seguro de la presente invención puede estar integrado en cualquier sistema existente adecuado a fin de proporcionar el uso de su funcionalidad a cada entorno respectivo del sistema. La figura 27 muestra un diagrama de bloques de un sistema (2600) ilustrativo, que puede incluir, software, hardware o ambos para implementar cualquier aplicación adecuada. El sistema (2600) puede ser un sistema existente al que se puede retroadaptar un analizador sintáctico de datos seguro (2602) como componente integrado. Alternativamente, el analizador sintáctico de datos seguro (2602) puede estar integrado en cualquier sistema (2600) adecuado desde, por ejemplo, su primera fase de diseño. El analizador sintáctico de datos seguro (2602) puede estar integrado a cualquier nivel adecuado del sistema (2600). Por ejemplo, el analizador sintáctico de datos seguro (2602) puede estar integrado en el sistema (2600) a un nivel lo suficientemente especializado, de manera que la presencia del analizador sintáctico de datos seguro (2602) pueda ser sustancialmente obvia para un usuario final del sistema (2600). El analizador sintáctico de datos seguro (2602) se puede usar para dividir y analizar sintácticamente 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 integrado en los mismos el analizador sintáctico de datos seguro.

El analizador sintáctico de datos seguro de la presente invención puede estar integrado en un núcleo de sistema operativo (por ejemplo, Linux, Unix o cualquier otro sistema operativo adecuado comercial o patentado). Esta integración se puede usar para proteger datos a nivel dispositivo, con lo que, por ejemplo, el analizador sintáctico de datos seguro integrado en el sistema operativo separa los datos en un número determinado de partes que, por lo general, se almacenarían en uno o más dispositivos y se almacenan entre el uno o más dispositivos. Cuando se intenta acceder a los datos originales, el software adecuado, también integrado en el sistema operativo, puede volver a combinar las partes de datos analizados sintácticamente en los datos originales de forma que pueda ser obvia para el usuario final.

El analizador sintáctico de datos seguro de la presente invención puede estar integrado en un gestor de volumen o en cualquier otro componente adecuado de un sistema de almacenamiento para proteger el almacenamiento de datos local y en red a través de cualquier plataforma soportada o en todas. Por ejemplo, con el analizador sintáctico de datos seguro integrado, un sistema de almacenamiento puede hacer uso de la redundancia que ofrece el analizador sintáctico de datos seguro (es decir, que se usa para implementar la característica de necesitar menos que el total de partes de datos separadas para reconstruir los datos originales) para proteger frente a la pérdida de datos. El analizador sintáctico de datos seguro también permite que todos los datos escritos en dispositivos de almacenamiento, usando o no redundancia, estén en forma de múltiples partes que se generan de acuerdo con el análisis sintáctico de la presente invención. Cuando se intenta acceder a los datos originales, el software apropiado, también integrado en el gestor de volumen u otro componente adecuado del sistema de almacenamiento, puede volver a combinar las partes de datos analizados sintácticamente en los datos originales de forma que pueda ser obvia para el usuario final.

En una solución adecuada, el analizador sintáctico de datos seguro de la presente invención puede estar integrado en un controlador de RAID (como hardware o software). Esto permite el almacenamiento seguro de datos en múltiples unidades de disco mientras mantiene la tolerancia a fallos en caso de avería de la unidad de disco.

El analizador sintáctico de datos seguro de la presente invención puede estar integrado en una base de datos a fin de, por ejemplo, proteger información confidencial de tablas. Por ejemplo, en una solución adecuada, datos asociados a celdas específicas de una tabla de base de datos (por ejemplo, celdas individuales, una o más columnas específicas, una o más filas específicas, cualquier combinación de las mismas o una tabla de base de datos entera) se puede analizar sintácticamente y separar de acuerdo con la presente invención (por ejemplo, si las diferentes partes están almacenadas en uno o más dispositivos de almacenamiento en una o más ubicaciones o en un único dispositivo de almacenamiento). Se puede conceder acceso para volver a combinar las partes a fin de ver los datos originales mediante procedimientos de autenticación tradicionales (por ejemplo, pedir nombre de usuario y contraseña).

El analizador sintáctico seguro de la presente invención puede estar integrado en cualquier sistema adecuado que conlleve datos en movimiento (es decir, transferencia de datos de una ubicación a otra). Dichos sistemas incluyen, por ejemplo, correo electrónico, difusiones de datos en continuo y comunicaciones inalámbricas (por ejemplo, WiFi). Respecto al correo electrónico, en una solución adecuada, el analizador sintáctico seguro se puede usar para analizar sintácticamente 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 partes de los datos analizados sintácticamente a lo largo de diferentes vías creando así múltiples flujos de datos. Si se pone en peligro alguno de estos flujos de datos, el mensaje original sigue seguro porque el sistema puede requerir que se combine más de una

de las partes, de acuerdo con la presente invención, a fin de generar los datos originales. En otra solución adecuada, las diferentes partes de datos se pueden comunicar secuencialmente a lo largo de una vía, de manera que si se obtiene una parte, puede no ser suficiente para generar los datos originales. Las diferentes partes llegan a la ubicación del destinatario deseado y se pueden combinar para generar los datos originales de acuerdo con la presente invención.

Las figuras 28 y 29 son diagramas de bloque ilustrativos de dichos sistemas de correo electrónico. La figura 28 muestra un sistema remitente (2700), que puede incluir cualquier hardware adecuado, tal como un terminal informático, ordenador personal, dispositivo portátil (por ejemplo, PDA, Blackberry), teléfono móvil, red informática, 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, video, etc.) o ambos. El analizador sintáctico de datos seguro (2702) analiza sintácticamente y divide el mensaje (2704) de acuerdo con la presente invención. Las partes de datos resultantes se pueden comunicar a través de una o más vías de comunicaciones independientes (2706) por red (2708) (por ejemplo, internet, una intranet, una LAN, WiFi, Bluetooth, cualquier otro medio de comunicaciones inalámbricas o por cable adecuado o cualquier combinación de los mismos) al sistema destinatario (2710). Las partes de datos se pueden comunicar paralelas en el tiempo o alternativamente, de acuerdo con cualquier retardo adecuado entre la comunicación de las diferentes partes de datos. El sistema destinatario (2710) puede ser cualquier hardware adecuado que se ha descrito anteriormente en relación con el sistema remitente (2700). Las partes de datos separadas llevadas a lo largo de vías de comunicaciones (2706) se vuelven a combinar en el sistema destinatario (2710) para generar los datos o mensaje 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 informático, ordenador personal, dispositivo portátil (por ejemplo, PDA), teléfono móvil, red informática, 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, video, etc.) o ambos. El analizador sintáctico de datos seguro (2802) analiza sintácticamente y divide el mensaje (2804) de acuerdo con la presente invención. Las partes de datos resultantes se pueden comunicar a través de una única vía de comunicaciones (2806) por 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 destinatario (2810). Las partes de datos se pueden comunicar en serie, entre sí, a través de una vía de comunicaciones (2806). El sistema destinatario (2810) puede ser cualquier hardware adecuado que se ha descrito anteriormente en relación con el sistema remitente (2800). Las partes de datos separadas llevadas a lo largo de la vía de comunicaciones (2806) se vuelven a combinar en el sistema destinatario (2810) para generar los datos o mensaje originales de acuerdo con la presente invención.

Se entenderá que la disposición de las Figuras 28 y 29 es sólo ilustrativa. Se puede usar cualquier otra disposición adecuada. Por ejemplo, en otra solución adecuada, las características de los sistemas de las figuras 28 y 29 se pueden combinar, con lo que se usa la solución de vías múltiples de la figura 29, y en la que se usa una o más vías de comunicaciones (2706) para llevar más de una parte de datos, al igual que lo hace la vía de comunicaciones (2806) en el contexto de la figura 29.

El analizador sintáctico de datos seguro puede estar integrado a cualquier nivel adecuado de un sistema de datos en movimiento. Por ejemplo, en el contexto de un sistema de correo electrónico, el analizador sintáctico seguro puede estar integrado a nivel de interfaz de usuario (por ejemplo, en Microsoft® Outlook), en cuyo caso el usuario puede tener el control sobre el uso de las características del analizador sintáctico de datos seguro al usar el correo electrónico. Alternativamente, el analizador sintáctico seguro se puede implementar en un componente especializado, tal como en el servidor de intercambio, en cuyo caso, los mensajes se pueden analizar sintácticamente, dividir y comunicar automáticamente a lo largo de diferentes vías, de acuerdo con la presente invención, sin intervención del usuario.

Asimismo, en el caso de difusiones de datos en continuo (por ejemplo, audio, video), los datos salientes se pueden analizar sintácticamente y separar en múltiples flujos conteniendo cada uno una parte de los datos analizados sintácticamente. Los múltiples flujos se pueden transmitir a lo largo de una o más vías y volver a combinar en la ubicación del destinatario, de acuerdo con la presente invención. Uno de los beneficios de esta solución es que evita la sobrecarga relativamente grande asociada al cifrado tradicional de datos tras la transmisión de los datos cifrados a través de un único canal de comunicaciones. El analizador sintáctico seguro de la presente invención permite enviar datos en movimiento en múltiples flujos paralelos, aumentando la velocidad y la eficacia.

Se entenderá que el analizador sintáctico de datos seguro puede estar integrado para protección y tolerancia a fallos de cualquier tipo de datos en movimiento a través de cualquier soporte de transporte, que incluye, por ejemplo, por cable, inalámbrico o físico. Por ejemplo, las aplicaciones de voz sobre protocolo de internet (VoIP) pueden hacer uso del analizador sintáctico de datos seguro de la presente invención. El transporte inalámbrico o por cable de datos desde o hacia cualquier dispositivo asistente personal digital (PDA), tales como Blackberrys y teléfonos inteligentes, se puede asegurar usando el analizador sintáctico de datos seguro de la presente invención. Comunicaciones que usan protocolos inalámbricos 802.11 para redes paritarias e inalámbricas centralizadas, comunicaciones por satélite, comunicaciones inalámbricas punto a punto, comunicaciones cliente/servidor por internet o cualquier otra comunicación adecuada, pueden conllevar las capacidades de los datos en movimiento del analizador sintáctico de datos seguro de acuerdo con la presente invención. La comunicación de datos entre un dispositivo periférico de ordenador (por ejemplo, impresora, escáner, monitor, teclado, enrutador de red, dispositivo de autenticación biométrica (por ejemplo, escáner de huellas dactilares) o cualquier otro dispositivo periférico), entre un ordenador y un dispositivo periférico de ordenador, entre un dispositivo periférico de ordenador y cualquier otro dispositivo o cualquier combinación de los mismos, puede hacer uso de las características de datos en movimiento de la presente invención.

Las características de datos en movimiento de la presente invención también se pueden aplicar a transporte físico de porciones seguras usando, por ejemplo, procedimientos, medios, rutas independientes, cualquier otro transporte físico adecuado o cualquier combinación de los mismos. Por ejemplo, el transporte físico de datos puede tener lugar en cintas magnéticas/digitales, disquetes, discos ópticos, testigos físicos, unidades de disco USB, unidades de disco duro extraíbles, dispositivos electrónicos con memoria flash (por ejemplo, IPODs Apple u otros reproductores de MP3), memoria flash, cualquier otro soporte adecuado que se use para transportar datos o cualquier combinación de los mismos.

El analizador sintáctico de datos seguro de la presente invención puede proporcionar seguridad con la capacidad de recuperación ante desastres. De acuerdo con la presente invención, a fin de recuperar los datos originales, pueden ser necesarias menos que el total de partes de los datos separados generados por el analizador sintáctico de datos seguro. Es decir, de m partes almacenadas, n puede ser el número mínimo de esas m partes necesarias para recuperar los datos originales, donde n <= m. Por ejemplo, si cada una de las partes se almacena en una ubicación física diferente respecto a las otras tres partes, entonces, si en este ejemplo n = 2, se pueden poner en peligro dos de las ubicaciones, con lo que los datos se destruyen o son inaccesibles y los datos originales se pueden seguir recuperando de las parte de las otras dos ubicaciones. Para n o m se puede usar cualquier valor adecuado.

Además, la característica de n de m de la presente invención se puede usar para crear una "regla de dos hombres" según la cual, a fin de evitar confiar el acceso total a lo que pueden ser datos confidenciales a un único individuo o cualquier otra entidad, puede ser necesario que dos o más entidades distintas, cada una con una parte de los datos separados analizados sintácticamente por el analizador sintáctico seguro de la presente invención, acepten poner sus partes juntas a fin de recuperar los datos originales.

El analizador sintáctico de datos seguro de la presente invención se puede usar para proporcionar un grupo de entidades con una clave para todo el grupo que permita a los miembros del grupo acceder a información específica a la que un grupo específico está autorizado a acceder. La clave de grupo puede ser una de las partes de datos generadas por el analizador sintáctico seguro de acuerdo con la presente invención, que se puede requerir que se combine con otra parte almacenada centralmente, por ejemplo, a fin de recuperar la información buscada. Esta característica permite, por ejemplo, la colaboración segura entre un grupo. Se puede aplicar, por ejemplo, en redes dedicadas, redes privadas virtuales, intranets o cualquier otra red adecuada.

Aplicaciones específicas de este uso del analizador sintáctico seguro incluyen, por ejemplo compartir información de coalición en la que, por ejemplo, se da a fuerzas gubernamentales multinacionales aliadas la capacidad de comunicar datos de funcionamiento y confidenciales de otro tipo, en un nivel de seguridad autorizado a cada país respectivo a través de una única red o una red doble (es decir, en comparación con las muchas redes que conllevan procesos manuales relativamente sustanciales que se usan actualmente). Esta capacidad también es aplicable a empresas u otras organizaciones en las que la información que es necesario que conozca uno o más individuos específicos (dentro de la organización o fuera de la misma) se puede comunicar a través de una única red sin la necesidad de preocuparse de que individuos no autorizados vean la información.

Otra aplicación específica incluye una jerarquía de seguridad de múltiples niveles para sistemas gubernamentales. Es decir, el analizador sintáctico seguro de la presente invención puede proporcionar la capacidad de hacer funcionar un sistema gubernamental a diferentes niveles de información clasificada (por ejemplo, no confidencial,

confidencial, secreta, de extrema reserva) usando una única red. Si se desea, se pueden usar más redes (por ejemplo, una red independiente para información de extrema reserva), sin embargo la presente invención permite sustancialmente menos que la disposición actual en la que se usa una red independiente para cada nivel de clasificación.

Se entenderá que se puede usar cualquier combinación de las aplicaciones que se han descrito anteriormente del analizador sintáctico seguro de la presente invención. Por ejemplo, la aplicación de claves de grupo se puede usar junto con la aplicación de seguridad de datos en movimiento (es decir, con la que sólo un miembro del grupo respectivo puede acceder a datos que se comunican a través de una red y en la que, mientras los datos están en movimiento, se dividen entre múltiples vías (o se envían en partes secuenciales) de acuerdo con la presente invención).

El analizador sintáctico de datos seguro de la presente invención puede estar integrado en una aplicación de soporte intermedio para habilitar aplicaciones para almacenar datos de manera segura en diferentes productos de base de datos o en diferentes dispositivos, sin modificar las aplicaciones ni la base de datos. Soporte intermedio es un término general para cualquier producto que permite que se comuniquen dos programas independientes y ya existentes. Por ejemplo, en una solución adecuada, soporte intermedio que tiene integrado el analizador sintáctico de datos seguro se puede usar para permitir que programas grabados para una base de datos específica se comuniquen con otras bases de datos sin una codificación a medida.

El analizador sintáctico de datos seguro de la presente invención se puede implementar teniendo cualquier combinación de cualquier capacidad adecuada, tales como las que se analizan en este documento. En algunas realizaciones de la presente invención, por ejemplo, el analizador sintáctico de datos seguro se puede implementar teniendo sólo determinadas capacidades, mientras que las otras capacidades se pueden obtener mediante el uso de hardware, software externo o ambos, interconectados directa o indirectamente con el analizador sintáctico de datos seguro.

Por ejemplo, la figura 30 muestra una implementación ilustrativa del analizador sintáctico de datos seguro como analizador sintáctico de datos seguro (3000). El analizador sintáctico de datos seguro (3000) se puede implementar con muy pocas capacidades incorporadas. Como se ilustra, el analizador sintáctico de datos seguro (3000) puede incluir capacidades incorporadas para analizar sintácticamente y dividir datos en partes (también denominadas en este documento porciones) de datos usando el módulo (3002), de acuerdo con la presente invención. El analizador sintáctico de datos seguro (3000) también puede incluir capacidades incorporadas para llevar a cabo redundancia a fin de poder implementar, por ejemplo, la característica de m de n que se ha descrito anteriormente (es decir, recrear los datos originales usando menos que el total de porciones de datos analizados sintácticamente y divididos) usando el módulo (3004). El analizador sintáctico de datos seguro (3000) también puede incluir capacidades de distribución de porciones usando el módulo (3006) para colocar las porciones de datos en memorias intermedias desde las que se envían para comunicación a una ubicación remota, para almacenamiento, etc. de acuerdo con la presente invención. Se entenderá que en el analizador sintáctico de datos seguro (3000) se puede incorporar cualquier otra capacidad adecuada.

La memoria intermedia de datos ensamblados (3008) puede ser cualquier memoria adecuada que se usa para almacenar los datos originales (aunque no necesariamente en su forma original) que analizará sintácticamente y dividirá el analizador sintáctico de datos seguro (3000). En una operación de división, la memoria intermedia de datos ensamblados (3008) proporciona entrada al analizador sintáctico de datos seguro (3008). En una operación de restablecimiento, la memoria intermedia de datos ensamblados (3008) se puede usar para almacenar la salida del analizador sintáctico de datos seguro (3000).

Las memorias intermedias de porciones divididas (3010) pueden ser uno o más módulos de memoria que se pueden usar para almacenar las múltiples porciones de datos que resultan del análisis sintáctico y la división de datos originales. En una operación de división, las memorias intermedias de porciones divididas (3010) tienen la salida del analizador sintáctico de datos seguro. En una operación de restablecimiento, las memorias intermedias de porciones divididas tienen la entrada al analizador sintáctico de datos seguro (3000).

Se entenderá que se puede incorporar cualquier otra disposición adecuada de capacidades para el analizador sintáctico de datos seguro (3000). Se puede incorporar cualquier característica adicional y se puede eliminar cualquiera de las características que se ilustran, hacer más robustas, hacer menos robustas o modificar de otro modo de cualquier forma adecuada. Las memorias intermedias (3008) y (3010) son asimismo sólo ilustrativas y se pueden modificar, eliminar o añadir de cualquier forma adecuada.

El analizador sintáctico de datos seguro (3000) puede llamar a cualquier módulo adecuado implementado en software, hardware o ambos o éstos pueden llamar al primero. Si se desea, incluso capacidades que están incorporadas en el analizador sintáctico de datos seguro (3000) se pueden sustituir por uno o más módulos externos. Como se ilustra, algunos módulos externos incluyen generador de números aleatorios (3012), generador de claves de realimentación de cifrado (3014), algoritmo de resumen (3016) y uno o más tipos de cifrado (3018), y gestión de claves (3020). Se entenderá que estos son módulos externos sólo ilustrativos. Se puede usar cualquier módulo adecuado además de los que se ilustran o en lugar de éstos.

El generador de claves de realimentación de cifrado (3014) puede, externamente al analizador sintáctico de datos seguro (3000), generar para cada operación del analizador sintáctico de datos seguro, una clave exclusiva o número aleatorio (usando por ejemplo, el generador de números aleatorios (3012) para que se use como valor esencial para una operación que amplia un tamaño original de clave de sesión (por ejemplo, un valor de 128, 256, 512 ó 1024 bits) a un valor igual a la longitud de los datos que se van a analizar sintácticamente y dividir. Se puede usar cualquier algoritmo adecuado para la generación de claves de realimentación de cifrado, que incluyen, por ejemplo, el algoritmo de generación de claves de realimentación de cifrado AES.

A fin de facilitar la integración del analizador sintáctico de datos seguro (3000) y sus módulos externos (es decir, capa de analizador sintáctico de datos seguro (3026) en una capa de aplicación (3024) (por ejemplo, aplicación de correo electrónico, aplicación de base de datos, etc.), se puede usar una capa envolvente que puede hacer uso de, por ejemplo, llamadas de funciones API. Se puede usar cualquier otra disposición adecuada para facilitar la integración de la capa de analizador sintáctico de datos seguro (3026) en la capa de aplicación (3024).

La figura 31 muestra, de manera ilustrativa, cómo se puede usar la disposición de la figura 30 cuando en una capa de aplicación (3024) se expide una orden de escritura (por ejemplo, a un dispositivo de almacenamiento), de inserción (por ejemplo, en un campo de base de datos) o de transmisión (por ejemplo, a través de una red). En la etapa (3100), se identifican los datos que se van a asegurar y se hace una llamada al analizador sintáctico de datos seguro. La llamada se pasa a través de la capa de envoltura (3022) cuando, en la etapa (3102), la capa de envoltura (3022) introduce los datos de entrada identificados en la etapa (3100) en la memoria intermedia de datos ensamblados (3008). Asimismo, en la etapa (3102), se puede almacenar cualquier información de porciones adecuada, nombres de archivos, cualquier otra información adecuada o cualquier combinación de los mismos (por ejemplo, como información (3106) en la capa de envoltura (3022). A continuación, el procesador de datos seguro (3000) analiza sintácticamente y divide los datos que toma como entrada de la memoria intermedia de datos ensamblados (3008) de acuerdo con la presente invención. Transmite las porciones de datos a las memorias intermedias de porciones divididas (3010). En la etapa (3104), la capa de envoltura (3022) obtiene de la información almacenada (3106) cualquier información de porciones adecuada (es decir almacenada por envoltura (3022) en la etapa (3102) y ubicaciones de porciones (por ejemplo, de uno o más archivos de configuración). A continuación, la capa de envoltura (3022) escribe las porciones de salida (obtenidas de memorias intermedias de porciones divididas (3010) de manera adecuada (por ejemplo, escritas en uno o más dispositivos de almacenamiento, comunicadas por una red, etc.).

La figura 32 muestra, de manera ilustrativa, cómo se puede usar la disposición de la figura 30 cuando tiene lugar una lectura (por ejemplo, desde un dispositivo de almacenamiento), selección (por ejemplo, de un campo de base de datos) o recepción (por ejemplo, desde una red). En la etapa (3200), se identifican los datos que se van a restablecer y se realiza una llamada al analizador sintáctico de datos seguro (3000) desde la capa de aplicación (3024). En la etapa (3202), desde la capa de envoltura (3022), se obtiene cualquier información de porciones adecuada y se determina la ubicación de porciones. La capa de envoltura (3022) carga las partes de datos identificadas en la etapa (3200) en memorias intermedias de porciones divididas (3010). A continuación, el analizador sintáctico de datos seguro (3000) procesa estas porciones de acuerdo con la presente invención (por ejemplo, si sólo están disponibles tres de cuatro porciones, se pueden usar las capacidades de redundancia del analizador sintáctico de datos seguro (3000) para restablecer los datos originales usando sólo las tres porciones). A continuación, los datos restablecidos se almacenan en la memoria 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 a la capa de aplicación (3024) los datos originales en su formato original.

Se entenderá que el análisis sintáctico y la división de datos originales que se ilustran en la figura 31 y el restablecimiento de partes de datos a datos originales que se ilustra en la figura 32 son sólo ilustrativos. Se puede usar cualquier otro componente, proceso adecuado o ambos además de los que se ilustran o en lugar de éstos.

La figura 33 es un diagrama de bloques de un flujo de procesos ilustrativo para analizar sintácticamente y dividir datos originales en dos o más partes de datos, de acuerdo con una realización de la presente invención. Como se ilustra, los datos originales que se desea analizar sintácticamente y dividir son texto sin formato (3306) (es decir, se usa como ejemplo la palabra "SUMMIT"). Se entenderá que se puede analizar sintácticamente y dividir cualquier otro tipo de datos 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), se puede generar una clave de sesión de realimentación de cifrado (3304).

En una solución adecuada, los datos originales (3306) se pueden cifrar antes de analizarlos sintácticamente, dividirlos o ambos. Por ejemplo, como ilustra la figura 33, se puede llevar a cabo la función XOR en los datos originales (3306) con cualquier valor adecuado (por ejemplo, con clave de sesión de realimentación de cifrado (3304) o con cualquier otro valora adecuado. Se entenderá que se puede usar cualquier otra técnica de cifrado adecuada en lugar de la técnica XOR que se ilustra o además de ésta. Se entenderá además que aunque la figura 33 se ilustra en cuanto a operaciones de byte a byte, la operación puede tener lugar a nivel de bit o a cualquier otro nivel adecuado. Se entenderá también que, si se desea, no es necesario cifrado alguno de los datos originales (3306).

Los datos cifrados resultantes (o datos originales si no tuvo lugar el cifrado) se resumen para determinar cómo dividir los datos cifrados (u originales) entre los compartimentos de salida (por ejemplo, de los que en el ejemplo que se ilustra hay cuatro). En el ejemplo que se ilustra, el resumen tiene lugar por bytes y es una función de la clave de sesión de realimentación de cifrado (3304). Se entenderá que esto es sólo ilustrativo. El resumen se puede llevar a cabo a nivel de bit, si se desea. El resumen puede ser una función de cualquier otro valor adecuado además de la clave de sesión de realimentación de cifrado (3304). En otra solución adecuada, no es necesario usar resúmenes. Por el contrario, se puede emplear cualquier otra técnica adecuada para dividir datos.

La figura 34 es un diagrama de bloques de un flujo de procesos ilustrativo para restablecer datos originales (3306) a partir de dos o más partes analizadas sintácticamente y divididas de datos originales (3306) de acuerdo con una realización de la presente invención. El proceso conlleva resumir las partes a la inversa (es decir, al proceso de la figura 33) como función de la clave de sesión de realimentación de cifrado (3304) para restablecer los datos originales cifrados (o datos originales si no se cifraron antes del análisis sintáctico y la división). A continuación, la clave de cifrado se puede usar para restablecer los datos originales (es decir, en el ejemplo que se ilustra, la clave de sesión de realimentación de cifrado (3304) se usa para descifrar el cifrado XOR llevando a cabo la función XOR con los datos cifrados). Esto restablece los datos originales (3306).

La figura 35 muestra cómo se puede implementar la división a nivel de bit en el ejemplo de las figuras 33 y 34. Se puede usar un resumen (por ejemplo, como función de la clave de sesión de realimentación de cifrado, como función de cualquier otro valor adecuado) para determinar un valor de bit al que dividir cada byte de datos. Se entenderá que esta es sólo una forma ilustrativa en la que implementar la división a nivel de bit. Se puede usar cualquier otra técnica adecuada.

Se entenderá que cualquier referencia que se haga en este documento a la funcionalidad de resumen se puede hacer respecto a cualquier algoritmo de resumen adecuado. Los mismos incluyen, por ejemplo, MD5 y SHA-1. Diferentes componentes de la presente invención pueden usar diferentes algoritmos de resumen y se pueden usar en diferentes momentos.

Tras haber determinado un punto de división, de acuerdo con el procedimiento ilustrativo anterior o mediante cualquier otro procedimiento o algoritmo, se puede tomar una determinación respecto a qué partes de datos adjuntar a cada uno de los segmentos izquierdo y derecho. Se puede usar cualquier algoritmo adecuado para tomar dicha determinación. Por ejemplo, en una solución adecuada, se puede crear una tabla de todas las posibles distribuciones (por ejemplo, en forma de parejas de destinos para el segmento izquierdo y para el segmento derecho), con lo que se puede determinar un valor de porción de destino para cada uno de los segmentos izquierdo y derecho usando cualquier función resumen adecuada en datos correspondientes de la clave de sesión, clave de sesión de realimentación de cifrado o cualquier otro valor aleatorio o seudoaleatorio adecuado, que se pueda generar y ampliar al tamaño de los datos originales. Por ejemplo, se puede realizar una función resumen de un byte correspondiente del valor aleatorio o seudoaleatorio. La salida de la función resumen se usa para determinar qué parejas 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. En función de este resultado, cada segmento de la unidad de datos dividida se adjunta a las dos porciones respectivas indicadas por medio del valor de tabla seleccionado como

resultado de la función resumen.

Se puede adjuntar información de redundancia a las partes de datos, de acuerdo con la presente invención, para permitir el restablecimiento de los datos originales usando menos que el total de las partes de datos. Por ejemplo, si se desea que dos de las cuatro partes sean suficientes para restablecer los datos, en consecuencia, se pueden adjuntar datos adicionales de las porciones a cada porción, por ejemplo, de manera circular (round-robin) (por ejemplo, cuando el tamaño de los datos originales es 4MB, la porción 1 obtiene sus propias porciones además de las de las porciones 2 y 3; la porción 2 obtiene su propia porción además de las de las porciones 3 y 4; la porción 3 obtiene su propia porción además de las de las porciones 4 y 1 y la porción 4 obtiene su propia porción además de las porciones 1 y 2). Cualquier redundancia adecuada de este tipo se puede usar de acuerdo con la presente invención.

Se entenderá que se puede usar cualquier otra solución adecuada de análisis sintáctico y división para generar partes de datos a partir de un conjunto de datos originales de acuerdo con la presente invención. Por ejemplo, el análisis sintáctico y la división se pueden procesar de manera aleatoria o seudoaleatoria bit a bit. Se puede usar un valor aleatorio o seudoaleatorio (por ejemplo, clave de sesión, clave de sesión de realimentación de cifrado, etc.), con lo que para cada bit de los datos originales el resultado de una función resumen en datos correspondientes del valor aleatorio o seudoaleatorio puede indicar a qué porción adjuntar el bit respectivo. En una solución adecuada, el valor aleatorio o seudoaleatorio se puede generar como, o ampliar a, 8 veces el tamaño de los datos originales, de manera que se pueda llevar a cabo la función resumen en un byte correspondiente del valor aleatorio o seudoaleatorio respecto a cada bit de los datos originales. Se puede usar cualquier otro algoritmo adecuado para analizar sintácticamente y dividir datos en un nivel bit a bit, de acuerdo con la presente invención. Se apreciará además que los datos de redundancia se pueden adjuntar a las porciones de datos tal como, por ejemplo, de la forma que se ha descrito justo anteriormente de acuerdo con la presente invención.

En una solución adecuada, no es necesario que el análisis sintáctico y la división sean aleatorios o seudoaleatorios. Por el contrario, se puede usar cualquier algoritmo determinista adecuado para analizar sintácticamente y dividir datos. Por ejemplo, se puede emplear fragmentación de los datos originales en porciones secuenciales como algoritmo de análisis sintáctico y división. Otro ejemplo es analizar sintácticamente y dividir los datos originales bit a bit, adjuntando cada bit respectivo a las porciones de datos secuencialmente de manera circular. Se apreciará además que los datos de redundancia se pueden adjuntar a las porciones de datos tal como, por ejemplo, de la forma que se ha descrito anteriormente de acuerdo con la presente invención.

En una realización de la presente invención, tras generar el analizador sintáctico de datos seguro un número de partes de datos originales, a fin de restablecer los datos originales, una determinada o más de las partes generadas puede ser obligatoria. Por ejemplo, si una de las partes se usa como porción de autenticación (por ejemplo, guardada en un dispositivo de testigos físicos) y si se está usando la característica de tolerancia a fallos del analizador sintáctico de datos seguro (es decir, cuando son necesarias menos que el total de las partes para restablecer los datos originales), aunque el analizador sintáctico de datos seguro pueda tener acceso a un número suficiente de partes de los datos originales a fin de restablecer los datos originales, puede requerir la porción de autenticación almacenada en el dispositivo de testigos físicos antes de restablecer los datos originales. Se entenderá que se puede requerir cualquier número y tipo de porciones específicas en función, por ejemplo, de la aplicación, el tipo de datos, el usuario, cualquier otro factor adecuado o cualquier combinación de los mismos.

En una solución adecuada, el analizador sintáctico de datos seguro o algún componente externo al analizador sintáctico de datos seguro pueden cifrar una o más partes de los datos originales. Se puede requerir proporcionar y descifrar las partes cifradas a fin de restablecer los datos originales. Las diferentes partes cifradas se pueden cifrar con diferentes claves de cifrado. Por ejemplo, esta característica se puede usar para implementar una "regla de dos hombres" más segura, según la cual un primer usuario necesitaría tener una porción específica cifrada usando un primer cifrado y un segundo usuario necesitaría tener una porción específica cifrada usando una segunda clave de cifrado. A fin de acceder a los datos originales, ambos usuarios necesitarían tener sus claves de cifrado respectivas y proporcionar sus partes respectivas de los datos originales. En una solución adecuada, se puede usar una clave pública para cifrar una o más partes de datos que puede ser una porción obligatoria que se requiere para restablecer los datos originales. A continuación, se puede usar una clave privada para descifrar la porción a fin de usarla para restablecer los datos originales.

Se puede usar cualquier paradigma adecuado de este tipo que haga uso de porciones obligatorias cuando se necesitan menos que el total de las porciones para restablecer los datos originales.

En una realización adecuada de la presente invención, la distribución de datos en un número finito de porciones de datos de puede procesar de manera aleatoria o seudoaleatoria, de manera que, con una perspectiva estadística, la probabilidad de que una porción específica de datos reciba una unidad específica de datos es igual a la probabilidad de que una cualquiera de las porciones restantes recibirá la unidad de datos. Por consiguiente, cada porción de datos tendrá una cantidad aproximadamente igual de bits de datos.

De acuerdo con otra realización de la presente invención, no es necesario que cada uno del número finito de porciones de datos tenga una probabilidad igual de recibir unidades de datos del análisis sintáctico y la división de los datos originales. Por el contrario, una determinada o más porciones pueden tener una probabilidad superior o inferior que el resto de porciones. Por consiguiente, determinadas porciones pueden tener un tamaño de bits mayor o menor respecto a otras porciones. Por ejemplo, en un escenario de dos porciones, una porción puede tener una probabilidad del 1% de recibir una unidad de datos, mientras que la segunda porción tiene una probabilidad del 99%. Lo que querría decir que, una vez que el analizador sintáctico de datos seguro ha distribuido las unidades de datos entre las dos porciones, la primera porción debería tener, aproximadamente, el 1% de los datos y la segunda porción el 99%. Se puede usar cualquier probabilidad adecuada de acuerdo con la presente invención.

Se entenderá que el analizador sintáctico de datos seguro también se puede programar para que distribuya datos a porciones de acuerdo con un porcentaje exacto (o casi exacto). Por ejemplo, el analizador sintáctico de datos seguro se puede programar para que distribuya el 80% de los datos a una primera porción y el 20% restante de los datos a una segunda porción.

De acuerdo con otra realización de la presente invención, el analizador sintáctico de datos seguro puede generar porciones de datos, de las que una o más tienen tamaños predefinidos. Por ejemplo, el analizador sintáctico de datos seguro puede dividir datos originales en partes de datos cuando una de las partes es exactamente de 256 bits. En una solución adecuada, si no es posible generar una parte de datos que tenga el tamaño requerido, el analizador sintáctico de datos seguro puede completar la parte para que tenga el tamaño correcto. Se puede usar cualquier tamaño adecuado.

En una solución adecuada, el tamaño de una parte 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 ha analizado anteriormente, el analizador sintáctico de datos seguro puede usar claves en el análisis sintáctico y la división de datos. A efectos de claridad y brevedad, en este documento dichas claves se denominarán "claves de división". Por ejemplo, la Clave Maestra de Sesión, que se ha presentado anteriormente, es un tipo de clave de división. Asimismo, como se ha analizado anteriormente, las claves de división se pueden asegurar dentro de porciones de datos generadas por el analizador sintáctico de datos seguro. Se puede usar cualquier algoritmo adecuado para asegurar claves de división, para asegurarlas entre las porciones de datos. Por ejemplo, se puede usar el algoritmo Shamir para asegurar las claves de división, con lo que se genera la información que se puede usar para reconstruir una clave de división y se adjunta a las porciones de datos. Se puede usar cualquier otro algoritmo adecuado de acuerdo con la presente invención.

Asimismo, se puede asegurar cualquier clave de cifrado adecuada dentro de una o más porciones de datos de acuerdo con cualquier algoritmo adecuado, tal como el algoritmo Shamir. Por ejemplo, claves de cifrado que se usan para cifrar un conjunto de datos antes del análisis sintáctico y la división, claves de cifrado que se usan para cifrar una parte de datos después del análisis sintáctico y la división o ambas se pueden asegurar usando, por ejemplo, el algoritmo Shamir o cualquier otro algoritmo adecuado.

De acuerdo con una realización de la presente invención, se puede usar una Transformación de Todo o Nada (AoNT), tal como una Transformación de Paquete Completo, para asegurar aún más los datos transformando claves de división, claves de cifrado, cualquier otro elemento de datos adecuado o cualquier combinación de los mismos. Por ejemplo, una clave de cifrado que se usa para cifrar un conjunto de datos antes del análisis sintáctico y la división, de acuerdo con la presente invención, se puede transformar por medio de un algoritmo AoNT. A continuación, la clave de cifrado transformada se puede distribuir entre las porciones de datos de acuerdo con, por ejemplo, el algoritmo Shamir o cualquier otro algoritmo adecuado. A fin de reconstruir la clave de cifrado, se puede restablecer el conjunto de datos cifrado (por ejemplo, sin usar necesariamente todas las porciones de datos si se usó redundancia de acuerdo con la presente invención) a fin de acceder a la información necesaria relativa a la transformación de acuerdo con AoNTs como bien conoce un experto en la materia. Cuando se recupera la clave de cifrado original, se puede usar para descifrar el conjunto de datos cifrado para recuperar el conjunto de datos original. Se entenderá que las características de tolerancia a fallos de la presente invención se pueden usar

conjuntamente con la característica de AoNT. Concretamente, los datos de redundancia se pueden incluir en las partes de datos, de manera que para restaurar el conjunto de datos cifrado sea necesario menos que el total de partes de datos.

Se entenderá que la AoNT se puede aplicar a claves de cifrado que se usan para cifrar las partes de datos tras el análisis sintáctico y la división, ya sea en lugar del cifrado y la AoNT de la respectiva clave de cifrado correspondiente al conjunto de datos antes del análisis sintáctico y la división o además de éstos. Del mismo modo, la AoNT se puede aplicar a claves de división.

En una realización de la presente invención, claves de cifrado, claves de división o ambas, tal y como se usan de acuerdo con la presente invención, se pueden cifrar aún más usando, por ejemplo, una clave de grupo de trabajo a fin de proporcionar un nivel extra de seguridad al conjunto de datos asegurado.

En una realización de la presente invención, se puede proporcionar un módulo de auditoría que haga un seguimiento cada vez que se invoque al analizador sintáctico de datos seguro para dividir datos.

La figura 36 ilustra posibles opciones (3600) para usar los componentes del analizador sintáctico de datos seguro de acuerdo con la invención. Más adelante se explica resumidamente cada combinación de opciones y se etiqueta con los números de etapa adecuados de la figura 36. El analizador sintáctico de datos seguros puede ser modular, lo que permite usar cualquier algoritmo conocido dentro de cada uno de los bloques de funciones que se muestran en la figura 36. Por ejemplo, se pueden usar otros algoritmos de división de claves (por ejemplo, compartición de secretos), tales como Blackley, en lugar de Shamir o el cifrado AES se podría sustituir por otros algoritmos de cifrado conocidos, tales como Triple DES. Las etiquetas que se muestran en el ejemplo de la figura 36 sólo representan una posible combinación de algoritmos para uso en una realización de la invención. Se debería entender que se puede usar cualquier algoritmo adecuado o combinación de algoritmos en lugar de los algoritmos etiquetados.

1) 3610, 3612, 3614, 3615, 3616, 3617, 3618, 3619

Usando datos encriptados previamente en la etapa (3610), los datos se pueden, finalmente, dividir en un número predefinido de porciones. Si el algoritmo de división requiere una clave, en la etapa (3612) se puede generar una clave de cifrado dividida usando un generador de números seudoaleatorios criptográficamente seguro. Opcionalmente, en la etapa (3614), la clave de cifrado dividida se puede transformar usando una Transformación de Todo o Nada (AoNT) en una clave dividida de transformación antes de dividir la clave en el número predefinido de porciones con tolerancia a fallos, en la etapa (3615). A continuación, en la etapa (3616), los datos se pueden dividir en el número predefinido de porciones. En la etapa (3617), se puede usar un esquema tolerante a fallos para permitir la regeneración de los datos a partir de menos que el número total de porciones. Una vez creadas las porciones, en la etapa (3618), se puede insertar en las porciones información de autenticación/integridad. Opcionalmente, cada porción se puede cifra posteriormente en la etapa (3619).

2) 3111, 3612, 3614, 3615, 3616, 3617, 3618, 3619

En algunas realizaciones, los datos de entrada se pueden cifrar usando una clave de cifrado proporcionada por un usuario o un sistema externo. En la etapa (3611), se proporciona la clave externa. Por ejemplo, la clave se puede proporcionar desde un almacén de claves externo. Si el algoritmo de división requiere una clave, en la etapa (3612), se puede generar la clave de cifrado dividida usando un generador de números seudoaleatorios criptográficamente seguro. Opcionalmente, en la etapa (3614), la clave dividida se puede transformar usando una Transformación de Todo o Nada (AoNT) en una clave de cifrado dividida de transformación antes de dividir la clave en el número predefinido de porciones con tolerancia a fallos, en la etapa (3615). A continuación, en la etapa (3616), los datos se dividen en un número predefinido de porciones. En la etapa (3617), se puede usar un esquema tolerante a fallos para permitir la regeneración de los datos a partir de menos que el número total de porciones. Una vez creadas las porciones, en la etapa (3618), se puede insertar en las porciones información de autenticación/integridad. Opcionalmente, cada porción se puede cifra posteriormente en la etapa (3619).

3) 3612, 3613, 3614, 3615, 3612, 3614, 3615, 3616, 3617, 3618, 3619

En algunas realizaciones, en la etapa (3612), se puede generar una clave de cifrado usando un generador de números aleatorios criptográficamente seguro para transformar los datos. En la etapa (3613), puede tener lugar el cifrado de los datos usando la clave de cifrado generada. Opcionalmente, en la etapa (3614), la clave de cifrado se puede transformar usando una Transformación de Todo o Nada (AoNT) en una clave de cifrado de transformación.

A continuación, en la etapa (3615), la clave de cifrado de transformación y/o la clave de cifrado generada se pueden dividir en el número predefinido de porciones con tolerancia a fallos. Si el algoritmo de división requiere una clave, en la etapa (3612), puede tener lugar la generación de la clave de cifrado dividida usando un generador de números seudoaleatorios criptográficamente seguro. Opcionalmente, en la etapa (3614), la clave dividida se puede transformar usando una Transformación de Todo o Nada (AoNT) en una clave de cifrado dividida de transformación antes de dividir la clave en el número predefinido de porciones con tolerancia a fallos, en la etapa (3615). A continuación, en la etapa (3616), los datos se pueden dividir en un número predefinido de porciones. En la etapa (3617), se puede usar un esquema tolerante a fallos para permitir la regeneración de los datos a partir de menos que el número total de porciones. Una vez creadas las porciones, en la etapa (3618), se puede insertar en las porciones información de autenticación/integridad. Opcionalmente, cada porción se puede cifra posteriormente en la etapa (3619).

4) 3612, 3614, 3615, 3616, 3617, 3618, 3619

En algunas realizaciones, los datos se pueden dividir en un número predefinido de porciones. Si el algoritmo de división requiere una clave, en la etapa (3612), puede tener lugar la generación de la clave de cifrado dividida usando un generador de números seudoaleatorios criptográficamente seguro. Opcionalmente, en la etapa (3614), la clave dividida se puede transformar usando una Transformación de Todo o Nada (AoNT) en una clave dividida transformada antes de dividir la clave en el número predefinido de porciones con tolerancia a fallos, en la etapa (3615). A continuación, en la etapa (3616) se pueden dividir los datos. En la etapa (3617), se puede usar un esquema tolerante a fallos para permitir la regeneración de los datos a partir de menos que el número total de porciones. Una vez creadas las porciones, en la etapa (3618), se puede insertar en las porciones información de autenticación/integridad. Opcionalmente, cada porción se puede cifra posteriormente en la etapa (3619).

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

El analizador sintáctico de datos seguro puede ofrecer protección de datos flexible facilitando la separación física. Primero se pueden cifrar los datos y, a continuación, dividir en porciones con tolerancia a fallos "m" de "n". Esto permite la regeneración de la información original cuando se dispone de menos que el número total de porciones. Por ejemplo, algunas porciones se pueden perder o alterar en la transmisión. Como se analiza más detalladamente más adelante, las porciones perdidas o alteradas se pueden recrear a partir de la información de integridad o tolerancia a fallos adjunta a las porciones.

A fin de crear las porciones, el analizador sintáctico de datos seguro utiliza opcionalmente una serie de claves. Dichas claves pueden incluir una o más de las siguientes:

Clave de cifrado previo: Cuando se selecciona el cifrado previo de las porciones, se puede pasar una clave externa al analizador sintáctico de datos seguro. Esta clave se puede generar y almacenar externamente en un almacén de claves (u otra ubicación) y se puede usar para cifrar datos opcionalmente antes de la división de datos.

Clave de cifrado dividida: El analizador sintáctico de datos seguro puede generar esta clave internamente y usarla para cifrar los datos antes de la división. Posteriormente, la clave se puede almacenar de manera segura dentro de las porciones usando un algoritmo de división de claves.

Clave de sesión dividida: Esta clave no se usa con un algoritmo de cifrado. Por el contrario, se puede usar para poner en clave los algoritmos de partición de datos cuando se selecciona la división aleatoria. Cuando se usa una división aleatoria, el analizador sintáctico de datos seguro puede generar internamente una clave de sesión dividida y usarla para particionar los datos en porciones. Esta clave se puede almacenar de manera segura usando un algoritmo de división de claves.

Clave de cifrado posterior: Cuando se selecciona el cifrado posterior de las porciones, se puede pasar una clave externa al analizador sintáctico de datos seguro y usar para cifrar posteriormente las porciones individuales. Esta clave se puede generar y almacenar externamente en un almacén de claves u otra ubicación adecuada.

En algunas realizaciones, cuando los datos se aseguran usando de esta forma el analizador sintáctico de datos seguro la información sólo se puede reensamblar si están presentes todas las claves de cifrado externas y las porciones requeridas.

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

Los principales procesos de clave asociados al analizador sintáctico de datos seguro (3706) pueden incluir uno o más de entre proceso de cifrado previo (3708), proceso para transformar/cifrar (3710), proceso para asegurar claves (3712), proceso para distribuir/analizar sintácticamente (3714), (3716), proceso de autenticación de porciones (3716) y proceso de cifrado posterior (3720). Estos procesos se pueden ejecutar en varios órdenes o combinaciones adecuados, como se detalla en la figura 36. La combinación y el orden de los procesos que se use puede depender del uso o aplicación específicos, del nivel de seguridad deseado, de si se desea cifrado previo, cifrado posterior opcionales o ambos, de la redundancia deseada, de las capacidades o el rendimiento de un sistema integrado o subyacente o de cualquier otro factor o combinación de factores.

La salida del proceso ilustrativo (3700) puede ser dos o más porciones (3722). Como se ha descrito anteriormente, en algunas realizaciones, los datos se pueden distribuir a cada una de estas porciones de manera aleatoria (o seudoaleatoria). En otras realizaciones, se puede usar un algoritmo determinista (o alguna combinación adecuada de algoritmos aleatorios, seudoaleatorios y deterministas).

Además de la protección individual del activo de información, a veces se requiere compartir información entre diferentes grupos de usuarios o comunidades de interés. Puede, por lo tanto, ser necesario controlar el acceso a las porciones individuales dentro de ese grupo de usuarios o compartir credenciales entre esos usuarios que sólo permitirían a miembros del grupo reensamblar las porciones. A tal efecto, en algunas realizaciones de la invención, se puede desplegar una clave de grupo de trabajo para miembros del grupo. La clave de grupo de trabajo se debería proteger y mantener confidencial, dado que la puesta en peligro de la clave de grupo de trabajo puede potencialmente permitir a los que no pertenecen al grupo acceder a la información. Más adelante se analizan algunos sistemas y procedimientos para el despliegue y protección de claves de grupo de trabajo.

El concepto de clave de grupo de trabajo permite una mayor protección del activo de información cifrando información de clave almacenada dentro de las porciones. Una vez llevada a cabo esta operación, aunque se descubran todas las claves externas y porciones necesarias, un atacante no tiene ninguna posibilidad de recrear la información sin acceder a la clave de grupo de trabajo.

La figura 38 muestra un diagrama de bloques ilustrativo (3800) para almacenar componentes de datos y claves dentro de las porciones. En el ejemplo del diagrama (3800), se omiten las etapas de cifrado previo y cifrado posterior opcionales, si bien estas etapas se pueden incluir en otras realizaciones.

El proceso simplificado para dividir los datos incluye cifrar los datos usando la clave de cifrado (3804) en la etapa de cifrado (3802). A continuación, partes de la clave de cifrado (3804) se pueden dividir y almacenar dentro de porciones (3810) de acuerdo con la presente invención. Partes de la clave de cifrado dividida (3806) también se pueden almacenar dentro de porciones (3810). Usando la clave de cifrado dividida, se dividen los datos (3808) y se almacenan en porciones (3810).

A fin de restablecer los datos, la clave de cifrado dividida (3806) se puede recuperar y restablecer de acuerdo con la presente invención. A continuación, se puede invertir la operación de división para restablecer el texto cifrado. La clave de cifrado (3804) también se puede recuperar y restablecer y, a continuación, se puede descifrar el texto cifrado usando la clave de cifrado.

Cuando se utiliza una clave de grupo de trabajo, el proceso anterior se puede cambiar ligeramente para proteger la clave de cifrado con la clave de grupo de trabajo. A continuación, la clave de cifrado se puede cifrar con la clave de grupo de trabajo antes de que se almacene dentro de las porciones. 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 cifrar primero los datos usando la clave de cifrado, en la etapa (3902). A continuación, en la etapa (3904), la clave de cifrado se puede cifrar con la clave de grupo de trabajo. A continuación, la clave de cifrado, cifrada con la clave de grupo de trabajo, se puede dividir en partes y almacenar con porciones (3912). La clave dividida (3908) también se puede dividir y

almacenar en porciones (3912). Por último, partes de datos (3910) se dividen y almacenan en porciones (3912) usando la clave dividida (3908).

A fin de restablecer los datos, la clave dividida se puede recuperar y restablecer de acuerdo con la presente invención. A continuación, se puede reinvertir la operación de división para restablecer el texto de acuerdo con la presente invención. La clave de cifrado (que se cifró con la clave de grupo de trabajo) se puede recuperar y restablecer. A continuación, la clave de cifrado se puede descifrar l usando la clave de grupo de trabajo. Por último, el texto cifrado se puede descifrar usando la clave de cifrado.

Existen varios procedimientos seguros para desplegar y proteger claves de grupo de trabajo. La elección de qué procedimiento usar para una aplicación específica depende de una serie de factores. Estos factores pueden incluir nivel de seguridad requerido, coste, conveniencia y el número de usuarios del grupo de trabajo. A continuación, se proporcionan algunas técnicas de uso común que se usan en algunas realizaciones:

Almacenamiento de claves basado en hardware

Las soluciones basadas en hardware, por lo general, proporcionan las mayores garantías para la seguridad de las claves de cifrado/descifrado de un sistema de cifrado. Ejemplos de soluciones de almacenamiento basadas en hardware incluyen dispositivos de testigos de claves resistentes a la falsificación que almacenan claves en un dispositivo portátil (por ejemplo, tarjeta inteligente/dispositivo de protección) o periféricos de almacenamiento de claves no portátiles. Estos dispositivos están diseñados para evitar la fácil duplicación de material de claves por partes no autorizadas. Una autoridad de confianza puede generar claves y distribuirlas a los usuarios o se pueden generar dentro del hardware. Adicionalmente, muchos sistemas de almacenamiento de claves prevén autenticación por múltiples factores, en los que el uso de claves requiere acceso tanto a un objeto físico (testigo) como a una frase de paso o dato biométrico.

Almacenamiento de claves basado en software

Si bien puede ser aconsejable el almacenamiento basado en hardware dedicado para aplicaciones o despliegues de alta seguridad, otros despliegues pueden elegir almacenar claves directamente en hardware local (por ejemplo, discos, RAM o almacenes de RAM no volátil, tales como memorias USB). Esto proporciona un nivel inferior de protección frente a ataques a información privilegiada o, en algunos casos, cuando un atacante puede acceder directamente a la máquina de cifrado.

Para asegurar claves en disco, la gestión de claves basada en software a menudo protege las claves almacenándolas de forma cifrada bajo una clave obtenida de una combinación de otras métricas de autenticación, que incluyen: contraseñas y frases de paso, presencia de otras claves (por ejemplo, de una solución basada en hardware), datos biométricos o cualquier combinación adecuada de los anteriores. El nivel de seguridad que proporcionan dichas técnicas puede abarcar desde 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 por múltiples factores.

El analizador sintáctico de datos seguro de la presente invención se puede usar, de manera ventajosa, en una serie de aplicaciones y tecnologías. Por ejemplo, sistema de correo electrónico, sistemas RAID, sistemas de difusión de vídeos, sistemas de bases de datos, sistemas de copia de seguridad en cinta o cualquier otro sistema adecuado, pueden tener el analizador sintáctico de datos seguro integrado a cualquier nivel adecuado. Como se ha analizado anteriormente, se entenderá que el analizador sintáctico de datos seguro también se puede integrar para protección y tolerancia a fallos de cualquier tipo de datos en movimiento mediante cualquier soporte de transporte, que incluyen, por ejemplo, soportes de transporte por cable, inalámbrico o físico. Como ejemplo, aplicaciones de voz sobre protocolo de internet (VoIP) pueden hacer uso del analizador sintáctico de datos seguro de la presente invención para solucionar problemas relacionados con ecos y retardos que normalmente se encuentran en la VoIP. La necesidad de reintento de red en paquetes perdidos se puede eliminar usando tolerancia a fallos, que garantiza la entrega de paquetes incluso con la pérdida de un número predeterminado de porciones. Paquetes de datos (por ejemplo, paquetes de red) también se pueden dividir y restablecer de manera eficaz "por el aire" con mínimo retardo y almacenamiento temporal, lo que tiene como resultado una solución integral para varios tipos de datos en movimiento. El analizador sintáctico de datos seguro puede actuar en paquetes de datos de red, paquetes de voz de red, bloques de datos de sistemas de archivos o cualquier otra unidad adecuada de información. Además de estar integrado con la aplicación VoIP, el analizador sintáctico de datos seguro puede estar integrado con una aplicación de compartición de archivos (por ejemplo, una aplicación de compartición de archivos entre iguales), una aplicación

de difusión de videos, una aplicación de sondeo o votación electrónicos (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 analizador sintáctico de datos seguro de la presente invención puede proporcionar soporte a datos de red en movimiento en dos fases distintas: una fase de generación de cabeceras y una fase de partición de datos. Un proceso simplificado de generación de cabeceras (4000) y un proceso simplificado de partición de datos (4010) se muestran en las figuras 40A y 40B, respectivamente. Uno o ambos de estos procesos se pueden llevar a cabo en paquetes de red, bloques de sistemas de archivos o cualquier otra información adecuada.

En algunas realizaciones, el proceso de generación de cabeceras (4000) se puede llevar a cabo una vez al inicio de un flujo de paquetes de red. En la etapa (4002), se puede generar una clave de cifrado dividida aleatoria (o seudoaleatoria), (K). A continuación, la clave de cifrado dividida (K) se puede cifrar opcionalmente (por ejemplo, usando la clave de grupo de trabajo que se ha descrito anteriormente) en la etapa de envoltura de claves AES (4004). Si bien en algunas realizaciones se puede usar una envoltura de claves AES, en otras realizaciones se puede usar cualquier algoritmo de envoltura de claves o cifrado de claves adecuado. La etapa de envoltura de claves AES (4004) se puede aplicar a toda la clave de cifrado dividida (K) o la clave de cifrado dividida se puede analizar sintácticamente en varios bloques (por ejemplo, bloques de 64 bits). La etapa de envoltura de claves AES (4004) se puede aplicar a bloques de la clave de cifrado dividida, si se desea.

En la etapa (4006), se puede usar un algoritmo de compartición de secretos (por ejemplo, Shamir) para dividir la clave de cifrado dividida (K) en porciones de clave. A continuación, cada porción de clave se puede incorporar a una de las porciones de salida (por ejemplo, en las cabeceras de porciones). Por último, se puede adjuntar un bloque de integridad de porciones y (opcionalmente) una etiqueta de autenticación posterior (por ejemplo, MAC) al bloque de cabecera de cada porción. Cada bloque de cabecera puede estar diseñado para adaptarse a un único paquete de datos.

Una vez concluida la generación de cabeceras (por ejemplo, usando el proceso simplificado de generación de cabeceras (4000)), el analizador sintáctico de datos seguro puede iniciar la fase de partición de datos usando el proceso simplificado de división de datos (4010). En la etapa, (4012), cada bloque de datos o paquete de datos entrante del flujo se cifra usando la clave de cifrado dividida (K). En la etapa (4014), información de integridad de porciones (por ejemplo, un resumen (H)) se puede calcular en el texto cifrado que resulta de la etapa (4012). Por ejemplo, se puede calcular un resumen SHA-256. En la etapa (4106), el paquete de datos o bloque de datos se puede particionar en dos o más porciones de datos usando uno de los algoritmos de división de datos que se han descrito anteriormente de acuerdo con la presente invención. En algunas realizaciones, se puede dividir el bloque de datos o paquete de datos de manera que cada porción de datos contenga una distribución sustancialmente aleatoria del bloque de datos o paquete de datos cifrado. A continuación, la información de integridad (por ejemplo, resumen (H)) se puede adjuntar a cada porción de datos. En algunas realizaciones, también se puede calcular una etiqueta de autenticación posterior opcional (por ejemplo, MAC) y adjuntar a cada porción de datos.

Cada porción de datos puede incluir metadatos, que pueden ser necesarios para permitir la correcta reconstrucción de los bloques de datos o paquetes de datos. Esta información puede estar incluida en la cabecera de porción. Los metadatos pueden incluir información tal como porciones de claves criptográficas, identidades de claves, número único de porciones, valores de firmas/MAC y bloques de integridad. A fin de maximizar la eficiencia del ancho de banda, los metadatos se pueden almacenar en un formato binario compacto.

Por ejemplo, en algunas realizaciones, la cabecera de porción incluye un trozo de cabecera de texto común, que no está cifrado y puede incluir elementos tales como la porciones de claves Shamir, número único por sesión, número único por porción, identificadores de claves (por ejemplo, un identificador de claves de grupo de trabajo y un identificador de claves de autenticación posterior). La cabecera de porción también puede incluir un trozo de cabecera cifrado, que está cifrado con la clave de cifrado dividida. Un trozo de cabecera de integridad, que puede incluir comprobaciones de identidad para que cualquier número de los bloques anteriores (por ejemplo, los dos bloques anteriores) se pueda incluir en la cabecera. En la cabecera de porción también se puede incluir cualquier otro valor o información adecuados.

Como se muestra en el formato de porción (4100) ilustrativo de la figura 41, el bloque de cabecera (4102) puede estar asociado a dos o más bloques de salida (4104). Cada bloque de cabecera, tal como el bloque de cabecera (4102), puede estar diseñado para encajar dentro de un único paquete de datos de red. En algunas realizaciones,

una vez que se ha transmitido el bloque de cabecera (4102) de una primera ubicación a una segunda ubicación, se pueden transmitir los bloques de salida. Alternativamente, el bloque de cabecera (4102) y los bloques de salida (4104) se pueden transmitir a la vez en paralelo. La transmisión puede tener lugar por una o más vías de comunicaciones similares o distintas.

Cada bloque de salida puede incluir una parte de datos (4106) y una parte de integridad/autenticidad (4108). Como se ha descrito anteriormente, cada porción de datos se puede asegurar usando una parte de integridad de porciones que incluya información de integridad de porciones (por ejemplo, un resumen SHA-256) de los datos cifrados y previamente particionados. Para verificar la integridad de los bloque de salida en el momento de la recuperación, el analizador sintáctico de datos seguro puede comparar los bloques de integridad de porciones y, a continuación, invertir el algoritmo de división. A continuación, se puede verificar el resumen de los datos recuperados con el resumen de la porción.

Como se ha mencionado anteriormente, en algunas realizaciones de la presente invención, el analizador sintáctico de datos seguro se puede usar conjuntamente con un sistema de copia de seguridad en cinta. Por ejemplo, se puede usar una cinta individual como nodo (es decir, parte/porción) de acuerdo con la presente invención. Se puede usar cualquier otra disposición adecuada. Por ejemplo, un subsistema o biblioteca de cintas, que esté formado de dos o más cintas, se puede tratar como nodo único.

La redundancia también se puede usar con las cintas de acuerdo con la presente invención. Por ejemplo, si un conjunto de datos está repartido entre cuatro cintas (es decir, partes/porciones), dos de las cuatro cintas pueden ser necesarias a fin de restablecer los datos originales. Se entenderá que se puede requerir cualquier número de nodos (es decir, menos que el número total de nodos) para restablecer los datos originales de acuerdo con las características de redundancia de la presente invención. Esto aumenta sustancialmente la probabilidad de restablecimiento cuando deja de estar disponible una cinta.

Cada cinta también se puede proteger digitalmente con un valor resumen SHA-256, HMAC, cualquier otro valor adecuado o cualquier combinación de los mismos para asegurarla contra la falsificación. En caso de que cambie cualquier dato de la cinta o el valor resumen, esa cinta no sería candidata para la restauración y para restablecer los datos se usaría cualquier número mínimo requerido de cintas del resto de cintas.

En los sistemas convencionales de copia de seguridad en cinta, cuando un usuario pide que los datos se escriban en una cinta o se lean de ésta, el sistema de gestión de cintas (TMS) presenta un número que corresponde a un montaje físico de cintas. Este montaje físico de cintas indica una unidad de disco física en la que se montarán los datos. Un operador de cintas o un robot de cintas pueden cargar la cinta en un archivo de cintas.

En la presente invención, el montaje físico de cintas se puede considerar un punto de montaje lógico que indica un número de cintas físicas. Esto no sólo aumenta la capacidad de datos, sino que, gracias al paralelismo, también mejora el rendimiento.

Para mayor rendimiento, los nodos de cinta pueden ser o pueden incluir un conjunto RAID de discos que se usan para almacenar imágenes de cinta. Esto permite un restablecimiento a alta velocidad porque los datos siempre pueden estar disponibles en el RAID protegido.

En cualquiera de las realizaciones anteriores, los datos que se van a asegurar se pueden distribuir en una pluralidad de porciones usando técnicas de distribución de datos deterministas, probabilísticas o tanto deterministas como probabilísticas. A fin de evitar que un atacante inicie un ataque criptográfico en cualquier bloque de cifrado, los bits de los bloques de cifrado se pueden distribuir a las porciones de manera determinista. Por ejemplo, la distribución se puede llevar a cabo usando la rutina BitSegmento o se puede modificar la rutina BloqueSegmento para permitir la distribución de partes de bloques a múltiples porciones. Esta estrategia puede defender de un atacante que ha acumulado menos que "M" porciones.

En algunas realizaciones, se puede emplear una rutina de compartición de secretos en clave usando dispersión de información en clave (por ejemplo, mediante el uso de un algoritmo de dispersión de información en clave o "IDA"). La clave correspondiente al IDA en clave también se puede proteger con una o más claves externas de grupo de trabajo, con una o más claves compartidas o con cualquier combinación de claves de grupo de trabajo y claves compartidas. De este modo, se puede emplear un esquema de compartición de secretos por múltiples factores. Para reconstruir los datos, en algunas realizaciones, se pueden requerir al menos "M" porciones más las claves de grupo de trabajo (y/o claves compartidas). El IDA (o la clave correspondiente al IDA) también se puede introducir en el

proceso de cifrado. Por ejemplo, la transformación se puede introducir en el texto común (por ejemplo, durante la capa de procesamiento previo antes del cifrado) y puede proteger aún más el texto común antes de que se cifre.

Por ejemplo, en algunas realizaciones, la dispersión de información en clave se usa para distribuir partes exclusivas de datos de un conjunto de datos en dos o más porciones. La dispersión de información en clave puede usar una clave de sesión para, primero, cifrar el conjunto de datos, para distribuir partes exclusivas de los datos cifrados del conjunto de datos en dos o más porciones del conjunto de datos cifrados o tanto cifrar el conjunto de datos como distribuir partes exclusivas de los datos cifrados del conjunto de datos en las dos o más porciones de conjunto de datos cifrados. Por ejemplo, para distribuir partes exclusivas del conjunto de datos o conjunto de datos cifrados, se puede usar la compartición de secretos (o los procedimientos que se han descrito anteriormente, tales como BitSegmento o BloqueSegmento). A continuación, la clave de sesión se puede transformar opcionalmente (por ejemplo usando una transformación de paquete completo o AoNT) y compartir usando, por ejemplo, compartición de secretos (o la clave de sesión y dispersión de información en clave).

En algunas realizaciones, la clave de sesión se puede cifrar usando una clave compartida (por ejemplo, una clave de grupo de trabajo) antes de que se distribuyan partes exclusivas de la clave en dos o más porciones de clave de sesión o se compartan. A continuación, se pueden formar dos o más porciones de usuario combinando al menos una porción de conjunto de datos cifrados y al menos una porción de clave de sesión. En algunas realizaciones, al formar una porción de usuario la al menos una porción de clave de sesión se puede intercalar en una porción de conjunto de datos cifrados. En otras realizaciones, la al menos una porción de clave de sesión se puede insertar en una porción de conjunto de datos cifrados en una ubicación, en función, al menos en parte, de la clave de grupo de trabajo compartida. Por ejemplo, se puede usar dispersión de información en clave para distribuir cada porción de clave de sesión en un conjunto exclusivo de datos cifrados para formar una porción de usuario. Intercalar o insertar una porción de clave de sesión en una porción de conjunto de datos cifrados en una ubicación, en función, al menos en parte, del grupo de trabajo compartido puede proporcionar mayor seguridad ante ataques criptográficos. En otras realizaciones, una o más porciones de clave de sesión se pueden adjuntar al principio o al final de una porción de conjunto de datos cifrado para formar una porción de usuario. A continuación, la recopilación de porciones de usuario se puede almacenar de manera independiente en al menos un depósito de datos. El depósito o depósitos de datos pueden estar ubicados en la misma ubicación física (por ejemplo, en el mismo dispositivo de almacenamiento magnético o en cinta) o separados geográficamente (por ejemplo, en servidores separados físicamente en diferentes ubicaciones geográficas). Para reconstruir el conjunto de datos original, se puede requerir un conjunto autorizado de porciones de usuario y la clave de grupo de trabajo compartida.

La dispersión de información en clave puede ser segura incluso ante oráculos de recuperación de claves. Por ejemplo, tómese un cifrado en bloque E y un oráculo de recuperación de claves para E que lleva 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 coherente con los ejemplos de entrada/salida (por ejemplo, $Y_i = E_K(X_i)$ para toda i). El oráculo puede devolver el valor diferenciado $\perp$ si no existe clave coherente. Este oráculo puede modelar un ataque criptoanalítico que puede recuperar una clave de una lista de ejemplos de entrada/salida.

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

Si π^{IDA} es un esquema de IDA y π^{Enc} es un esquema de cifrado dado por un modo de operación de algún cifrado en bloque E, entonces (π^{IDA}, π^{Enc}) proporciona seguridad ante un ataque de recuperación de claves si los dos esquemas, cuando se combinan con un esquema perfecto de compartición de secretos (PSS) arbitrario, de acuerdo con HK1 o HK2, logra el objetivo de compartición robusta de secretos por ordenador (RCSS), pero en el modelo en que el adversario tiene un oráculo de recuperación de claves.

Si existe un esquema de IDA π^{IDA} y un esquema de cifrado π^{Enc} tal que el par de esquemas proporciona seguridad ante ataques de recuperación de claves, una forma de logar dicho par puede ser tener un IDA "listo" y un esquema de cifrado "tonto". Otra forma de lograr dicho par de esquemas puede ser tener un IDA "tonto" y un esquema de cifrado "listo".

Para ilustrar el uso de un IDA listo y un esquema de cifrado tonto, en algunas realizaciones, el esquema de cifrado puede ser CBC y el IDA puede tener una propiedad de "escasa privacidad". La propiedad de escasa privacidad significa, por ejemplo, que si la entrada del IDA es una secuencia aleatoria de bloques $M = M_1 \ldots M_1$ y el adversario obtiene porciones de una recopilación no autorizada, entonces existe algún índice de bloques *i* de manera que es

imposible que el adversario calcule M_i. Tal IDA escasamente privado se puede construir, primero, aplicando a *M* una AoNT de información teórica, tal como AoNT de Stinson y, a continuación, aplicando un IDA simple, tal como BloqueSegmento o un IDA de eficiencia de bits, como el esquema de Rabin (por ejemplo, codificación Reed-Solomon).

Para ilustrar el uso de un IDA tonto y un esquema de cifrado listo, en algunas realizaciones, se puede usar un modo CBC con cifrado doble en lugar de cifrado único. En este caso, se puede usar cualquier IDA, incluso la reiteración. Tener el oráculo de recuperación de claves para el cifrado en bloque sería inútil para un adversario, dado que se denegará al adversario cualquier ejemplo de entrada/salida de cifrado único.

Aunque un IDA listo tiene valor, también puede ser innecesario en algunos contextos, en el sentido de que los "inteligentes" necesarios para proporcionar seguridad frente a un ataque de recuperación de claves podrían haber sido "empujados" a otro sitio. Por ejemplo, en algunas realizaciones, no importa lo inteligente que sea el IDA ni qué objetivo se está intentando logar con el IDA en el contexto de HK1/HK2, se puede apartar a los inteligentes del IDA e introducirlos en el esquema de cifrado, quedando con un IDA fijo y tonto.

En función de lo anterior, en algunas realizaciones, se puede usar un IDA inteligente "universalmente válido" π^{IDA}. Por ejemplo, se proporciona un IDA tal que, para todos los esquemas de cifrado π^{Enc}, el par (π^{IDA}, π^{Enc}) proporciona universalmente seguridad ante ataques de recuperación de claves.

En algunas realizaciones se proporciona un esquema de cifrado que es una RCSS segura ante un oráculo de recuperación de claves. El esquema puede estar integrado con HK1/HK2, con cualquier IDA, para lograr seguridad ante recuperación de claves. Usar el nuevo esquema puede ser especialmente útil, por ejemplo, para hacer esquemas de cifrado simétrico más seguros frente a ataques de recuperación de claves.

Como se ha mencionado anteriormente, los conceptos clásicos de compartición de secretos son normalmente sin clave. Por lo tanto, un secreto se fragmenta en porciones, o se reconstruye a partir de las mismas, de manera que no requiere que el comerciante ni la parte que reconstruye el secreto tengan algún tipo de clave simétrica o asimétrica. No obstante, el analizador sintáctico de datos seguro, que se describe en este documento, es con clave. El comerciante puede proporcionar una clave simétrica que, si se usa para compartir datos, se puede requerir para recuperar datos. El analizador sintáctico de datos seguro puede usar la clave simétrica para dispersar o distribuir partes exclusivas del mensaje para que se aseguren en una o más porciones.

La clave compartida puede posibilitar la compartición de secretos por múltiples factores o por dos factores (2FSS). Por lo tanto, puede requerir que el adversario navegue a través de dos tipos fundamentalmente diferentes de seguridad a fin de romper el mecanismo de seguridad. Por ejemplo, para infringir los objetivos de compartición de secretos, el adversario (1) puede necesitar obtener las porciones de un conjunto autorizado de participantes y (2) puede necesitar obtener una clave secreta que no debería ser capaz de obtener (o romper el mecanismo criptográfico puesto en clave con esa clave).

En algunas realizaciones, se añade un nuevo conjunto de requisitos adicionales al objetivo de RCCS. Los requisitos adicionales pueden incluir posesión de la clave de "segundo factor". Estos requisitos adicionales se pueden añadir sin reducir el conjunto original de requisitos. Un conjunto de requisitos se puede referir a la incapacidad del adversario para romper el esquema si conoce la clave secreta pero no obtiene porciones suficientes (por ejemplo, los requisitos *clásicos* o *de primer factor*), mientras que el otro conjunto de requisitos se puede referir a la incapacidad del adversario para romper el esquema si no tiene la clave secreta, pero logra hacerse con todas las porciones (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 darse el caso de que el entorno seleccione una clave secreta *K* y un bit *b* En este caso, el adversario suministra un par de mensajes de igual longitud en el dominio del esquema de compartición de secretos, M_1^0 y M_1^1. El entorno calcula las porciones de M_1^b para obtener un vector de porciones, $\boldsymbol{S}_1$ = ($\boldsymbol{S}_1$ [1], …, $\boldsymbol{S}_1$ [*n*] y da las pociones $\boldsymbol{S}_1$ (todas) al adversario. Ahora, el adversario puede elegir otro par de mensajes (M_2^0 y M_2^1) y todo pasa como antes, usando la misma clave *K* y un bit oculto *b*. La tarea del adversario es enviar el bit *b'* que cree que es *b*. La ventaja de privacidad del adversario es una menos que el doble de la probabilidad de que b = b'. Este caso insiste en el concepto de que, incluso enterándose de todas las porciones, el adversario seguirá sin poder enterarse del secreto compartido si le falta la clave secreta.

En el requisito de autenticidad, puede darse el caso de que el entorno elija una clave secreta *K* y la use en las

llamadas subsiguientes a *Compartir* y *Recuperar.* En algunas realizaciones, *Compartir* y *Recuperar* pueden tener su sintaxis modificada para reflejar la presencia de dicha clave. A continuación, el adversario realiza peticiones de *Compartir* para cualquiera de los mensajes M_1, …, M_q que elija en el dominio del esquema de compartición de secretos. En respuesta a cada petición de *Compartir* obtiene el correspondiente n-vector de porciones, $\boldsymbol{S}_1$, …, $\boldsymbol{S}_q$. La intención del adversario es crear un nuevo texto sin formato. Gana si envía un vector de porciones $\boldsymbol{S}'$ tal que, cuando lo pasa al algoritmo de *Recuperación*, tiene como resultado algo *no* incluido en $\{M_1, \ldots, M_q\}$. Esto es un concepto de "integridad de texto sin formato".

Existen dos soluciones para lograr la compartición de secretos por múltiples factores. La primera es una solución genérica, genérica en el sentido de usar un esquema de (R)CSS subyacente a modo de caja negra. Para cifrar el mensaje que se va a compartir por CSS se usa un esquema de cifrado autenticado y, a continuación, se puede compartir el texto cifrado resultante, por ejemplo, usando un algoritmo de compartición de secretos, tal como Blakely o Shamir.

Una solución potencialmente más eficaz es permitir que la clave compartida sea la clave de grupo de trabajo. Concretamente, (1) la clave de sesión generada aleatoriamente del esquema de (R)CSS se puede cifrar usando la clave compartida y (2) el esquema de cifrado aplicado al mensaje (por ejemplo, el archivo) se puede sustituir por un esquema de cifrado autenticado. Esta solución puede suponer sólo una mínima degradación del rendimiento.

El analizador sintáctico de datos seguro de la presente invención se puede usar para implementar una solución de seguridad informática en la nube. La informática en la nube es el almacenamiento, la informática basada en la red o ambos en los que recursos informáticos y de almacenamiento se pueden proporcionar a sistemas informáticos y a otros dispositivos por una red. Por lo general, a los recursos informáticos en la nube se accede por internet, pero la informática en la nube se podría llevar a cabo a través de cualquier red pública o privada adecuada. La informática en la nube puede proporcionar un nivel de abstracción entre recursos informáticos y sus componentes de hardware subyacentes (por ejemplo, servidores, dispositivos de almacenamiento, redes), que posibilitan el acceso remoto a una fuente de recursos informáticos. Estos recursos informáticos en la nube se pueden denominar colectivamente la "nube". La informática en la nube se puede usar para proporcionar recursos dinámicamente escalables y, a menudo, virtualizados como un servicio por internet o cualquier red o combinación de redes adecuada.

La seguridad es un asunto importante en la informática en la nube porque los datos privados se pueden transmitir a través de redes públicas y se pueden procesar y almacenar en sistemas compartidos o públicamente accesibles. El analizador sintáctico de datos seguro se puede usar para proteger recursos informáticos en la nube y los datos que se comunican entre la nube y un dispositivo o usuario final. Por ejemplo, el analizador sintáctico de datos seguro se puede usar para asegurar el almacenamiento de datos en la nube, datos en movimiento en la nube, acceso a red en la nube, servicios de datos en la nube, acceso a recursos informáticos de alto rendimiento en la nube y cualquier otra operación en la nube.

La figura 42 es un diagrama de bloques ilustrativo de una solución de seguridad informática en la nube. El sistema (4200), que incluye un analizador sintáctico de datos seguro (4210), está acoplado a la nube (4250) que incluye recursos en la nube (4260). El sistema (4200) puede incluir cualquier hardware adecuado, tal como un terminal informático, un ordenador personal, un dispositivo portátil (por ejemplo, PDA, Blackberry, teléfono inteligente, dispositivo tableta), teléfono móvil, red informática, cualquier otro hardware adecuado o cualquier combinación de los mismos. El analizador sintáctico de datos seguro (4210) puede estar integrado a cualquier nivel del sistema (4200). Por ejemplo, el analizador de datos seguro (4210) puede estar integrado en el hardware y/o software del sistema (4200) a un nivel lo suficientemente especializado de manera que la presencia del analizador sintáctico de datos seguro (4210) pueda ser sustancialmente obvia para un usuario final del sistema (4200). La integración del analizador sintáctico de datos seguro en un sistema se ha descrito más detalladamente anteriormente por ejemplo, en relación con las figuras 27 y 28. La nube (4250) incluye múltiples recursos ilustrativos en la nube (4260) que incluyen, recursos de almacenamiento de datos (4260a) y (4260e), recursos de servicios de datos (4260b) y (4260g), recursos de control de acceso a red (4260c) y (4260h) y recursos informáticos de alto rendimiento (4260d) y (4260f). Cada uno de estos recursos se describirá más detalladamente más adelante en relación con las figuras 43 a 47. Estos recursos informáticos en la nube son sólo ilustrativos. Se debería entender que desde el sistema (4200) se podría acceder a cualquier número y tipo de recursos informáticos en la nube.

Una ventaja de la informática en la nube es que el usuario del sistema (4200) podría acceder a múltiples recursos informáticos en la nube sin tener que invertir en hardware informático dedicado. El usuario tendría la capacidad de controlar dinámicamente el número y el tipo de recursos informáticos en la nube a los que puede acceder el sistema (4200). Por ejemplo, el sistema (4200) puede estar provisto de recursos de almacenamiento en la nube, bajo

demanda, que tienen capacidades que se pueden ajustar dinámicamente en función de las necesidades del momento. En algunas realizaciones, una o más aplicaciones de software ejecutadas en el sistema (4200) pueden acoplar el sistema (4200) a recursos en la nube (4260). Por ejemplo, se puede usar un navegador de internet para acoplar el sistema (4200) a uno o más recursos en la nube (4260) a través de internet. En algunas realizaciones, hardware con el sistema (4200) integrado o conectado a éste puede acoplar el sistema (4200) a recursos en la nube (4260). En ambas realizaciones, el analizador sintáctico de datos seguro (4210) puede asegurar comunicaciones con los recursos en la nube (4260) y/o los datos almacenados dentro de los recursos en la nube (4260). El acoplamiento de los recursos en la nube (4260) al sistema (4200) puede ser obvio para el sistema (4200) o los usuarios del sistema (4200), de manera que los recursos en la nube (4260) parezcan recursos de hardware local del sistema (4200). Además, los recursos compartidos en la nube (4260) pueden parecer recursos de hardware dedicado del sistema (4200).

El analizador sintáctico de datos seguro (4210) puede cifrar y dividir datos de manera que ningún dato discernible, a efectos legales, cruzará la nube o se almacenará en la misma. Los componentes de hardware subyacentes de la nube (por ejemplo, servidores, dispositivos de almacenamiento, redes) se pueden repartir geográficamente para garantizar la continuidad de los recursos en la nube en caso de corte en la red eléctrica, fenómeno meteorológico u otro fenómeno natural o artificial. Por consiguiente, aunque algunos de los componentes de hardware, dentro la nube, sufran un fallo catastrófico, se puede seguir accediendo a los recursos en la nube. Los recursos en la nube (4260) pueden estar diseñados con redundancias para proporcionar un servicio ininterrumpido a pesar de uno o más fallos de hardware.

La figura 43 es un diagrama de bloques ilustrativo de una solución de seguridad informática en la nube para asegurar datos en movimiento (es decir, durante la transferencia de datos de una ubicación a otra) a través de la nube. La figura 43 muestra un sistema remitente (4300) que puede incluir cualquier hardware adecuado, tal como un terminal informático, ordenador personal, dispositivo portátil (por ejemplo, PDA, Blackberry), teléfono móvil, red informática, cualquier otro hardware adecuado o cualquier combinación de los mismos. El sistema remitente (4300) se usa para generar y/o almacenar datos, que pueden ser, por ejemplo, un mensaje de correo electrónico, un archivo de datos binarios (por ejemplo, gráficos, voz, video, etc.) o ambos. El analizador sintáctico de datos seguro (4310) analiza sintácticamente y divide los datos de acuerdo con la presente invención. Las partes de datos resultantes se pueden comunicar por la nube (4350) al sistema destinatario (4370). El sistema destinatario (4370) puede ser cualquier hardware adecuado que se ha descrito anteriormente en relación con el sistema remitente (4300). Las partes de datos separadas se pueden volver a combinar en el sistema destinatario (4370) para generar los datos originales de acuerdo con la presente invención. Al desplazarse a través de la nube (4310) las partes de datos se pueden comunicar por una o más vías de comunicaciones que incluyen internet y/o una o más intranets, LANs, WiFi, Bluetooth, cualquier otra red de comunicaciones inalámbricas o por cable adecuada o cualquier combinación de los mismos. Como se ha descrito anteriormente en relación con las figuras 28 y 29, el analizador sintáctico de datos seguro asegura los datos originales aunque se pongan en peligro algunas de las partes de datos.

La figura 44 es un diagrama de bloques ilustrativo de una solución de seguridad informática en la nube para asegurar servicios de datos en la nube. En esta realización, un usuario (4400) puede proporcionar servicios de datos (4420) a un usuario final (4440) por la nube (4430). El analizador sintáctico seguro (4410) puede asegurar los servicios de datos de acuerdo con las realizaciones que se han descrito. Servicio de datos (4420) puede ser cualquier servicio de aplicación o software adecuado al que se puede acceder por la nube (4430). Por ejemplo, servicio de datos (4420) puede ser una aplicación basada en la red implementada como parte de un sistema de arquitectura orientada a servicios (SOA). El servicio de datos (4420) se puede almacenar y ejecutar en uno o más sistemas dentro de la nube (4430). La abstracción que proporciona esta implementación de informática en la nube permite que el servicio de datos (4420) parezca un recurso virtualizado del usuario final (4440), independientemente de los recursos de hardware subyacentes. El analizador sintáctico seguro (4410) puede asegurar datos en movimiento entre el servicio de datos (4420) y el usuario final (4440). El analizador sintáctico seguro (4410) también puede asegurar datos almacenados asociados al servicio de datos (4420). Los datos almacenados asociados al servicio de datos (4420) se pueden asegurar dentro del sistema o sistemas que implementan el servicio de datos (4420) y/o dentro de dispositivos independientes de almacenamiento de datos seguro en la nube, que se describirán más detalladamente más adelante. Aunque el servicio de datos (4420) y otras partes de la figura 44 se muestran fuera de la nube (4430), se debería entender que cualquiera de estos elementos puede estar incorporado en la nube (4430).

La figura 45 es un diagrama de bloques ilustrativo de una solución de seguridad informática en la nube para asegurar recursos de almacenamiento de datos en la nube. El sistema (4500), que incluye un analizador sintáctico de datos seguro (4510), está acoplado a la nube (4550) que incluye recursos de almacenamiento de datos (4560). El

analizador sintáctico de datos seguro (4510) se puede usar para analizar sintácticamente y dividir datos entre uno o más recursos de almacenamiento de datos (4560). Cada recurso de almacenamiento de datos (4560) puede representar uno o más dispositivos de almacenamiento en red. Estos dispositivos de almacenamiento se pueden asignar a un único usuario/sistema o los pueden compartir múltiples usuarios/sistemas. La seguridad que proporciona el analizador sintáctico de datos seguro (4510) puede permitir que datos de múltiples usuarios/sistemas coexistan de manera segura en los mismos dispositivos de almacenamiento. La abstracción que proporciona esta implementación de informática en la nube permite que los recursos de almacenamiento de datos (4560) parezcan un único recurso de almacenamiento virtualizado del sistema (4500) independientemente del número y la ubicación de los recursos de almacenamiento de datos subyacentes. Cuando los datos se escriben en los recursos de almacenamiento de datos (4560) o se leen de estos, el analizador sintáctico de datos seguro (4510) puede dividir y volver a combinar los datos de manera que puedan ser obvios para el usuario final. De este modo, un usuario final podría acceder bajo demanda a un almacenamiento dinámicamente escalable.

El almacenamiento de datos en la nube, usando el analizador sintáctico de datos seguro (4510) es seguro, resiliente, persistente y privado. El analizador sintáctico de datos seguro (4510) asegura los datos garantizando que ningún dato discernible, a efectos legales, cruce la nube o se almacene en un único dispositivo de almacenamiento. El sistema de almacenamiento de datos en la nube es resiliente debido a la redundancia que ofrece el analizador sintáctico de datos seguro (es decir, se necesitan menos que el total de partes separadas de datos para reconstruir los datos originales). Almacenar las partes separadas dentro de múltiples dispositivos de almacenamiento y/o dentro de múltiples recursos de almacenamiento de datos (4560) garantiza que los datos se puedan reconstruir aunque falle uno o más de los dispositivos de almacenamiento o no se pueda acceder a los mismos. El sistema de almacenamiento en la nube es persistente porque la pérdida de un dispositivo de almacenamiento dentro de los recursos de almacenamiento de datos (4560) no afecta al usuario final. Si falla un dispositivo de almacenamiento, las partes de datos que se almacenaron dentro de ese dispositivo de almacenamiento se pueden reconstruir en otro dispositivo de almacenamiento sin tener que comprometer los datos. Además, los recursos de almacenamiento (4560) (o incluso los múltiples dispositivos de almacenamiento en red que forman un recurso de almacenamiento de datos (4560)) se pueden dispersar geográficamente para limitar el riesgo de múltiples fallos. Por último, los datos almacenados en la nube se pueden mantener privados usando una o más claves. Como se ha descrito anteriormente, los datos se pueden asignar a un usuario o a una comunidad de interés mediante claves exclusivas, de manera que sólo ese usuario o comunidad tendrá acceso a los datos.

El almacenamiento de datos en la nube usando el analizador de datos seguro también puede aumentar el rendimiento respecto al almacenamiento en red o local tradicional. El rendimiento del sistema se puede mejorar escribiendo partes separadas de datos en múltiples dispositivos de almacenamiento en paralelo o leyéndolas de éstos. Este aumento de rendimiento puede permitir usar dispositivos de almacenamiento más económicos y lentos, sin que afecte sustancialmente a la velocidad global del sistema de almacenamiento.

La figura 46 es un diagrama de bloques ilustrativo para asegurar el acceso a red usando un analizador sintáctico de datos seguro de acuerdo con las realizaciones que se han descrito. El analizador sintáctico de datos seguro (4610) se puede usar con un bloque de control de acceso a red (4620) para controlar el acceso a recursos de red. Como se ilustra en la figura 46, el boque de control de acceso a red (4620) se puede usar para proporcionar comunicaciones de red seguras entre usuario (4600) y usuario final (4640). En algunas realizaciones, el bloque de control de acceso a red (4620) puede proporcionar acceso seguro a red para uno o más recursos de red en la nube (por ejemplo, nube (4250), figura 42). Usuarios autorizados (por ejemplo, usuario (4600) y usuario final (4640) pueden estar provistos de claves a nivel de grupo que proporcionan a los usuarios la capacidad de comunicarse de manera segura por una red y/o acceder a recursos de red seguros. Los recursos de red seguros no responderán a menos que se presenten las credenciales apropiadas (por ejemplo, claves de grupo). Esto puede evitar ataques comunes a redes, tales como, por ejemplo, ataques de denegación de servicio, ataques de exploración de puertos, ataques intermediarios y ataques de reproducción.

Además de proporcionar seguridad para datos en reposo, almacenados dentro de una red de comunicaciones, y seguridad para datos en movimiento, a través de la red de comunicaciones, el bloque de control de acceso a red (4620) se puede usar con el analizador sintáctico de datos seguro (4620) para compartir información entre diferentes grupos de usuarios o comunidades de interés. Se pueden crear grupos de colaboración para que participen como comunidades de interés seguras en redes virtuales seguras. Se puede desplegar una clave de grupo de trabajo para miembros del grupo para proporcionar a los miembros del grupo acceso a la red y a recursos en red. Los sistemas y procedimientos para desplegar claves de grupo de trabajo se han analizado anteriormente.

La figura 47 es un diagrama de bloques ilustrativo para asegurar el acceso a recursos informáticos de alto

rendimiento usando un analizador sintáctico de datos seguro de acuerdo con las realizaciones que se han descrito. El analizador sintáctico de datos seguro (4710) se puede usar para proporcionar acceso seguro a recursos informáticos de alto rendimiento (4720). Como se ilustra en la figura 47, un usuario final (4740) puede acceder a recursos informáticos de alto rendimiento (4720). En algunas realizaciones, el analizador sintáctico de datos seguro (4710) puede proporcionar acceso a recursos de alto rendimiento en la nube (por ejemplo, nube (4250), figura 42). Recursos informáticos de alto rendimiento pueden ser servidores informáticos grandes o parques de servidores. Estos recursos informáticos de alto rendimiento pueden proporcionar a usuarios servicios de almacenamiento de datos y servicios de datos flexibles, escalables y configurables.

De acuerdo con otra realización, se puede usar un analizador sintáctico de datos seguro para asegurar el acceso a datos usando máquinas virtuales. Un hipervisor, también denominado monitor de máquina virtual (MMV) es un sistema informático que permite que múltiples máquinas virtuales se ejecuten en un único ordenador anfitrión. La figura 48 muestra un diagrama de bloques ilustrativo que incluye un hipervisor (4800) y una serie de máquinas virtuales (4810) que se ejecutan en el hipervisor (4800). El hipervisor (4800) ejecuta un sistema operativo fundamental (por ejemplo, Microsoft Windows® y Linux). Las máquinas virtuales (4810) se pueden separar del sistema operativo fundamental con cortafuegos, de manera que los ataques (por ejemplo, virus, gusanos, pirateos, etc.) al sistema operativo fundamental no afecten a las máquinas virtuales (4810). Uno o más analizadores sintácticos de datos seguros se pueden integrar con el hipervisor (4800) para asegurar máquinas virtuales (4810). En particular, usando el analizador sintáctico de datos seguro, las máquinas virtuales (4810) se pueden comunicar de manera segura con uno o más servidores o usuarios finales. De acuerdo con esta realización, el acceso a datos seguro se puede desplegar en usuarios proveyendo a los usuarios de imágenes de máquinas virtuales seguras. Esta realización puede permitir compartir información bajo demanda a la vez que asegura la confidencialidad e integridad de los datos.

Las figuras 49 y 50 muestran realizaciones alternativas para integrar un analizador sintáctico de datos seguro con un hipervisor. En la figura 49, el analizador sintáctico de datos seguro (4930) está implementado encima del hipervisor (4920). Por ejemplo, el analizador sintáctico de datos seguro (4930) se puede implementar como un módulo o aplicación de software que funciona en el hipervisor (4920). En algunas realizaciones, el analizador sintáctico de datos seguro (4930) se puede implementar por medio de una máquina virtual que se ejecuta en el hipervisor (4920). Una máquina virtual que se ejecuta en el hipervisor (4920) se puede acoplar de manera segura al servidor (4940) y a usuarios finales (4950) usando el analizador sintáctico de datos seguro (4930). En la figura 50, el analizador sintáctico de datos seguro (5030) está implementado debajo del hipervisor (5020). Por ejemplo, el analizador sintáctico de datos seguro (5030) se puede implementar dentro del hardware del hipervisor (5020). La máquina virtual que se ejecuta en el hipervisor (5020) se puede comunicar de manera segura con el servidor (5040) y usuarios finales (5050) usando el analizador sintáctico de datos seguro (5030).

De acuerdo con otra realización, el analizador sintáctico de datos seguro se puede usar para asegurar canales de comunicaciones de multiplexación por división ortogonal (OFDM). OFDM es un esquema de multiplexación que se usa para comunicación digital de banda ancha. Estándares inalámbricos de banda ancha (por ejemplo, WiMAX y LTE) y banda ancha por línea eléctrica (BPL) usan OFDM. La OFDM es exclusiva porque todos los canales adyacentes son realmente ortogonales. Esto elimina interferencias, cancelación e inducción de ruido. Actualmente, en estos estándares de OFDM, los datos se transmiten a través de un único canal de comunicaciones OFDM. El analizador sintáctico de datos seguro puede asegurar las comunicaciones OFDM dividiendo los datos entre múltiples canales de comunicaciones OFDM. Como se ha descrito anteriormente, dividir datos entre múltiples canales de datos usando el analizador sintáctico de datos seguro asegura los datos porque por cada canal sólo se transmite una parte de los datos. Como beneficio adicional, el analizador sintáctico de datos seguro puede transmitir simultáneamente múltiples partes de datos sobre múltiples canales de datos. Estas transmisiones simultáneas pueden aumentar el ancho de banda real de la transmisión de datos. Adicional o alternativamente, el analizador sintáctico de datos seguro puede transmitir las mismas partes de datos sobre múltiples canales de datos. Esta técnica de transmisión redundante puede aumentar la fiabilidad de transmisión. La figura 51 es un diagrama de bloques ilustrativo para asegurar una red de comunicaciones OFDM. Como se ilustra en la figura 51 un usuario final (5110) puede usar el analizador sintáctico de datos seguro (5120) para enviar datos a través de una red de OFDM (5140) al usuario final (5150). La red de OFDM (5140) puede ser una red de banda ancha inalámbrica, una red de banda ancha por línea eléctrica o cualquier otra red de OFDM adecuada.

De acuerdo con algunas otras realizaciones, el analizador sintáctico de datos seguro se puede usar para proteger controles de infraestructuras críticas que incluyen, por ejemplo, la red eléctrica. El Protocolo de Internet, versión 6 (IPv6) es el Protocolo de Internet de próxima generación. IPv6 tiene un espacio de direcciones más amplio que el Protocolo de Internet actual. Cuando se implemente, el IPv6 permitirá acceder directamente por internet a más

dispositivos. Es importante que se restrinjan los controles de infraestructuras críticas para limitar el acceso a individuos autorizados. Como se ha descrito anteriormente, el analizador sintáctico de datos seguro puede limitar el acceso a recursos de red a usuarios y grupos autorizados. Los sistemas críticos se pueden proteger usando la "regla de dos hombres" según la cual sería necesario que al menos dos usuarios proporcionaran sus claves respectivas para acceder a los sistemas críticos. La figura 52 es un diagrama de bloques ilustrativo para asegurar la red eléctrica. Como se ilustra en la figura 52, un usuario (5210) puede usar un analizador sintáctico de datos seguro (5220) para proporcionar a un usuario final (5250) acceso seguro a la red eléctrica (5240).

En algunas realizaciones, sistemas de red eléctrica se pueden acoplar a internet usando redes de banda ancha por línea eléctrica para eliminar el cableado de red y el equipo asociado de las redes de comunicaciones típicas. Acoplar sistemas de red eléctrica a internet puede posibilitar tecnologías de red inteligente que permiten un uso más eficaz de la energía eléctrica informando del uso en tiempo real. Como otro beneficio, recursos informáticos de gran potencia y/ o equipos de almacenamiento de datos se pueden instalar en equipos de supervisión de potencia conectados a internet. Estos recursos pueden proporcionar un almacenamiento fiable y nodos de procesamiento para proteger datos en la nube.

Como se ha analizado anteriormente haciendo referencia a las figuras 48 a 50, las técnicas de analizador sintáctico de datos seguro que se describen en este documento se pueden aplicar al acceso de datos usando máquinas virtuales y, en particular, a la comunicación entre una máquina virtual y uno o más servidores o usuarios finales. Más adelante se describen sistemas y procedimientos para proporcionar características adicionales de seguridad dentro de entornos informáticos de máquinas virtuales que integran operaciones de seguridad de máquinas anfitrionas y máquinas virtuales.

La figura 53 es un diagrama de bloques de un entorno informático de máquina virtual típico (5300). El entorno (5300) puede incluir hardware subyacente (5302) (que puede incluir componentes de soporte de hardware, tales como aceleradores) y núcleo (5306) (que puede incluir soporte de máquina virtual basada en núcleo (MVN) (5664)). El entorno (5300) también puede incluir una capa de virtualización (5308), que puede incluir QEMU (5660) (un emulador de procesador que actúa como monitor de máquina virtual hospedado, o MMV, como se ha analizado anteriormente haciendo referencia a los hipervisores (4920) y (5020) de las figuras 49 y 50, respectivamente) y vTPM (5662) (un módulo de plataforma virtual de confianza implementado en software). El núcleo (5306) y la virtualización (5308) pueden ser componentes del sistema operativo anfitrión (5380). Una máquina virtual (5310), que puede funcionar en un sistema operativo anfitrión (5380), puede incluir su propio sistema operativo con núcleo (5330) y puede implementar cualquiera de un número de aplicaciones (5320).

La figura 54 es un diagrama de flujo del proceso (5400) para asegurar una máquina virtual, tal como la máquina virtual (5310) de la figura 53. En la etapa (5402), se puede recibir una petición de una operación de seguridad. Una primera máquina virtual que funciona en un sistema operativo anfitrión de un primer dispositivo puede generar la petición. La operación de seguridad pedida en la etapa (5402) puede incluir cualquier operación u operaciones (tales como generar un conjunto de porciones en función de un conjunto de datos, cifrar, descifrar, firmar digitalmente, autenticar, codificar o decodificar una suma de control o cualquier otra operación de seguridad) que mejoran la seguridad de los datos almacenados dentro de la primera máquina virtual o transferidos entre la primera máquina virtual y cualquier dispositivo, servidor, usuario u otra máquina virtual. En algunas implementaciones, la petición recibida en la etapa (5402) puede venir de una aplicación que se ejecuta en la primera máquina virtual. En algunas implementaciones, la petición recibida en la etapa (5402) puede incluir una petición desde la primera máquina virtual para asegurar una comunicación entre la primera máquina virtual y una segunda máquina virtual. La primera máquina virtual puede estar funcionando en el mismo sistema operativo que la segunda máquina virtual o la primera máquina virtual puede estar funcionando en un sistema operativo diferente al de la segunda máquina virtual. La primera máquina virtual, el sistema operativo anfitrión, una segunda máquina virtual, un servidor o cualquier dispositivo informático pueden recibir la petición recibida en la etapa (5406).

En respuesta a la recepción de la petición en la etapa (5402), la operación de seguridad se ejecuta, en la etapa (5404), en un primer módulo de seguridad implementado en un núcleo del sistema operativo anfitrión. El primer módulo de seguridad se puede cargar y descargar en el núcleo bajo demanda, sin que se requiera un reinicio del sistema operativo anfitrión o una reconstrucción del núcleo. Implementando el primer módulo de seguridad como módulo de núcleo, el sistema operativo anfitrión puede proporcionar funcionalidad de módulo de seguridad a nivel del sistema operativo anfitrión a la que pueden acceder las aplicaciones que funcionan a niveles de red, sistema de archivos o virtualización. En algunas implementaciones, la primera máquina virtual y el primer módulo de seguridad del núcleo del sistema operativo anfitrión se pueden comunicar a través de un conducto entre los componentes. Por ejemplo, la petición de la etapa (5402) puede incluir una petición, desde una aplicación de la primera máquina

virtual, para que el primer módulo de seguridad del sistema operativo anfitrión ejecute una operación de seguridad. En otro ejemplo, la petición de la etapa (5402) puede incluir una petición, desde un núcleo del sistema operativo de la primera máquina virtual, para que el primer módulo de seguridad del sistema operativo anfitrión ejecute una operación de seguridad. Llevando a cabo operaciones en el núcleo del sistema operativo anfitrión, el entorno informático de la máquina virtual que funciona de acuerdo con el proceso (5400) se puede beneficiar, por ejemplo, de una gestión centralizada de operaciones de seguridad y componentes de hardware que se controlan de manera más eficaz por medio del sistema operativo anfitrión. Por ejemplo, en algunas implementaciones, en la etapa (5404), el primer módulo de seguridad puede llamar a un componente o aplicación de soporte, tal como un acelerador de hardware. En algunas implementaciones, el primer módulo de seguridad incluye un analizador sintáctico seguro, como se ha descrito en este documento, o está configurado para implementar una o más de las funciones de un analizador sintáctico seguro.

La petición recibida en la etapa (5402) y la subsiguiente ejecución de la operación de seguridad pedida, en la etapa (5404), no es necesario que sean una petición directa al primer módulo de seguridad del núcleo del sistema operativo anfitrión. En algunas implementaciones, la petición de la etapa (5402) incluye una petición para que un segundo módulo de seguridad implementado en un núcleo del sistema operativo de la primera máquina virtual ejecute una operación de seguridad. En la etapa (5404), el primer módulo de seguridad puede ejecutar la operación de seguridad pedida cuando se satisfacen una o más condiciones programadas. En algunas implementaciones, la etapa (5404) puede incluir determinar que el segundo módulo de seguridad (del sistema operativo de la primera máquina virtual) no puede ejecutar la operación de seguridad pedida. El segundo módulo de seguridad podría no poder ejecutar la operación pedida porque el segundo módulo de seguridad está ocupado, no está configurado para llevar a cabo la operación de seguridad pedida, está programado para llevar a cabo la operación de seguridad sólo cuando el primer módulo de seguridad no está disponible o por cualquier otra razón. Por ejemplo, cuando el segundo módulo de seguridad está programado para llevar a cabo la operación de seguridad sólo cuando el primer módulo de seguridad no está disponible, el segundo módulo de seguridad puede transmitir una petición al primer módulo de seguridad para que ejecute la operación de seguridad pedida en la etapa (5402). Si el primer módulo de seguridad responde afirmativamente a la petición (indicando que el primer módulo de seguridad puede llevar a cabo la operación pedida), el segundo módulo de seguridad no llevará a cabo la operación pedida.

En la etapa (5406), el resultado de la operación de seguridad pedida se proporciona a la primera máquina virtual. En algunas implementaciones, el proporcionar el resultado a la primera máquina virtual puede tener lugar cuando los datos se transmiten a otro dispositivo, aplicación o máquina virtual o desde éstos. Por ejemplo, si la primera máquina virtual pide la transferencia segura de datos a una segunda máquina virtual, en la etapa (5402), el resultado de la operación de seguridad pedida se puede proporcionar a la primera máquina virtual cuando el primer módulo de seguridad transfiere los datos de manera segura a la segunda máquina virtual.

La figura 55 es un diagrama de bloques de un entorno informático de máquina virtual seguro (5500) que puede estar configurado para implementar varias técnicas de seguridad de máquinas virtuales, tales como el proceso (5400) que se ha descrito anteriormente. El entorno (5500) puede incluir hardware (5502) y sistema operativo (5580) (que incluye núcleo (5506) y capa de virtualización (5508)). El entorno (5500) también puede incluir un número de máquinas virtuales, tales como máquinas virtuales (5510), (5512) y (5514), una máquina virtual auxiliar (5516) y una máquina virtual de seguridad (5518). Cada una de las máquinas virtuales (5510), (5512) y (5514) puede incluir su propio sistema operativo con núcleos (5530), (5532) y (5534), respectivamente, y aplicaciones (5520), (5522) y (5524), respectivamente. La máquina virtual auxiliar (5516) puede incluir núcleo (5536) y puede estar configurada con servicios (5526) que ayudan en funciones de máquina virtual, tales como crear máquinas virtuales a partir de una máquina física, recuperar máquinas virtuales que fallan y otras tareas de administración de máquinas virtuales. La máquina virtual de seguridad (5518) puede estar configurada para ejecutar operaciones de seguridad en nombre de otras máquinas virtuales implementadas en el entorno (5500) o aplicaciones locales o remotas.

La figura 55 también ilustra un número de módulos de seguridad que se pueden implementar en diferentes ubicaciones en el entorno (5500). El número y la ubicación de los módulos de seguridad de la figura 55 son sólo ilustrativos y se puede usar uno cualquiera o más de dichos módulos de seguridad en cualquiera de un número de capas o máquinas virtuales diferentes del sistema operativo anfitrión (5580). Por ejemplo, el entorno (5500) incluye un módulo de seguridad (5576) implementado en un núcleo (5506) del sistema operativo (5580). El entorno (5500) puede estar configurado para funcionar de acuerdo con el proceso (5400) de la figura 54, que se ha analizado anteriormente, en el que el módulo de seguridad (5576) puede ejecutar operaciones de seguridad para una cualquiera o más de las máquinas virtuales (5510), (5512), (5514), (5516) y (5518).

El entorno (5500) también ilustra un número de módulos de seguridad que se pueden implementar en varias

máquinas virtuales. Un módulo de seguridad (5570) está implementado en un núcleo (5530) de la máquina virtual (5510) y puede llevar a cabo operaciones de seguridad para aplicaciones (5520) que se ejecutan en la máquina virtual (5510) o para cualquier otra máquina virtual o aplicación que pida una operación de seguridad. Los módulos de seguridad (5576) (del núcleo (5506) del sistema operativo anfitrión (5580)) y (5570) (del núcleo (5530) de la máquina virtual (5510)) pueden estar configurados para funcionar como el primer y el segundo módulo de seguridad, respectivamente, que se han analizado anteriormente haciendo referencia al proceso (5400) de la figura 54. Por ejemplo, operaciones de seguridad pedidas por aplicaciones (5520) de la máquina virtual (5510) se pueden transmitir al módulo de seguridad (5570). Si el módulo de seguridad (5576) está disponible para llevar a cabo la operación de seguridad, el módulo de seguridad (5570) puede remitir la petición al módulo de seguridad (5576), de lo contrario, el módulo de seguridad (5570) puede llevar a cabo la operación pedida.

El entorno (5500) también ilustra un módulo de seguridad (5572), que está implementado como parte de aplicaciones (5524) de la máquina virtual (5514). En una configuración de este tipo, un usuario u otra aplicación pueden invitar al módulo de seguridad (5572) a llevar a cabo operaciones de seguridad. El módulo de seguridad (5572) puede pedir que el módulo de seguridad (5576) (del núcleo (5506) del sistema operativo anfitrión (5580)) lleve a cabo una operación de seguridad (por ejemplo, cifrar datos, generar una pluralidad de porciones de datos) en nombre de aplicaciones (5524). Un módulo de seguridad también se puede implementar en una máquina virtual de seguridad dedicada, tal como un módulo de seguridad (5574) de la máquina virtual de seguridad (5518). El módulo de seguridad (5574) puede proporcionar operaciones de seguridad o una u otras más máquinas virtuales, locales o remotas, y también puede estar configurado para comunicarse con el módulo de seguridad (5576) del sistema operativo anfitrión (5580), como se ha descrito anteriormente haciendo referencia al proceso (5400) de la figura 54. En algunas implementaciones, otras máquinas virtuales (tales como las máquinas virtuales (5510), (5512), (5514) y (5516) pueden invitar a la máquina virtual (5518) a ejecutar operaciones de seguridad para funciones de máquinas virtuales internas o funciones de máquinas intervirtuales.

La configuración de un entorno informático de máquina virtual seguro con uno o más módulos de seguridad se puede llevar a cabo con uno o más componentes de hardware o software proporcionados a un entrono informático.

Si bien anteriormente se han descrito algunas aplicaciones de las técnicas de seguridad de datos, se debería entender claramente que la presente invención se puede integrar con cualquier aplicación de red a fin de aumentar la seguridad, la tolerancia a fallos, el anonimato y cualquier combinación adecuada de los anteriores. Por ejemplo, los procedimientos y sistemas de seguridad de máquinas virtuales que se describen en este documento se pueden usar conjuntamente con un algoritmo de dispersión de información que se describe en este documento (por ejemplo, los que lleva a cabo el analizador sintáctico de datos seguro) o cualquier otro algoritmo de dispersión de información que genere porciones de datos.

Adicionalmente, otras combinaciones, incorporaciones, sustituciones y modificaciones resultarán evidentes para el experto en la materia en vista de la descripción de este documento.

REIVINDICACIONES

1. Un procedimiento para asegurar datos, comprendiendo el procedimiento:

recibir una petición de una operación de seguridad desde una primera máquina virtual que funciona en un sistema operativo anfitrión de un primer dispositivo, donde la petición la llevará a cabo uno de una pluralidad de módulos de seguridad que incluyen un primer módulo de seguridad y donde la petición comprende una petición para asegurar la comunicación entre la primera máquina virtual y una segunda máquina virtual;

en respuesta a la recepción de la petición, ejecutar la operación de seguridad en el primer módulo de seguridad implementado en un núcleo del sistema operativo anfitrión y

proporcionar un resultado de la operación de seguridad a la primera máquina virtual.

2. El procedimiento de la reivindicación 1, donde la petición desde la primera máquina virtual es una petición desde una aplicación que se ejecuta en la primera máquina virtual.

3. El procedimiento de la reivindicación 2, donde la petición desde la aplicación que se ejecuta en la primera máquina virtual es una petición para que el primer módulo de seguridad ejecute una operación de seguridad.

4. El procedimiento de la reivindicación 1, donde ejecutar la operación de seguridad en el primer módulo de seguridad comprende generar una pluralidad de porciones, donde cada una de la pluralidad de porciones contiene una distribución de datos a partir de un conjunto de datos.

5. El procedimiento de la reivindicación 4, donde ejecutar la operación de seguridad en el primer módulo de seguridad comprende además cifrar el conjunto de datos.

6. El procedimiento de la reivindicación 1, donde la petición de la operación de seguridad desde la primera máquina virtual es una petición para que un segundo módulo de seguridad implementado en un núcleo de un sistema operativo de la primera máquina virtual ejecute una operación de seguridad, donde el segundo módulo de seguridad es uno de una pluralidad de módulos de seguridad.

7. El procedimiento de la reivindicación 6, donde ejecutar la operación de seguridad en el primer módulo de seguridad comprende determinar que el segundo módulo de seguridad no puede ejecutar la operación de seguridad pedida.

8. El procedimiento de la reivindicación 7, donde ejecutar la operación de seguridad en el primer módulo de seguridad comprende recibir una petición, en el primer módulo de seguridad desde el segundo módulo de seguridad, para ejecutar la operación pedida.

9. El procedimiento de la reivindicación 6, donde ejecutar la operación de seguridad en el primer módulo de seguridad comprende determinar que el primer módulo de seguridad puede ejecutar la operación de seguridad pedida.

10. El procedimiento de la reivindicación 1, donde la segunda máquina virtual está funcionando en el sistema operativo anfitrión del primer dispositivo.

11. El procedimiento de la reivindicación 1, donde ejecutar la operación de seguridad del primer módulo de seguridad comprende llamar a un acelerador de hardware desde el núcleo del sistema operativo anfitrión.

12. El procedimiento de la reivindicación 1, donde el primer módulo de seguridad incluye un analizador sintáctico seguro.

13. Un sistema para asegurar datos, comprendiendo el sistema:

un procesador configurado para:

ejecutar un sistema operativo anfitrión que tiene un núcleo y

llevar a cabo el procedimiento de acuerdo con una cualquiera de las reivindicaciones 1 a 12.

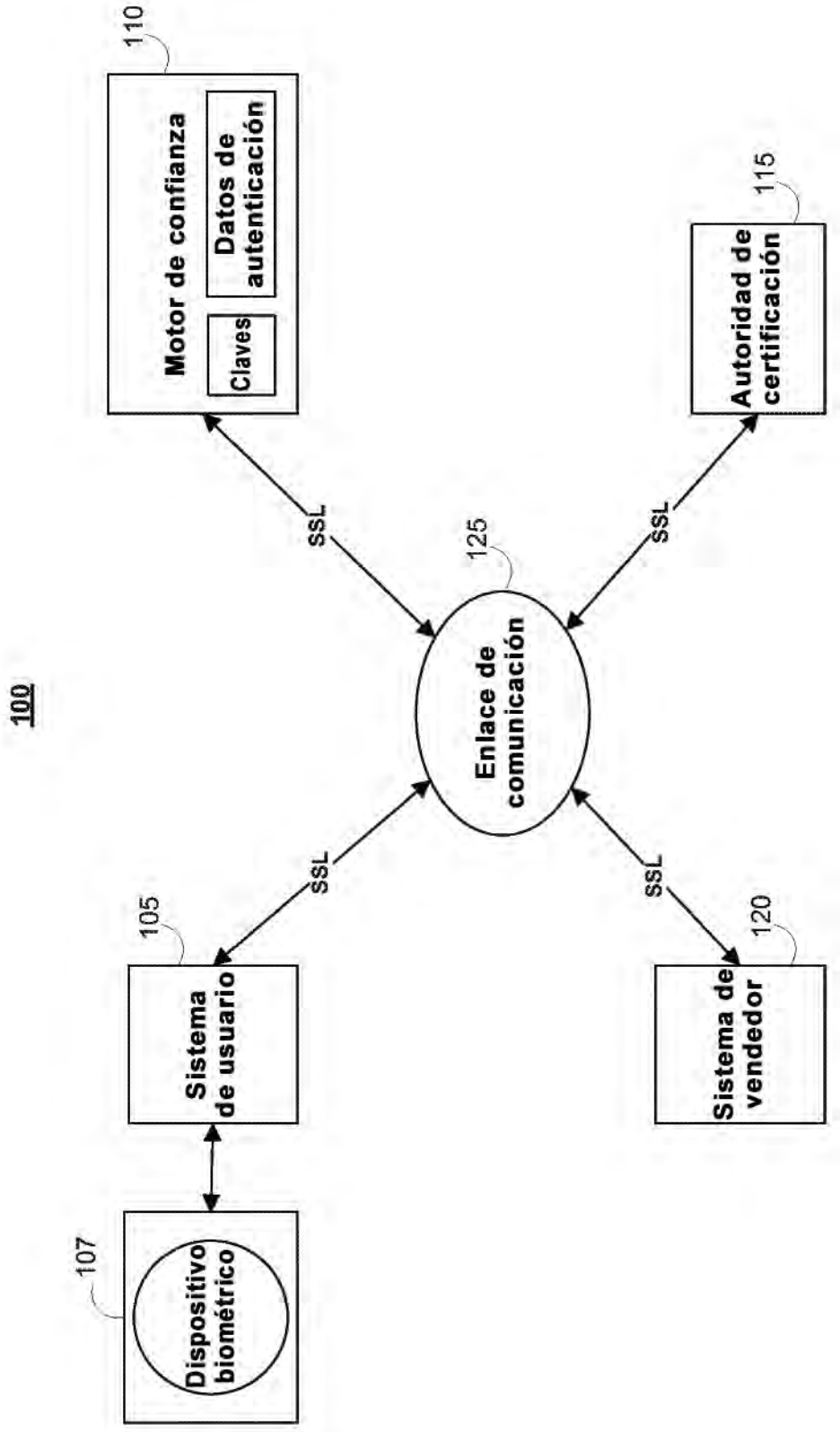

100
110
Motor de confianza
Datos de autenticación
Claves
115
Autoridad de certificación
SSL
SSL
125
Enlace de comunicación
SSL
SSL
105
Sistema de usuario
120
Sistema de vendedor
107
Dispositivo biométrico

FIG. 1

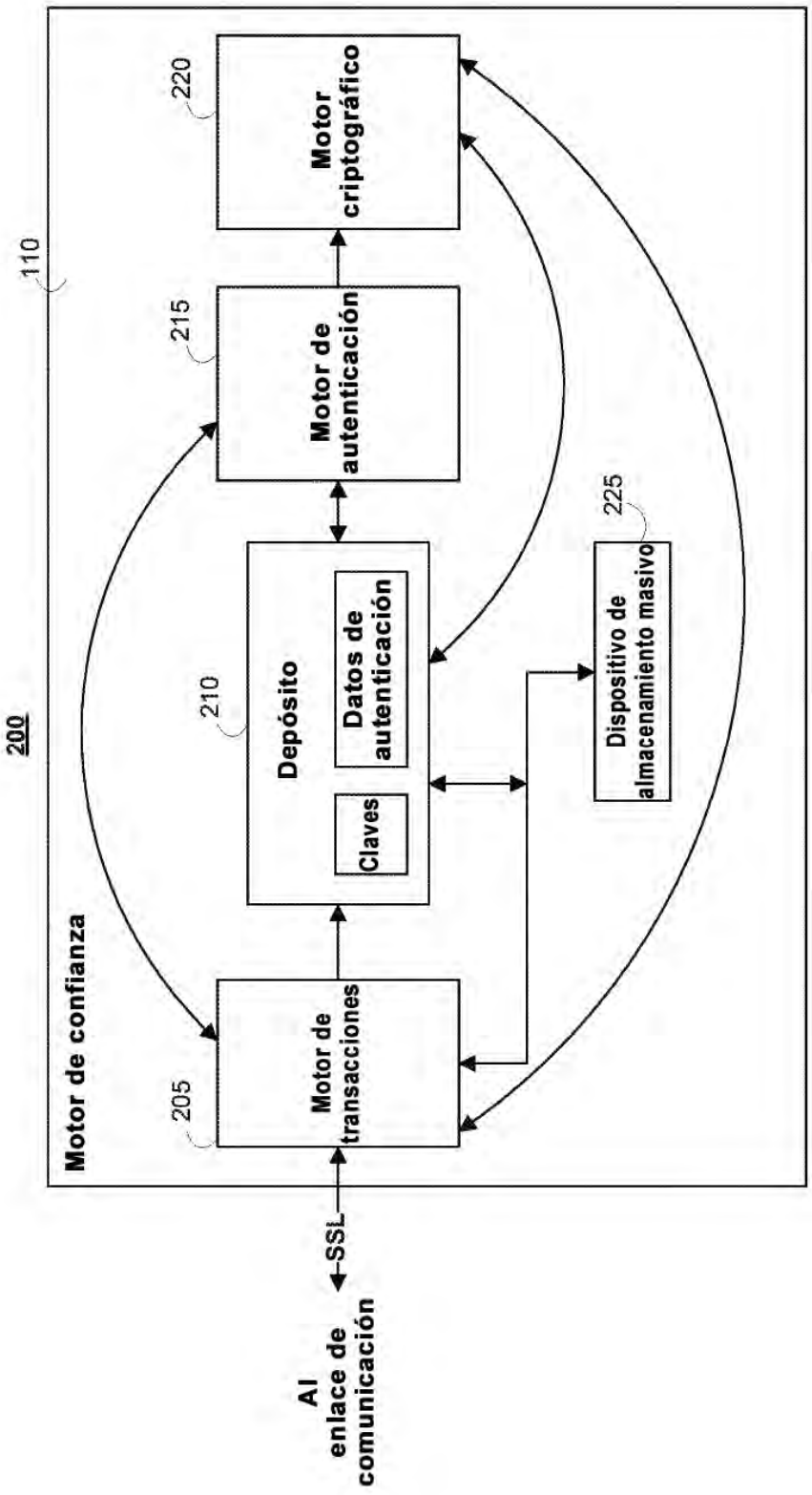

200
Motor de confianza
110
Motor de transacciones
205
Depósito
210
Claves
Datos de autenticación
Motor de autenticación
215
Motor criptográfico
220
Dispositivo de almacenamiento masivo
225
SSL
Al enlace de comunicación

FIG. 2

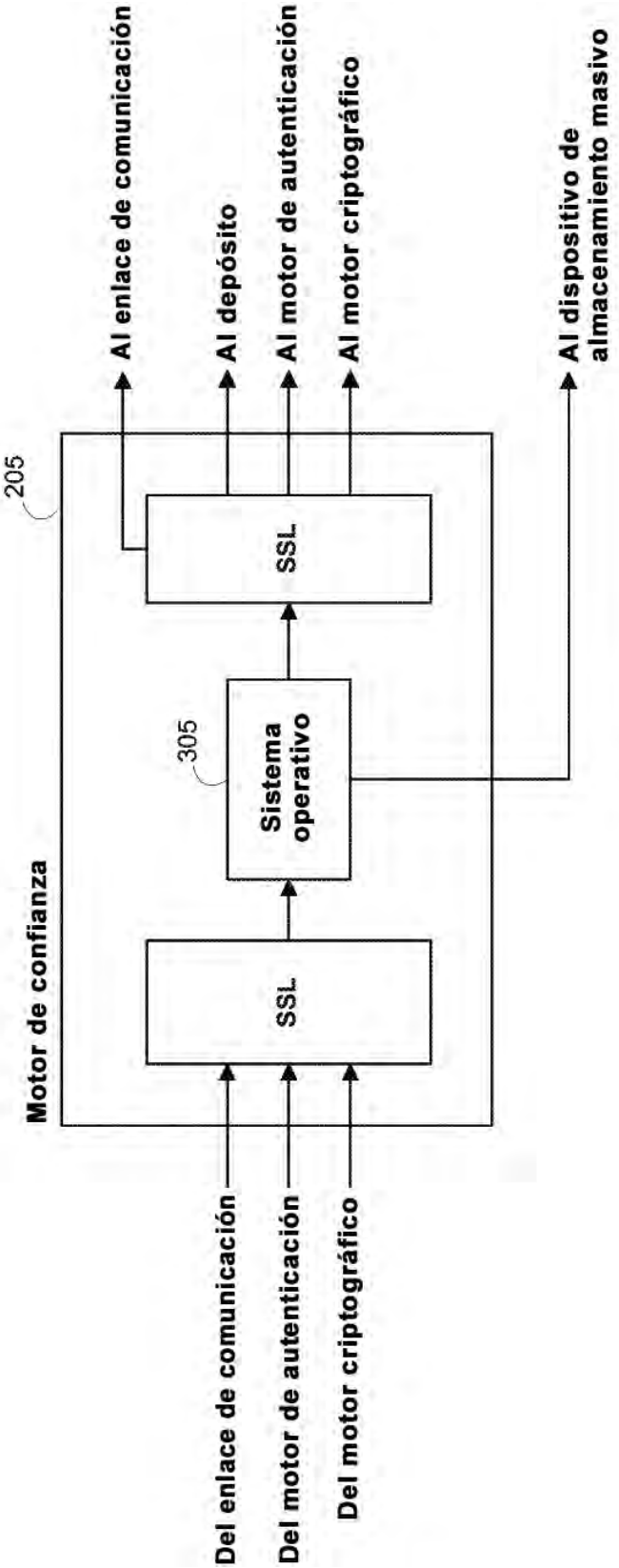

Al enlace de comunicación
Al depósito
Al motor de autenticación
Al motor criptográfico
Al dispositivo de almacenamiento masivo
205
SSL
305
Sistema operativo
SSL
Motor de confianza
Del enlace de comunicación
Del motor de autenticación
Del motor criptográfico

FIG. 3

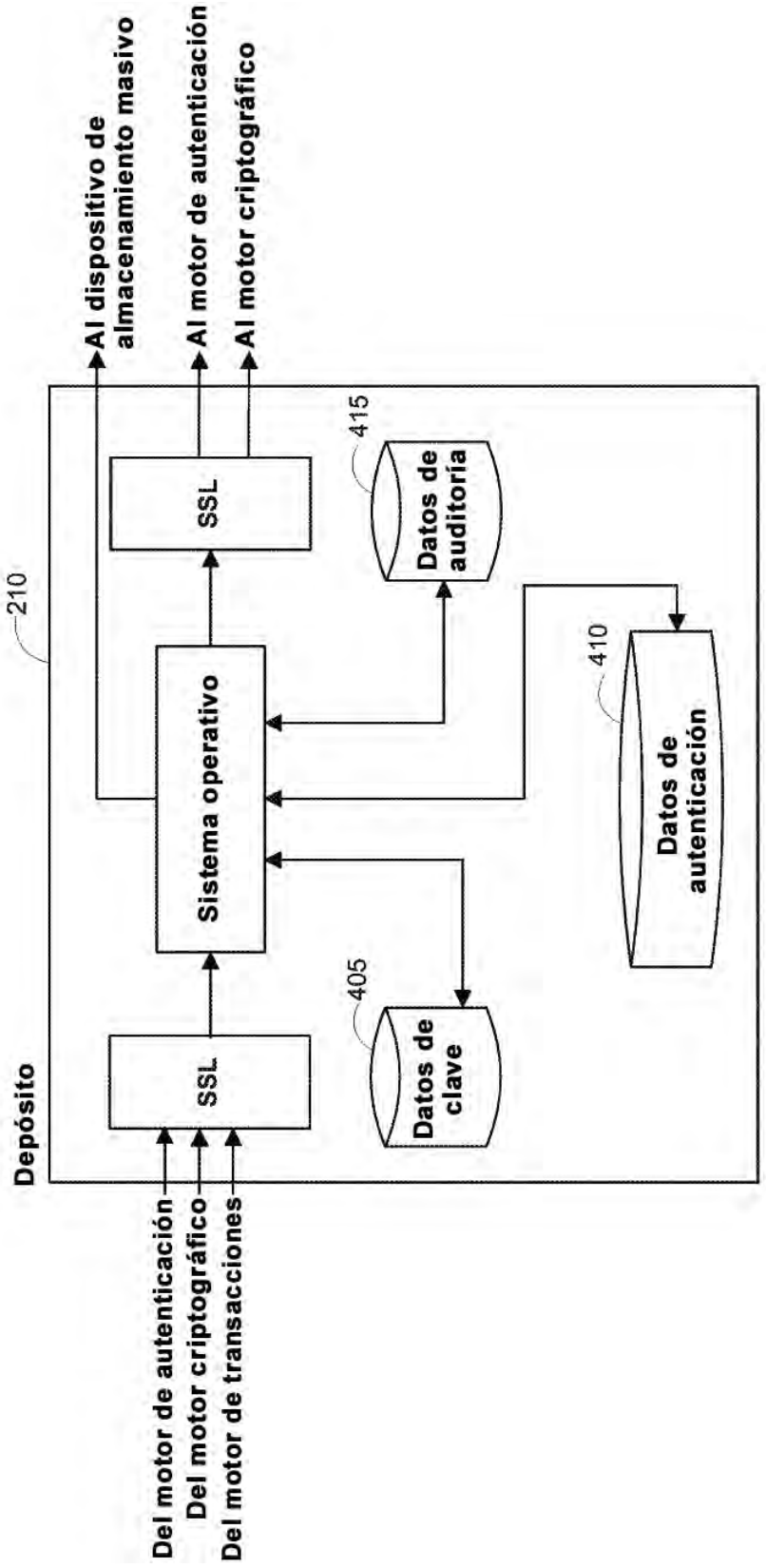

Depósito
210
Del motor de autenticación
Del motor criptográfico
Del motor de transacciones
SSL
SSL
Sistema operativo
405
Datos de clave
410
Datos de autenticación
415
Datos de auditoría
Al dispositivo de almacenamiento masivo
Al motor de autenticación
Al motor criptográfico

FIG. 4

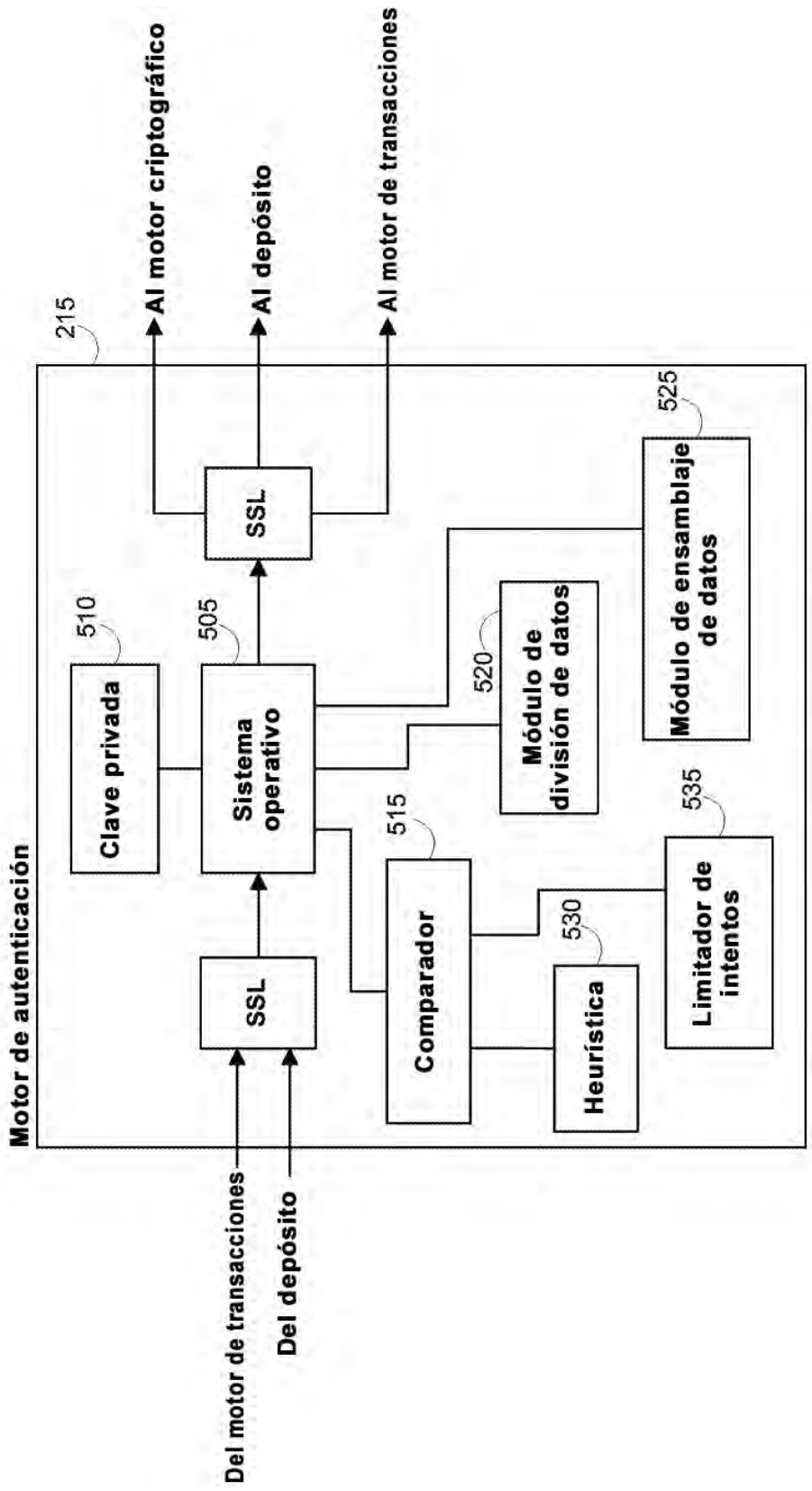

Motor de autenticación
215
Al motor criptográfico
Al depósito
Al motor de transacciones
SSL
Clave privada
510
Sistema operativo
505
SSL
Comparador
515
Heurística
530
Módulo de división de datos
520
Módulo de ensamblaje de datos
525
Limitador de intentos
535
Del motor de transacciones
Del depósito

FIG. 5

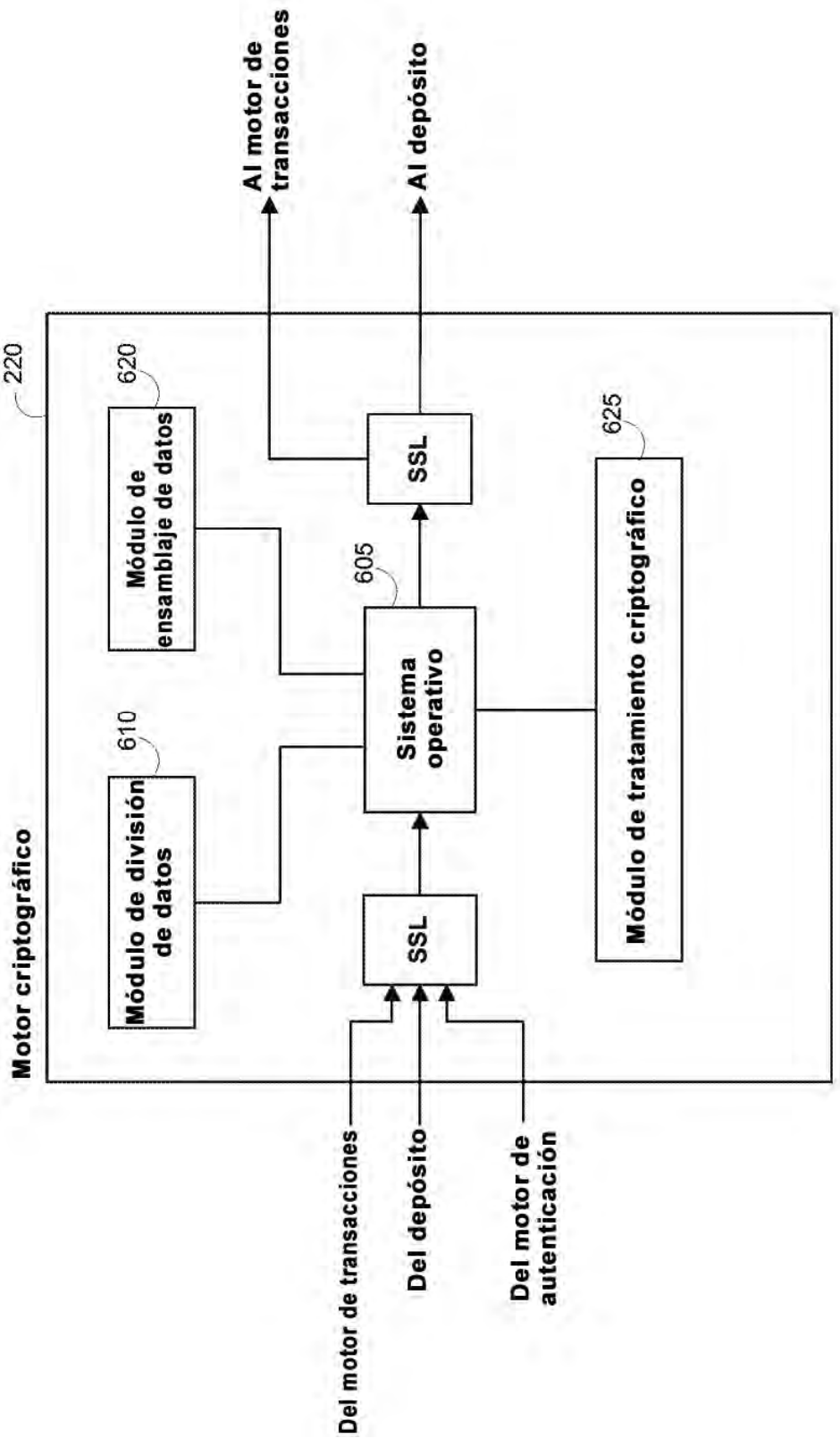

Motor criptográfico
220
Módulo de división de datos
610
Módulo de ensamblaje de datos
620
Sistema operativo
605
SSL
SSL
Módulo de tratamiento criptográfico
625
Del motor de transacciones
Del depósito
Del motor de autenticación
Al motor de transacciones
Al depósito

FIG. 6

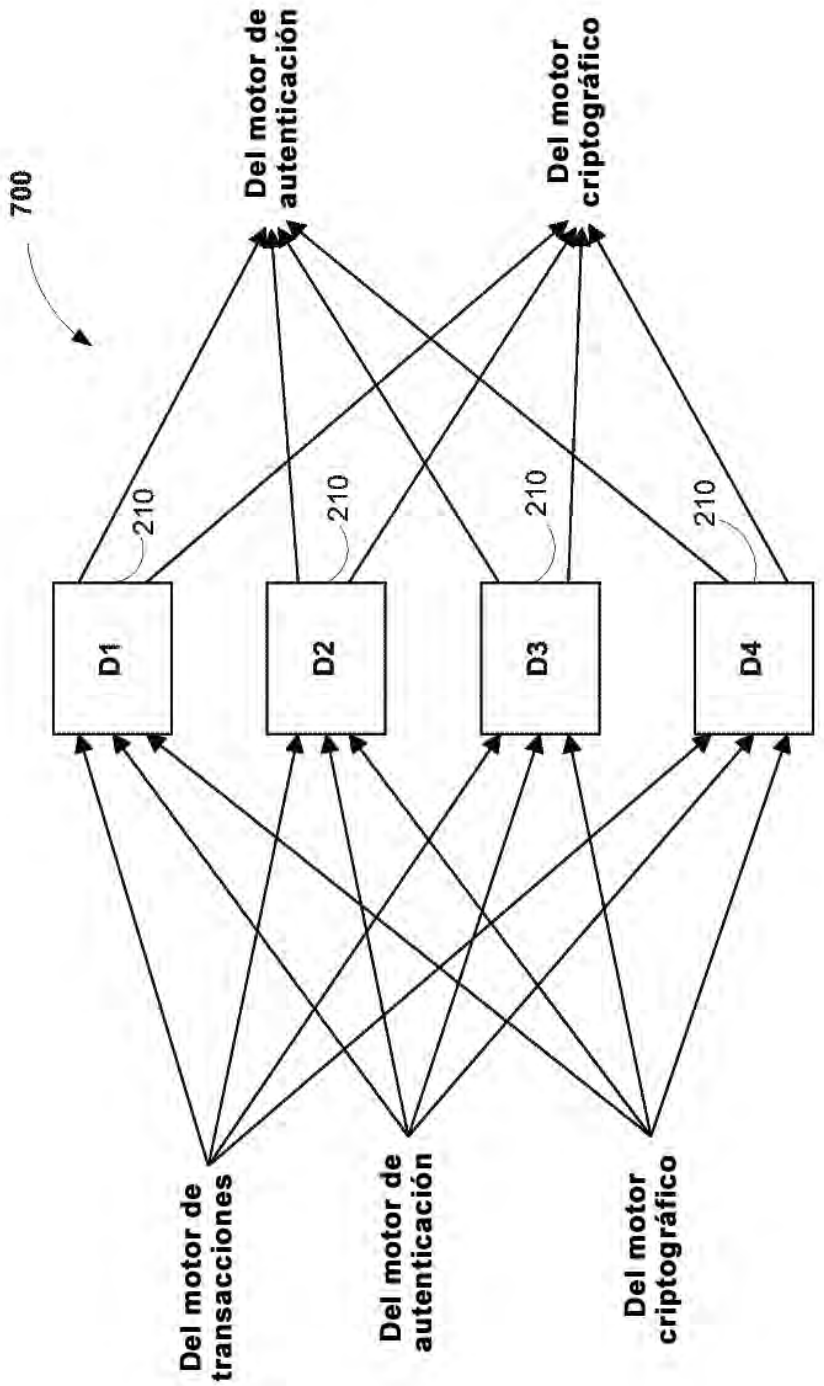

700
Del motor de autenticación
Del motor criptográfico
210
210
210
210
D1
D2
D3
D4
Del motor de transacciones
Del motor de autenticación
Del motor criptográfico

FIG. 7

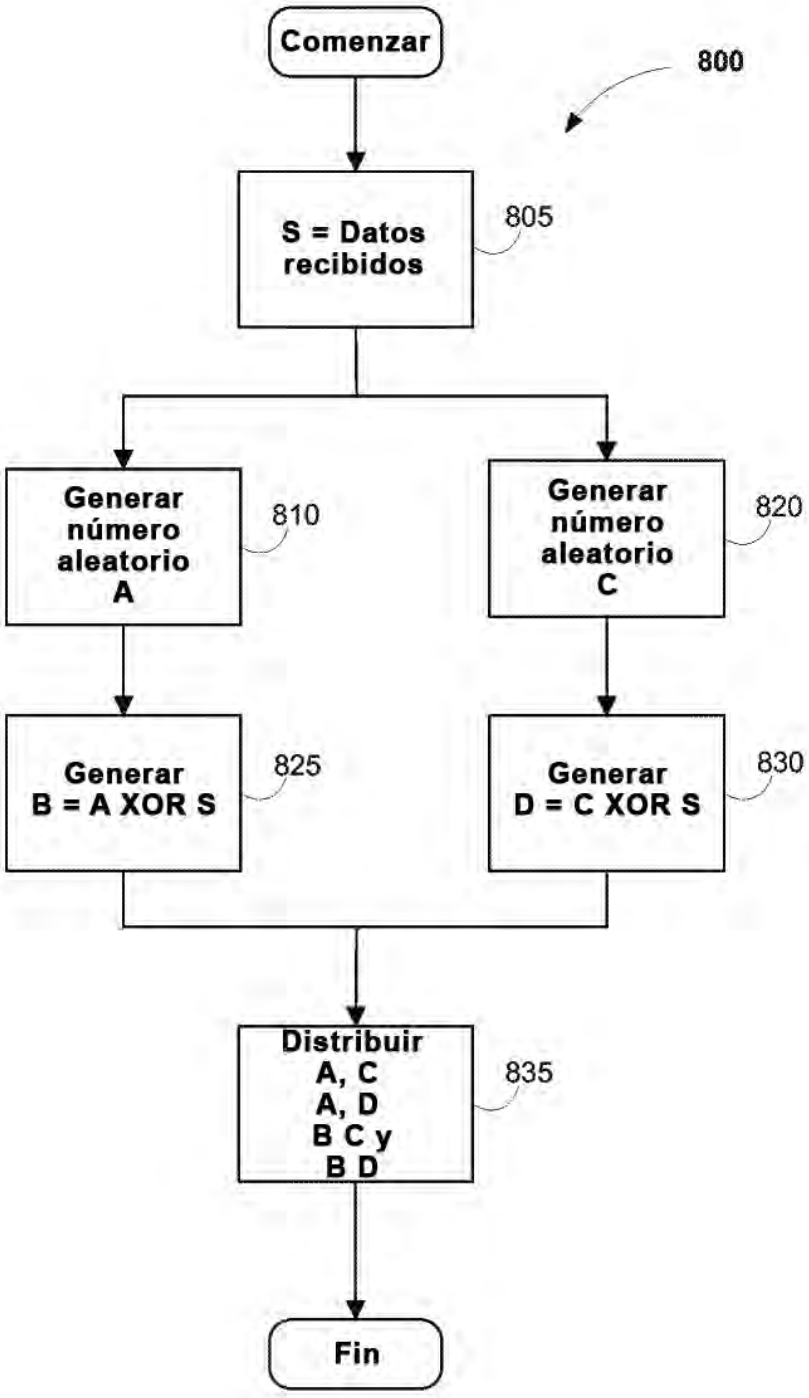
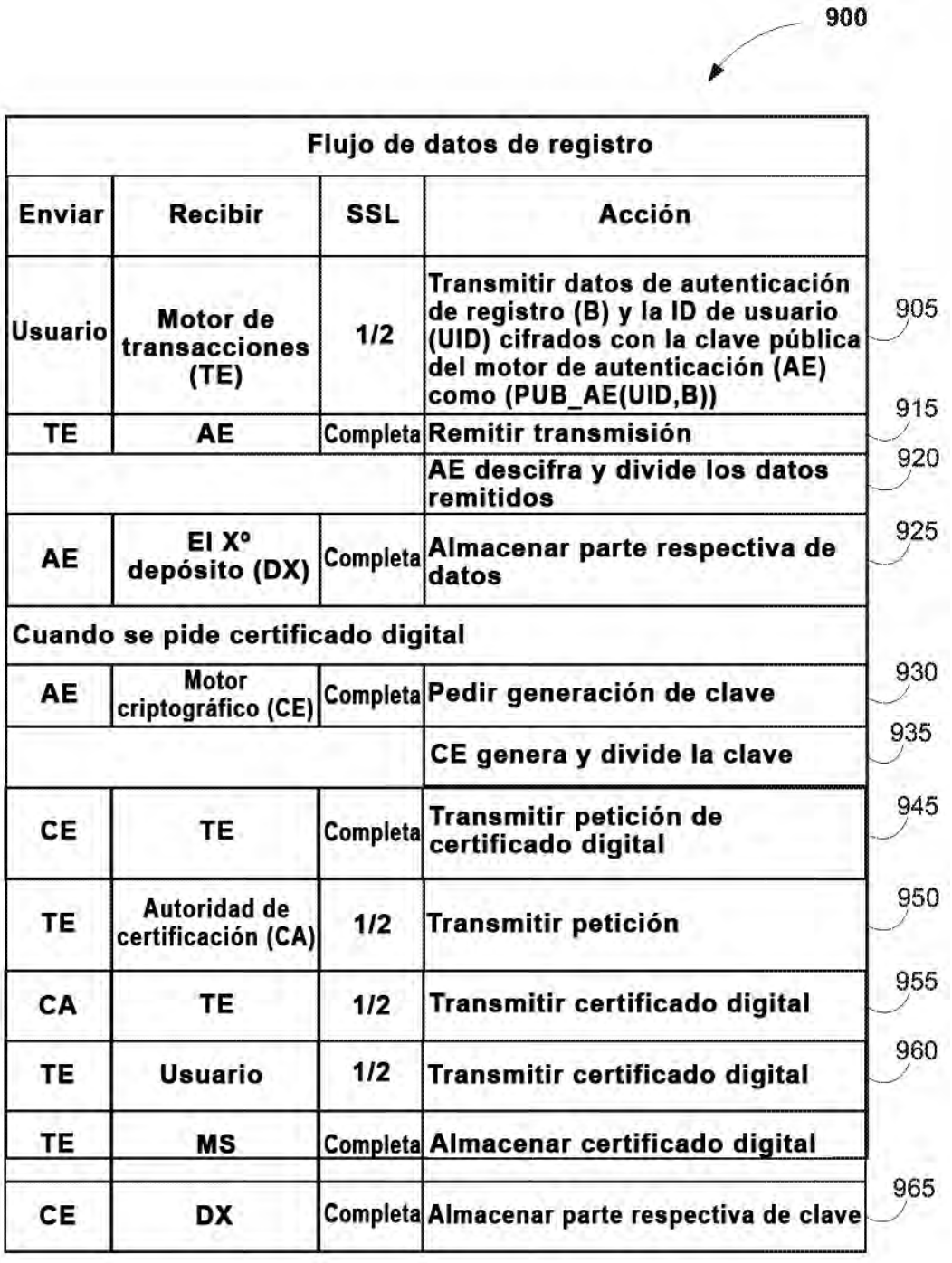

Comenzar
800
S = Datos recibidos
805
Generar número aleatorio A
810
Generar número aleatorio C
820
Generar B = A XOR S
825
Generar D = C XOR S
830
Distribuir A, C A, D B C y B D
835
Fin

FIG. 8



Flujo de datos de registro			
Enviar	**Recibir**	**SSL**	**Acción**
Usuario	Motor de transacciones (TE)	1/2	Transmitir datos de autenticación de registro (B) y la ID de usuario (UID) cifrados con la clave pública del motor de autenticación (AE) como (PUB_AE(UID,B))
TE	AE	Completa	Remitir transmisión
			AE descifra y divide los datos remitidos
AE	El Xº depósito (DX)	Completa	Almacenar parte respectiva de datos
Cuando se pide certificado digital			
AE	Motor criptográfico (CE)	Completa	Pedir generación de clave
			CE genera y divide la clave
CE	TE	Completa	Transmitir petición de certificado digital
TE	Autoridad de certificación (CA)	1/2	Transmitir petición
CA	TE	1/2	Transmitir certificado digital
TE	Usuario	1/2	Transmitir certificado digital
TE	MS	Completa	Almacenar certificado digital
CE	DX	Completa	Almacenar parte respectiva de clave

FIG. 9, Panel A

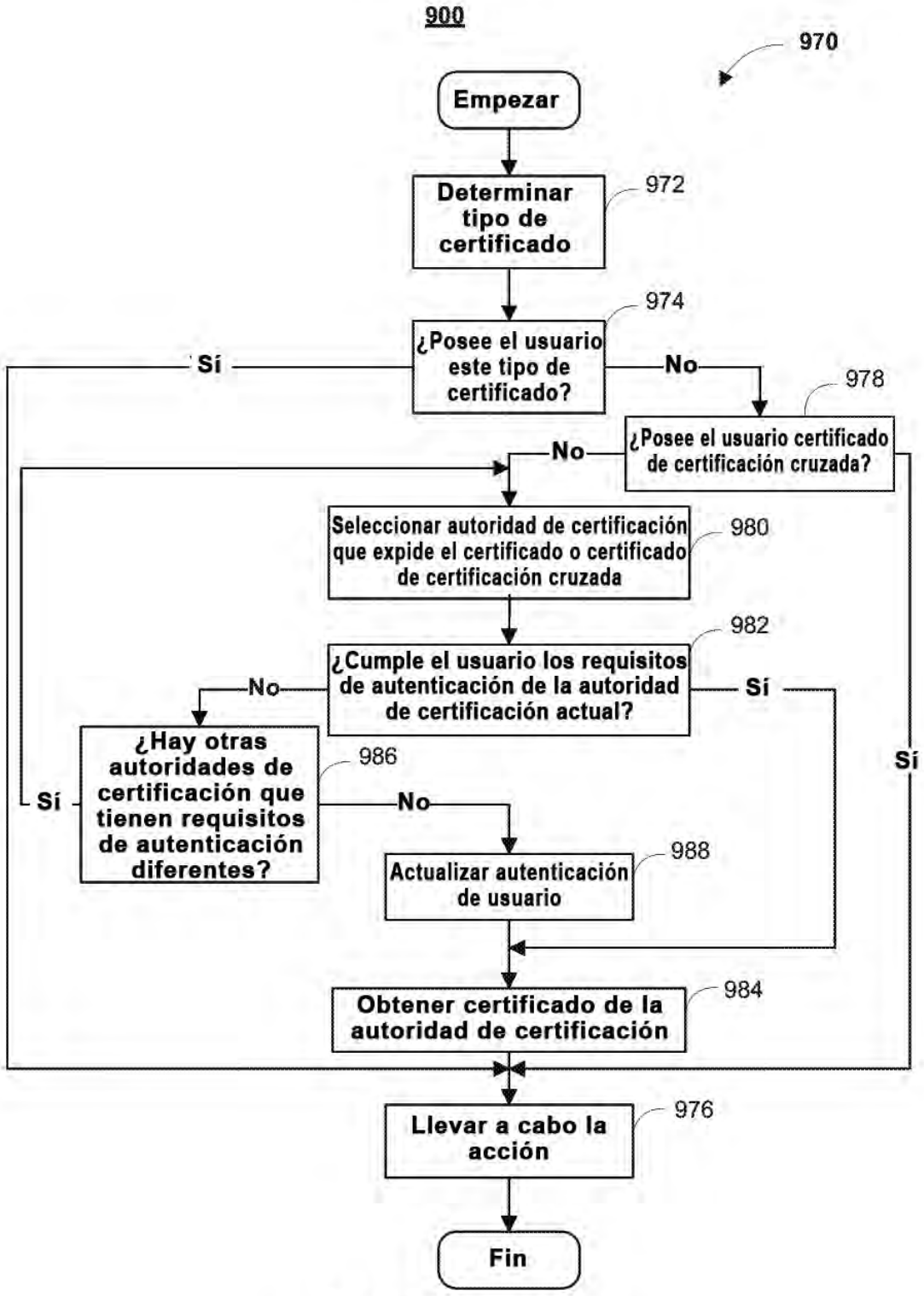

900
970
Empezar
Determinar tipo de certificado
972
¿Posee el usuario este tipo de certificado?
974
Sí
No
¿Posee el usuario certificado de certificación cruzada?
978
No
Seleccionar autoridad de certificación que expide el certificado o certificado de certificación cruzada
980
¿Cumple el usuario los requisitos 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
Sí
Actualizar autenticación de usuario
988
Obtener certificado de la autoridad de certificación
984
Llevar a cabo la acción
976
Fin

FIG. 9, Panel B

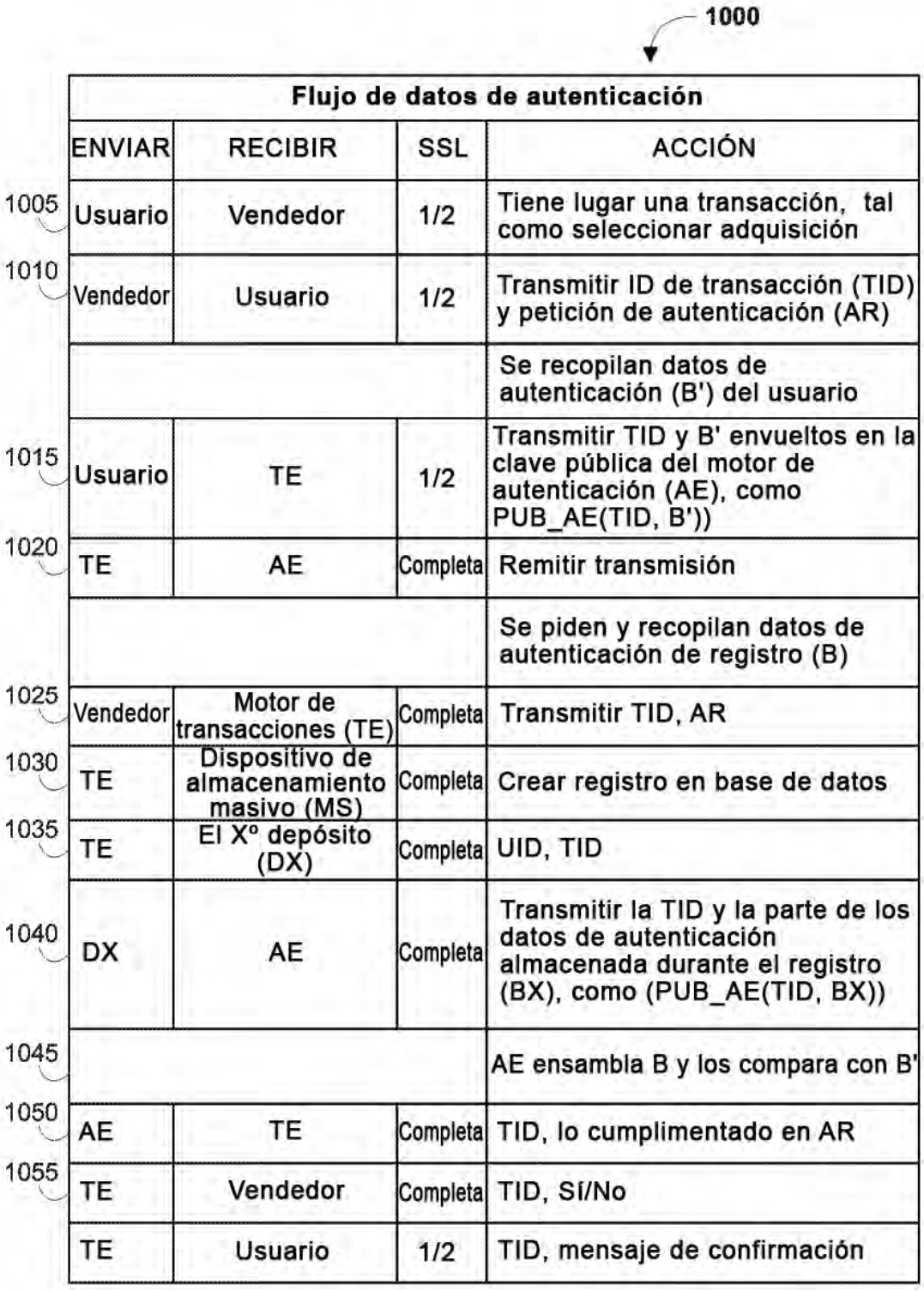
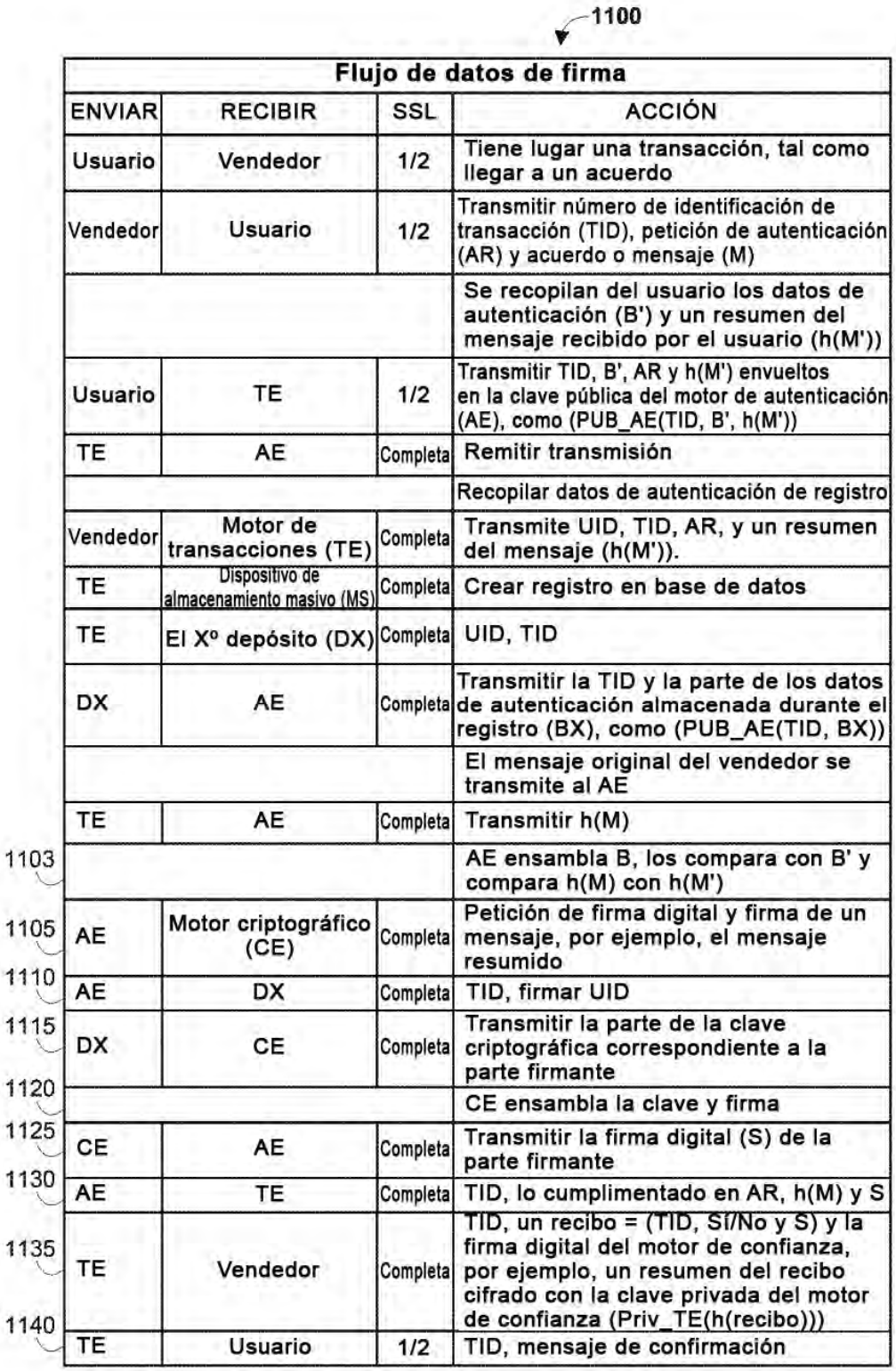

1000
Flujo de datos de autenticación
ENVIAR
RECIBIR
SSL
ACCIÓN
1005
Usuario
Vendedor
1/2
Tiene lugar una transacción, tal como seleccionar adquisición
1010
Vendedor
Usuario
1/2
Transmitir ID de transacción (TID) y petición de autenticación (AR)
Se recopilan datos de autenticación (B') del usuario
1015
Usuario
TE
1/2
Transmitir TID y B' envueltos en la clave pública del motor de autenticación (AE), como PUB_AE(TID, B'))
1020
TE
AE
Completa
Remitir transmisión
Se piden y recopilan datos de autenticación de registro (B)
1025
Vendedor
Motor de transacciones (TE)
Completa
Transmitir TID, AR
1030
TE
Dispositivo de almacenamiento masivo (MS)
Completa
Crear registro en base de datos
1035
TE
El Xº depósito (DX)
Completa
UID, TID
1040
DX
AE
Completa
Transmitir la TID y la parte de los datos de autenticación almacenada durante el registro (BX), como (PUB_AE(TID, BX))
1045
AE ensambla B y los compara con B'
1050
AE
TE
Completa
TID, lo cumplimentado en AR
1055
TE
Vendedor
Completa
TID, Sí/No
TE
Usuario
1/2
TID, mensaje de confirmación

FIG. 10



Flujo de datos de firma			
ENVIAR	RECIBIR	SSL	ACCIÓN
Usuario	Vendedor	1/2	Tiene lugar una transacción, tal como llegar a un acuerdo
Vendedor	Usuario	1/2	Transmitir número de identificación de transacción (TID), petición de autenticación (AR) y acuerdo o mensaje (M)
			Se recopilan del usuario los datos de autenticación (B') y un resumen 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	Remitir transmisión
			Recopilar datos de autenticación de registro
Vendedor	Motor de transacciones (TE)	Completa	Transmite UID, TID, AR, y un resumen del mensaje (h(M')).
TE	Dispositivo de almacenamiento masivo (MS)	Completa	Crear registro en base de datos
TE	El Xº depósito (DX)	Completa	UID, TID
DX	AE	Completa	Transmitir la TID y la parte de los datos de autenticación almacenada durante el registro (BX), como (PUB_AE(TID, BX))
			El mensaje original del vendedor se transmite al AE
TE	AE	Completa	Transmitir h(M)
			AE ensambla B, los compara con B' y compara h(M) con h(M')
AE	Motor criptográfico (CE)	Completa	Petición de firma digital y firma de un mensaje, por ejemplo, el mensaje resumido
AE	DX	Completa	TID, firmar UID
DX	CE	Completa	Transmitir la parte de la clave criptográfica correspondiente a la parte firmante
			CE ensambla la clave y firma
CE	AE	Completa	Transmitir la firma digital (S) de la parte firmante
AE	TE	Completa	TID, lo cumplimentado en AR, h(M) y S
TE	Vendedor	Completa	TID, un recibo = (TID, Sí/No y S) y la firma digital del motor de confianza, por ejemplo, un resumen del recibo cifrado con la clave privada del motor de confianza (Priv_TE(h(recibo)))
TE	Usuario	1/2	TID, mensaje de confirmación

FIG. 11

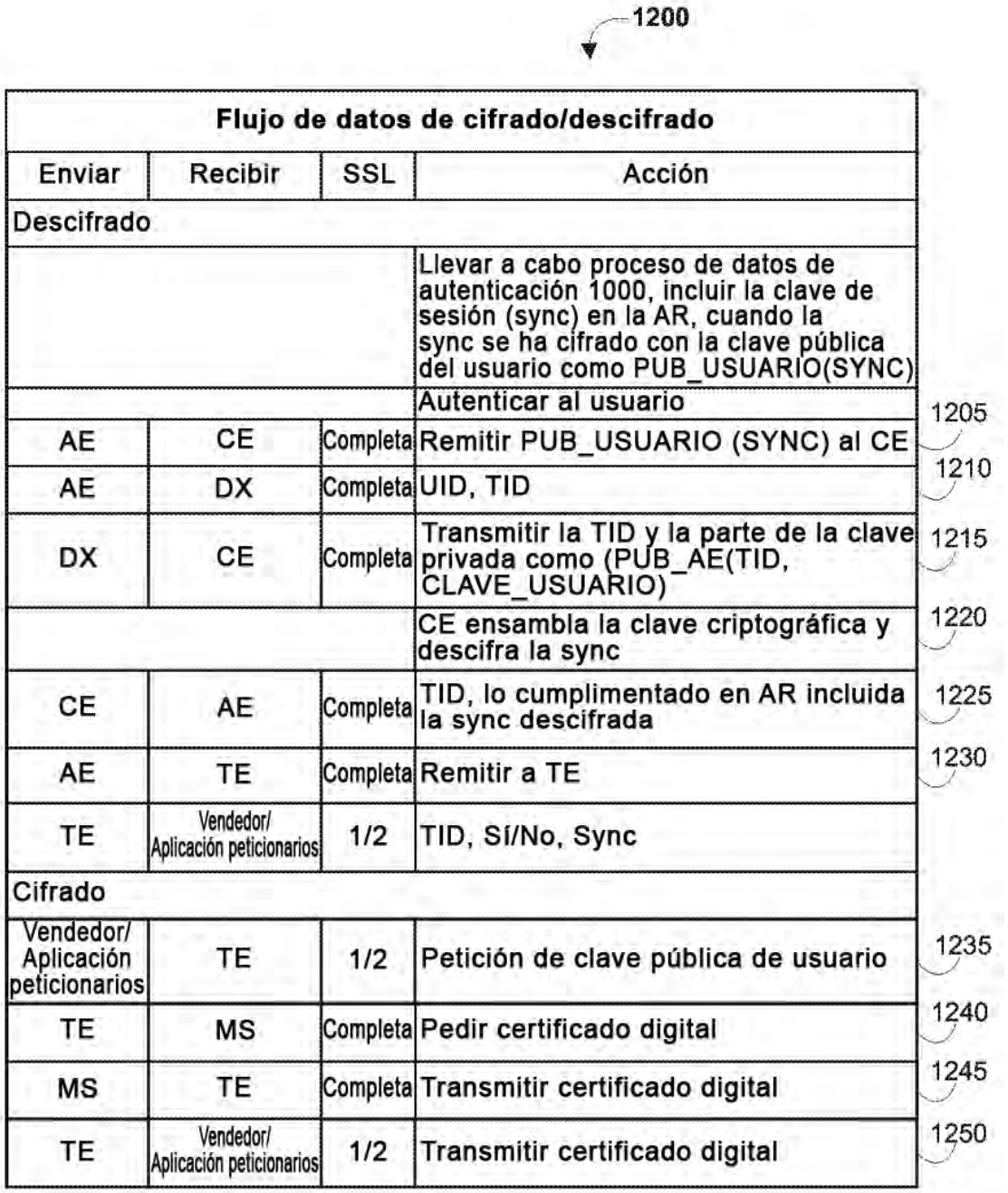

1200
Flujo de datos de cifrado/descifrado
Enviar
Recibir
SSL
Acción
Descifrado
Llevar a cabo proceso de datos de autenticación 1000, incluir la clave de sesión (sync) en la AR, cuando la sync se ha cifrado con la clave pública del usuario como PUB_USUARIO(SYNC)
Autenticar al usuario
1205
AE
CE
Completa
Remitir PUB_USUARIO (SYNC) al CE
1210
AE
DX
Completa
UID, TID
DX
CE
Completa
Transmitir la TID y la parte de la clave privada como (PUB_AE(TID, CLAVE_USUARIO)
1215
1220
CE ensambla la clave criptográfica y descifra la sync
CE
AE
Completa
TID, lo cumplimentado en AR incluida la sync descifrada
1225
AE
TE
Completa
Remitir a TE
1230
TE
Vendedor/ Aplicación peticionarios
1/2
TID, Sí/No, Sync
Cifrado
Vendedor/ Aplicación peticionarios
TE
1/2
Petición de clave pública de usuario
1235
TE
MS
Completa
Pedir certificado digital
1240
MS
TE
Completa
Transmitir certificado digital
1245
TE
Vendedor/ Aplicación peticionarios
1/2
Transmitir certificado digital
1250

FIG. 12

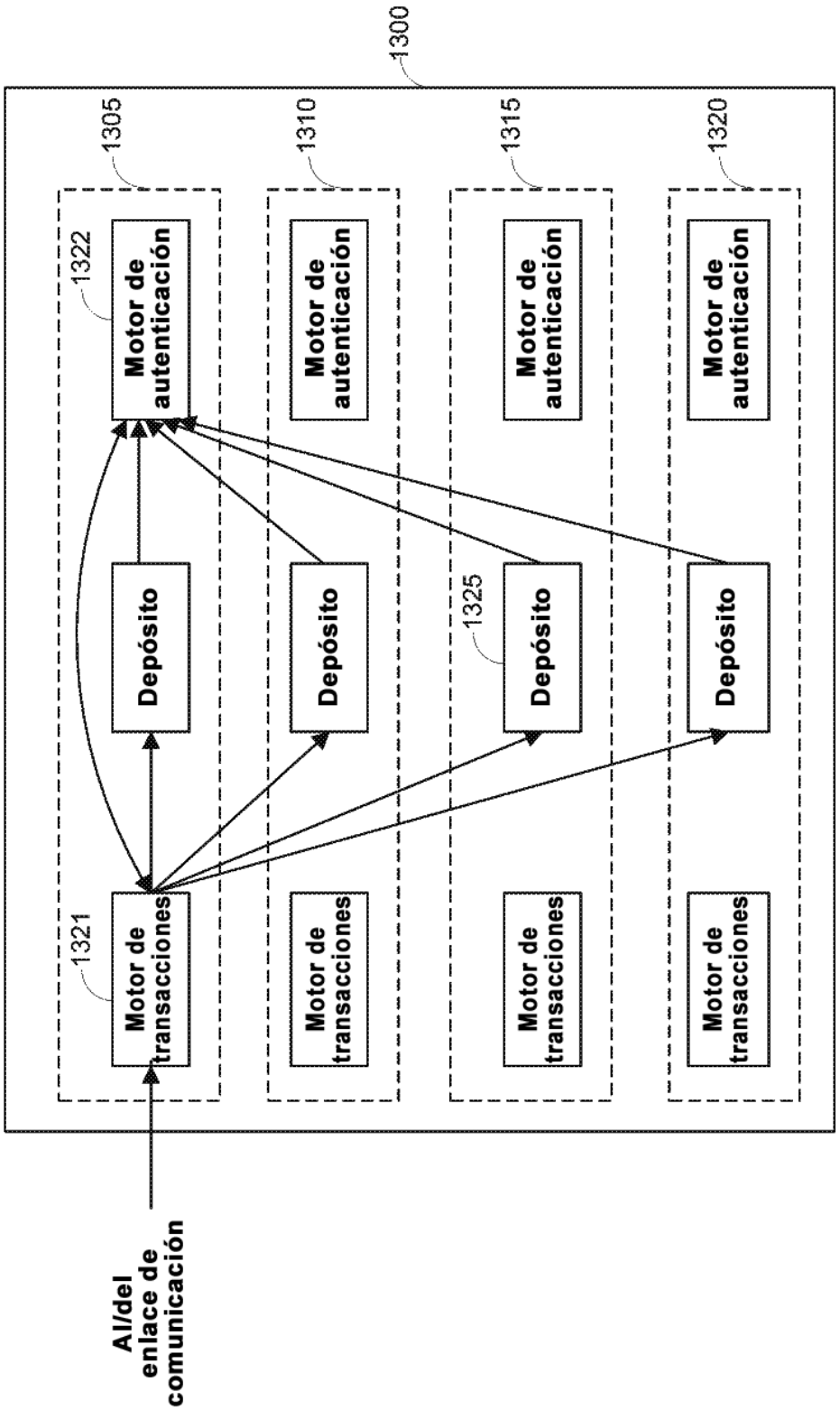

1300
1305
1310
1315
1320
1322
1321
1325
Motor de autenticación
Depósito
Motor de transacciones
Al/del enlace de comunicación

FIG. 13

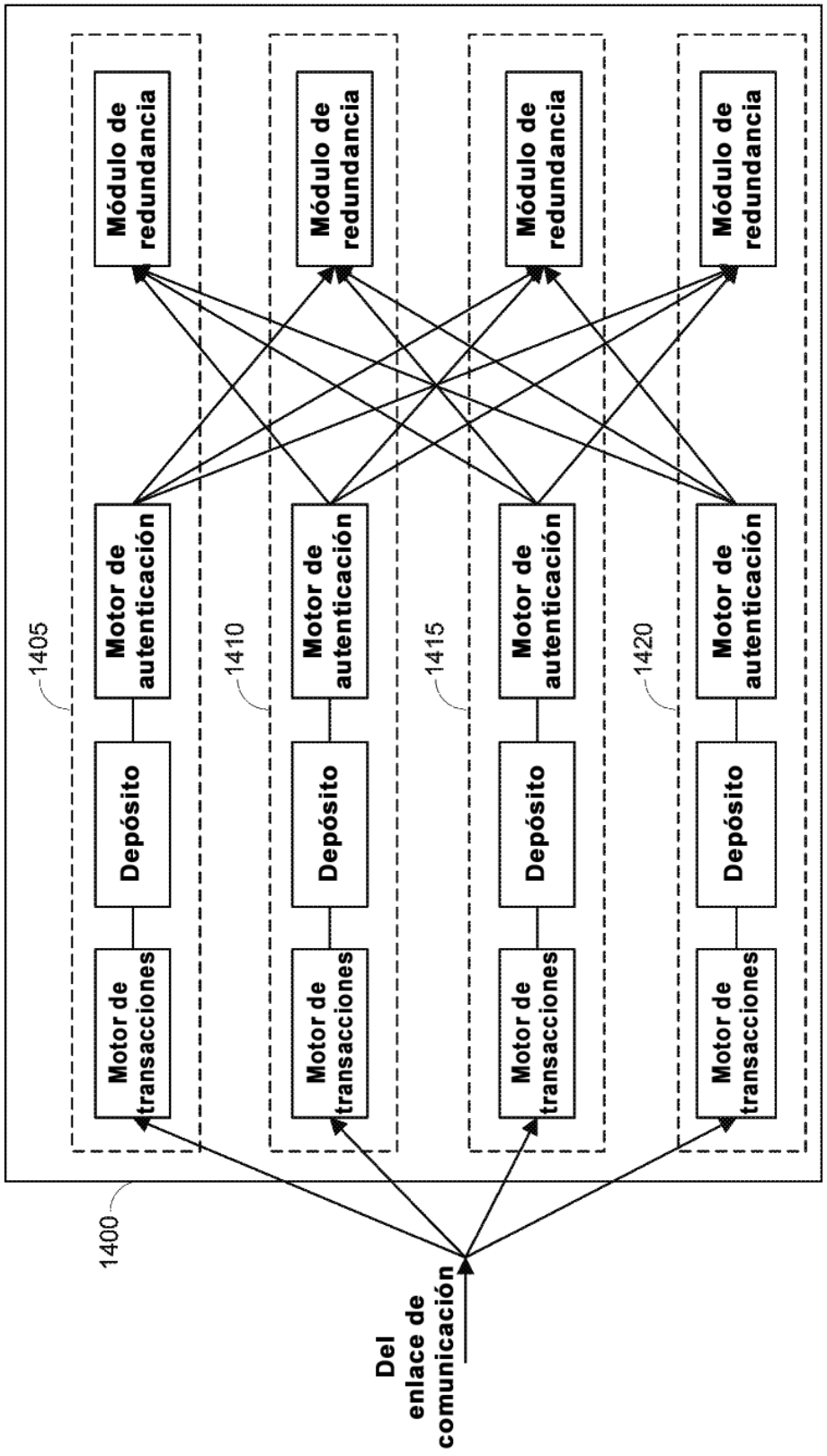

Del enlace de comunicación
1400
1405
1410
1415
1420
Motor de transacciones
Depósito
Motor de autenticación
Módulo de redundancia

FIG. 14

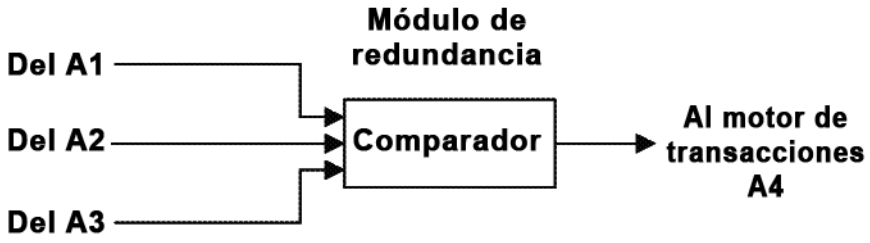

Módulo de redundancia
Del A1
Del A2
Del A3
Comparador
Al motor de transacciones A4

FIG. 15

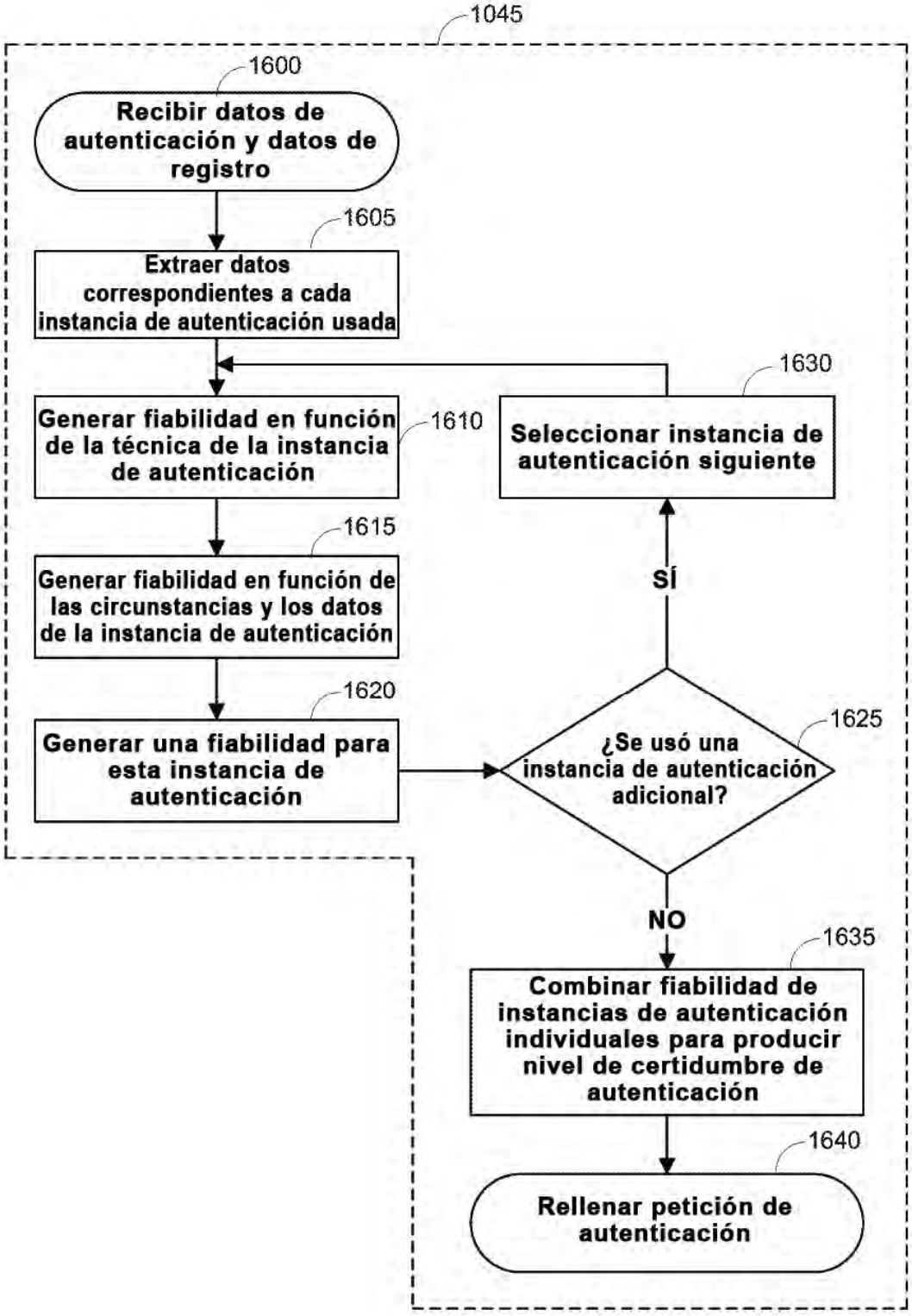

1045
1600
Recibir datos de autenticación y datos de registro
1605
Extraer datos correspondientes a cada instancia de autenticación usada
1610
Generar fiabilidad en función de la técnica de la instancia de autenticación
1615
Generar fiabilidad en función de las circunstancias y los datos de la instancia de autenticación
1620
Generar una fiabilidad para esta instancia de autenticación
1625
¿Se usó una instancia de autenticación adicional?
SÍ
1630
Seleccionar instancia de autenticación siguiente
NO
1635
Combinar fiabilidad de instancias de autenticación individuales para producir nivel de certidumbre de autenticación
1640
Rellenar petición de autenticación

FIG. 16

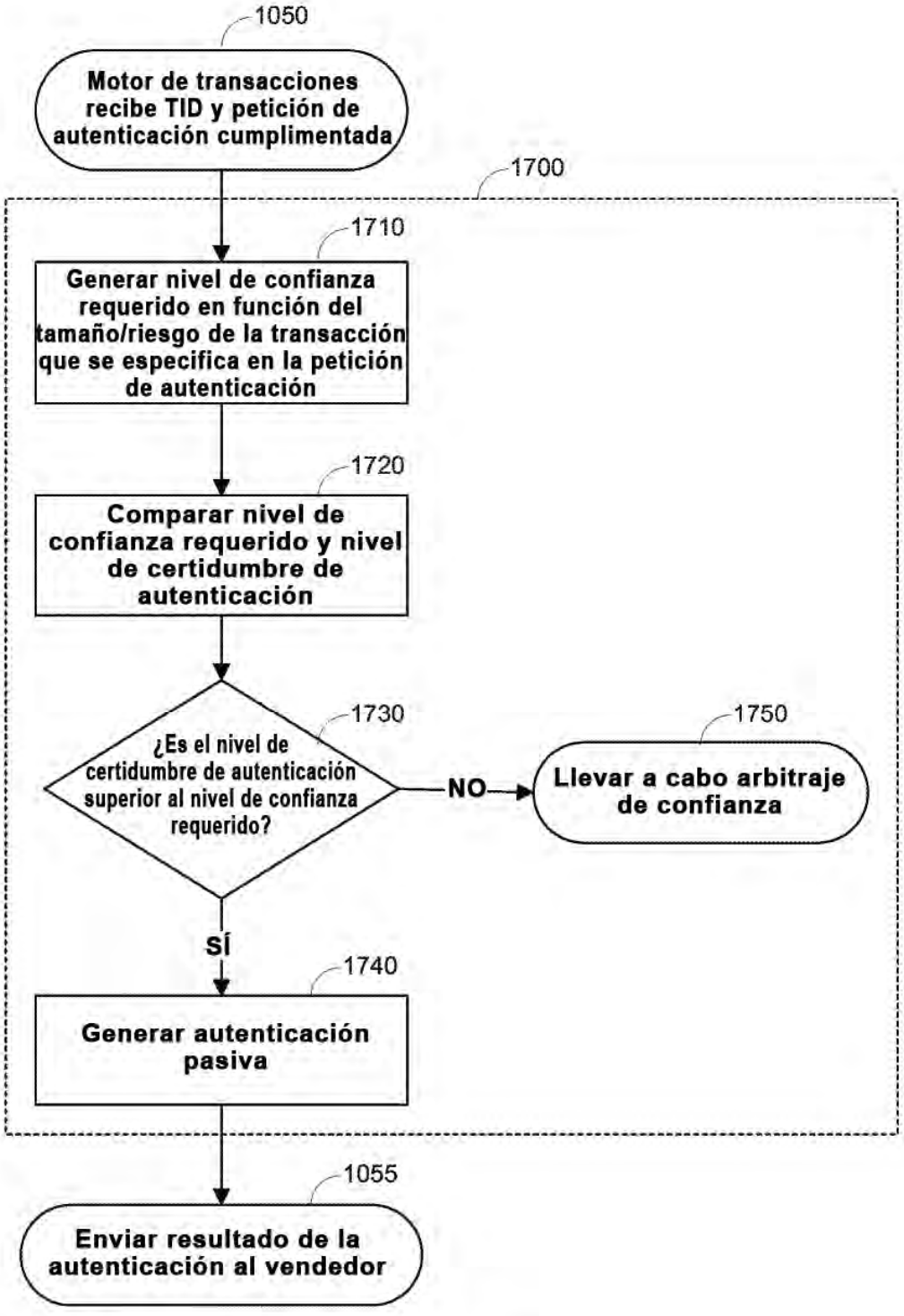

1050
Motor de transacciones recibe TID y petición de autenticación cumplimentada
1700
1710
Generar nivel de confianza requerido en función del tamaño/riesgo de la transacción que se especifica en la petición de autenticación
1720
Comparar nivel de confianza requerido y nivel de certidumbre de autenticación
1730
¿Es el nivel de certidumbre de autenticación superior al nivel de confianza requerido?
NO
1750
Llevar a cabo arbitraje de confianza
SÍ
1740
Generar autenticación pasiva
1055
Enviar resultado de la autenticación al vendedor

FIG. 17

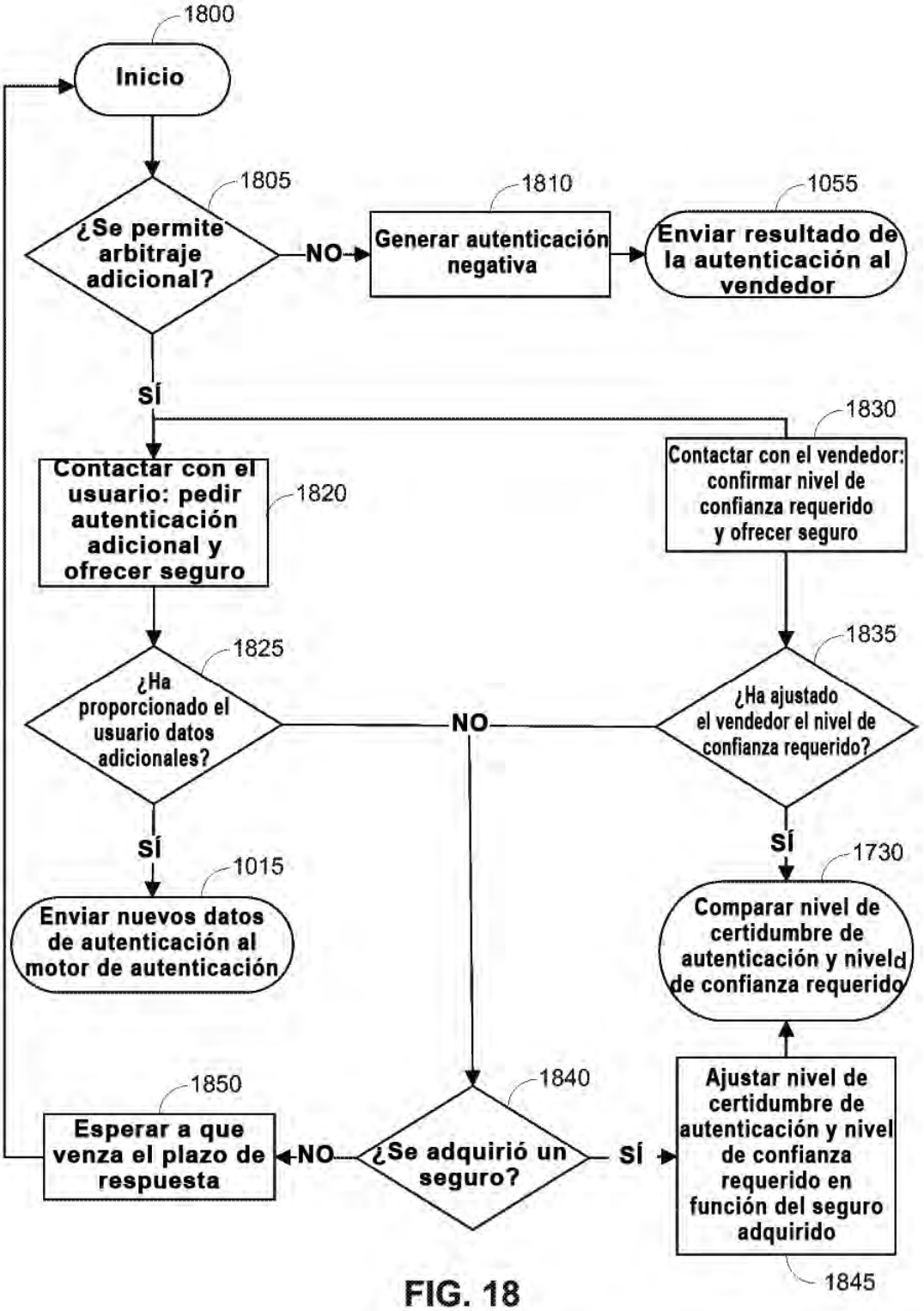

1800
Inicio
1805
¿Se permite arbitraje adicional?
NO
1810
Generar autenticación negativa
1055
Enviar resultado de la autenticación al vendedor
SÍ
1830
Contactar con el vendedor: confirmar nivel de confianza requerido y ofrecer seguro
Contactar con el usuario: pedir autenticación adicional y ofrecer seguro
1820
1825
¿Ha proporcionado el usuario datos adicionales?
NO
1835
¿Ha ajustado el vendedor el nivel de confianza requerido?
SÍ
1730
Comparar nivel de certidumbre de autenticación y nivel de confianza requerido
SÍ
1015
Enviar nuevos datos de autenticación al motor de autenticación
1850
Esperar a que venza el plazo de respuesta
NO
1840
¿Se adquirió un seguro?
SÍ
Ajustar nivel de certidumbre de autenticación y nivel de confianza requerido en función del seguro adquirido
1845

FIG. 18

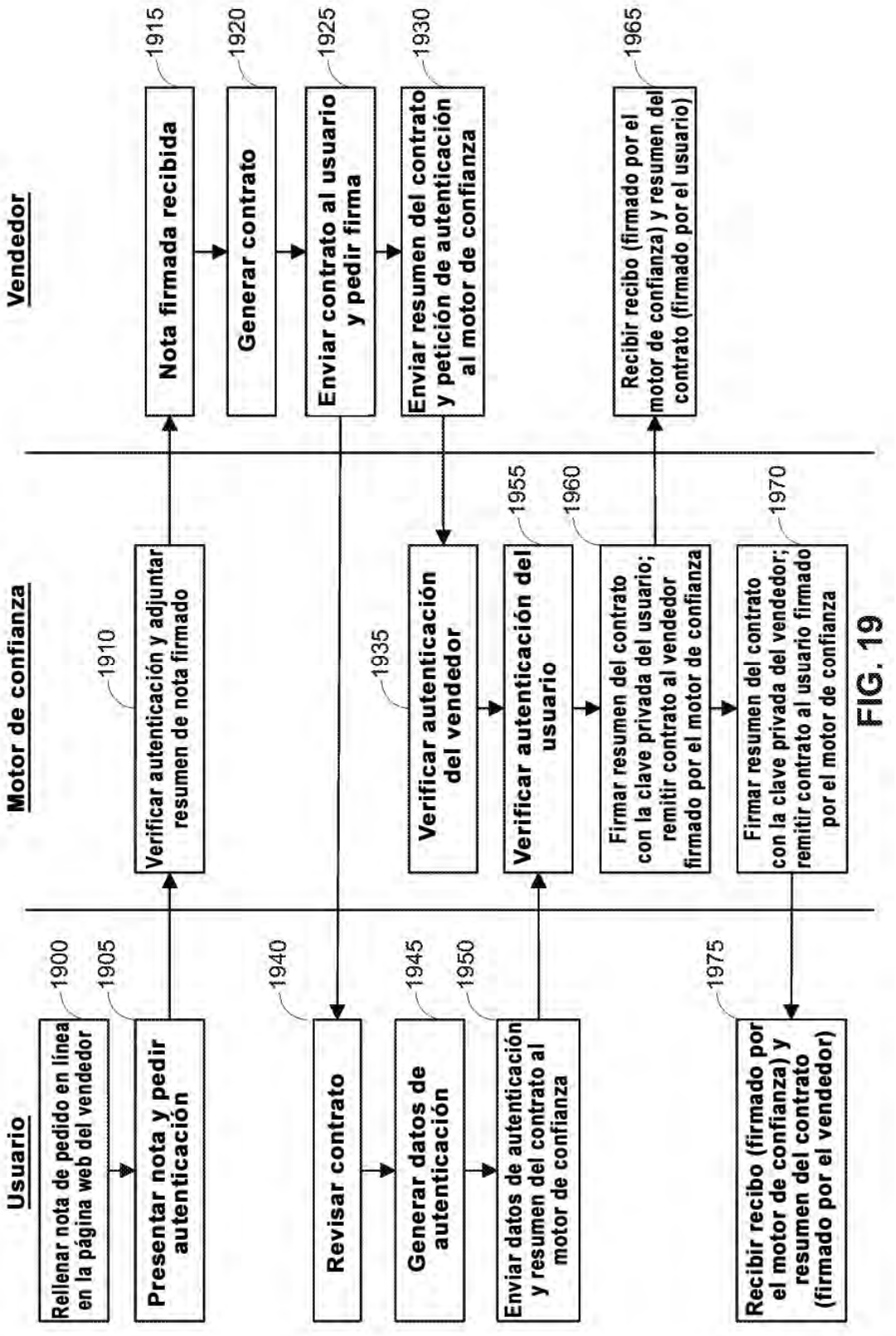

Usuario
Motor de confianza
Vendedor
Rellenar nota de pedido en línea en la página web del vendedor
1900
Presentar nota y pedir autenticación
1905
Verificar autenticación y adjuntar resumen de nota firmado
1910
Nota firmada recibida
1915
Generar contrato
1920
Enviar contrato al usuario y pedir firma
1925
Enviar resumen del contrato y petición de autenticación al motor de confianza
1930
Revisar contrato
1940
Generar datos de autenticación
1945
Enviar datos de autenticación y resumen del contrato al motor de confianza
1950
Verificar autenticación del vendedor
1935
Verificar autenticación del usuario
1955
Firmar resumen del contrato con la clave privada del usuario; remitir contrato al vendedor firmado por el motor de confianza
1960
Recibir recibo (firmado por el motor de confianza) y resumen del contrato (firmado por el usuario)
1965
Firmar resumen del contrato con la clave privada del vendedor; remitir contrato al usuario firmado por el motor de confianza
1970
Recibir recibo (firmado por el motor de confianza) y resumen del contrato (firmado por el vendedor)
1975

FIG. 19

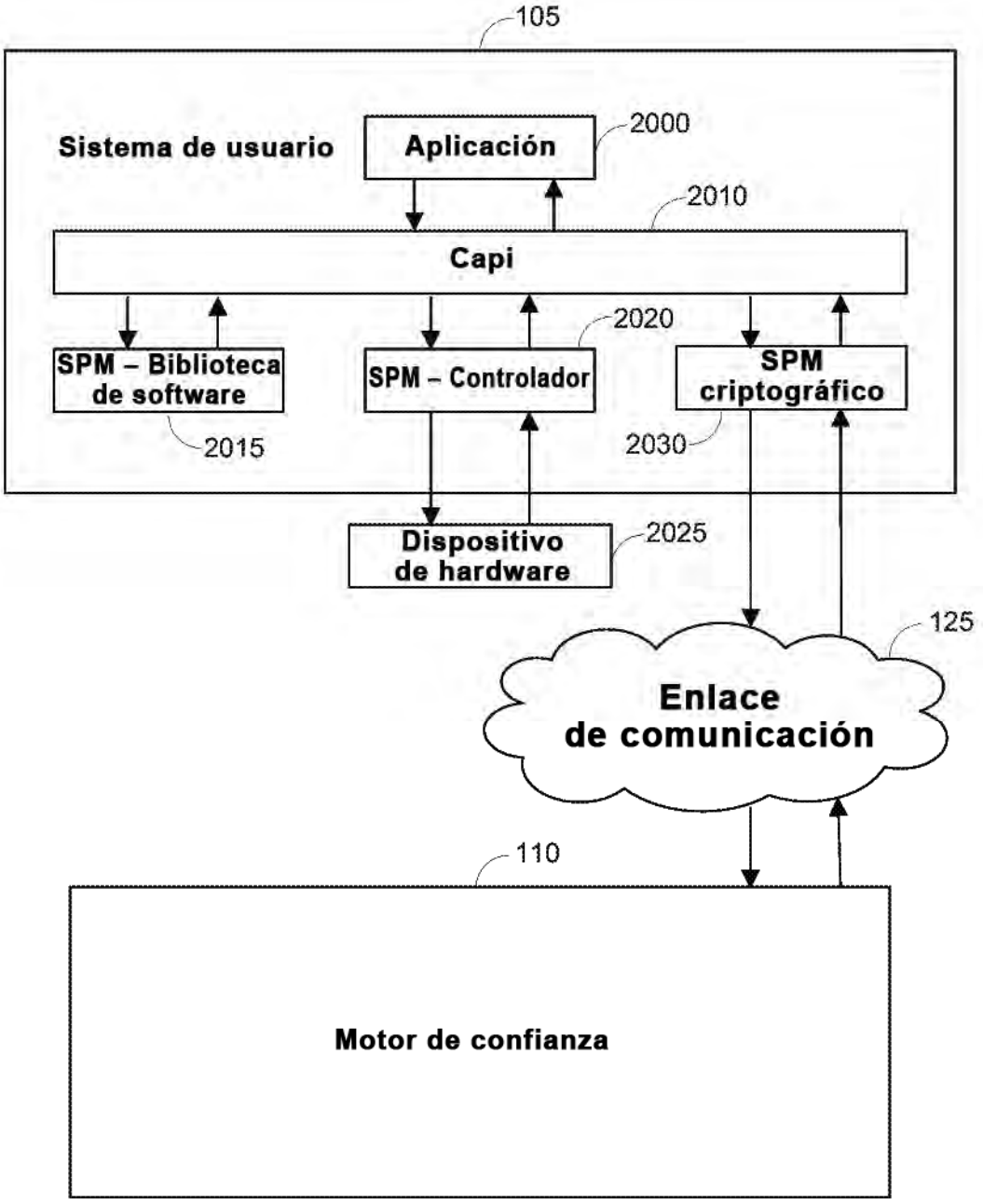

105
Sistema de usuario
Aplicación
2000
2010
Capi
2020
SPM – Biblioteca de software
SPM – Controlador
SPM criptográfico
2015
2030
Dispositivo de hardware
2025
125
Enlace de comunicación
110
Motor de confianza

FIG. 20

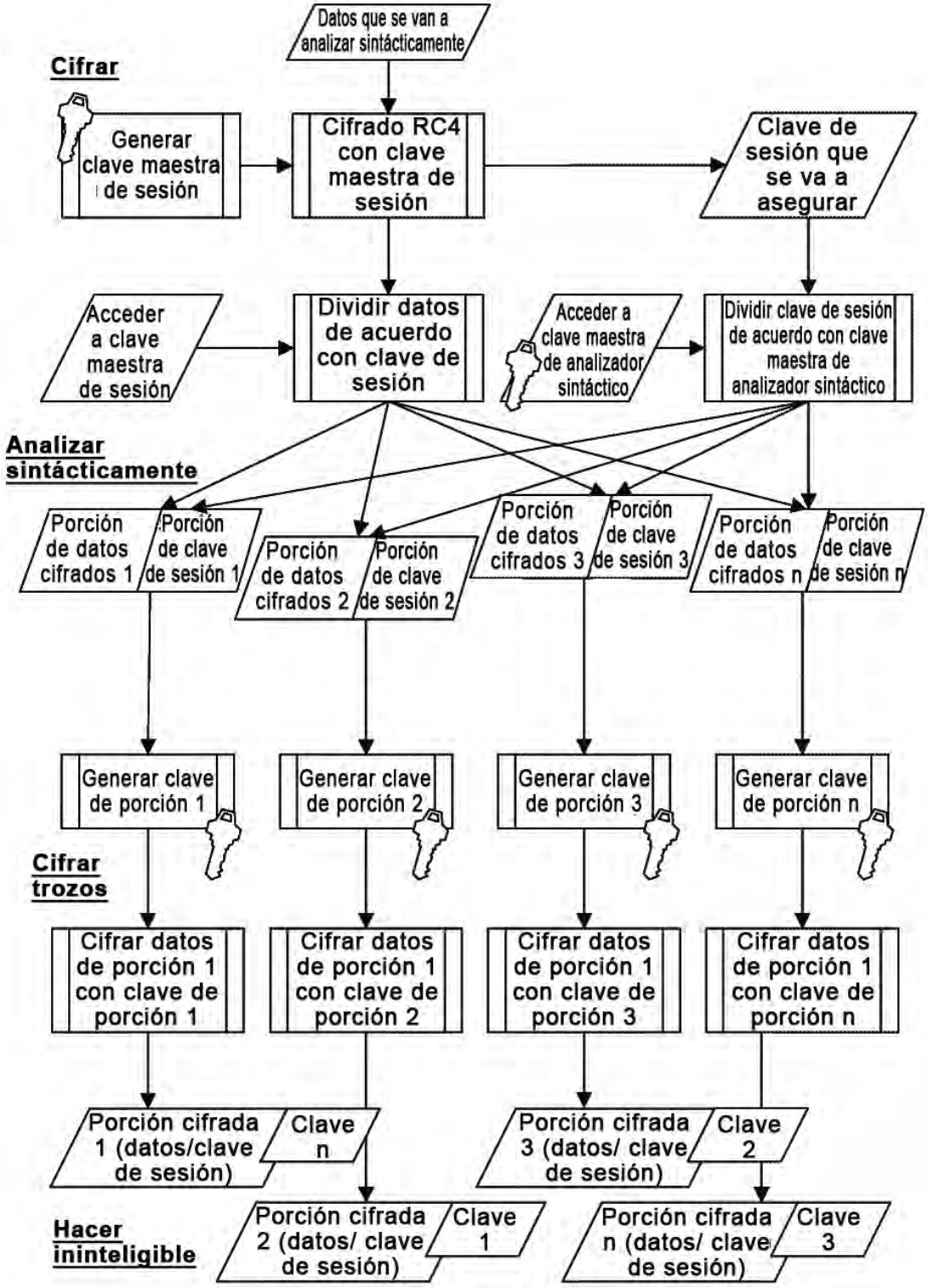

Datos que se van a analizar sintácticamente
Cifrar
Generar clave maestra de sesión
Cifrado RC4 con clave maestra de sesión
Clave de sesión que se va a asegurar
Acceder a clave maestra de sesión
Dividir datos de acuerdo con clave de sesión
Acceder a clave maestra de analizador sintáctico
Dividir clave de sesión de acuerdo con clave maestra de analizador sintáctico
Analizar sintácticamente
Porción de datos cifrados 1
Porción de clave de sesión 1
Porción de datos cifrados 2
Porción de clave de sesión 2
Porción de datos cifrados 3
Porción de clave de sesión 3
Porción de datos cifrados n
Porción de clave de sesión n
Generar clave de porción 1
Generar clave de porción 2
Generar clave de porción 3
Generar clave de porción n
Cifrar trozos
Cifrar datos de porción 1 con clave de porción 1
Cifrar datos de porción 1 con clave de porción 2
Cifrar datos de porción 1 con clave de porción 3
Cifrar datos de porción 1 con clave de porción n
Porción cifrada 1 (datos/clave de sesión)
Clave n
Porción cifrada 3 (datos/ clave de sesión)
Clave 2
Hacer ininteligible
Porción cifrada 2 (datos/ clave de sesión)
Clave 1
Porción cifrada n (datos/ clave de sesión)
Clave 3

FIG. 21

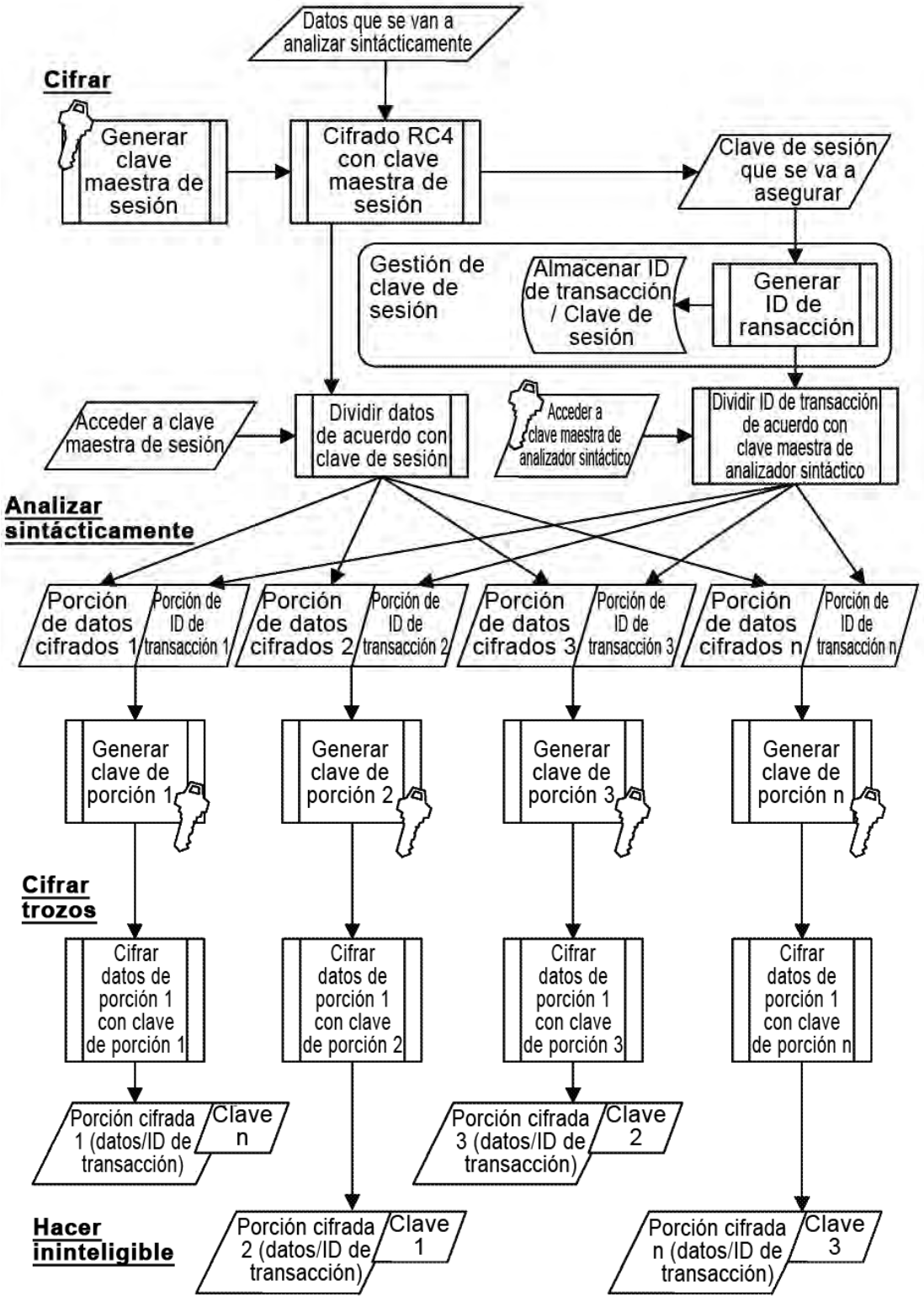

Datos que se van a analizar sintácticamente
Cifrar
Generar clave maestra de sesión
Cifrado RC4 con clave maestra de sesión
Clave de sesión que se va a asegurar
Gestión de clave de sesión
Almacenar ID de transacción / Clave de sesión
Generar ID de ransacción
Acceder a clave maestra de sesión
Dividir datos 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
Porción de datos cifrados 1
Porción de ID de transacción 1
Porción de datos cifrados 2
Porción de ID de transacción 2
Porción de datos cifrados 3
Porción de ID de transacción 3
Porción de datos cifrados n
Porción de ID de transacción n
Generar clave de porción 1
Generar clave de porción 2
Generar clave de porción 3
Generar clave de porción n
Cifrar trozos
Cifrar datos de porción 1 con clave de porción 1
Cifrar datos de porción 1 con clave de porción 2
Cifrar datos de porción 1 con clave de porción 3
Cifrar datos de porción 1 con clave de porción n
Porción cifrada 1 (datos/ID de transacción)
Clave n
Porción cifrada 3 (datos/ID de transacción)
Clave 2
Hacer ininteligible
Porción cifrada 2 (datos/ID de transacción)
Clave 1
Porción cifrada n (datos/ID de transacción)
Clave 3

FIG. 22

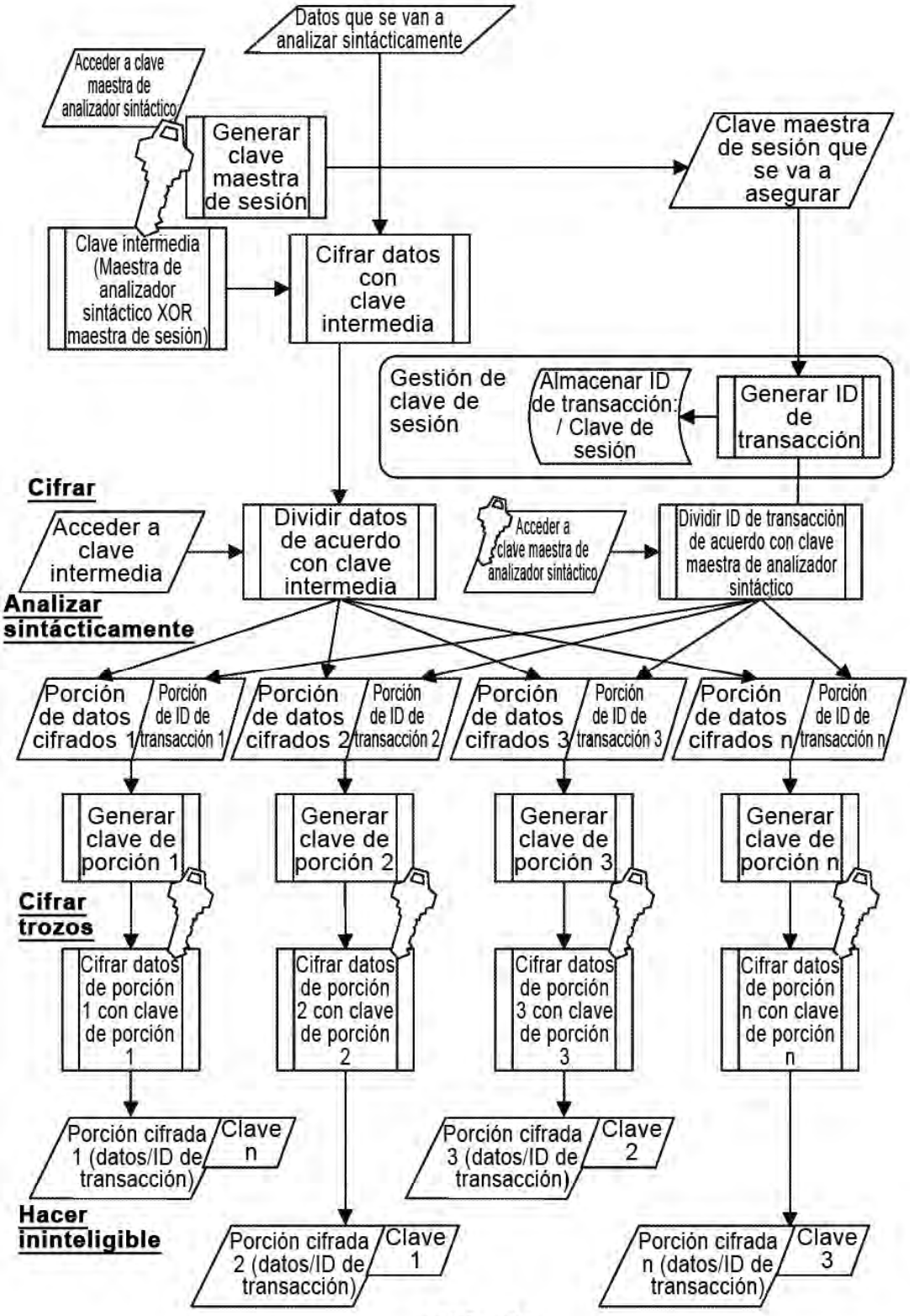

Datos que se van a analizar sintácticamente
Acceder a clave maestra de analizador sintáctico
Generar clave maestra de sesión
Clave maestra de sesión que se va a asegurar
Clave intermedia (Maestra de analizador sintáctico XOR maestra de sesión)
Cifrar datos con clave intermedia
Gestión de clave de sesión
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
Porción de datos cifrados 1
Porción de ID de transacción 1
Porción de datos cifrados 2
Porción de ID de transacción 2
Porción de datos cifrados 3
Porción de ID de transacción 3
Porción de datos cifrados n
Porción de ID de transacción n
Generar clave de porción 1
Generar clave de porción 2
Generar clave de porción 3
Generar clave de porción n
Cifrar trozos
Cifrar datos de porción 1 con clave de porción 1
Cifrar datos de porción 2 con clave de porción 2
Cifrar datos de porción 3 con clave de porción 3
Cifrar datos de porción n con clave de porción n
Porción cifrada 1 (datos/ID de transacción)
Clave n
Porción cifrada 3 (datos/ID de transacción)
Clave 2
Hacer ininteligible
Porción cifrada 2 (datos/ID de transacción)
Clave 1
Porción cifrada n (datos/ID de transacción)
Clave 3

FIG. 23

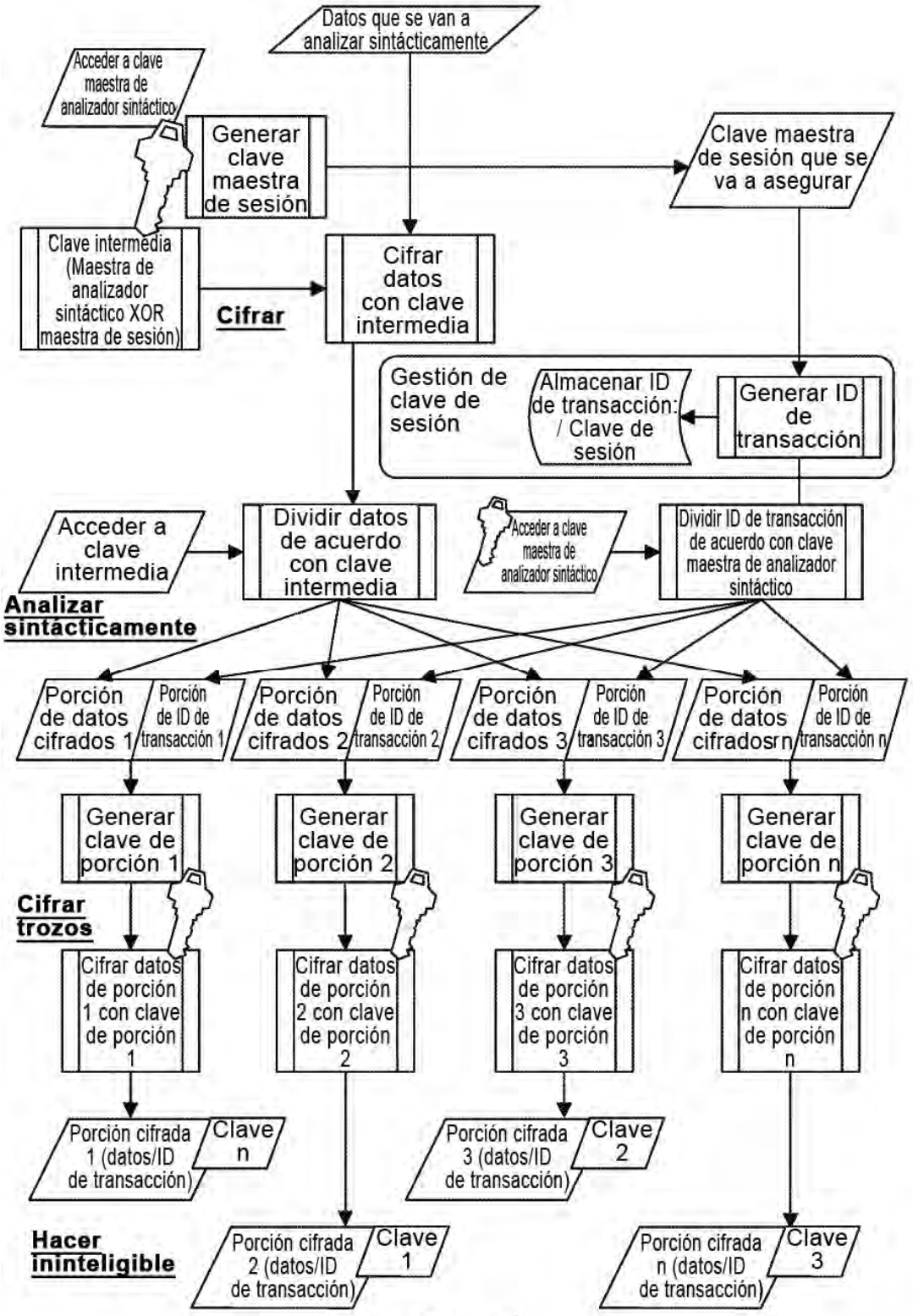

Datos que se van a analizar sintácticamente
Acceder a clave maestra de analizador sintáctico
Generar clave maestra de sesión
Clave maestra de sesión que se va a asegurar
Clave intermedia (Maestra de analizador sintáctico XOR maestra de sesión)
Cifrar
Cifrar datos con clave intermedia
Gestión de clave 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
Porción de datos cifrados 1
Porción de ID de transacción 1
Porción de datos cifrados 2
Porción de ID de transacción 2
Porción de datos cifrados 3
Porción de ID de transacción 3
Porción de datos cifrados n
Porción de ID de transacción n
Generar clave de porción 1
Generar clave de porción 2
Generar clave de porción 3
Generar clave de porción n
Cifrar trozos
Cifrar datos de porción 1 con clave de porción 1
Cifrar datos de porción 2 con clave de porción 2
Cifrar datos de porción 3 con clave de porción 3
Cifrar datos de porción n con clave de porción n
Porción cifrada 1 (datos/ID de transacción)
Clave n
Porción cifrada 3 (datos/ID de transacción)
Clave 2
Hacer ininteligible
Porción cifrada 2 (datos/ID de transacción)
Clave 1
Porción cifrada n (datos/ID de transacción)
Clave 3

FIG. 24

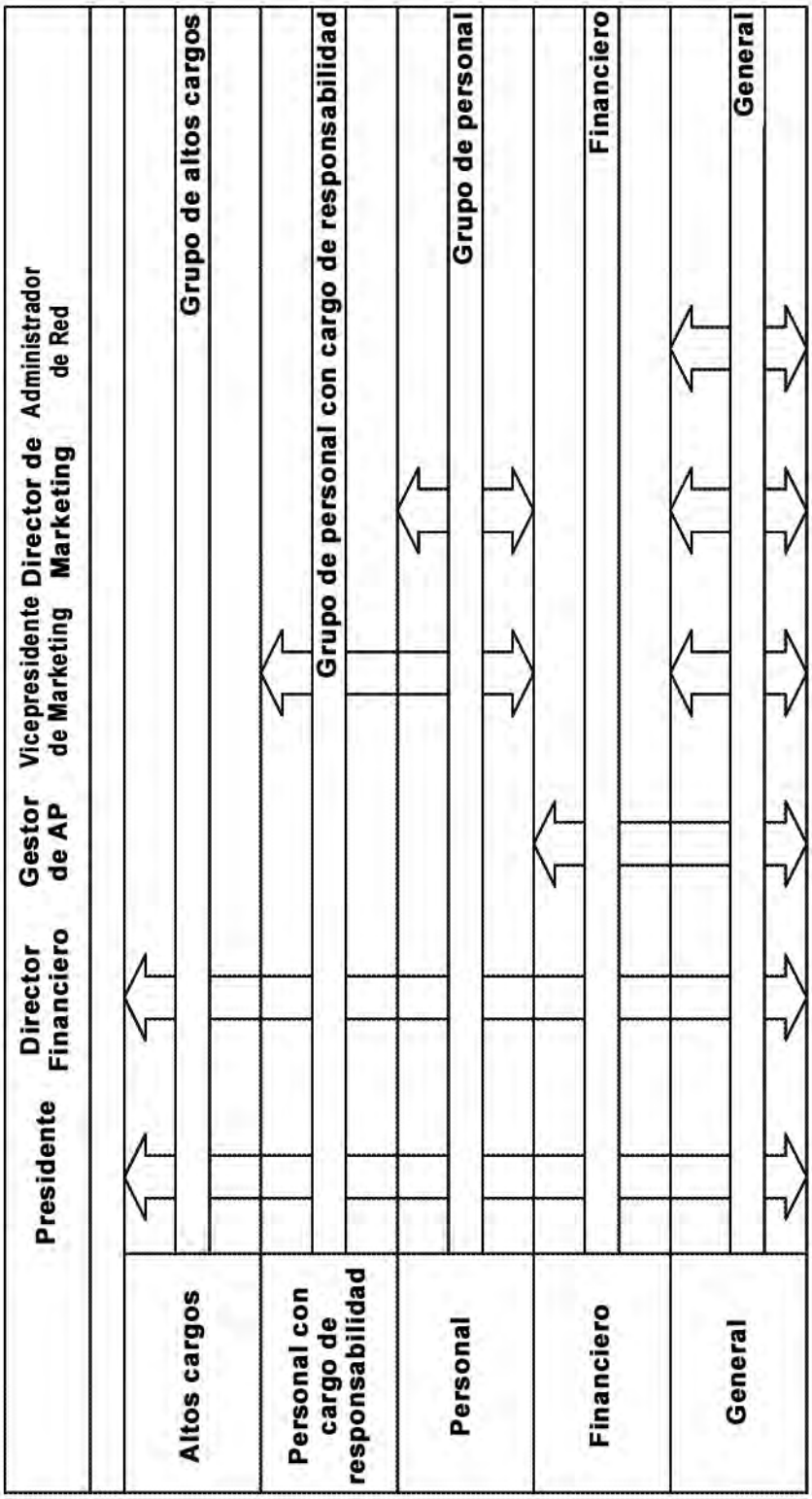

Presidente
Director Financiero
Gestor de AP
Vicepresidente de Marketing
Director de Marketing
Administrador de Red
Altos cargos
Grupo de altos cargos
Personal con cargo de responsabilidad
Grupo de personal con cargo de responsabilidad
Personal
Grupo de personal
Financiero
Financiero
General
General

FIG. 25


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

FIG. 26

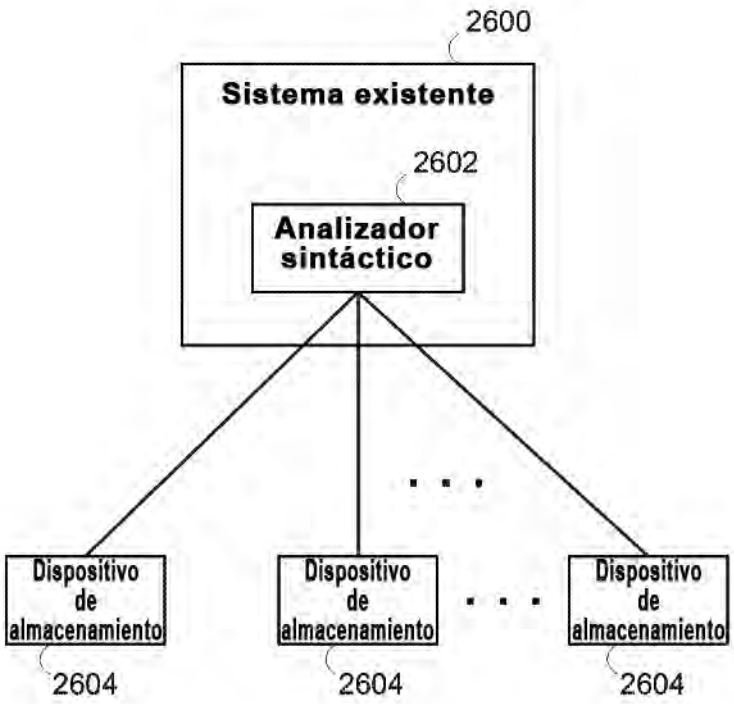

2600
Sistema existente
2602
Analizador sintáctico
Dispositivo de almacenamiento
2604
Dispositivo de almacenamiento
2604
Dispositivo de almacenamiento
2604

FIG. 27

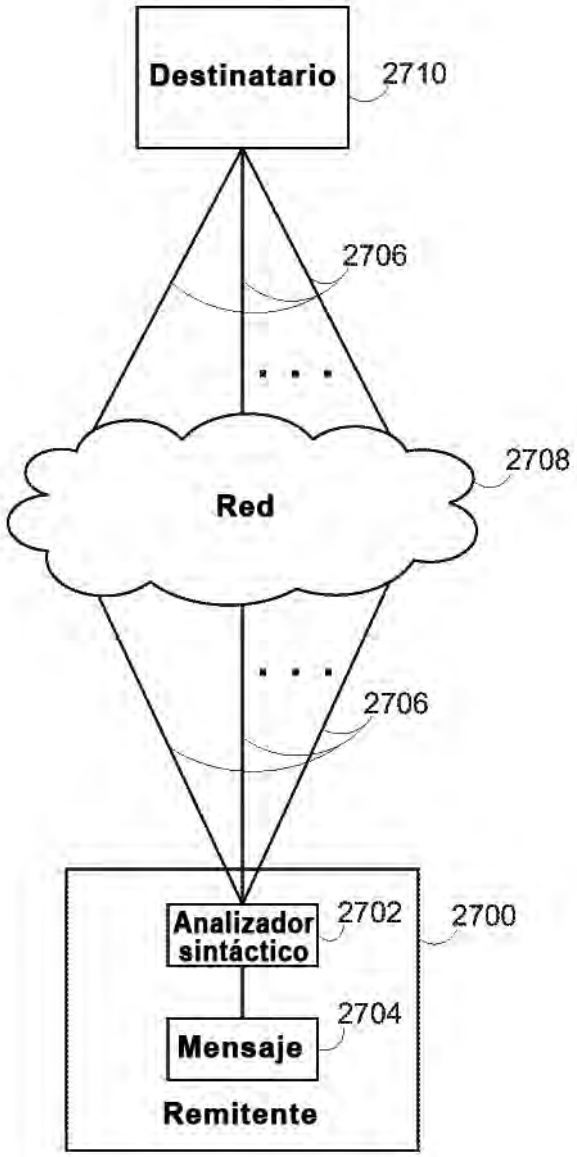

Destinatario
2710
2706
2708
Red
2706
Analizador sintáctico
2702
2700
2704
Mensaje
Remitente

FIG. 28

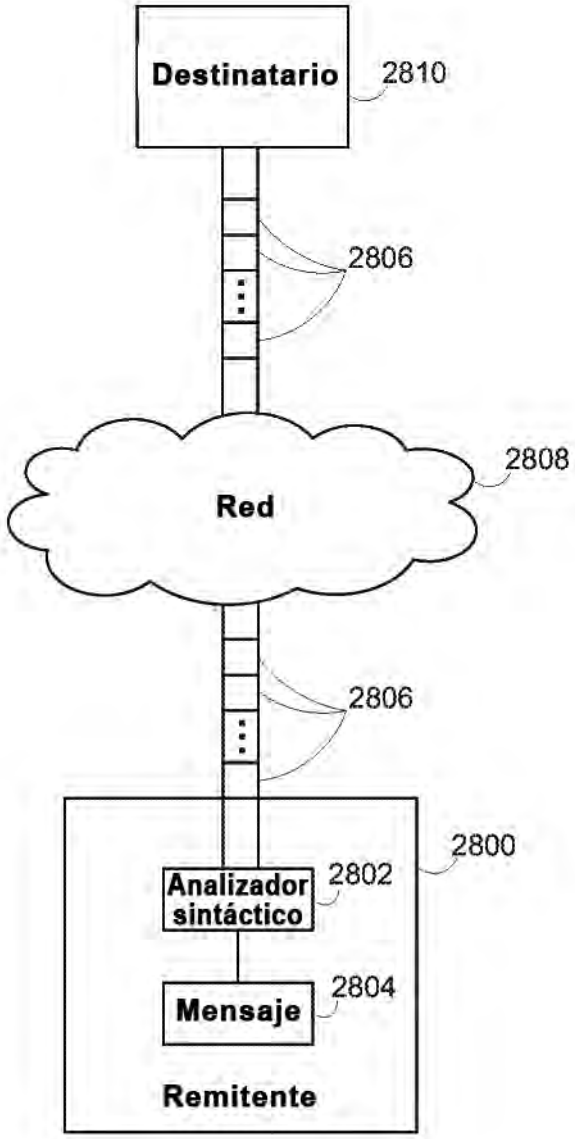

Destinatario
2810
2806
2808
Red
2806
2800
Analizador sintáctico
2802
Mensaje
2804
Remitente

FIG. 29

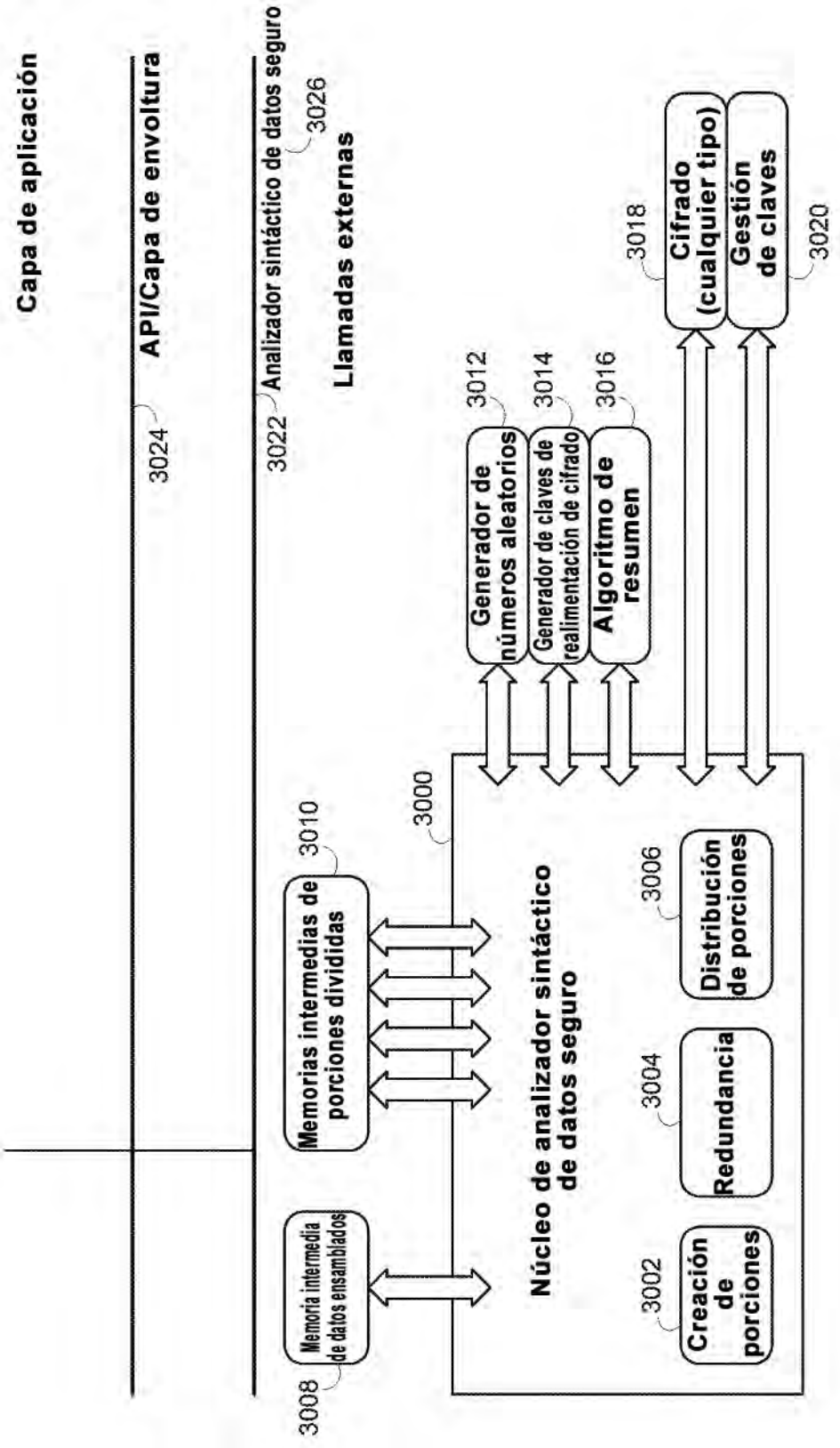

Capa de aplicación
API/Capa de envoltura
3024
Analizador sintáctico de datos seguro
3022
3026
Llamadas externas
Generador de números aleatorios
3012
Generador de claves de realimentación de cifrado
3014
Algoritmo de resumen
3016
Cifrado (cualquier tipo)
3018
Gestión de claves
3020
3000
Memorias intermedias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

FIG. 30

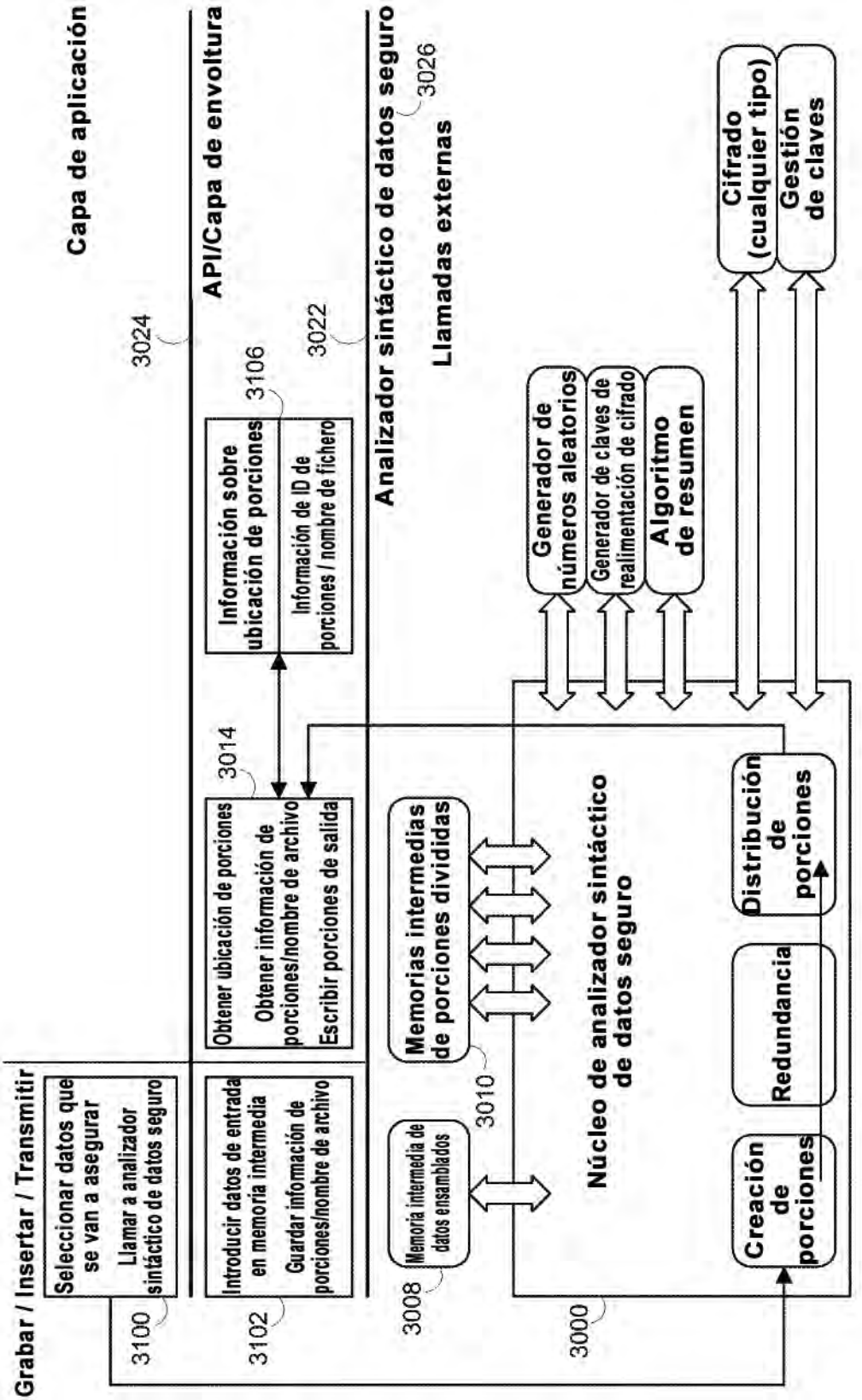

Grabar / Insertar / Transmitir
Capa de aplicación
API/Capa de envoltura
Analizador sintáctico de datos seguro
Llamadas externas
3024
3022
3026
3106
3014
3010
3008
3000
3100
3102
Seleccionar datos que se van a asegurar
Llamar a analizador sintáctico de datos seguro
Introducir datos de entrada en memoria intermedia
Guardar información de porciones/nombre de archivo
Información sobre ubicación de porciones
Información de ID de porciones / nombre de fichero
Obtener ubicación de porciones
Obtener información de porciones/nombre de archivo
Escribir porciones de salida
Memorias intermedias de porciones divididas
Memoria intermedia de datos ensamblados
Núcleo de analizador sintáctico de datos seguro
Generador de números aleatorios
Generador de claves de realimentación de cifrado
Algoritmo de resumen
Cifrado (cualquier tipo)
Gestión de claves
Distribución de porciones
Redundancia
Creación de porciones

FIG. 31

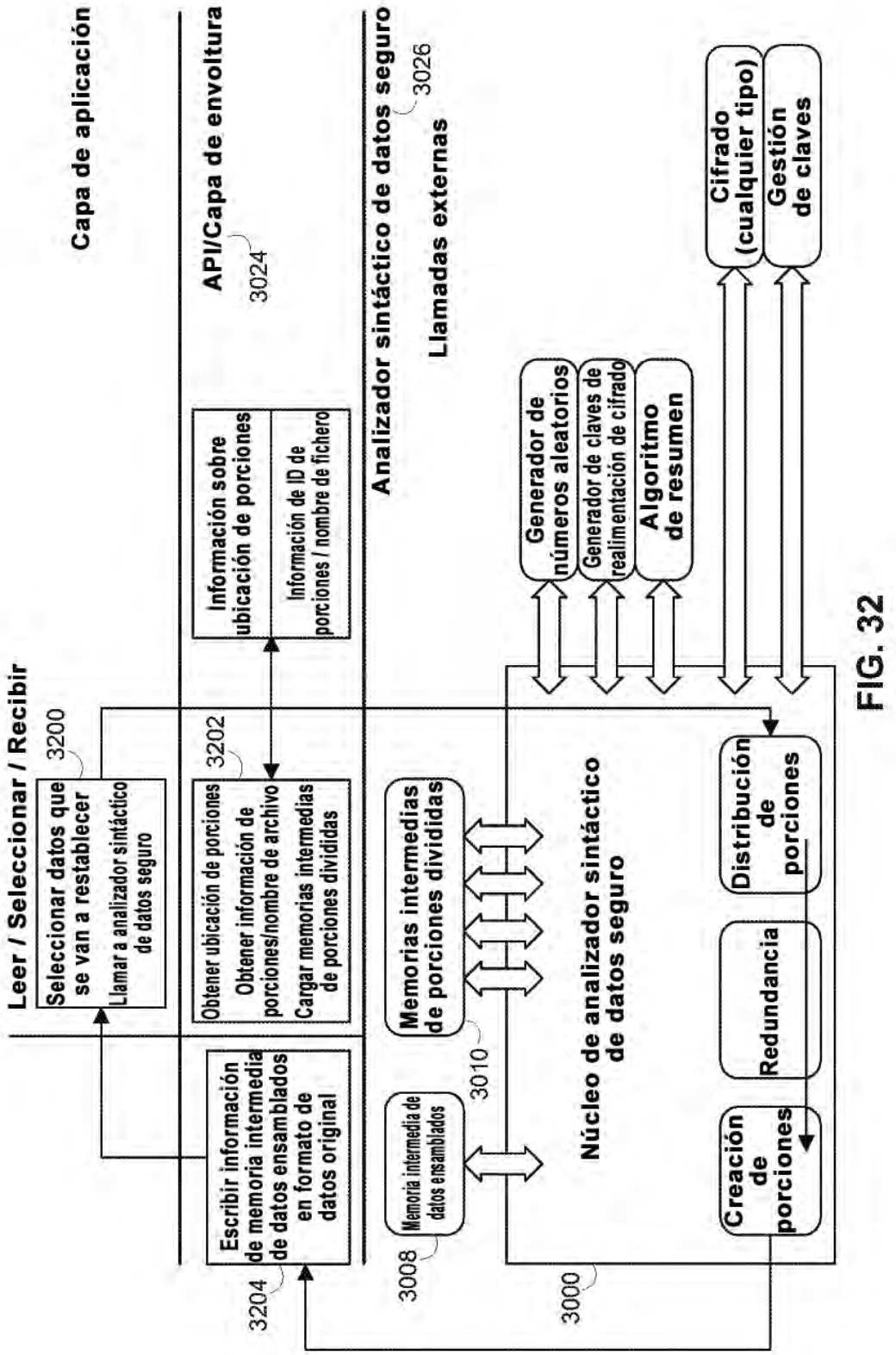

Capa de aplicación
API/Capa de envoltura
3024
Analizador sintáctico de datos seguro
3026
Llamadas externas
Leer / Seleccionar / Recibir
Seleccionar datos que se van a restablecer
Llamar a analizador sintáctico de datos seguro
3200
Obtener ubicación de porciones
Obtener información de porciones/nombre de archivo
Cargar memorias intermedias de porciones divididas
3202
Información sobre ubicación de porciones
Información de ID de porciones / nombre de fichero
Escribir información de memoria intermedia de datos ensamblados en formato de datos original
3204
Memoria intermedia de datos ensamblados
3008
Memorias intermedias de porciones divididas
3010
Núcleo de analizador sintáctico de datos seguro
3000
Generador de números aleatorios
Generador de claves de realimentación de cifrado
Algoritmo de resumen
Cifrado (cualquier tipo)
Gestión de claves
Distribución de porciones
Redundancia
Creación de porciones

FIG. 32

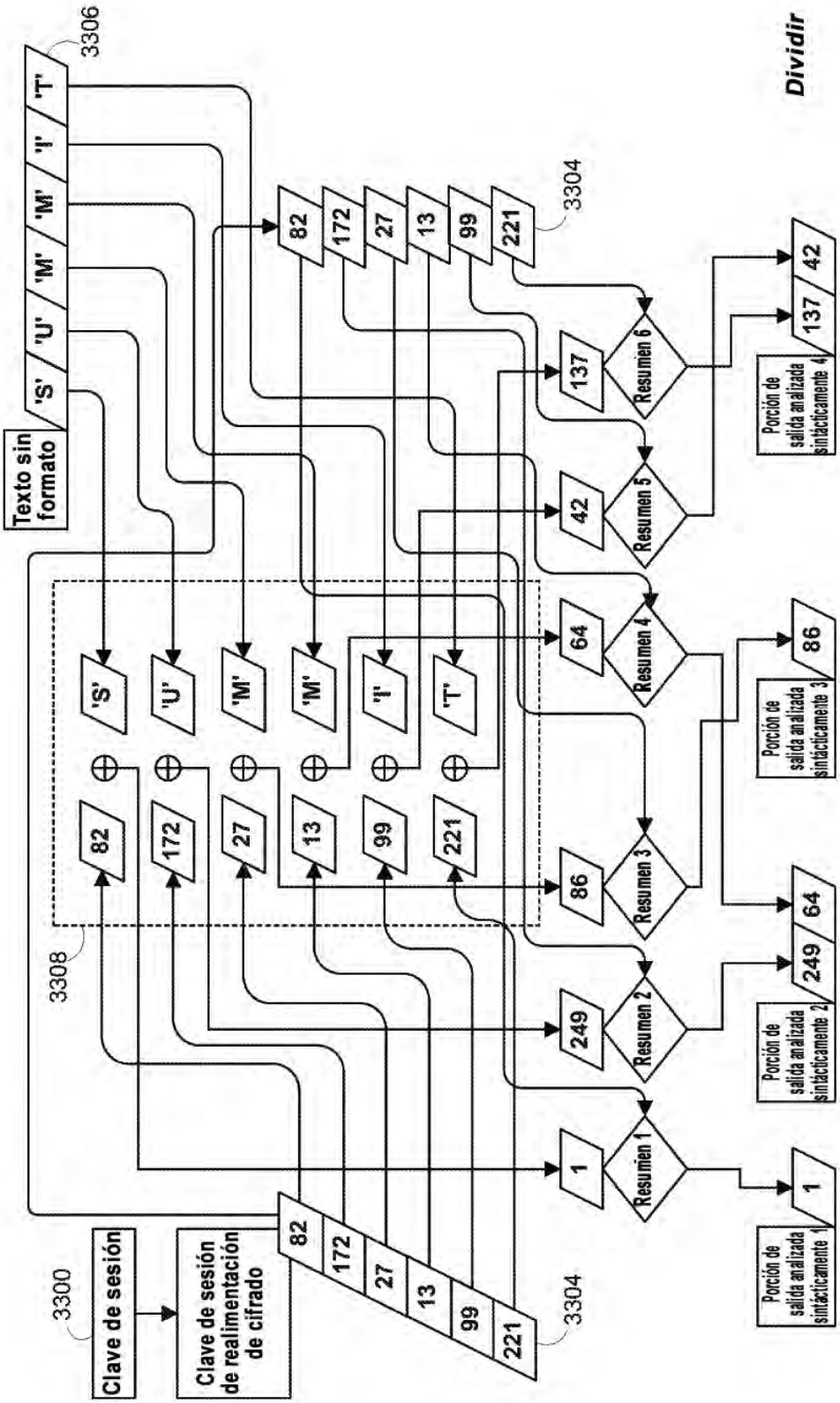

3306
Texto sin formato
'S' 'U' 'M' 'M' 'I' 'T'
3304
82 172 27 13 99 221
3308
'S' 'U' 'M' 'M' 'I' 'T'
82 172 27 13 99 221
3300
Clave de sesión
Clave de sesión de realimentación de cifrado
82 172 27 13 99 221
3304
Dividir
Resumen 1
Resumen 2
Resumen 3
Resumen 4
Resumen 5
Resumen 6
1
249
86
64
42
137
Porción de salida analizada sintácticamente 1
Porción de salida analizada sintácticamente 2
Porción de salida analizada sintácticamente 3
Porción de salida analizada sintácticamente 4

FIG. 33

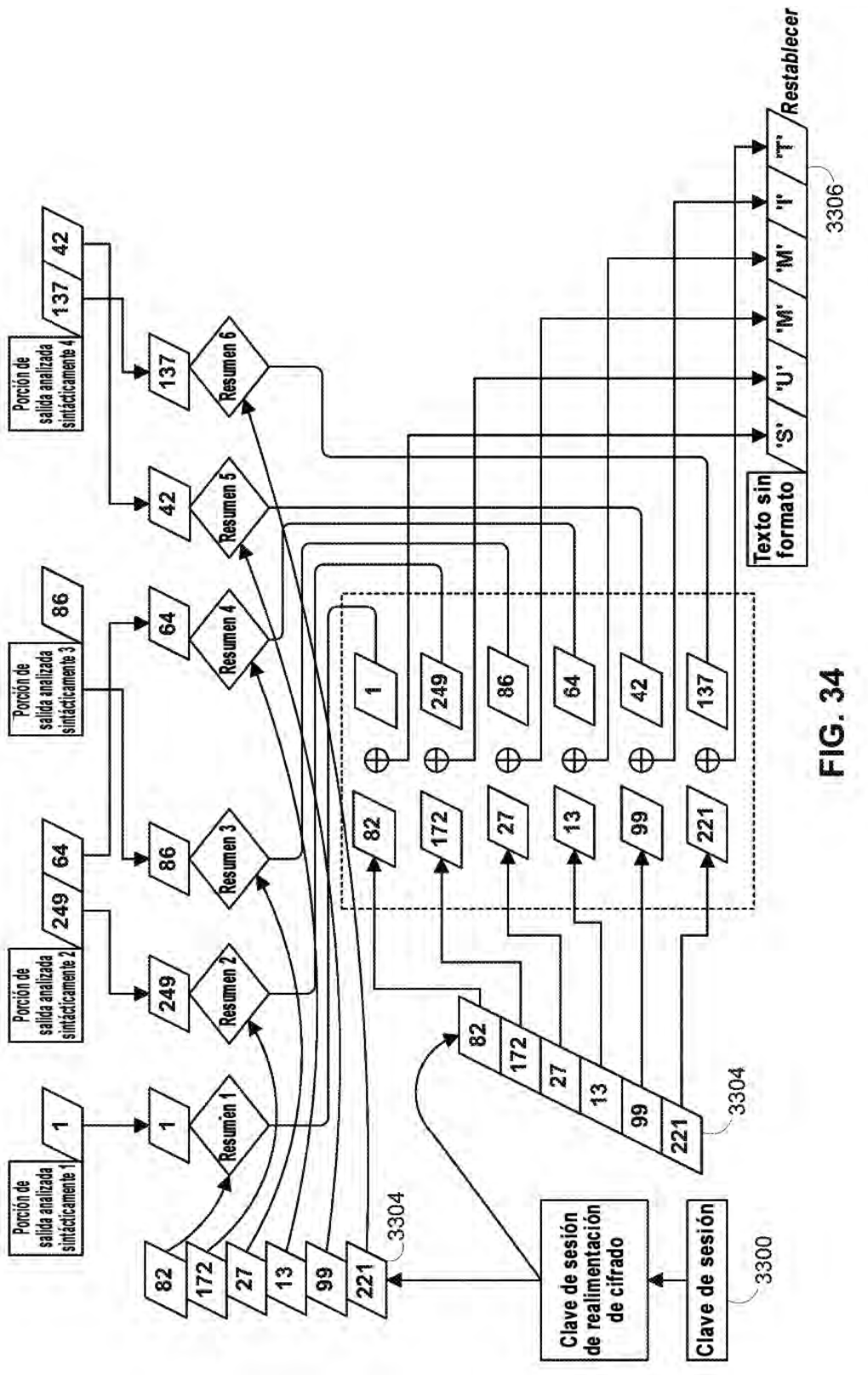

Porción de salida analizada sintácticamente 1
Porción de salida analizada sintácticamente 2
Porción de salida analizada sintácticamente 3
Porción de salida analizada sintácticamente 4
Resumen 1
Resumen 2
Resumen 3
Resumen 4
Resumen 5
Resumen 6
Texto sin formato
'S' 'U' 'M' 'M' 'I' 'T'
Restablecer
3306
3304
3304
Clave de sesión de realimentación de cifrado
Clave de sesión
3300

FIG. 34

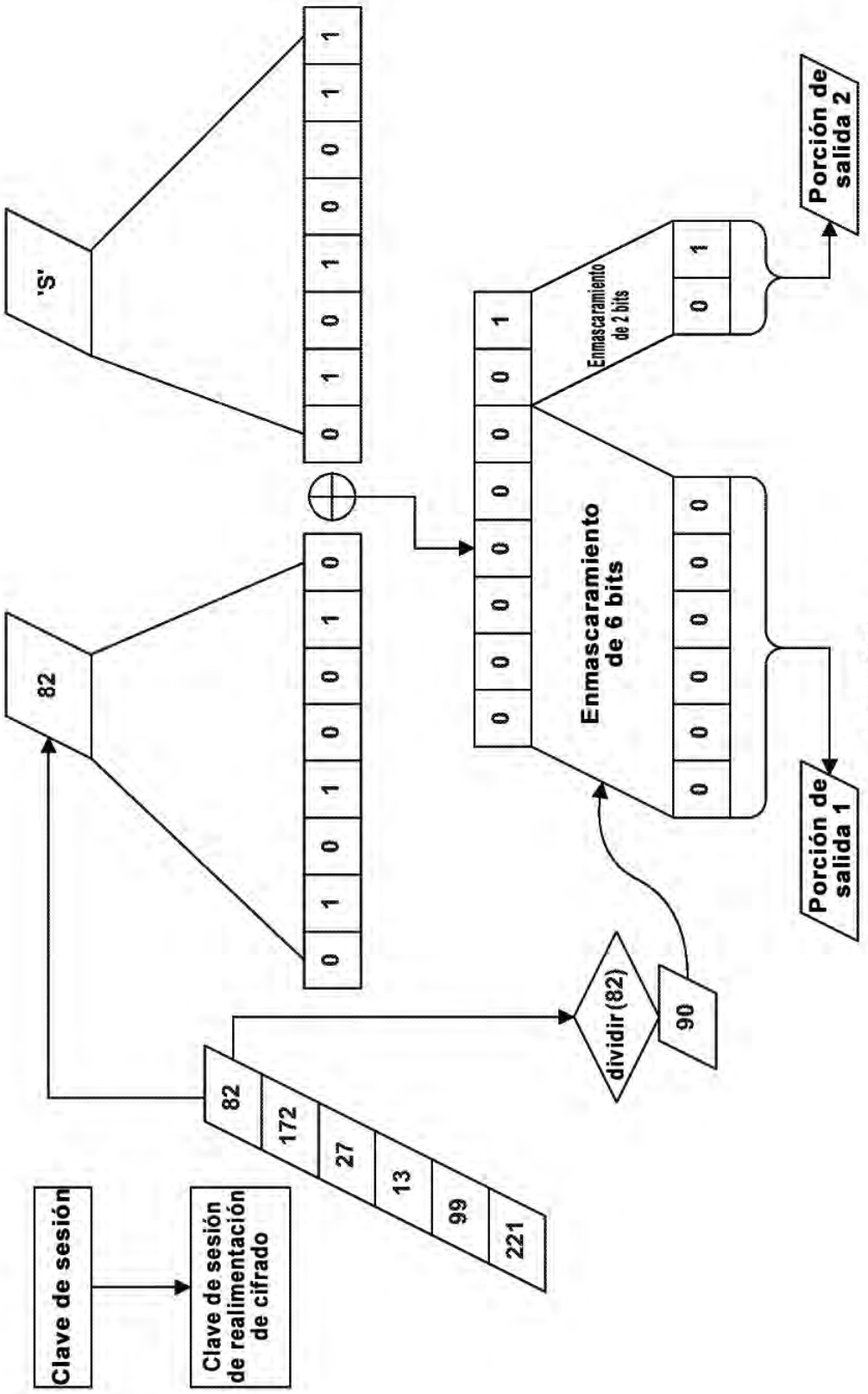

Clave de sesión
Clave de sesión de realimentación de cifrado
82
172
27
13
99
221
dividir (82)
90
82
'S'
Enmascaramiento de 6 bits
Enmascaramiento de 2 bits
Porción de salida 1
Porción de salida 2

FIG. 35

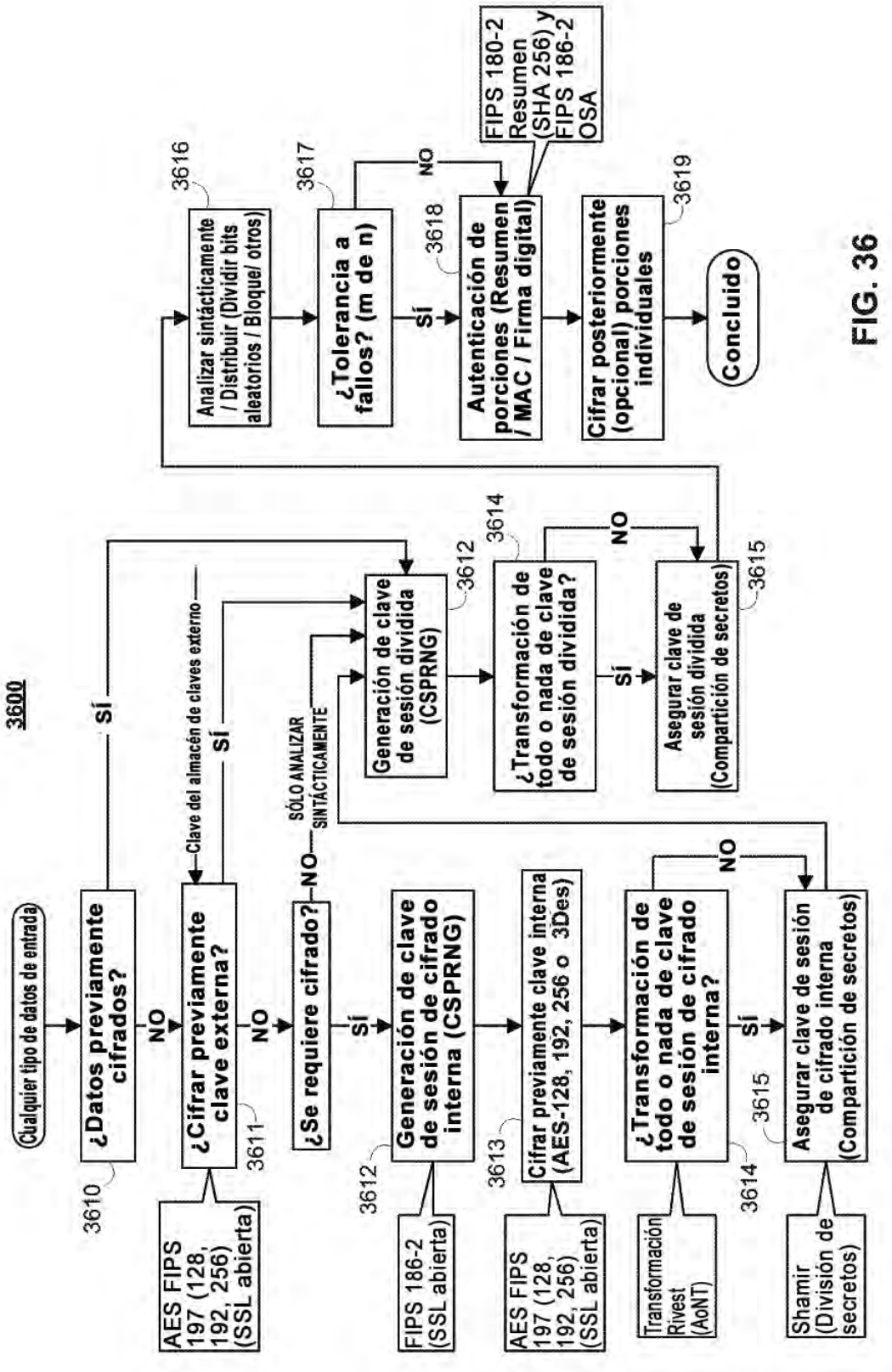

3600
Cualquier tipo de datos de entrada
¿Datos previamente cifrados?
SÍ
NO
3610
¿Cifrar previamente clave externa?
Clave del almacén de claves externo
SÍ
NO
3611
AES FIPS 197 (128, 192, 256) (SSL abierta)
¿Se requiere cifrado?
NO
SÓLO ANALIZAR SINTÁCTICAMENTE
SÍ
Generación de clave de sesión de cifrado interna (CSPRNG)
3612
FIPS 186-2 (SSL abierta)
Cifrar previamente clave interna (AES-128, 192, 256 o 3Des)
3613
AES FIPS 197 (128, 192, 256) (SSL abierta)
¿Transformación de todo o nada de clave de sesión de cifrado interna?
NO
SÍ
3614
Transformación Rivest (AoNT)
Asegurar clave de sesión de cifrado interna (Compartición de secretos)
3615
Shamir (División de secretos)
Generación de clave de sesión dividida (CSPRNG)
3612
¿Transformación de todo o nada de clave de sesión dividida?
NO
SÍ
3614
Asegurar clave de sesión dividida (Compartición de secretos)
3615
Analizar sintácticamente / Distribuir (Dividir bits aleatorios / Bloque/ otros)
3616
¿Tolerancia a fallos? (m de n)
NO
SÍ
3617
3618
Autenticación de porciones (Resumen / MAC / Firma digital)
FIPS 180-2 Resumen (SHA 256) y FIPS 186-2 OSA
Cifrar posteriormente (opcional) porciones individuales
3619
Concluido

FIG. 36

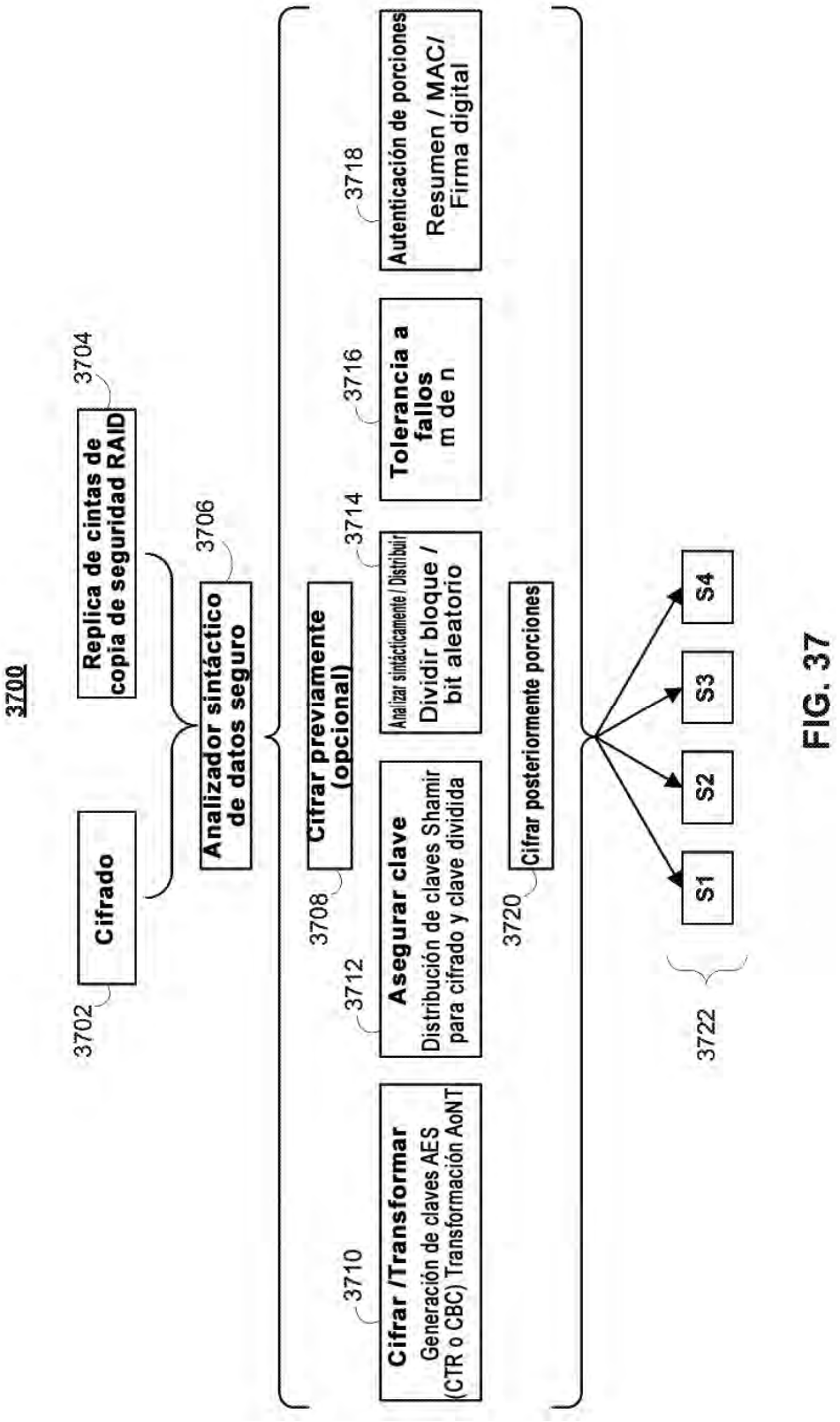

3700
Cifrado
3702
Replica de cintas de copia de seguridad RAID
3704
Analizador sintáctico de datos seguro
3706
Cifrar previamente (opcional)
3708
Asegurar clave
Distribución de claves Shamir para cifrado y clave dividida
3712
Cifrar /Transformar
Generación de claves AES (CTR o CBC) Transformación AoNT
3710
Analizar sintácticamente / Distribuir
Dividir bloque / bit aleatorio
3714
Tolerancia a fallos
m de n
3716
Autenticación de porciones
Resumen / MAC/ Firma digital
3718
Cifrar posteriormente porciones
3720
S1
S2
S3
S4
3722

FIG. 37

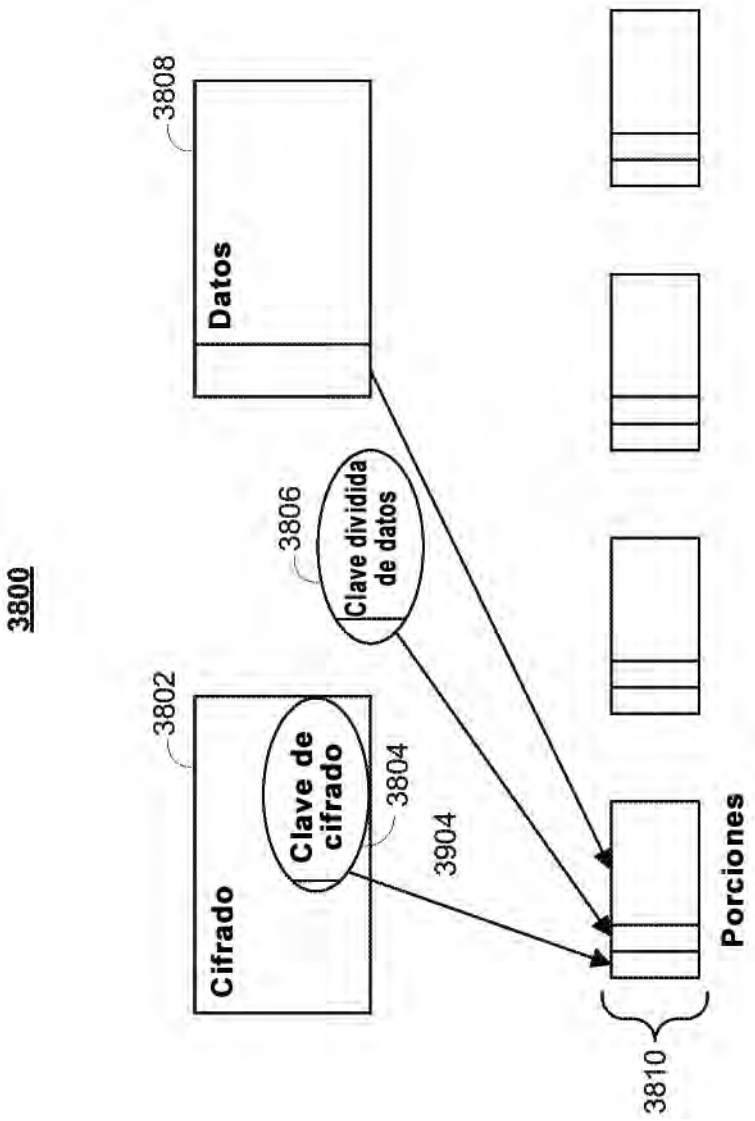

3800
3808
Datos
3806
Clave dividida de datos
3802
Cifrado
Clave de cifrado
3804
3904
Porciones
3810

FIG. 38

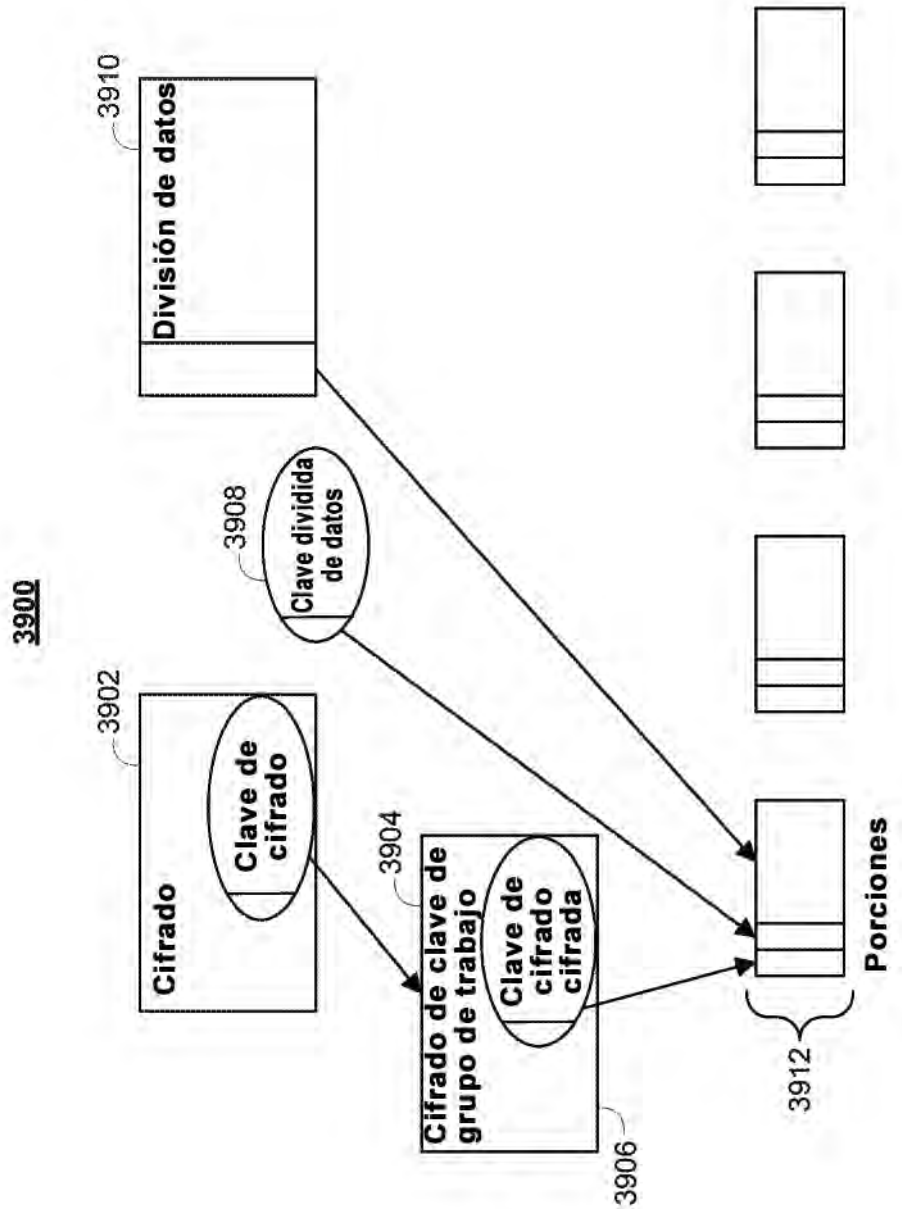

3900
3902
Cifrado
Clave de cifrado
3904
Cifrado de clave de grupo de trabajo
Clave de cifrado cifrada
3906
3908
Clave dividida de datos
3910
División de datos
3912
Porciones

FIG. 39

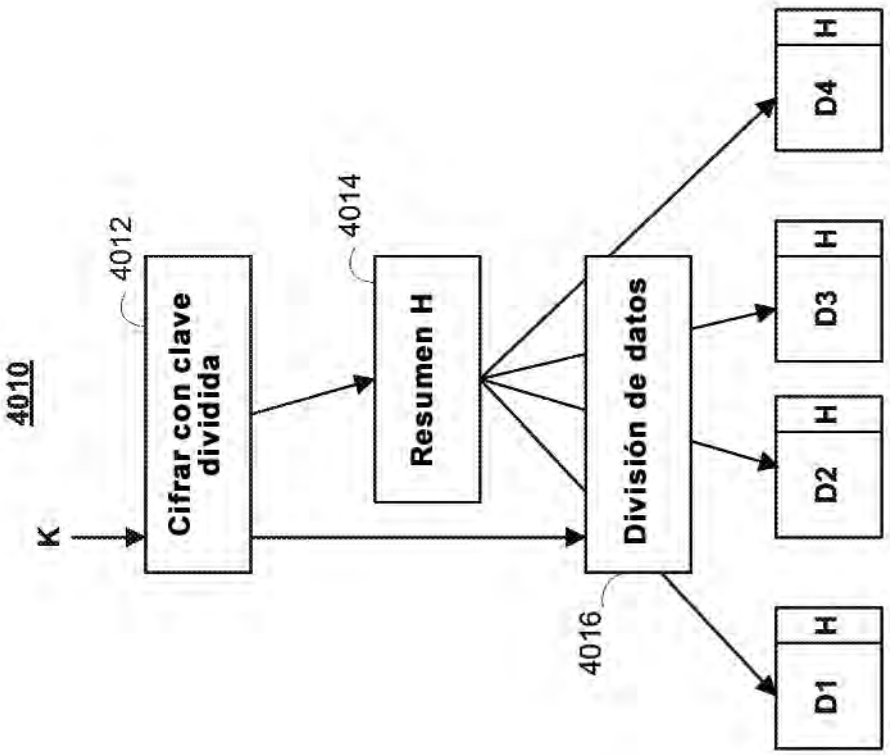


FIG. 40B

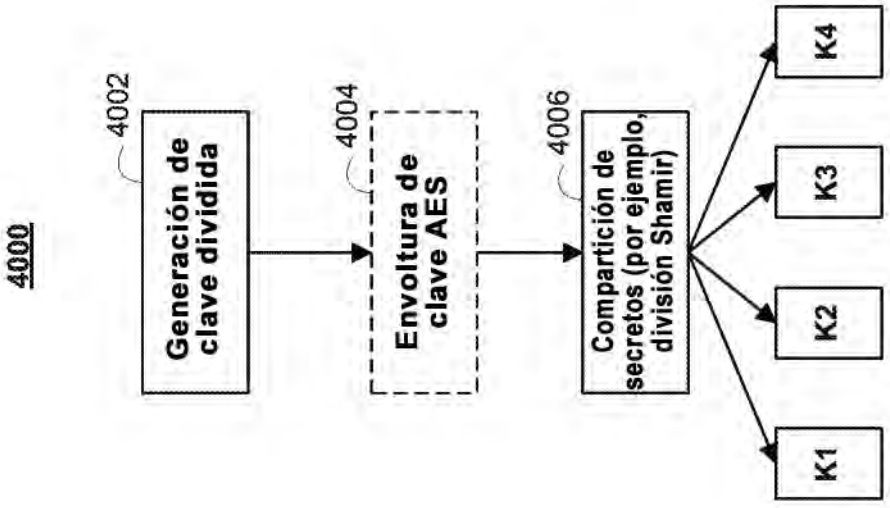


FIG. 40A

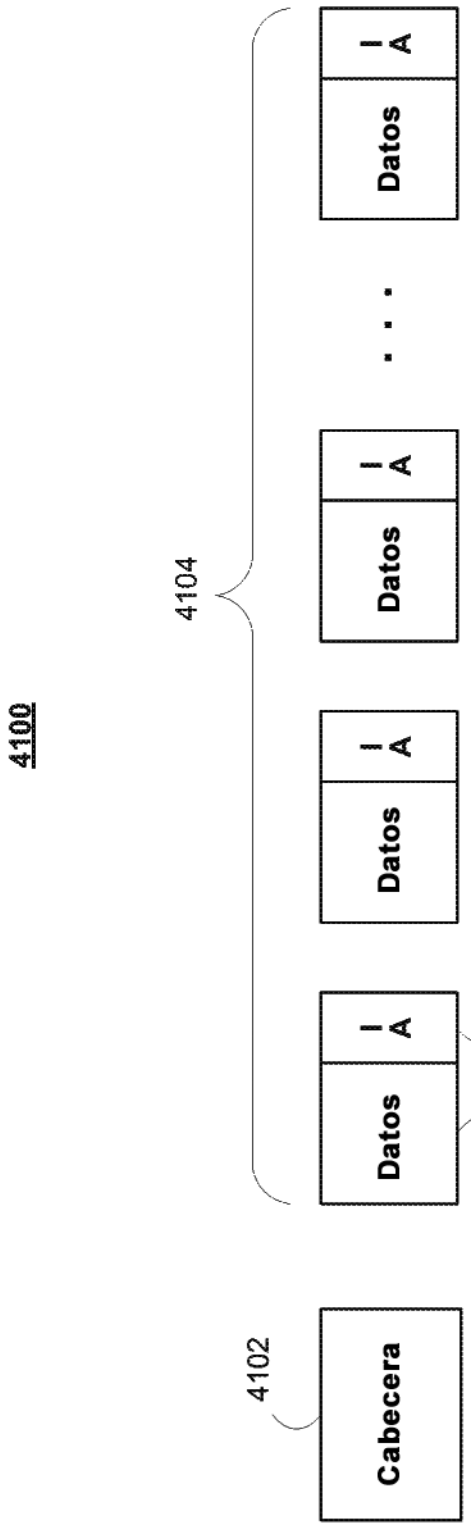


FIG. 41

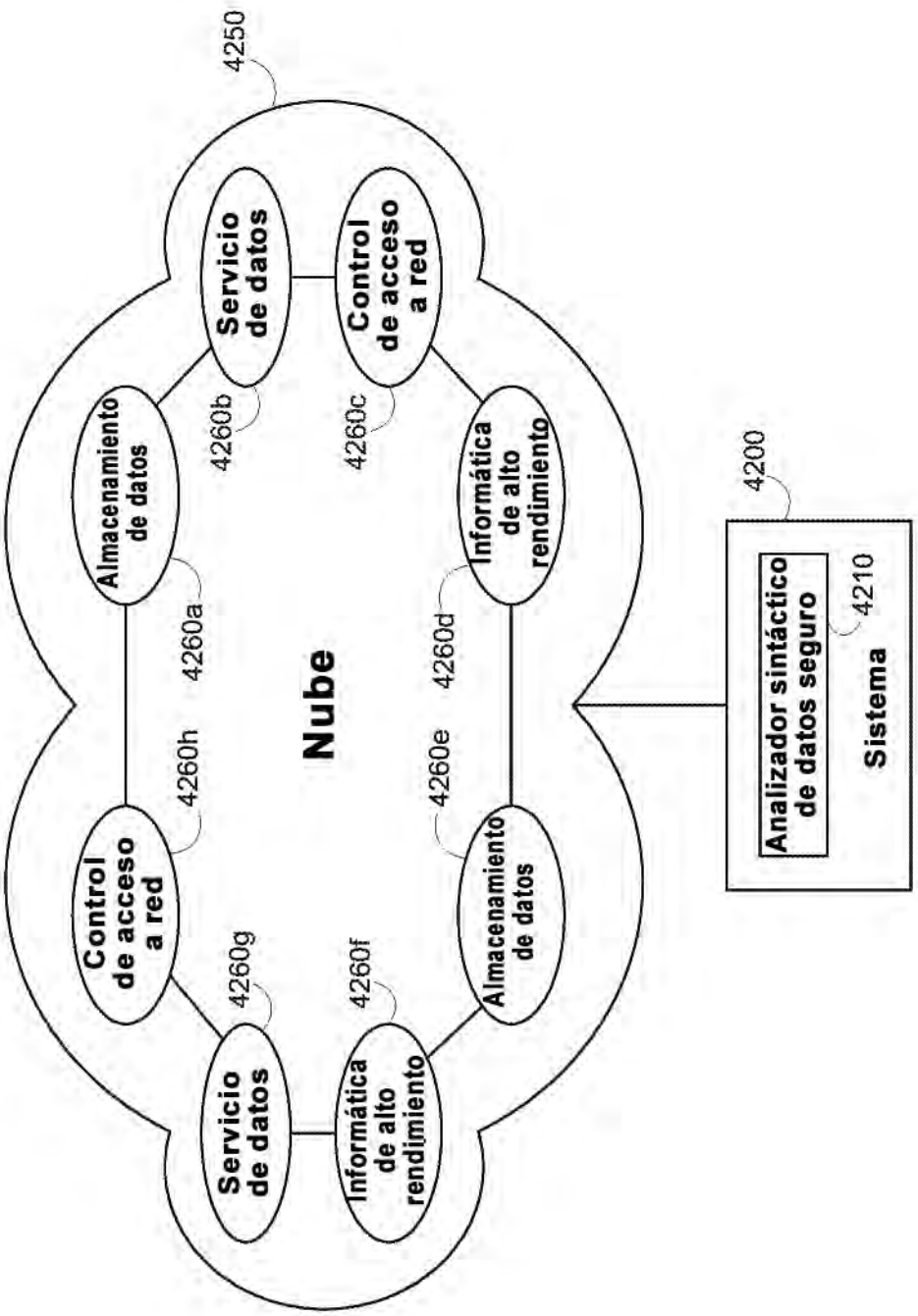

4250
Servicio de datos
Control de acceso a red
Almacenamiento de datos
Informática de alto rendimiento
4260a
4260b
4260c
4260d
4260e
4260f
4260g
4260h
Nube
Control de acceso a red
Servicio de datos
Informática de alto rendimiento
Almacenamiento de datos
4200
Analizador sintáctico de datos seguro
4210
Sistema

FIG. 42

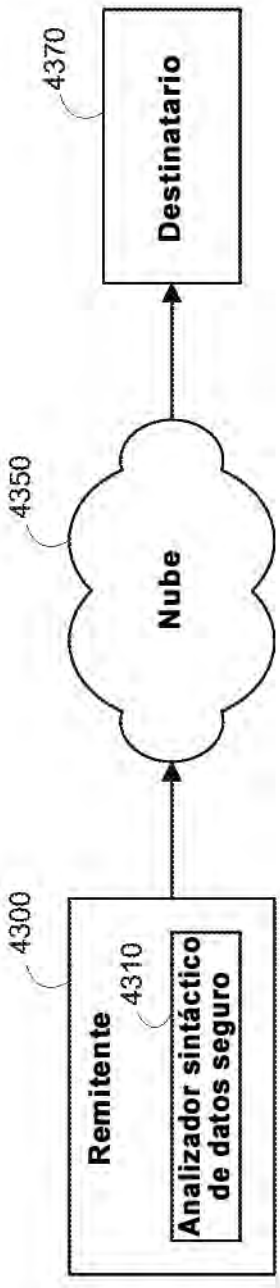

4370
Destinatario
4350
Nube
4300
Remitente
4310
Analizador sintáctico de datos seguro

FIG. 43

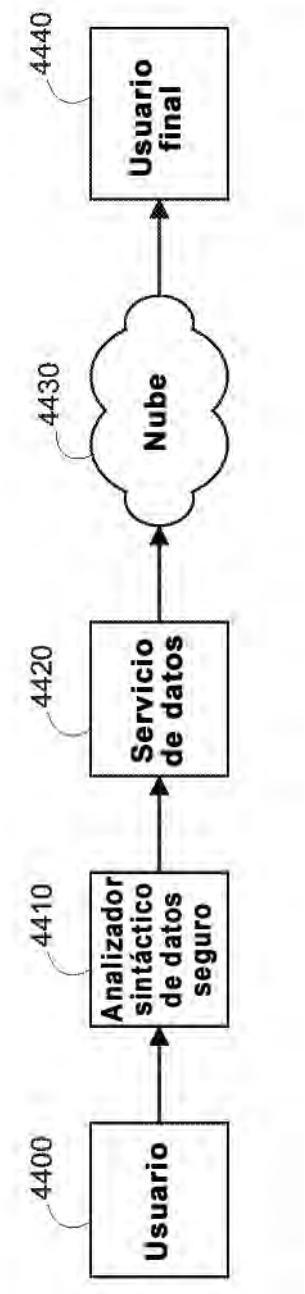

4400
Usuario
4410
Analizador sintáctico de datos seguro
4420
Servicio de datos
4430
Nube
4440
Usuario final

FIG. 44

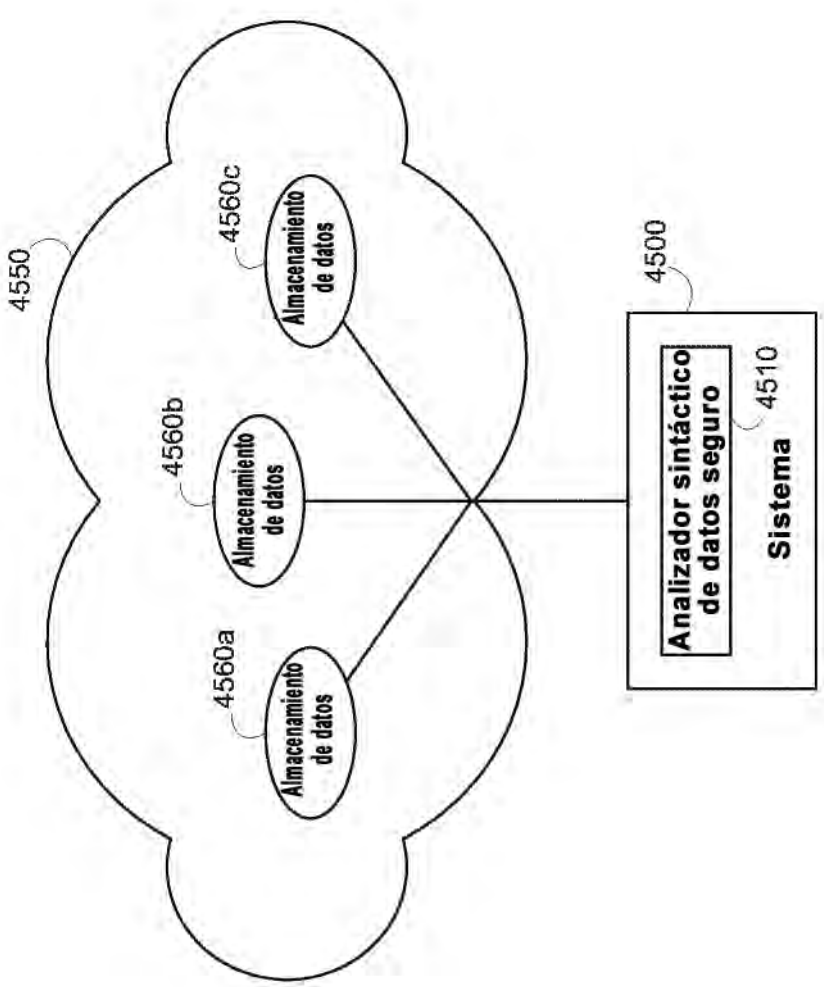

4550
4560c
Almacenamiento de datos
4560b
Almacenamiento de datos
4560a
Almacenamiento de datos
4500
Analizador sintáctico de datos seguro
4510
Sistema

FIG. 45

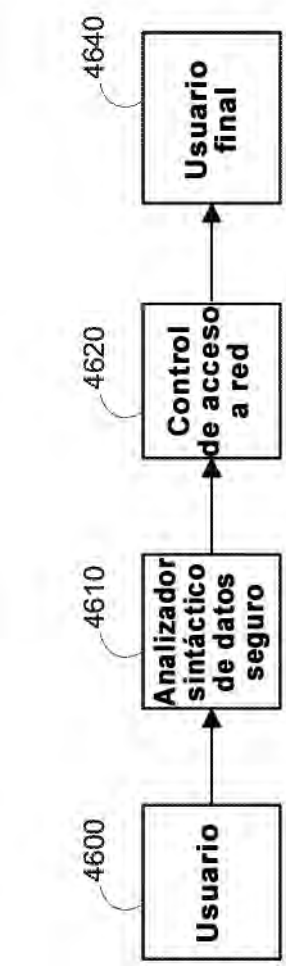

4600
Usuario
4610
Analizador sintáctico de datos seguro
4620
Control de acceso a red
4640
Usuario final

FIG. 46

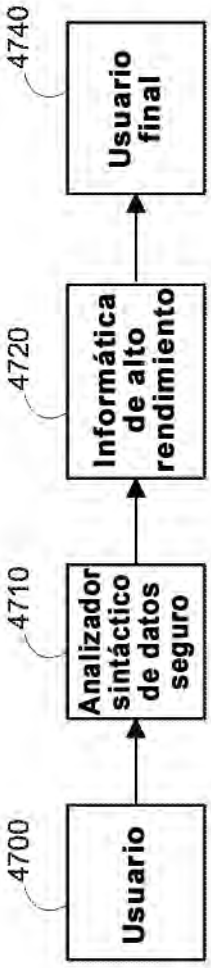

4700
Usuario
4710
Analizador sintáctico de datos seguro
4720
Informática de alto rendimiento
4740
Usuario final

FIG. 47

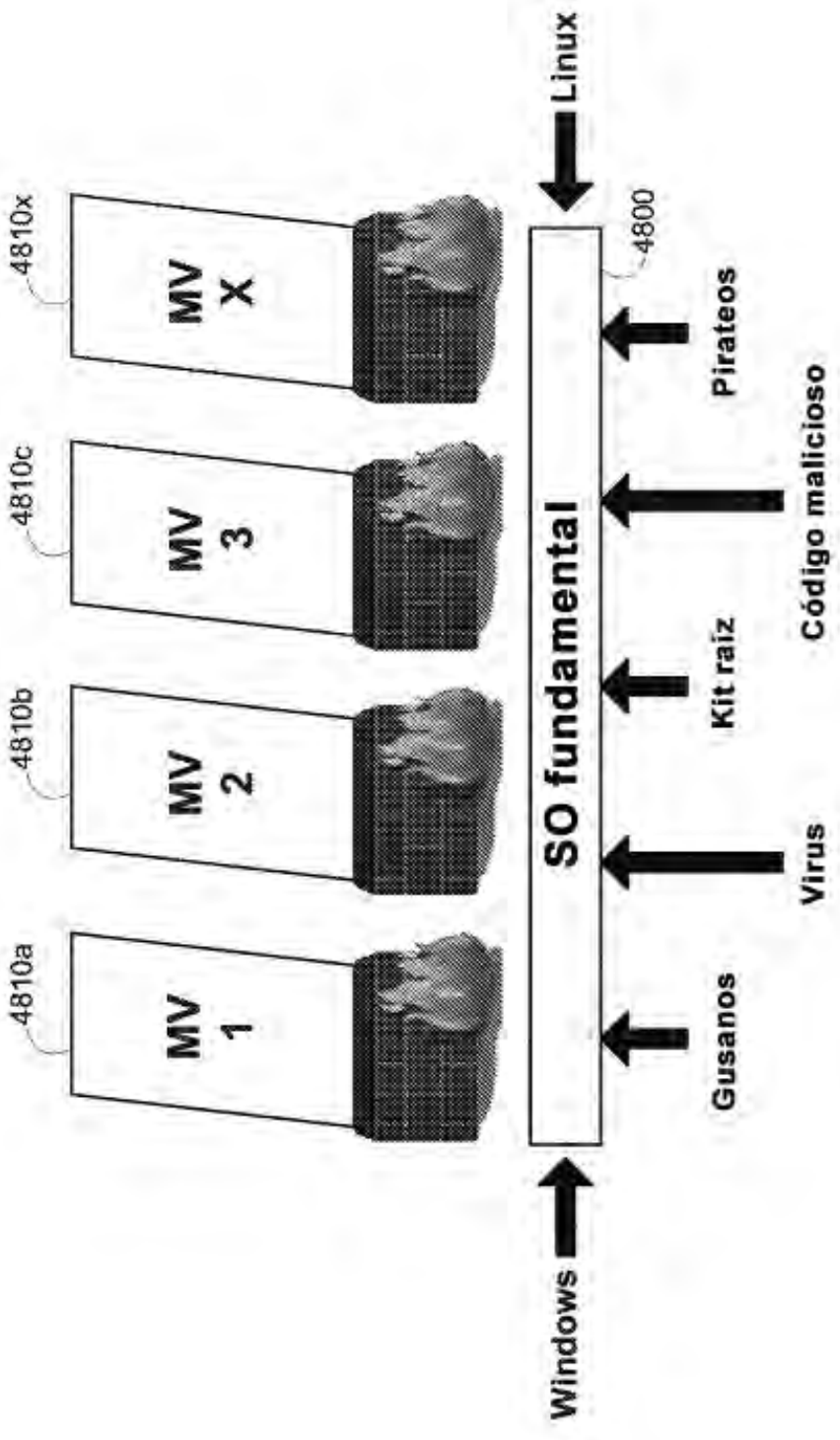

4810a
MV 1
4810b
MV 2
4810c
MV 3
4810x
MV X
Windows
Linux
4800
SO fundamental
Gusanos
Virus
Kit raíz
Código malicioso
Pirateos

FIG. 48

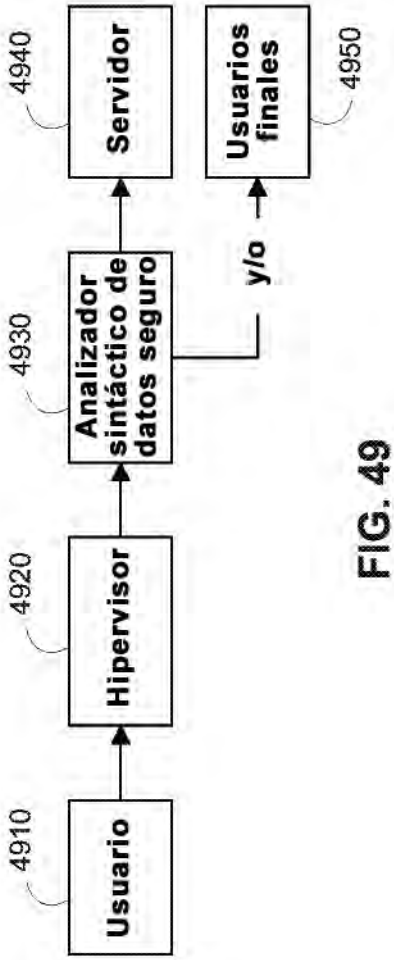

4910
Usuario
4920
Hipervisor
4930
Analizador sintáctico de datos seguro
y/o
4940
Servidor
Usuarios finales
4950

FIG. 49

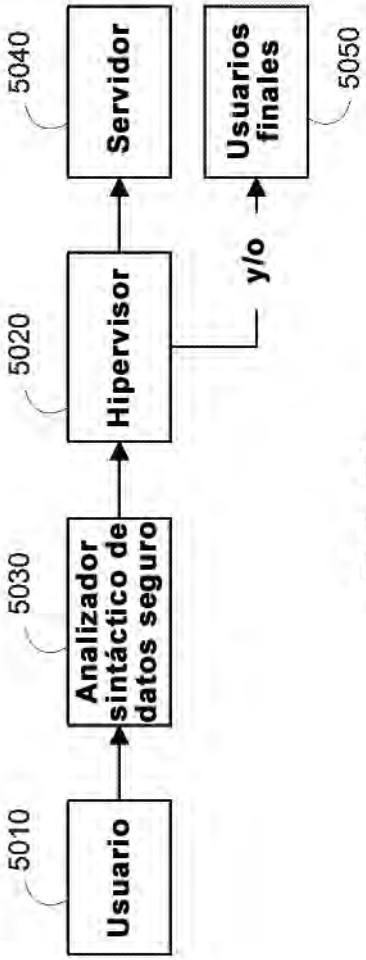

5010
Usuario
5030
Analizador sintáctico de datos seguro
5020
Hipervisor
y/o
5040
Servidor
Usuarios finales
5050

FIG. 50

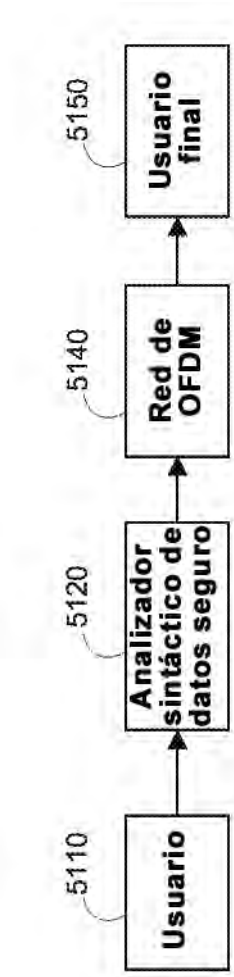

5110
Usuario
5120
Analizador sintáctico de datos seguro
5140
Red de OFDM
5150
Usuario final

FIG. 51

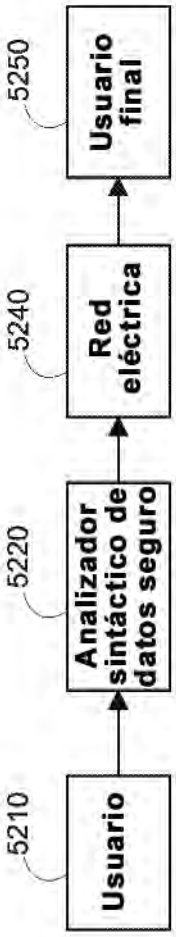

5210
Usuario
5220
Analizador sintáctico de datos seguro
5240
Red eléctrica
5250
Usuario final

FIG. 52

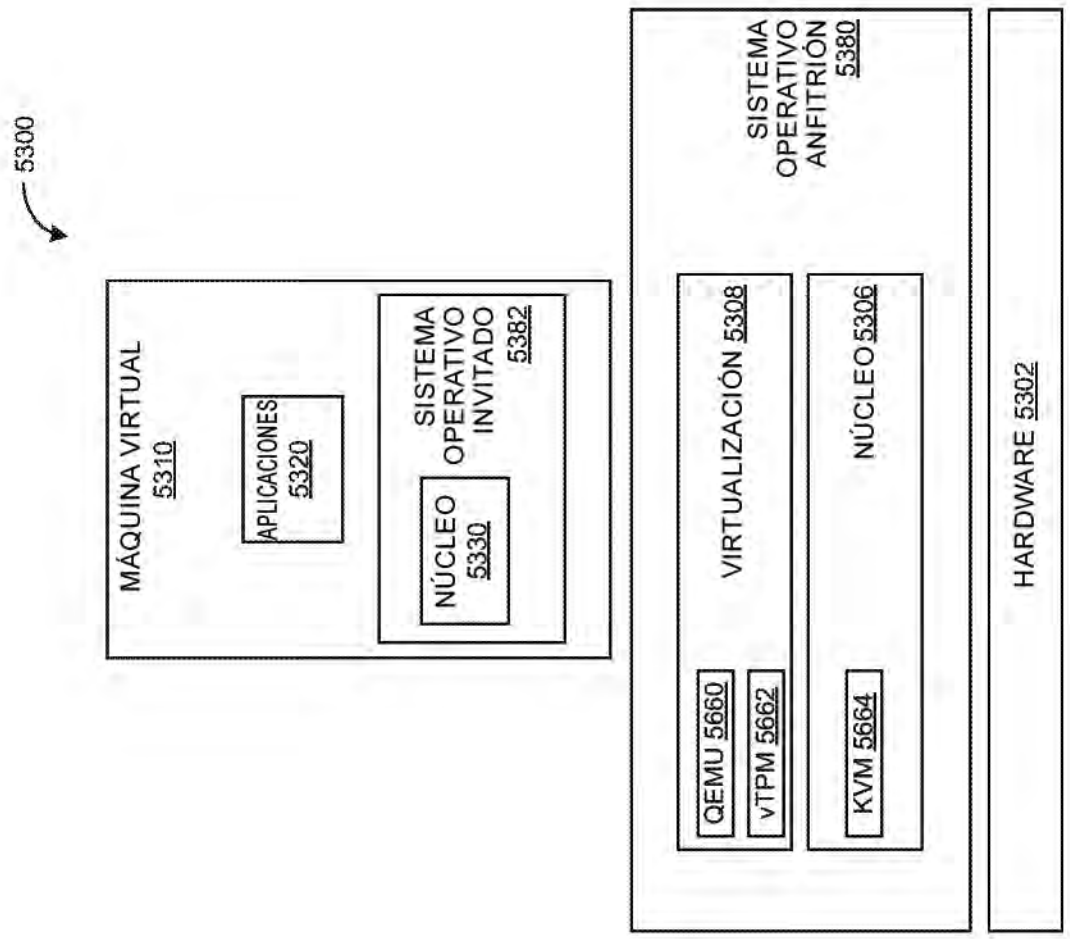

5300
MÁQUINA VIRTUAL
5310
APLICACIONES
5320
SISTEMA OPERATIVO INVITADO
5382
NÚCLEO
5330
SISTEMA OPERATIVO ANFITRIÓN
5380
VIRTUALIZACIÓN 5308
QEMU 5660
vTPM 5662
NÚCLEO 5306
KVM 5664
HARDWARE 5302

FIG. 53

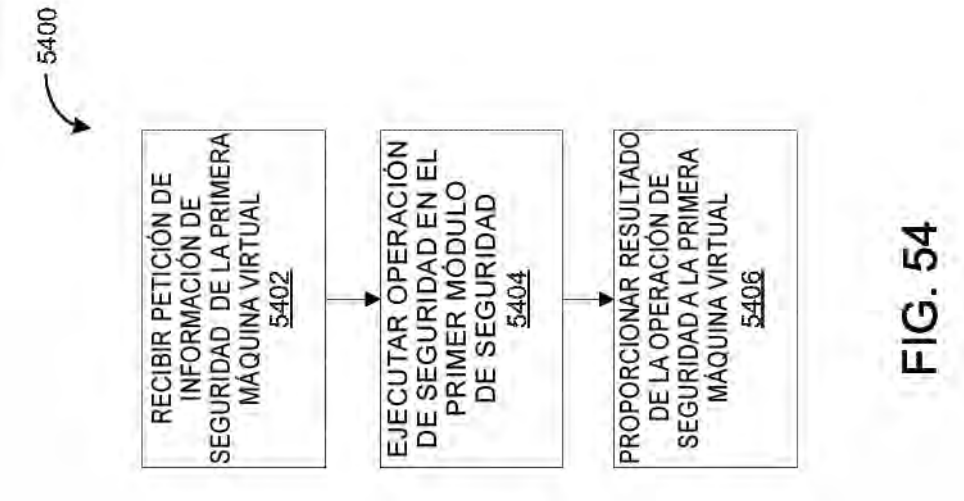

5400
RECIBIR PETICIÓN DE INFORMACIÓN DE SEGURIDAD DE LA PRIMERA MÁQUINA VIRTUAL
5402
EJECUTAR OPERACIÓN DE SEGURIDAD EN EL PRIMER MÓDULO DE SEGURIDAD
5404
PROPORCIONAR RESULTADO DE LA OPERACIÓN DE SEGURIDAD A LA PRIMERA MÁQUINA VIRTUAL
5406

FIG. 54

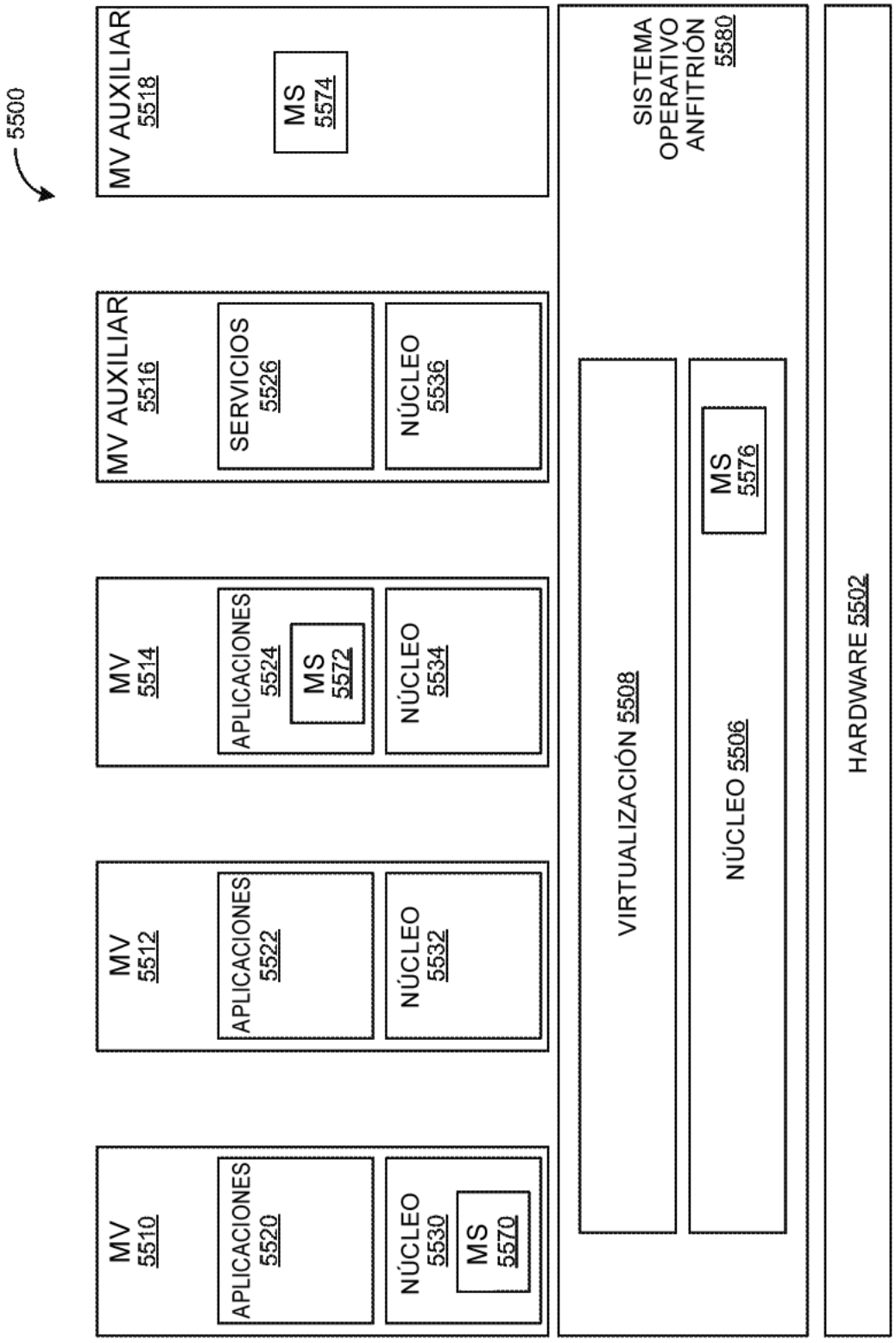

5500
MV AUXILIAR 5518
MS 5574
MV AUXILIAR 5516
SERVICIOS 5526
NÚCLEO 5536
MV 5514
APLICACIONES 5524
MS 5572
NÚCLEO 5534
MV 5512
APLICACIONES 5522
NÚCLEO 5532
MV 5510
APLICACIONES 5520
NÚCLEO 5530
MS 5570
SISTEMA OPERATIVO ANFITRIÓN 5580
VIRTUALIZACIÓN 5508
NÚCLEO 5506
MS 5576
HARDWARE 5502

FIG. 55