(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 676 143**

(51) Int. CI.:

G06F 11/18 (2006.01)
G06F 21/60 (2006.01)
G06F 21/62 (2006.01)
H04L 29/06 (2006.01)
G06F 21/72 (2006.01)
G06F 11/10 (2006.01)
G06F 11/20 (2006.01)
H04L 9/08 (2006.01)
H04L 29/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **31.03.2011 PCT/US2011/030811**

(87) Fecha y número de publicación internacional: **06.10.2011 WO11123699**

(96) Fecha de presentación y número de la solicitud europea: **31.03.2011 E 11714195 (2)**

(97) Fecha y número de publicación de la concesión europea: **09.05.2018 EP 2553905**

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

(30) Prioridad:

01.04.2010 US 320242 P
31.03.2010 US 319658 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
17.07.2018

(73) Titular/es:

SECURITY FIRST CORP. (33.3%)
29811 Santa Margarita Parkway, Suite 600
Rancho Santa Margarita, CA 92688, US;
ORSINI, RICK L. (33.3%) y
O'HARE, MARK S. (33.3%)

(72) Inventor/es:

O'HARE, MARK S. y
ORSINI, RICK L.

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Sistemas y métodos para asegurar datos en movimiento

Referencia cruzada a solicitudes relacionadas

La presente solicitud reivindica el beneficio de la solicitud de patente provisional de los Estados Unidos con n.º de serie 61/319.658, presentada el 31 de marzo de 2010, y a la solicitud de patente provisional de los Estados Unidos con n.º de serie 61/320.242, presentada el 1 de abril de 2010.

Campo de la invención

La presente invención se refiere a sistemas y métodos para asegurar datos en movimiento. Los sistemas y métodos que se describen en el presente documento se pueden usar junto con otros sistemas y métodos que se describen en la patente de los Estados Unidos publicada del mismo solicitante con n.º 7.391.865 y en las solicitudes de patente de Estados Unidos del mismo solicitante con n.º 2006/0177061 A1, presentada el 25 de octubre 2005, 2007/0160198 A1, presentada el 20 de noviembre de 2006, 2008/0137857, presentada el 7 de noviembre de 2007, 2008/0183992 A1, presentada el 5 de diciembre de 2007, 2008/0244277 A1, presentada el 18 de abril de 2008, 2009/0097661 A1, presentada el 12 de septiembre de 2008, 2009/0177894 A1, presentada el 7 de enero de 2009, 2009/0226375 A1, presentada el 23 de febrero de 2009, 2010/0299313 A1, presentada el 19 de mayo de 2010, 2011/0202755 A1, presentada el 24 de noviembre de 2010 y en las solicitudes de patentes Provisionales de Estados Unidos con n.º 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 y 61/384.583, presentada el 20 de septiembre de 2010.

El documento US 7.577.689 divulga un método y sistema para archivar datos en los que los datos originales se convierten en una pluralidad de comparticiones y se distribuyen. El documento WO 2008/142440 divulga un aparato de procesamiento de mensajes que retiene y edita una cola ordenada de los mensajes electrónicos. El documento US 6.260.125 divulga un sistema de creación de reflejos de disco asíncrono con un primer volumen de almacenamiento, una cola de escritura conectada para recibir también solicitudes de escritura que están dirigidas al primer volumen de almacenamiento, y un segundo volumen de almacenamiento que está conectado con la cola de escritura. El documento US 2007/0079082 A1 divulga un sistema de almacenamiento de archivos de datos digitales en el que se dispersan archivos de datos en un número de “rebanadas” de archivo. Cuando se están escribiendo comparticiones de archivo dispersadas en una red de almacenamiento dispersada que no se encuentra disponible, los clientes de la red designan las comparticiones de datos que no se podrían escribir en ese instante en una lista de reconstrucción. El documento US 2008/0281879 A1 divulga un controlador de almacenamiento para ejecutar una recuperación de datos usando contenidos de almacenamiento de un volumen primario y un volumen de base. Klensin, J., “*Simple Main Transfer Protocol, RFC 5321*”, octubre de 2008, norma del Grupo de Tareas Especiales de Ingeniería en Internet (IETF, *Internet Engineering Task Force*), Sociedad de Internet (ISOC, *Internet Society*), Suiza, expone la especificación del protocolo básico para el transporte de correo electrónico en Internet. Granger, G., et al, “*PASIS: A Distributed Framework for Perpetually Available and Secure Information Systems*” divulga un sistema de almacenamiento descentralizado en el que la información se divide en particiones entre nodos usando esquemas de distribución y de redundancia de datos.

Sumario

De acuerdo con un aspecto, un método para leer y escribir un conjunto de datos comprende dividir el conjunto de datos en una o más comparticiones de datos usando un algoritmo de dispersión de información, almacenar las una o más comparticiones de datos en localizaciones de compartición, determinar que al menos una de las localizaciones de compartición se encuentra no disponible para las operaciones de almacenamiento de datos, y almacenar las operaciones de almacenamiento de datos entrantes que están asociadas con cada una de las localizaciones de compartición no disponibles en colas respectivas únicas para cada una de las localizaciones de compartición no disponibles.

El presente aspecto también proporciona un sistema que está adaptado para realizar un método de este tipo.

De esta forma, se pueden proporcionar sistemas y métodos para leer y escribir un conjunto de datos. El método se puede usar para identificar y registrar las operaciones de almacenamiento de datos que están asociadas con una o más comparticiones de datos que están almacenadas en una o más localizaciones de compartición. Las localizaciones de compartición pueden incluir cualquier instalación de almacenamiento de datos adecuada o combinaciones adecuadas de instalaciones de almacenamiento de datos, tales como un disco duro local o en red, un almacenamiento extraíble tal como una llave de USB, o los recursos de un proveedor de almacenamiento en la nube tal como DropBox o Amazon S3. El método puede usar registros para registrar cada una de las solicitudes de lectura y de escritura en las localizaciones de compartición. En algunas formas de realización, el registro puede ser

una estructura de datos de cola que almacena información que está asociada con operaciones de almacenamiento de datos fallidas.

En algunas formas de realización, la cola puede mantener información que está asociada con el estado de cada localización de compartición. Por ejemplo, el método puede determinar que una o más de las localizaciones de compartición se encuentra no disponible para procesar las operaciones de almacenamiento de datos. A continuación, se puede establecer y mantener una cola para cada una de las localizaciones de compartición no disponibles. En algunas formas de realización, las colas pueden ser únicas con respecto a cada una de las localizaciones de compartición no disponibles. En algunas formas de realización, las colas pueden almacenar las operaciones de almacenamiento de datos entrantes que están asociadas con cada una de las localizaciones de compartición no disponibles. Cuando una localización de compartición particular pasa a estar disponible, se pueden ejecutar las operaciones de almacenamiento de datos que están almacenadas en la cola única para esa localización de compartición.

En algunas formas de realización, el método puede aprovechar tanto la memoria como el almacenamiento en disco con el fin de mantener la cola. Por ejemplo, se puede establecer un límite que define la cantidad de operaciones de almacenamiento de datos que se pueden almacenar en las colas. Si se determina que se supera el límite de cola para una cola particular, los mensajes en la cola se pueden transferir de la memoria al almacenamiento en disco. De esta forma, el método puede asegurar que no se supera la memoria del sistema que está ejecutando el método.

En algunas formas de realización, el método puede definir una cantidad máxima de tiempo que una localización de compartición se encuentra no disponible para las operaciones de almacenamiento de datos. Si se determina que se supera esta cantidad máxima de tiempo para una localización de compartición particular, el método puede rechazar aceptar las operaciones de almacenamiento de datos entrantes para la localización de compartición particular. De esta forma, la localización de compartición particular se marca como un fallo catastrófico y todas las operaciones de almacenamiento de datos que están asociadas con la localización de compartición se detienen hasta que se haya reparado o reconstruido la localización de compartición.

En algunas formas de realización, el método puede determinar que ya no se puede confiar en la integridad de los datos dentro de una localización de compartición particular. El método puede tomar esta determinación basándose en el número de operaciones de almacenamiento de datos que han fallado para una localización de compartición particular. Si este número supera un número máximo establecido, la localización de compartición se puede marcar como que se encuentra en un estado de fallo crítico, y se pueden descartar las operaciones de almacenamiento de datos que están almacenadas en la cola que está asociada con esa localización de compartición. Además, se puede descartar cualquier operación de almacenamiento de datos entrante para la localización de compartición en el estado de fallo crítico. De esta forma, el método puede asegurar que se conserva la memoria o el espacio en disco del sistema que está ejecutando el método.

En algunas formas de realización, el método puede prever que se reconstruya una compartición al tiempo que se mantienen otras comparticiones en el sistema como disponibles para su uso normal. Este proceso de reconstrucción puede usar otras localizaciones de compartición que están en línea y contienen unos datos similares a la localización de compartición que se está reconstruyendo. En algunas formas de realización, se puede mantener una lista de archivos que se han restaurado en la localización de compartición que se está reconstruyendo. Cuando se recibe una solicitud para realizar una operación de almacenamiento de datos sobre un archivo que está asociado con la localización de compartición que se está reconstruyendo, el servicio de registro diario puede determinar si el archivo se encuentra la lista. Si el archivo se encuentra la lista, la operación de almacenamiento de datos se puede registrar y ejecutar una vez que la localización de compartición ha acabado de reconstruirse. Si el archivo no se encuentra en la lista, se puede descartar la operación de almacenamiento de datos.

Breve descripción de los dibujos

Algunas formas de realización a modo de ejemplo se describen con detalle a continuación junto con los dibujos adjuntos, que tienen por objeto 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 algunos aspectos de una forma de realización de la invención;
la figura 2 ilustra un diagrama de bloques del motor de confianza de la figura 1, de acuerdo con algunos aspectos de una forma de realización de la invención;
la figura 3 ilustra un diagrama de bloques del motor de transacción de la figura 2, de acuerdo con algunos aspectos de una forma de realización de la invención;
la figura 4 ilustra un diagrama de bloques del depósito de la figura 2, de acuerdo con algunos aspectos de una forma de realización de la invención;
la figura 5 ilustra un diagrama de bloques del motor de autenticación de la figura 2, de acuerdo con algunos aspectos de una forma de realización de la invención;
la figura 6 ilustra un diagrama de bloques del motor criptográfico de la figura 2, de acuerdo con algunos aspectos de una forma de realización de la invención;

la figura 7 ilustra un diagrama de bloques de un sistema depósito, de acuerdo con algunos aspectos de otra forma de realización de la invención;
la figura 8 ilustra un diagrama de flujo de un proceso de división de datos de acuerdo con algunos aspectos de una forma de realización de la invención;
la figura 9, Panel A ilustra un flujo de datos de un proceso de inscripción de acuerdo con algunos aspectos de una forma de realización de la invención;
la figura 9, Panel B ilustra un diagrama de flujo de un proceso de interoperabilidad de acuerdo con algunos aspectos de una forma de realización de la invención;
la figura 10 ilustra un flujo de datos de un proceso de autenticación de acuerdo con algunos aspectos de una forma de realización de la invención;
la figura 11 ilustra un flujo de datos de un proceso de firma de acuerdo con algunos aspectos de una forma de realización de la invención;
la figura 12 ilustra un flujo de datos y un proceso de encriptación / desencriptación de acuerdo con algunos aspectos y otra forma de realización más de la invención;
la figura 13 ilustra un diagrama de bloques simplificado de un sistema de motor de confianza de acuerdo con algunos aspectos de otra forma de realización de la invención;
la figura 14 ilustra un diagrama de bloques simplificado de un sistema de motor de confianza de acuerdo con algunos aspectos de otra forma de realización de la invención;
la figura 15 ilustra un diagrama de bloques del módulo de redundancia de la figura 14, de acuerdo con algunos aspectos de una forma de 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 tal como se muestra en la figura 16 de la invención;
la figura 18 ilustra un proceso para realizar arbitraje de confianza en un aspecto de la invención tal como se muestra en la figura 17; y
la figura 19 ilustra una transacción de muestra entre un usuario y un distribuidor de acuerdo con algunos aspectos de una forma de realización de la invención en donde un contacto basado en web inicial conduce 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 servicio criptográfico que proporciona funciones de seguridad a un sistema de usuario.
La figura 21 ilustra un proceso para analizar, dividir y / o separar datos con encriptación y almacenamiento de la clave maestra de encriptación con los datos.
La figura 22 ilustra un proceso para analizar, dividir y / o separar datos con encriptación y almacenar la clave maestra de encriptación de manera separada de los datos.
La figura 23 ilustra el proceso de clave intermedio para analizar, dividir y / o separar datos con encriptación y almacenamiento de la clave maestra de encriptación con los datos.
La figura 24 ilustra el proceso de clave intermedio para analizar, dividir y / o separar datos con encriptación y almacenar la clave maestra de encriptación de manera separada de los datos.
La figura 25 ilustra la utilización de los métodos y sistemas criptográficos de la presente invención con un pequeño grupo de trabajo.
La figura 26 es un diagrama de bloques de un sistema de seguridad de testigo físico ilustrativo que emplea el analizador de datos seguro de acuerdo con una forma de realización de la presente invención.
La figura 27 es un diagrama de bloques de una disposición ilustrativa en la que el analizador de datos seguro está integrado en un sistema de acuerdo con una forma de 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 forma de realización de la presente invención.
La figura 29 es un diagrama de bloques de otro sistema de datos en movimiento ilustrativo de acuerdo con una forma de realización de la presente invención.
Las figuras 30 - 32 son diagramas de bloques de un sistema ilustrativo que tiene el analizador de datos seguro integrado de acuerdo con una forma de realización de la presente invención.
La figura 33 es un diagrama de flujo de proceso de un proceso ilustrativo para analizar y dividir datos de acuerdo con una forma de realización de la presente invención.
La figura 34 es un diagrama de flujo de proceso de un proceso ilustrativo para restaurar porciones de datos en datos originales de acuerdo con una forma de realización de la presente invención.
La figura 35 es un diagrama de flujo de proceso de un proceso ilustrativo para dividir datos al nivel de bits de acuerdo con una forma de realización de la presente invención.
La figura 36 es un diagrama de flujo de proceso de etapas y características ilustrativas, que se pueden usar en cualquier combinación adecuada, con cualquier adición, borrado o modificación adecuada de acuerdo con una forma de realización de la presente invención.
La figura 37 es un diagrama de flujo de proceso de etapas y características ilustrativas que se pueden usar en cualquier combinación adecuada, con cualquier adición, borrado o modificación adecuada de acuerdo con una forma de realización de la presente invención.
La figura 38 es un diagrama de bloques simplificado del almacenamiento de la clave y componentes de datos en las comparticiones, que se puede usar en cualquier combinación adecuada, con cualquier adición, borrado o modificación adecuada de acuerdo con una forma de realización de la presente invención.

La figura 39 es un diagrama de bloques simplificado del almacenamiento de la clave y componentes de datos en las comparticiones usando una clave de grupo de trabajo, que se puede usar en cualquier combinación adecuada, con cualquier adición, borrado o modificación adecuada de acuerdo con una forma de realización de la presente invención.

Las figuras 40A y 40B son diagramas de flujo de proceso simplificados e ilustrativos para la generación de encabezamientos y división de datos para datos en movimiento, que se pueden usar en cualquier combinación adecuada, con cualquier adición, borrado o modificación adecuada de acuerdo con una forma de realización de la presente invención.

La figura 41 es un diagrama de bloques simplificado de un formato de compartición ilustrativo, que se puede usar en cualquier combinación adecuada, con cualquier adición, borrado o modificación adecuada de acuerdo con una forma de realización de la presente invención.

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

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

La figura 44 es un diagrama de bloques de una disposición ilustrativa en la que se usa el analizador de datos seguro para servicios de datos seguros en la nube de acuerdo con una forma de realización de la presente invención.

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

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

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

La figura 48 es un diagrama esquemático de una disposición ilustrativa en la que se usa el analizador de datos seguro para almacenamiento de datos seguro en una pluralidad de dispositivos de almacenamiento en una nube de acuerdo con una forma de realización de la presente invención.

La figura 49 es un diagrama esquemático de una disposición ilustrativa en la que se usa el analizador de datos seguro para almacenamiento de datos seguro en una pluralidad de nubes privadas y públicas de acuerdo con una forma de realización de la presente invención.

La figura 50 es un diagrama esquemático de una disposición ilustrativa en la que se usa el analizador de datos seguro para almacenamiento de datos seguro en una pluralidad de nubes privadas y públicas mediante una Internet pública de acuerdo con una forma de realización de la presente invención.

La figura 51 es un diagrama esquemático de una disposición ilustrativa en la que se usa el analizador de datos seguro para almacenamiento de datos seguro en un dispositivo de almacenamiento extraíble del usuario de acuerdo con una forma de realización de la presente invención.

La figura 52 es un diagrama esquemático de una disposición ilustrativa en la que se usa el analizador de datos seguro para almacenamiento de datos seguro en una pluralidad de dispositivos de almacenamiento de usuario de acuerdo con una forma de realización de la presente invención.

La figura 53 es un diagrama esquemático de una disposición ilustrativa en la que se usa el analizador de datos seguro para almacenamiento de datos seguro en una pluralidad de nubes públicas y privadas y al menos un dispositivo de almacenamiento de usuario de acuerdo con una forma de realización de la presente invención.

La figura 54 es un diagrama esquemático de un dispositivo de aceleración de coprocesador para el analizador de datos seguro de acuerdo con una forma de realización de la presente invención.

La figura 55 es un primer diagrama de flujo de proceso de un proceso de aceleración ilustrativo que usa el dispositivo de aceleración de coprocesador de la figura 54 para el analizador de datos seguro de acuerdo con una forma de realización de la presente invención.

La figura 56 es un segundo diagrama de flujo de proceso de un proceso de aceleración ilustrativo que usa el dispositivo de aceleración de coprocesador de la figura 54 para el analizador de datos seguro de acuerdo con una forma de realización de la presente invención.

La figura 57 ilustra un proceso por el que los datos se dividen en N comparticiones y se almacenan, de acuerdo con una forma de realización ilustrativa de la presente invención.

La figura 58 ilustra un proceso por el que las comparticiones de datos se reconstruyen y / o se vuelve a aplicar la clave, de acuerdo con una forma de realización ilustrativa de la presente invención.

La figura 59 es un proceso ilustrativo para operar un servicio de registro diario en una forma de realización de la presente invención.

La figura 60 es un proceso ilustrativo para operar un servicio de registro diario en una forma de realización de la presente invención.

La figura 61 es un proceso ilustrativo para operar un servicio de registro diario usando un estado de fallo crítico en una forma de realización de la presente invención.

La figura 62 es un proceso ilustrativo para operar un servicio de registro diario usando un estado de reconstrucción crítico en una forma de realización de la presente invención.

Descripción detallada de las formas de realización ilustrativas

Un aspecto de la presente invención es proporcionar un sistema criptográfico en donde uno o más servidores seguros, o un motor de confianza, almacenan claves criptográficas y datos de autenticación de usuario. El sistema puede almacenar datos a través de uno o más dispositivos de almacenamiento en una nube. La nube puede incluir dispositivos de almacenamiento privados (accesibles únicamente para un conjunto particular de usuarios) o dispositivos de almacenamiento públicos (accesibles para cualquier conjunto de usuarios que se suscribe en el proveedor de almacenamiento).

Los usuarios acceden a la funcionalidad de los sistemas criptográficos convencionales a través del acceso de red al motor de confianza, no obstante, el motor de confianza no libera las claves reales y otros datos de autenticación y por lo tanto, las claves y los datos permanecen seguros. Este almacenamiento de claves céntrico en servidor y los datos de autenticación proporcionan seguridad independiente del usuario, portabilidad, disponibilidad y sencillez.

Debido a que los usuarios pueden estar seguros de, o confiar en, el sistema criptográfico para realizar autenticación de usuarios y documentos y otras funciones criptográficas, se puede incorporar en el sistema una amplia diversidad de funcionalidades. Por ejemplo, el proveedor de motor de confianza puede garantizar contra repudiación del acuerdo mediante, por ejemplo, la autentificación de los participantes del acuerdo, firmando de forma digital el acuerdo en nombre de o para los participantes, y almacenar un registro del acuerdo firmado de forma digital por cada participante. Además, el sistema criptográfico puede monitorizar acuerdos y determinar aplicar grados variables de autenticación, basándose en, por ejemplo, precio, usuario, distribuidor, localización geográfica, lugar de uso o similares.

Para facilitar un entendimiento completo de la invención, el resto de la descripción detallada describe la invención con referencia a las figuras, en las que se hace referencia a los elementos similares con los mismos números a lo largo de todo el presente documento.

La figura 1 ilustra un diagrama de bloques de un sistema criptográfico 100, de acuerdo con algunos aspectos de una forma de realización de la invención. Tal 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 distribuidor 120, que se comunica a través de un enlace de comunicación 125.

De acuerdo con una forma de realización de la invención, el sistema de usuario 105 comprende un ordenador de fin general convencional que tiene uno o más microprocesadores, tales como, por ejemplo, un procesador basado en Intel. Además, el sistema de usuario 105 incluye un sistema operativo apropiado, tal como, por ejemplo, un sistema operativo que puede incluir gráficos o ventanas, tal como Windows, Unix, Linux o similares. Tal como se muestra en la figura 1, el sistema de usuario 105 puede incluir un dispositivo biométrico 107. El dispositivo biométrico 107 puede captar de forma ventajosa una biométrica del usuario y transferir la biométrica captada al motor de confianza 110. De acuerdo con una forma de realización de la invención, el dispositivo biométrico puede comprender de forma ventajosa un dispositivo que tiene atributos y características similares a las que se divulgan en la solicitud de patente de los Estados Unidos con n.º 08/926.277, presentada el 5 de septiembre de 1997, que se titula "*RELIEF OBJECT IMAGE GENERATOR*", la solicitud de patente de los Estados Unidos con n.º 09/558.634, presentada el 26 de abril de 2000, que se titula "*IMAGING DEVICE FOR A RELIEF OBJECT AND SYSTEM AND METHOD OF USING THE IMAGE DEVICE*", la solicitud de patente de los Estados Unidos con n.º 09/435.011, presentada el 5 de noviembre de 1999, que se titula "*RELIEF OBJECT SENSOR ADAPTOR*" y la solicitud de patente de los Estados Unidos con n.º 09/477.943, presentada el 5 de enero de 2000, que se titula "*PLANAR OPTICAL IMAGE SENSOR AND SYSTEM FOR GENERATING AN ELECTRONIC IMAGE OF A RELIEF OBJECT FOR FINGERPRINT READING*", todas las cuales son de propiedad del cesionario actual, y la totalidad de las cuales se incorporan por la presente por referencia en el presente documento.

Además, el sistema de usuario 105 se puede conectar con el enlace de comunicación 125 a través de un proveedor de servicio convencional, tal como, por ejemplo, una marcación, línea de abonado digital (DSL, *digital subscriber line*), cable módem, conexión de fibra o similares. De acuerdo con otra forma de realización, el sistema de usuario 105 se conecta con el enlace de comunicación 125 a través de una conectividad de red tal como, por ejemplo, una red de área local o extensa. De acuerdo con una forma de realización, el sistema operativo incluye una pila de TCP / IP que maneja todo el tráfico de mensajes entrantes y salientes pasados a través del enlace de comunicación 125.

A pesar de que el sistema de usuario 105 se divulga con referencia a las formas de realización anteriores, la invención no tiene por objeto estar limitada de esta manera. En su lugar, un experto en la materia reconocerá a partir de la divulgación del presente documento, un número amplio de formas de realización alternativas del sistema de usuario 105, que incluyen casi cualquier dispositivo informático que pueda enviar o recibir información desde otro sistema informático. Por ejemplo, el sistema de usuario 105 puede incluir, pero sin limitación, una estación de trabajo informática, una televisión interactiva, un quiosco interactivo, un dispositivo informático móvil personal, tal como un asistente digital, un teléfono móvil, un portátil, o similares, un dispositivo de comunicaciones inalámbricas, una tarjeta inteligente, un dispositivo informático embebido, o similares, que puede interactuar con el enlace de comunicación

125. En tales sistemas alternativos, los sistemas operativos se diferenciarán de la misma manera y estarán adaptados para el dispositivo particular. No obstante, de acuerdo con una forma de realización, los sistemas operativos continúan proporcionando de forma ventajosa 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 forma de realización, el motor de confianza 110 comprende uno o más servidores seguros para acceder y almacenar información sensible, que puede estar en cualquier tipo o forma de datos, tales como, pero sin limitación texto, audio, vídeo, datos de autenticación de usuario y claves criptográficas públicas y privadas. De acuerdo con una forma de realización, los datos de autenticación incluyen datos designados para identificar de manera inequívoca a un usuario del sistema criptográfico 100. Por ejemplo, los datos de autenticación pueden incluir un número de identificación de usuario, una o más biométricas, y una serie de preguntas y respuestas generadas mediante el motor de confianza 110 o el usuario, pero contestadas inicialmente por el usuario en la inscripción. Las preguntas anteriores pueden incluir datos demográficos, tales como lugar de nacimiento, dirección, aniversarios, o similares, datos personales, tales como nombre de soltera de la madre, helado favorito, o similares, u otros datos designados para identificar de manera inequívoca al usuario. El motor de confianza 110 compara unos datos de autenticación del usuario que están asociados con una transacción actual, con los datos de autenticación proporcionados en un tiempo anterior, tal como, por ejemplo, durante la inscripción. El motor de confianza 110 puede requerir de forma ventajosa que el usuario produzca los datos de autenticación en el momento de cada transacción, o, el motor de confianza 110 puede permitir de forma ventajosa al usuario producir de forma periódica datos de autenticación, tales como en el comienzo de una cadena de transacciones o en el inicio de sesión en un sitio web de un distribuidor particular.

De acuerdo con la forma de realización en donde el usuario produce datos biométricos, el usuario proporciona una característica física, tal como, pero sin limitación, exploración facial, exploración de mano, exploración de oreja, exploración de iris, exploración de retina, patrón vascular, ADN, una huella digital, escritura o el habla, al dispositivo biométrico 107. El dispositivo biométrico produce de forma ventajosa un patrón electrónico, o biométrico, de la característica física. El patrón electrónico se transfiere a través del sistema de usuario 105 al motor de confianza 110 para cualquiera de los fines de inscripción 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 esos datos de autenticación (datos de autenticación actuales) y los datos de autenticación proporcionados en el momento de la inscripción (datos de autenticación de inscripción), el motor de confianza 110 proporciona al usuario con la funcionalidad criptográfica completa. Por ejemplo, el usuario autenticado de forma apropiada puede emplear de forma ventajosa el motor de confianza 110 para realizar troceo, firma digital, encriptación y desencriptación (a menudo denominadas juntas como únicamente encriptación), creación o distribución de 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, asegurando de esta manera la integridad de las claves criptográficas.

De acuerdo con una forma de realización, el motor de confianza 110 genera y almacena claves criptográficas. De acuerdo con otra forma de realización, al menos una clave criptográfica está asociada con cada usuario. Además, cuando las claves criptográficas incluyen tecnología de clave pública, cada clave privada que está asociada con un usuario se genera en, y no se libera de, el motor de confianza 110. Por lo tanto, siempre que el usuario tenga acceso al motor de confianza 110, el usuario puede realizar funciones criptográficas usando su clave privada o pública. Tal acceso remoto proporciona de forma ventajosa a los usuarios permanecer completamente móviles y acceder a la funcionalidad criptográfica a través de prácticamente cualquier conexión de Internet, tal como teléfonos celulares y satélites, quioscos, portátiles, habitaciones de hotel y similares.

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

Un experto en la materia reconocerá a partir de la divulgación del presente documento que las claves criptográficas pueden incluir de forma ventajosa alguna o todas de las claves simétricas, claves públicas, y claves privadas. Además, un experto en la materia reconocerá a partir de la divulgación del presente documento que las claves anteriores se pueden implementar con un amplio número de algoritmos disponibles de tecnologías comerciales, tales como, por ejemplo, RSA, ELGAMAL, o similares.

La figura 1 ilustra también la autoridad de certificación 115. De acuerdo con una forma de realización, la autoridad de certificación 115 puede comprender de forma ventajosa una organización o compañía de terceros de confianza que expide certificados digitales, tales como, por ejemplo, VeriSign, Baltimore, Entrust, o similares. El motor de confianza 110 puede transmitir de forma ventajosa solicitudes de certificados digitales, a través de uno o más protocolos de certificados digitales convencionales, tales como, por ejemplo, PKCS10, a la autoridad de certificación 115. En respuesta, la autoridad de certificación 115 expedirá un certificado digital en uno más de un número de diferentes

protocolos, tales como, por ejemplo, PKCS7. De acuerdo con una forma de realización de la invención, el motor de confianza 110 solicita certificados digitales desde varios o todas las autoridades de certificados 115 importantes de tal modo que el motor de confianza 110 tenga acceso a un certificado digital que se corresponde con la norma de certificado de cualquier parte solicitante.

De acuerdo con otra forma de realización, el motor de confianza 110 realiza de forma interna expediciones de certificados. En esta forma de realización, el motor de confianza 110 puede acceder a un sistema de certificados para generar certificados y / o puede generar de forma interna certificados cuando se soliciten, tal como, por ejemplo, en el momento de generación de claves o en la norma de certificado solicitada en el momento de la solicitud. El motor de confianza 110 se divulgará en mayor detalle a continuación.

La figura 1 ilustra también el sistema de distribuidor 120. De acuerdo con una forma de realización, el sistema de distribuidor 120 comprende de forma ventajosa un servidor web. Los servidores web habituales sirven en general contenido a través de Internet usando uno de varios lenguajes de marcas de Internet o normas de formato de documento, tales como el Lenguaje de Marcas de Híper Texto (HTML, *Hyper-Text Markup Language*) o el Lenguaje de Marcas Extensible (XML, *Extensible Markup Language*). El servidor web acepta solicitudes desde exploradores como Netscape e Internet Explorer y a continuación devuelve los documentos electrónicos apropiados. Se puede usar un número de tecnologías de lado de servidor o de lado de cliente para aumentar la potencia del servidor web más allá de su capacidad para entregar documentos electrónicos convencionales. Por ejemplo, estas tecnologías pueden incluir secuencias de comandos de Interfaz Común de Pasarela (CGI, *Common Gateway Interface*), seguridad de Capa de Conexiones Seguras (SSL, *Secure Sockets Layer*), y Páginas de Servidor Activas (ASP, *Active Server Page*). El sistema de distribuidor 120 puede proporcionar de forma ventajosa contenido electrónico relacionado con transacciones comerciales, personales, educacionales u otras.

A pesar de que el sistema de distribuidor 120 se divulga con referencia a las formas de realización anteriores, la invención no tiene por objeto estar limitada de esta manera. En su lugar, un experto en la materia reconocerá a partir de la divulgación del presente documento que el sistema de distribuidor 120 puede comprender de forma ventajosa cualquiera de los dispositivos que se describen con referencia al sistema de usuario 105 o combinaciones de los mismos.

La figura 1 ilustra también 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 distribuidor 120. De acuerdo con una forma de realización, el enlace de comunicación 125 comprende preferiblemente Internet. Internet, tal como se usa a lo largo de toda esta divulgación es una red global de ordenadores. La estructura de Internet, que es bien conocida para los expertos en la materia, incluye una red troncal con redes que se ramifican a partir de la parte troncal. Estas ramificaciones, a su vez, tienen redes que se ramifican a partir de las mismas, y así sucesivamente. Los encaminadores mueven paquetes de información entre niveles de red, y a continuación desde red a red, hasta que el paquete alcanza la proximidad de su destino. Desde el destino, los anfitriones de red de destino dirigen el paquete de información al terminal apropiado o nodo. En una forma de realización ventajosa, los concentradores de encaminamiento de Internet comprenden servidores de sistema de nombre de dominio (DNS, *domain name system*) que usan el Protocolo de Control de Transmisión / Protocolo de Internet (TCP / IP, *Transmission Control Protocol / Internet Protocol*) como es bien conocido en la técnica. Los concentradores de encaminamiento se conectan a uno o más otros conmutadores de encaminamiento mediante enlaces de comunicación a alta velocidad.

Una parte conocida de Internet es la red informática mundial. La red informática mundial contiene diferentes ordenadores, que almacenan documentos que pueden presentar información gráfica y textual. Los ordenadores que proporcionan información en la red informática mundial se denominan por lo general “sitios web”. Un sitio web se define mediante una dirección de Internet que tiene una página electrónica asociada. La página electrónica se puede identificar mediante un Localizador Uniforme de Recursos (URL, *Uniform Resource Locator*). En general, una página electrónica es un documento que organiza la presentación de texto, imágenes gráficas, audio, vídeo, y así sucesivamente.

A pesar de que el enlace de comunicación 125 se divulga en términos de su forma de realización preferida, un experto en la materia reconocerá a partir de la divulgación del presente documento que el enlace de comunicación 125 puede incluir un amplio intervalo de enlaces de comunicaciones interactivos. Por ejemplo, el enlace de comunicación 125 puede incluir redes de televisión interactiva, redes de telefonía, sistemas de transmisión de datos inalámbricos, sistemas de cable bidireccionales, redes informáticas privadas o públicas personalizadas, redes de quiosco interactivas, redes de máquinas de cajeros automáticos, enlaces directos, redes de satélite o celulares y similares.

La figura 2 ilustra un diagrama de bloques del motor de confianza 110 de la figura 1 de acuerdo con algunos aspectos de una forma de realización de la invención. Tal como se muestra en la figura 2, el motor de confianza 110 incluye un motor de transacción 205, un depósito 210, un motor de autenticación 215 y un motor criptográfico 220. De acuerdo con una forma de realización de la invención, el motor de confianza 110 incluye también el almacenamiento masivo 225. Tal como se muestra adicionalmente en la figura 2, el motor de transacción 205 se comunica con el depósito 210, el motor de autenticación 215, y el motor criptográfico 220, junto con el

almacenamiento masivo 225. Además, el depósito 210 se comunica con el motor de autenticación 215, el motor criptográfico 220, y el almacenamiento masivo 225. Además, el motor de autenticación 215 se comunica con el motor criptográfico 220. De acuerdo con una forma de realización de la invención, algunas o todas las comunicaciones anteriores pueden comprender de forma ventajosa la transmisión de documentos XML a direcciones de IP que se corresponden con el dispositivo de recepción. Tal como se ha mencionado en lo que antecede, los documentos XML permiten de forma ventajosa a los diseñadores crear sus propias etiquetas de documento personalizadas, que posibilitan la definición, transmisión, validación e interpretación de datos entre aplicaciones y entre organizaciones. Además, algunas o todas las comunicaciones anteriores pueden incluir tecnologías de SSL convencionales.

De acuerdo con una forma de realización, el motor de transacción 205 comprende un dispositivo de encaminamiento de datos, tal como un servidor web convencional disponible a partir de Netscape, Microsoft, Apache, o similares. Por ejemplo, el servidor web puede recibir de forma ventajosa datos entrantes desde el enlace de comunicación 125. De acuerdo con una forma de realización de la invención, los datos entrantes se direccionan a un sistema de seguridad de extremo frontal para el motor de confianza 110. Por ejemplo, el sistema de seguridad de extremo frontal puede incluir de forma ventajosa un cortafuegos, un sistema de detección de intrusión que busca perfiles de ataque conocidos y / o un explorador de virus. Después de despejar el sistema de seguridad de extremo frontal, los datos se reciben mediante el motor de transacción 205 y se encaminan a uno del depósito 210, el motor de autenticación 215, el motor criptográfico 220, y el almacenamiento masivo 225. Además, el motor de transacción 205 monitoriza datos entrantes desde el motor de autenticación 215 y el motor criptográfico 220, y encamina los datos a sistemas particulares a través del enlace de comunicación 125. Por ejemplo, el motor de transacción 205 puede encaminar datos de forma ventajosa al sistema de usuario 105, a la autoridad de certificación 115, o al sistema de distribuidor 120.

De acuerdo con una forma de realización, los datos se encaminan usando técnicas de encaminamiento de HTTP convencionales, tales como, por ejemplo, emplear URL o Indicadores de Recursos Uniformes (URL, *Uniform Resource Locator*). Los URI son similares a los URL, no obstante, los URI indican por lo general la fuente de ficheros o acciones, tal como, por ejemplo, ejecutables, secuencias de comandos, y similares. Por lo tanto, de acuerdo con una forma de realización, el sistema de usuario 105, la autoridad de certificación 115, el sistema de distribuidor 120, y los componentes del motor de confianza 210, incluyen, de forma ventajosa, suficientes datos en los URL o URI de comunicación para que el motor de transacción 205 encamine de forma apropiada datos lo largo de todo el sistema criptográfico.

A pesar de que el encaminamiento de datos se divulga con referencia a su forma de realización preferida, un experto en la materia reconocerá un amplio número de soluciones o estrategias de encaminamiento de datos posibles. Por ejemplo, XML u otros paquetes de datos pueden, de forma ventajosa, desempaquetarse y reconocerse por su formato, contenido, o similares, de tal modo que el motor de transacción 205 pueda encaminar de forma apropiada datos a través del motor de confianza 110. Además, un experto en la materia reconocerá que el encaminamiento de datos se puede adaptar de forma ventajosa a los protocolos de transferencia de datos conforme a sistemas de redes particulares, tales como, por ejemplo, cuando el enlace de comunicación 125 comprende una red local.

De acuerdo con otra forma de realización más de la invención, el motor de transacción 205 incluye tecnologías de encriptación de SSL convencionales, de tal modo que los sistemas anteriores se pueden autenticar a sí mismos, y viceversa, con el motor de transacción 205, durante comunicaciones particulares. Tal como se usará a lo largo de toda esta divulgación, la expresión “½ SSL” se refiere a comunicaciones en donde un servidor pero no necesariamente el cliente, está autenticado por SSL, y la expresión “SSL TOTAL” se refiere a comunicaciones en donde el cliente y el servidor están autenticados por SSL. Cuando la divulgación actual usa la expresión “SSL”, la comunicación puede comprender ½ SSL o TOTAL.

A medida que el motor de transacción 205 encamina datos a los diversos componentes del sistema criptográfico 100, el motor de transacción 205 puede crear de forma ventajosa un recorrido de auditoría. De acuerdo con una forma de realización, el recorrido de auditoría incluye un registro de al menos el tipo y formato de datos encaminados mediante el motor de transacción 205 a lo largo de todo el sistema criptográfico 100. Tales datos de auditoría se pueden almacenar de forma ventajosa en el almacenamiento masivo 225.

La figura 2 ilustra también el depósito 210. De acuerdo con una forma de realización, el depósito 210 comprende una o más instalaciones de almacenamiento, tales como, por ejemplo, un servidor de directorio, un servidor de base de datos o similares. Tal como se muestra en la figura 2, el depósito 210 almacena claves criptográficas y datos de autenticación de inscripción. Las claves criptográficas se pueden corresponder de forma ventajosa con el motor de confianza 110 o a los usuarios del sistema criptográfico 100, tales como el usuario o el distribuidor. Los datos de autenticación de inscripción pueden incluir de forma ventajosa datos diseñados para identificar de manera inequívoca a un usuario, tales como, ID de usuario, contraseñas, respuestas a preguntas, datos biométricos o similares. Estos datos de autenticación de inscripción se pueden obtener de forma ventajosa en la inscripción de un usuario o en otro momento alternativo más tarde. Por ejemplo, el motor de confianza 110 puede incluir la renovación periódica u otra o la reexpedición de los datos de autenticación de inscripción.

De acuerdo con una forma de realización, la comunicación desde el motor de transacción 205 a y desde el motor de autenticación 215 y el motor criptográfico 220 comprende comunicación segura, tal como, por ejemplo tecnología de SSL convencional. Además, tal como se ha mencionado en lo que antecede, los datos de las comunicaciones a y desde el depósito 210 se pueden transferir usando URL, URI, HTTP o documentos XML, con cualquiera de los anteriores teniendo de forma ventajosa solicitudes de datos y formatos embebidos en los mismos.

Tal como se ha mencionado en lo que antecede, el depósito 210 puede comprender de forma ventajosa una pluralidad de instalaciones de almacenamiento de datos seguras. En una forma de realización de este tipo, las instalaciones de almacenamiento de datos seguras se pueden configurar de tal modo que un compromiso de la seguridad en una instalación de almacenamiento de datos individual no comprometerá las claves criptográficas o los datos de autenticación almacenados en la misma. Por ejemplo, de acuerdo con esta forma de realización, las claves criptográficas y los datos de autenticación se operan matemáticamente para aleatorizar estadística y sustancialmente los datos almacenados en cada instalación de almacenamiento de datos. De acuerdo con una forma de realización, la aleatorización de los datos de una instalación de almacenamiento de datos individual presenta esos datos indescifrables. Por lo tanto, el compromiso de una instalación de almacenamiento de datos individual produce únicamente un número indescifrable aleatorizado y no compromete la seguridad de ninguna clave criptográfica o de los datos de autenticación como una totalidad.

La figura 2 ilustra también el motor de confianza 110 que incluye el motor de autenticación 215. De acuerdo con una forma de realización, el motor de autenticación 215 comprende un comparador configurado para comparar datos a partir del motor de transacción 205 con datos a partir del depósito 210. Por ejemplo, durante la autenticación, un usuario suministra datos de autenticación actuales al motor de confianza 110 de tal modo que el motor de transacción 205 recibe los datos de autenticación actuales. Tal como se ha mencionado en lo que antecede, el motor de transacción 205 reconoce las solicitudes de datos, preferiblemente en el URL o URI, y encamina los datos de autenticación al motor de autenticación 215. Además, tras la solicitud, el depósito 210 reenvía los datos de autenticación de inscripción que se corresponden con el usuario al motor de autenticación 215. Por lo tanto, el motor de autenticación 215 tiene tanto los datos de autenticación actuales como los datos de autenticación de inscripción para comparar.

De acuerdo con una forma de realización, las comunicaciones al motor de autenticación comprenden comunicaciones seguras, tal como, por ejemplo, tecnología de SSL. Además, se puede proporcionar seguridad en los componentes del motor de confianza 110, tal como, por ejemplo, superencriptación usando tecnologías de clave pública. Por ejemplo, de acuerdo con una forma de realización, el usuario encripta los datos de autenticación actuales con la clave pública del motor de autenticación 215. Además, el depósito 210 encripta también los datos de autenticación de inscripción con la clave pública del motor de autenticación 215. De esta manera, únicamente se puede usar la clave privada del motor de autenticación para desencriptar las transmisiones.

Tal como se muestra en la figura 2, el motor de confianza 110 incluye también el motor criptográfico 220. De acuerdo con una forma de realización, el motor criptográfico comprende un módulo de manejo criptográfico, configurado para proporcionar de forma ventajosa funciones criptográficas convencionales, tales como, por ejemplo, funcionalidad de infraestructura de clave pública (PKI, *public key infrastructure*). Por ejemplo, el motor criptográfico 220 puede expedir de forma ventajosa claves públicas y privadas para usuarios del sistema criptográfico 100. De esta manera, las claves criptográficas se generan en el motor criptográfico 220 y se reenvían al depósito 210 de tal modo que al menos las claves criptográficas privadas no estén disponibles fuera del motor de confianza 110. De acuerdo con otra forma de realización, el motor criptográfico 220 aleatoriza y divide al menos los datos de clave criptográfica privada, almacenando de esta manera únicamente los datos de división aleatorizada. Similar a la división de los datos de autenticación de inscripción, el proceso de división asegura que las claves almacenadas no están disponibles fuera del motor criptográfico 220. De acuerdo con otra forma de realización, las funciones del motor criptográfico se pueden combinar con y realizarse mediante el motor de autenticación 215.

De acuerdo con una forma de realización, las comunicaciones a y desde el motor criptográfico incluyen comunicaciones seguras, tal como tecnología de SSL. Además, se pueden emplear de forma ventajosa documentos XML para transferir datos y / o realizar solicitudes de función criptográfica.

La figura 2 ilustra también el motor de confianza 110 que tiene el almacenamiento masivo 225. Tal como se ha mencionado en lo que antecede, el motor de transacción 205 mantiene los datos que se corresponden con un recorrido de auditoría y almacena tales datos en el almacenamiento masivo 225. De manera similar, de acuerdo con una forma de realización de la invención, el depósito 210 mantiene datos que se corresponden con un recorrido de auditoría y almacena tales datos en el dispositivo de almacenamiento masivo 225. Los datos de recorrido de auditoría del depósito son similares a los del motor de transacción 205 en que los datos de recorrido de auditoría comprenden un registro de las solicitudes recibidas mediante el depósito 210 y la respuesta de las mismas. Además, el almacenamiento masivo 225 se puede usar para almacenar certificados digitales que tienen la clave pública de un usuario contenida en el mismo.

A pesar de que el motor de confianza 110 se divulga con referencia a sus formas de realización preferida y alternativa, la invención no tiene por objeto estar limitada de esta manera. En su lugar, un experto en la materia

reconocerá en la divulgación en el presente documento, un amplio número de alternativas para el motor de confianza 110. Por ejemplo, el motor de confianza 110, puede realizar de forma ventajosa únicamente autenticación, o como alternativa, únicamente algunas o todas las funciones criptográficas, tales como encriptación y desencriptación de datos. De acuerdo con tales formas de realización, uno del motor de autenticación 215 y el motor criptográfico 220 se puede eliminar de forma ventajosa, creando de esta manera un diseño más sencillo para el motor de confianza 110. Además, el motor criptográfico 220 se puede comunicar también con una autoridad de certificación de tal modo que la autoridad de certificación esté incorporada en el motor de confianza 110. De acuerdo con otra forma de realización más, el motor de confianza 110 puede realizar de forma ventajosa autenticación y una o más funciones criptográficas, tales como, por ejemplo, firma digital.

La figura 3 ilustra un diagrama de bloques del motor de transacción 205 de la figura 2, de acuerdo con algunos aspectos de una forma de realización de la invención. De acuerdo con esta forma de realización, el motor de transacción 205 comprende un sistema operativo 305 que tiene un hilo de manejo y un hilo de escucha. El sistema operativo 305 puede ser, de forma ventajosa, similar a los encontrados en servidores de alto volumen convencionales, tales como, por ejemplo, servidores web disponibles a partir de Apache. El hilo de escucha monitoriza la comunicación entrante desde uno del enlace de comunicación 125, el motor de autenticación 215, y el motor criptográfico 220 para el flujo de datos entrantes. El hilo de manejo reconoce estructuras de datos particulares del flujo de datos entrantes, tales como, por ejemplo, las estructuras de datos anteriores, encaminando de esta manera los datos entrantes a uno del enlace de comunicación 125, el depósito 210, el motor de autenticación 215, el motor criptográfico 220, o el almacenamiento masivo 225. Tal como se muestra en la figura 3, los datos entrantes y salientes se pueden asegurar de forma ventajosa a través de, por ejemplo, tecnología de SSL.

La figura 4 ilustra un diagrama de bloques del depósito 210 de la figura 2 de acuerdo con algunos aspectos de una forma de realización de la invención. De acuerdo con esta forma de realización, el depósito 210 comprende uno o más servidores de protocolo ligero de acceso al directorio (LDAP, *lightweight directory access protocol*). Los servidores de directorio LDAP están disponibles a partir de una amplia diversidad de fabricantes tales como Netscape, ISO, y otros. La figura 4 muestra también que el servidor de directorio almacena preferiblemente datos 405 que se corresponden con las claves criptográficas y datos 410 que se corresponden con los datos de autenticación de inscripción. De acuerdo con una forma de realización, el depósito 210 comprende una estructura de memoria lógica única que indexa datos de autenticación y datos de clave criptográfica a una única ID de usuario. La estructura de memoria lógica única incluye preferiblemente mecanismos para asegurar un alto grado de confianza, o seguridad, en los datos almacenados en la misma. Por ejemplo, la localización física del depósito 210 puede incluir de forma ventajosa un amplio número de medidas de seguridad convencionales, tales como acceso de empleado limitado, sistemas de vigilancia de módem, y similares. Además de, o en lugar de, las seguridades físicas, el sistema o servidor informático puede incluir de forma ventajosa soluciones de soporte lógico para proteger los datos almacenados. Por ejemplo, el depósito 210 puede crear y almacenar de forma ventajosa datos 415 que se corresponden con un recorrido de auditoría de acciones emprendidas. Además, las comunicaciones entrantes y salientes se pueden encriptar de forma ventajosa con la encriptación de clave pública acoplada con tecnologías de SSL convencionales.

De acuerdo con otra forma de realización, el depósito 210 puede comprender instalaciones de almacenamiento de datos distintas y físicamente separadas, tal como se divulga adicionalmente con referencia a la figura 7.

La figura 5 ilustra un diagrama de bloques del motor de autenticación 215 de la figura 2 de acuerdo con algunos aspectos de una forma de realización de la invención. Similar al motor de transacción 205 de la figura 3, el motor de autenticación 215 comprende un sistema operativo 505 que tiene al menos un hilo de escucha y uno de manejo de una versión modificada de un servidor web convencional, tal como, por ejemplo, servidores web disponibles a partir de Apache. Tal como se muestra en la figura 5, el motor de autenticación 215 incluye acceso a al menos una clave privada 510. La clave privada 510 se puede usar de forma ventajosa por ejemplo, para desencriptar datos a partir del motor de transacción 205 o el depósito 210, que se encriptaron con una clave pública correspondiente del motor de autenticación 215.

La figura 5 ilustra también 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 forma de realización preferida de la invención, el comparador 515 incluye tecnología que puede comparar patrones potencialmente complejos relacionados con los datos biométricos de autenticación anteriores. La tecnología puede incluir soporte físico, soporte lógico, o soluciones combinadas para comparaciones de patrones, tales como, por ejemplo, los que representan patrones de huellas digitales o patrones de voz. Además, de acuerdo con una forma de realización, el comparador 515 del motor de autenticación 215 puede comparar de forma ventajosa troceos convencionales de documentos para presentar un resultado de comparación. De acuerdo con una forma de realización de la invención, el comparador 515 incluye la aplicación de heurística 530 a la comparación. La heurística 530 puede tratar de forma ventajosa circunstancias que rodean un intento de autenticación, tales como, por ejemplo, la hora del día, dirección de IP o máscara de subred, perfil de compra, dirección de correo electrónico, número de serie de procesador o ID, o similares.

Además, la naturaleza de las comparaciones de datos biométricos pueden dar como resultado grados variables de confianza que se producen desde la coincidencia de datos de autenticación biométricos actuales a datos de inscripción. Por ejemplo, a diferencia de una contraseña tradicional que puede devolver únicamente una coincidencia positiva o negativa, una huella digital se puede determinar que es una coincidencia parcial, por ejemplo una coincidencia del 90 %, una coincidencia del 75 %, o una coincidencia del 10 %, en lugar de simplemente correcto o incorrecto. Otros identificadores biométricos tales como análisis de huella vocal o reconocimiento facial pueden compartir esta propiedad de autenticación probabilística, en lugar de autenticación absoluta.

Cuando se trabaja con tal autenticación probabilista o en otros casos cuando se considera una autenticación menos de absolutamente fiable, es deseable aplicar la heurística 530 para determinar que el nivel de confianza en la autenticación proporcionada es suficientemente alto para autenticar la transacción que se está realizando.

En ocasiones se dará el caso de que la transacción en expedición sea una transacción de valor relativamente bajo en donde es aceptable autenticarse a un nivel de confianza inferior. Esto podría incluir una transacción que tenga un valor bajo de dólares que está asociado con la misma (por ejemplo, una compra de 10 $) o una transacción con bajo riesgo (por ejemplo, admisión a un sitio web de únicamente miembros).

A la inversa, para autenticar otras transacciones, puede ser deseable requerir un alto grado de confianza en la autenticación antes de permitir que la transacción continúe. Tales transacciones pueden incluir transacciones de elevado valor en dólares (por ejemplo, firmar un contrato de suministro de varios millones de dólares) o transacción con un alto riesgo si tiene lugar una autenticación inapropiada (por ejemplo, iniciar sesión de forma remota en un ordenador gubernamental).

El uso de la heurística 530 en combinación con niveles de confianza y valores de transacción se puede usar tal como se describirá a continuación para permitir al comparador proporcionar un sistema de autenticación sensible al contexto dinámico.

De acuerdo con otra forma de realización de la invención, el comparador 515 puede rastrear de forma ventajosa intentos de autenticación para una transacción particular. Por ejemplo, cuando una transacción falla, el motor de confianza 110 puede solicitar al usuario volver a introducir sus datos de autenticación actuales. El comparador 515 del motor de autenticación 215 puede emplear de forma ventajosa un limitador de intentos 535 para limitar el número de intentos de autenticación, prohibiendo de esta manera intentos de fuerza bruta para suplantar unos datos de autenticación del usuario. De acuerdo con una forma de realización, el limitador de intentos 535 comprende un módulo de soporte lógico que monitoriza transacciones de intentos de autenticación repetidos y, por ejemplo, limita los intentos de autenticación para una transacción dada a tres. Por lo tanto, el limitador de intentos 535 limitará un intento automatizado para suplantar unos datos de autenticación del individuo para, por ejemplo, simplemente tres “oportunidades”. Tras tres fallos, el limitador de intentos 535 puede denegar de forma ventajosa intentos de autenticación adicionales. Tal denegación se puede implementar de forma ventajosa a través de, por ejemplo, devolviendo el comparador 515 un resultado negativo con independencia de los datos de autenticación actuales que se están transmitiendo. Por otra parte, el motor de transacción 205 puede bloquear de forma ventajosa cualquier intento de autenticación adicional que pertenezca a una transacción en la que hayan fallado previamente tres intentos.

El motor de autenticación 215 incluye también el módulo de división de datos 520 y el módulo de ensamblaje de datos 525. El módulo de división de datos 520 comprende de forma ventajosa un módulo de soporte lógico, soporte físico, o combinación que tiene la capacidad de operar matemáticamente en diversos datos para aleatorizar sustancialmente y dividir los datos en porciones. De acuerdo con una forma de realización, los datos originales no son recreables desde una porción individual. El módulo de ensamblaje de datos 525 comprende de forma ventajosa un módulo de soporte lógico, soporte físico, o combinación configurado para operar matemáticamente en las anteriores porciones sustancialmente aleatorizadas, de tal modo que la combinación de las mismas proporciona los datos descifrados originales. De acuerdo con una forma de realización, el motor de autenticación 215 emplea el módulo de división de datos 520 para aleatorizar y dividir los datos de autenticación de inscripción en porciones, y emplea el módulo de ensamblaje de datos 525 para reensamblar las porciones en datos de autenticación de inscripción utilizables.

La figura 6 ilustra un diagrama de bloques del motor criptográfico 220 del motor de confianza 200 de la figura 2 de acuerdo con algunos aspectos de una forma de realización de la invención. Similar al motor de transacción 205 de la figura 3, el motor criptográfico 220 comprende un sistema operativo 605 que tiene al menos un hilo de escucha y uno de manejo de una versión modificada de un servidor web convencional, tal como, por ejemplo, servidores web disponibles de Apache. Tal 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 forma similar a los de la figura 5. No obstante, de acuerdo con una forma de realización, el módulo de división de datos 610 y el módulo de ensamblaje de datos 620 procesan datos de clave criptográfica, a diferencia de los anteriores datos de autenticación de inscripción. A pesar de que, un experto en la materia reconocerá a partir de la divulgación del presente 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 comprende también un módulo de manejo criptográfico 625 configurado para realizar una, alguna o todas de un amplio número de funciones criptográficas. De acuerdo con una forma de realización, el módulo de manejo criptográfico 625 puede comprender módulos de soporte lógico o programas, soporte físico, o ambos. De acuerdo con otra forma de realización, el módulo de manejo criptográfico 625 puede realizar comparaciones de datos, análisis de datos, división de datos, separación de datos, troceo de datos, encriptación o desencriptación de datos, verificación o creación de firma digital, generación de certificado digital, almacenamiento o solicitudes, generación de clave criptográfica, o similares. Además, un experto en la materia reconocerá a partir de la divulgación del presente documento que el módulo de manejo criptográfico 825 puede comprender de forma ventajosa una infraestructura de clave pública, tal como Privacidad Bastante Buena (PGP, *Pretty Good Privacy*), un sistema de clave pública basado en RSA, o un amplio número de sistemas de gestión de claves alternativos. Además, el módulo de manejo criptográfico 625 puede realizar encriptación de clave pública, encriptación de clave simétrica o ambas. Además de lo anterior, el módulo de manejo criptográfico 625 puede incluir uno o más programas o módulos informáticos, soporte físico, o ambos, para implementar funciones de interoperabilidad sin interrupciones, transparentes.

Un experto en la materia reconocerá a partir de la divulgación del presente documento que la funcionalidad criptográfica puede incluir un amplio número de diversidad de funciones relacionadas en general con sistemas de gestión de claves criptográficas.

La figura 7 ilustra un diagrama de bloques simplificado de un sistema depósito 700 de acuerdo con algunos aspectos de una forma de realización de la invención. Tal como se muestra en la figura 7, el sistema depósito 700 comprende de forma ventajosa múltiples instalaciones de almacenamiento de datos, por ejemplo, las instalaciones de almacenamiento de datos D1, D2, D3, y D4. No obstante, se entiende fácilmente por los expertos en la materia que el sistema depósito puede tener únicamente una instalación de almacenamiento de datos. De acuerdo con una forma de realización de la invención, cada una de las instalaciones de almacenamiento de datos D1 a D4 puede comprender de forma ventajosa algunos o todos los elementos que se divulgan con referencia al depósito 210 de la figura 4. Similar al depósito 210, las instalaciones de almacenamiento de datos D1 a D4 se comunican con el motor de transacción 205, el motor de autenticación 215, y el motor criptográfico 220, preferiblemente a través de SSL convencional. Enlaces de comunicación que transfieren, por ejemplo, documentos XML. Las comunicaciones desde el motor de transacción 205 pueden incluir de forma ventajosa solicitudes de datos, en el que la solicitud se difunde de forma ventajosa a la dirección de IP de cada instalación de almacenamiento de datos D1 a D4. Por otra parte, el motor de transacción 205 puede difundir solicitudes a instalaciones de almacenamiento de datos particulares basándose en un amplio número de criterios, tales como, por ejemplo, tiempo de respuesta, cargas de servidor, planificaciones de mantenimiento, o similares.

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

De acuerdo con una forma de realización, cada instalación de almacenamiento de datos, D1 a D4, comprende un sistema de almacenamiento separado e independiente, tal como, por ejemplo, un servidor de directorio. De acuerdo con otra forma de realización de la invención, el sistema depósito 700 comprende múltiples sistemas de almacenamiento de datos independientes separados geográficamente. Distribuyendo los datos sensibles en distintas e independientes instalaciones de almacenamiento D1 a D4, algunas o todas de las cuales pueden estar de forma ventajosa separadas geográficamente, el sistema depósito 700 proporciona redundancia junto con medidas de seguridad adicionales. Por ejemplo, de acuerdo con una forma de realización, únicamente son necesarios los datos desde dos de las múltiples instalaciones de almacenamiento de datos, D1 a D4, para descifrar y reensamblar los datos sensibles. Por tanto, hasta dos de las cuatro instalaciones de almacenamiento de datos D1 a D4 pueden estar inoperativas debido a mantenimiento, fallo de sistema, fallo de alimentación, o similares, sin afectar la funcionalidad del motor de confianza 110. Además, debido a que, de acuerdo con una forma de realización, los datos almacenados en cada instalación de almacenamiento de datos están aleatorizados y son indescifrables, el compromiso de cualquier instalación de almacenamiento de datos individual no compromete necesariamente los datos sensibles. Además, en la forma de realización que tiene separación geográfica de las instalaciones de almacenamiento de datos, un compromiso de múltiples instalaciones remotas geográficamente se hace cada vez más difícil. De hecho, incluso un empleado deshonesto se verá desafiado enormemente para trastornar las necesarias múltiples instalaciones de almacenamiento de datos remotas geográficamente independientes.

A pesar de que el sistema depósito 700 se divulga con referencia a sus formas de realización preferida y alternativa, la invención no tiene por objeto estar limitada de esta manera. En su lugar, un experto en la materia reconocerá a partir de la divulgación del presente documento, un amplio número de alternativas para el sistema depósito 700. Por

ejemplo, el sistema depósito 700 puede comprender una, dos o más instalaciones de almacenamiento de datos. Además, los datos sensibles se pueden operar matemáticamente de tal modo que las porciones desde dos o más instalaciones de almacenamiento de datos son necesarias para reensamblar y descifrar los datos sensibles.

Tal como se ha mencionado en lo que antecede, el motor de autenticación 215 y el motor criptográfico 220 incluyen cada uno un módulo de división de datos 520 y 610, de forma respectiva, para dividir cualquier tipo o forma de datos sensibles, tales como, por ejemplo, texto, audio, vídeo, datos de autenticación y los datos de clave criptográfica. La figura 8 ilustra un diagrama de flujo de un proceso de división de datos 800 realizado mediante el módulo de división de datos de acuerdo con algunos aspectos de una forma de realización de la invención. Tal como se muestra en la figura 8, el proceso de división de datos 800 comienza en la etapa 805 cuando se reciben los datos sensibles “S” mediante el módulo de división de datos del motor de autenticación 215 o el motor criptográfico 220. Preferiblemente, en la etapa 810, el módulo de división de datos a continuación genera un número, valor o cadena o conjunto de bits sustancialmente aleatorio, “A”. Por ejemplo, el número aleatorio A se puede generar en un amplio número de diversas técnicas convencionales disponibles para un experto en la materia, para producir números aleatorios de alta calidad adecuados para su uso en aplicaciones criptográficas. Además, de acuerdo con una forma de realización, el número aleatorio A comprende una longitud de bits que puede ser cualquier longitud adecuada, tal como más corta, más larga o igual a la longitud de bits de los datos sensibles, S.

Además, en la etapa 820 el proceso de división de datos 800 genera otro número estadísticamente aleatorio “C”. De acuerdo con la forma de realización preferida, la generación de los números estadísticamente aleatorios A y C se puede hacer de forma ventajosa en paralelo. El módulo de división de datos a continuación combina los números A y C con los datos sensibles S de tal modo que se generan nuevos números “B” y “D”. Por ejemplo, el número B puede comprender la combinación binaria de A XOR S y el número D puede comprender la combinación binaria de C XOR S. La función XOR, o la función “o exclusivo”, es bien conocida para los expertos en la materia. Las combinaciones anteriores preferiblemente tienen lugar en las etapas 825 y 830, de forma respectiva, y, de acuerdo con una forma de realización, las combinaciones anteriores también tienen lugar en paralelo. El proceso de división de datos 800 a continuación continúa a la etapa 835 en donde los números aleatorios A y C y los números B y D se emparejan de tal modo que ninguno de los emparejamientos contenga datos suficientes, por sí mismos, para reorganizar y descifrar los datos sensibles originales S. Por ejemplo, los números se pueden emparejar tal como sigue: AC, AD, BC y BD. De acuerdo con una forma de realización, cada uno de los emparejamientos anteriores se distribuye a uno de los depósitos D1 a D4 de la figura 7. De acuerdo con otra forma de realización, cada uno de los emparejamientos anteriores se distribuye de forma aleatoria a uno de los depósitos D1 a D4. Por ejemplo, durante un primer proceso de división de datos 800, el emparejamiento AC se puede enviar al depósito D2, a través de, por ejemplo, una selección aleatoria de dirección de IP de D2. A continuación, durante un segundo proceso de división de datos 800, el emparejamiento AC se puede enviar al depósito D4, a través de, por ejemplo, una selección aleatoria de la dirección de IP de D4. Además, los emparejamientos se pueden almacenar todos en un depósito, y se pueden almacenar en localizaciones separadas en dicho depósito.

Basándose en lo que antecede, el proceso de división de datos 800 coloca de forma ventajosa porciones de los datos sensibles en cada una de las cuatro instalaciones de almacenamiento de datos D1 a D4, de tal modo que ninguna instalación de almacenamiento de datos D1 a D4 única incluya suficientes datos encriptados para recrear los datos sensibles originales S. Tal como se ha mencionado en lo que antecede, tal aleatorización de los datos en porciones encriptadas no utilizables de forma individual aumenta la seguridad y proporciona que se mantenga la confianza en los datos incluso si se compromete una de las instalaciones de almacenamiento de datos, D1 a D4.

A pesar de que el proceso de división de datos 800 se divulga con referencia a su forma de realización preferida, la invención no tiene por objeto estar limitada de esta manera. En su lugar un experto en la materia reconocerá a partir de la divulgación del presente documento, un amplio número de alternativas para el proceso de división de datos 800. Por ejemplo, el proceso de división de datos puede dividir de forma ventajosa los datos en dos números, por ejemplo, el número aleatorio A y el número B y, distribuir de forma aleatoria A y B a través de dos instalaciones de almacenamiento de datos. Además, el proceso de división de datos 800 puede dividir de forma ventajosa los datos entre un amplio número de instalaciones de almacenamiento de datos a través de la generación de números aleatorios adicionales. Los datos se pueden dividir en cualquier unidad deseada, seleccionada, predeterminada o de tamaño asignado de forma aleatoria incluyendo pero sin limitación, un bit, bits, bytes, kilobytes, megabytes o mayor, o cualquier combinación o secuencia de tamaños. Además, variar los tamaños de las unidades de datos resultantes del proceso de división puede presentar los datos más difíciles de restaurar a una forma utilizable, aumentando de esta manera la seguridad de los datos sensibles. Es inmediatamente evidente para los expertos en la materia que los tamaños de unidad de datos divididos pueden ser una amplia diversidad de tamaños de unidad de datos o patrones de tamaños o combinaciones de tamaños. Por ejemplo, los tamaños de unidad de datos se pueden seleccionar o predeterminarse para que sean todos del mismo tamaño, un conjunto fijo de diferentes tamaños, una combinación de tamaños o tamaños generados de forma aleatoria. De manera similar, las unidades de datos se pueden distribuir en una o más comparticiones 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 de forma aleatoria por compartición.

Tal como se ha mencionado en lo que antecede, para recrear los datos sensibles S, las porciones de datos necesitan desaleatorizarse y reorganizarse. Este procedimiento puede tener lugar de forma ventajosa en los módulos de ensamblaje de datos, 525 y 620, del motor de autenticación 215 y del motor criptográfico 220, de forma respectiva. El módulo de ensamblaje de datos, por ejemplo, el módulo de ensamblaje de datos 525, recibe porciones de datos desde las instalaciones de almacenamiento de datos D1 a D4, y reensambla los datos en forma utilizable. Por ejemplo, de acuerdo con una forma de realización en donde 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 porciones de datos desde al menos dos de las instalaciones de almacenamiento de datos D1 a D4 para recrear los datos sensibles S. Por ejemplo, los emparejamientos de AC, AD, BC, y BD, se distribuyeron de tal modo que dos cualquiera proporcionan uno de A y B, o, C y D. Observando que S = A XOR B o S = C XOR D indica que cuando el módulo de ensamblaje de datos recibe uno de A y B, o, C y D, el módulo de ensamblaje de datos 525 puede reensamblar de forma ventajosa los datos sensibles S. Por tanto, el módulo de ensamblaje de datos 525 puede ensamblar los datos sensibles S, cuando, por ejemplo, recibe porciones de datos desde al menos las primeras dos de las instalaciones de almacenamiento de datos D1 a D4 para responder a una solicitud de reensamblaje mediante el motor de confianza 110.

Basándose en los procesos de división y ensamblaje de datos anteriores, existen los datos sensibles S en formato utilizable únicamente en un área limitada del motor de confianza 110. Por ejemplo, cuando los datos sensibles S incluyen datos de autenticación de inscripción, los datos de autenticación de inscripción no aleatorizados utilizables están disponibles únicamente en el motor de autenticación 215. De forma análoga, cuando los datos sensibles S incluyen datos de clave criptográfica privada, los datos de clave criptográfica privada no aleatorizados utilizables están disponibles únicamente en el motor criptográfico 220.

A pesar de que los procesos de división y ensamblaje de datos se divulgan con referencia a sus formas de realización preferidas, la invención no tiene por objeto estar limitada de esta manera. En su lugar, un experto en la materia reconocerá a partir de la divulgación del presente documento, un amplio número de alternativas para dividir y reensamblar los datos sensibles S. Por ejemplo, se puede usar encriptación de clave pública para asegurar adicionalmente los datos en las instalaciones de almacenamiento de datos D1 a D4. Además, es inmediatamente evidente para los expertos en la materia que el módulo de división de datos que se describe en el presente documento es también una forma de realización separada y distinta de la presente invención que se puede incorporar en, combinarse con o hacerse parte de otra manera de cualquier sistema informático preexistente, paquetes de soporte lógico, bases de datos o combinaciones de los mismos, u otras formas de realización de la presente invención, tal como el motor de confianza, el motor de autenticación, y el motor de transacción que se divulgan y que se describen en el presente documento.

La figura 9A ilustra un flujo de datos de un proceso de inscripción 900 de acuerdo con algunos aspectos de una forma de realización de la invención. Tal como se muestra en la figura 9A, el proceso de inscripción 900 comienza en la etapa 905 cuando un usuario se desea inscribir con el motor de confianza 110 del sistema criptográfico 100. De acuerdo con esta forma de realización, el sistema de usuario 105 incluye de forma ventajosa una miniaplicación del lado de cliente, tal como una basada en Java, que requiere que el usuario introduzca datos de inscripción, tales como datos demográficos y datos de autenticación de inscripción. De acuerdo con una forma de realización, los datos de autenticación de inscripción incluyen ID de usuario, contraseña o contraseñas, biométrica o biométricas o similares. De acuerdo con una forma de realización, durante el proceso de consulta, la miniaplicación del lado de cliente se comunica preferiblemente con el motor de confianza 110 para asegurar que una ID de usuario elegida es única. Cuando la ID de usuario no es única, el motor de confianza 110 puede sugerir de forma ventajosa una ID de usuario única. La miniaplicación del lado de cliente recoge los datos de inscripción y transmite los datos de inscripción, por ejemplo, a través de un documento de XML, al motor de confianza 110, y en particular, al motor de transacción 205. De acuerdo con una forma de realización, la transmisión se codifica con la clave pública del motor de autenticación 215.

De acuerdo con una forma de realización, el usuario realiza una única inscripción durante la etapa 905 del proceso de inscripción 900. Por ejemplo, el usuario se inscribe a sí mismo como una persona particular, tal como el Usuario Joe. Cuando el Usuario Joe se desea inscribir como el Usuario Joe, Director General de Mega Corp., entonces de acuerdo con esta forma de realización, el Usuario Joe se inscribe una segunda vez, recibe un segundo ID de usuario único y el motor de confianza 110 no asocia las dos identidades. De acuerdo con otra forma de realización de la invención, el proceso de inscripción 900 proporciona múltiples identidades de usuario para una única ID de usuario. Por tanto, en el ejemplo anterior, el motor de confianza 110 asociará de forma ventajosa las dos identidades del Usuario Joe. Tal como se entenderá por un experto en la materia a partir de la divulgación del presente documento, un usuario puede tener muchas identidades, por ejemplo, el Usuario Joe cabeza de familia, el Usuario Joe miembro de Charitable Foundations, y similares. Incluso a pesar de que el usuario pueda tener múltiples identidades, de acuerdo con esta forma de realización, el motor de confianza 110 almacena preferiblemente únicamente un conjunto de datos de inscripción. Además, los usuarios pueden, de forma ventajosa, añadir, editar / actualizar, o borrar identidades a medida que lo necesiten.

A pesar de que el proceso de inscripción 900 se divulga con referencia a su forma de realización preferida, la invención no tiene por objeto estar limitada de esta manera. En su lugar, un experto en la materia reconocerá a partir

de la divulgación del presente documento, un amplio número de alternativas para recogida de datos de inscripción, y en particular, datos de autenticación de inscripción. Por ejemplo, la miniaplicación puede ser una miniaplicación basada en modelo de objeto común (COM, *common object model*) o similar.

Por otra parte, el proceso de inscripción puede incluir inscripción gradual. Por ejemplo, en un nivel más bajo de la inscripción, el usuario se puede inscribir a través del enlace de comunicación 125 sin producir documentación en cuanto a su identidad. De acuerdo con un nivel de inscripción aumentado, el usuario se inscribe usando un tercero de confianza, tal como un notario digital. Por ejemplo, y el usuario puede aparecer en persona en el tercero de confianza, producir credenciales tales como un certificado de nacimiento, un permiso de conducir, una ID militar o similares, y la parte tercera de confianza puede incluir de forma ventajosa, por ejemplo, su firma digital en la emisión de la inscripción. La parte tercera de confianza puede incluir un notario real, una agencia gubernamental, tal como el Servicio Postal o el Departamento de Vehículos de Motor, una persona de recursos humanos en una gran compañía que inscriba un empleado, o similares. Un experto en la materia entenderá a partir de la divulgación del presente documento que puede tener lugar un amplio número de niveles variables de inscripción durante el proceso de inscripción 900.

Después de recibir los datos de autenticación de inscripción, en la etapa 915, el motor de transacción 205, usando tecnología de SSL TOTAL convencional reenvía los datos de autenticación de inscripción al motor de autenticación 215. En la etapa 920, el motor de autenticación 215 desencripta los datos de autenticación de inscripción usando la clave privada del motor de autenticación 215. Además, el motor de autenticación 215 emplea el módulo de división de datos para operar matemáticamente en los datos de autenticación de inscripción para dividir los datos en al menos dos números aleatorizados independientemente indescifrables. Tal como se ha mencionado en lo que antecede, al menos dos números pueden comprender un número aleatoriamente estadístico y un número binario al que se le ha realizado la operación XOR. En la etapa 925, el motor de autenticación 215 reenvía cada porción de los números aleatorizados a una de las instalaciones de almacenamiento de datos D1 a D4. Tal como se ha mencionado en lo que antecede, el motor de autenticación 215 puede aleatorizar de forma ventajosa qué porciones se transfieren a qué depósitos.

A menudo durante el proceso de inscripción 900, el usuario deseará también tener un certificado digital expedido de tal modo que él mismo pueda recibir documentos encriptados desde otros usuarios fuera del sistema criptográfico 100. Tal como se ha mencionado en lo que antecede, la autoridad de certificación 115 emite en general certificados de acuerdo con una o más de varias normas convencionales. En general, el certificado digital incluye una clave pública del usuario o sistema, que es conocida para todo el mundo.

Si el usuario solicita un certificado digital en la inscripción, o en otro momento, la solicitud se transfiere a través del motor de confianza 110 al motor de autenticación 215. De acuerdo con una forma de realización, la solicitud incluye un documento de XML que tiene, por ejemplo, el nombre apropiado del usuario. De acuerdo con la etapa 935, el motor de autenticación 215 transfiere la solicitud al motor criptográfico 220 que ordena al motor criptográfico 220 generar una clave o par de claves criptográficas.

Tras la solicitud, en la etapa 935, el motor criptográfico 220 genera al menos una clave criptográfica. De acuerdo con una forma de realización, el módulo de manejo criptográfico 625 genera un par de claves, en donde una clave se usa como una clave privada, y una se usa como una clave pública. El motor criptográfico 220 almacena la clave privada y, de acuerdo con una forma de realización, una copia de la clave pública. En la etapa 945, el motor criptográfico 220 transmite una solicitud de un certificado digital al motor de transacción 205. De acuerdo con una forma de realización, la solicitud incluye de forma ventajosa una solicitud normalizada, tal como PKCS10, embebida en, por ejemplo, un documento XML. La solicitud de un certificado digital se puede corresponder de forma ventajosa con una o más autoridades de certificación y al uno o más formatos convencionales que requieren las autoridades de certificación.

En la etapa 950 el motor de transacción 205 reenvía esta solicitud a la autoridad de certificación 115, que, en la etapa 955, devuelve un certificado digital. El certificado digital devuelto puede estar de forma ventajosa en un formato normalizado, tal como PKCS7, o en un formato propietario de una o más de las autoridades de certificación 115. En la etapa 960, el certificado digital se recibe mediante el motor de transacción 205, y se reenvía una copia al usuario y se almacena una copia con el motor de confianza 110. El motor de confianza 110 almacena una copia del certificado de tal modo que el motor de confianza 110 no necesitará basarse en la disponibilidad de la autoridad de certificación 115. Por ejemplo, cuando el usuario desea enviar un certificado digital, o un tercero solicita el certificado digital del usuario, la solicitud del certificado digital por lo general se envía a la autoridad de certificación 115. No obstante, si la autoridad de certificación 115 está realizando mantenimiento o ha sido víctima de un fallo o compromiso de seguridad, el certificado digital puede no estar disponible.

En cualquier momento después de expedir las claves criptográficas, el motor criptográfico 220 puede emplear de forma ventajosa el proceso de división de datos 800 que se ha descrito en lo que antecede de tal modo que las claves criptográficas se dividen en números aleatorizados independientemente indescifrables. Similar a los datos de autenticación, en la etapa 965 el motor criptográfico 220 transfiere los números aleatorizados a las instalaciones de almacenamiento de datos D1 a D4.

Un experto en la materia reconocerá a partir de la divulgación del presente documento que el usuario puede solicitar un certificado digital en cualquier momento después de la inscripción. Además, las comunicaciones entre sistemas pueden incluir de forma ventajosa tecnologías de encriptación de SSL TOTAL o de clave pública. Además, el proceso de inscripción puede expedir múltiples certificados digitales desde múltiples autoridades de certificación, incluyendo una o más autoridades de certificación propietarias internas o externas al motor de confianza 110.

Tal como se divulga en las etapas 935 a 960, una forma de realización de la invención incluye la solicitud de un certificado que se almacena con el tiempo en el motor de confianza 110. Debido a que, de acuerdo con una forma de realización, el módulo de manejo criptográfico 625 expide las claves que son usadas por el motor de confianza 110, cada certificado se corresponde con la clave privada. Por lo tanto, el motor de confianza 110 puede proporcionar de forma ventajosa interoperabilidad a través de la monitorización de los certificados propiedad de, o que están asociados con, un usuario. Por ejemplo, cuando el motor criptográfico 220 recibe una solicitud de una función criptográfica, el módulo de manejo criptográfico 625 puede investigar los certificados propiedad del usuario solicitante para determinar si el usuario posee una clave privada que coincide con los atributos de la solicitud. Cuando existe un certificado de este tipo, el módulo de manejo criptográfico 625 puede usar el certificado o las claves públicas o privadas que están asociadas con el mismo, para realizar la función solicitada. Cuando un certificado de este tipo no existe, el módulo de manejo criptográfico 625 puede, de forma ventajosa y transparente, realizar un número de acciones para intentar remediar la ausencia de una clave apropiada. Por ejemplo, la figura 9B ilustra un diagrama de flujo de un proceso de interoperabilidad 970, que de acuerdo con algunos aspectos de una forma de realización de la invención, divulga las etapas anteriores para asegurar que el módulo de manejo criptográfico 625 realiza funciones criptográficas usando claves apropiadas.

Tal como se muestra en la figura 9B, el proceso de interoperabilidad 970 comienza con la etapa 972 en donde el módulo de manejo criptográfico 925 determina el tipo de certificado deseado. De acuerdo con una forma de realización de la invención, el tipo de certificado se puede especificar de forma ventajosa en la solicitud de funciones criptográficas, u otros datos proporcionados por el solicitante. De acuerdo con otra forma de realización, el tipo de certificado se puede determinar mediante el formato de datos de la solicitud. Por ejemplo, el módulo de manejo criptográfico 925 puede reconocer de forma ventajosa que la solicitud se corresponde con un tipo particular.

De acuerdo con una forma de realización, el tipo de certificado puede incluir una o más normas 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 encriptación fuerte tales como claves de 256 bits, claves menos seguras o similares. Además, el tipo de certificado puede incluir actualizaciones o sustituciones de una o más de las normas o claves de algoritmos anteriores, uno o más formatos de mensaje o datos, uno o más esquemas de encapsulación o codificación de datos, tales como Base 32 o Base 64. El tipo de certificado puede incluir también compatibilidad con una o más aplicaciones criptográficas o interfaces de terceros, uno o más protocolos de comunicación, o una o más normas o protocolos de certificado. Un experto en la materia reconocerá a partir de la divulgación del presente documento que pueden existir otras diferencias en tipos de certificados, y las traducciones a y desde estas diferencias se pueden implementar tal como se divulga en el presente documento.

Una vez que el módulo de manejo criptográfico 625 determina el tipo de certificado, el proceso de interoperabilidad 970 continúa a la etapa 974, y determina si el usuario posee un certificado que coincide el tipo determinado en la etapa 974. Cuando el usuario posee un certificado coincidente, por ejemplo, el motor de confianza 110 tiene acceso al certificado coincidente a través de, por ejemplo, un almacenamiento previo del mismo, el módulo de manejo criptográfico 825 conoce que se almacena también una clave privada coincidente en el motor de confianza 110. Por ejemplo, la clave privada coincidente se puede almacenar en el depósito 210 o sistema depósito 700. El módulo de manejo criptográfico 625 puede solicitar de forma ventajosa que se reensamble la clave privada coincidente desde, por ejemplo, el depósito 210, y a continuación en la etapa 976, usar la clave privada coincidente para realizar acciones o funciones criptográficas. Por ejemplo, tal como se ha mencionado en lo que antecede, el módulo de manejo criptográfico 625 puede realizar de forma ventajosa troceo, comparaciones de troceo, encriptación o desencriptación de datos, verificación o creación de firma digital, o similares.

Cuando el usuario no posee un certificado coincidente, el proceso de interoperabilidad 970 continúa a la etapa 978 en donde el módulo de manejo criptográfico 625 determina si el usuario posee un certificado de certificación cruzada. De acuerdo con una forma de realización, la certificación cruzada entre autoridades de certificación tiene lugar cuando una primera autoridad de certificación determina confiar certificados desde una segunda autoridad de certificación. En otras palabras, la primera autoridad de certificación determina que los certificados desde la segunda autoridad de certificación cumplen ciertas normas de calidad, y por lo tanto, se pueden “certificar” como equivalentes a los propios certificados de la primera autoridad de certificación. La certificación cruzada se hace más compleja cuando las autoridades de certificación expiden, por ejemplo, certificados que tienen niveles de confianza. Por ejemplo, la primera autoridad de certificación puede proporcionar tres niveles de confianza para un certificado particular, normalmente basándose en el grado de fiabilidad en el proceso de inscripción, mientras que la segunda autoridad de certificación puede proporcionar siete niveles de confianza. La certificación cruzada puede rastrear de forma ventajosa qué niveles y qué certificados desde la segunda autoridad de certificación se pueden sustituir para qué niveles y qué certificados desde la primera. Cuando se hace oficial y públicamente la anterior certificación

cruzada entre dos autoridades de certificación, el mapeo de los certificados y niveles entre sí se denomina en ocasiones “encadenamiento”.

De acuerdo con otra forma de realización de la invención, el módulo de manejo criptográfico 625 puede desarrollar de forma ventajosa certificaciones cruzadas fuera de las acordadas por las autoridades de certificación. Por ejemplo, el módulo de manejo criptográfico 625 puede acceder a una primera declaración de prácticas de certificación (CPS, *certificate practice statement*) de la autoridad de certificación, u otra declaración de política publicada, y usar, por ejemplo, los testigos de autenticación requeridos por niveles de confianza particulares, coincidir los primeros certificados de la autoridad de certificación con los de otra autoridad de certificación.

Cuando, en la etapa 978, el módulo de manejo criptográfico 625 determina que los usuarios poseen un certificado de certificación cruzada, el proceso de interoperabilidad 970 continúa a la etapa 976, y realiza la acción o función criptográfica usando la clave pública de certificación cruzada, la clave privada, o ambas. Como alternativa, cuando el módulo de manejo criptográfico 625 determina que el usuario no posee un certificado de certificación cruzada, el proceso de interoperabilidad 970 continúa a la etapa 980, en donde el módulo de manejo criptográfico 625 selecciona una autoridad de certificación que expide el tipo de certificado solicitado, o a un certificado de certificación cruzada al mismo. En la etapa 982, el módulo de manejo criptográfico 625 determina si los datos de autenticación de inscripción del usuario, analizados en lo que antecede, cumplen los requisitos de autenticación de la autoridad de certificación elegida. Por ejemplo, si el usuario se inscribe a través de una red contestando, por ejemplo, cuestiones demográficas y otras, los datos de autenticación proporcionados pueden establecer un nivel inferior de confianza que un usuario proporcione datos biométricos y aparezcan antes de un tercero, tal como, por ejemplo, un notario. De acuerdo con una forma de realización, los requisitos de autenticación anteriores se pueden proporcionar de forma ventajosa en el CPS de la autoridad de autenticación elegida.

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

De acuerdo con otra forma de realización, el motor de confianza 110 puede incluir de forma ventajosa uno o más módulos de expedición de certificados que pueden expedir uno o más tipos de certificado. De acuerdo con esta forma de realización, el módulo de expedición de certificado puede proporcionar el certificado anterior. Cuando el módulo de manejo criptográfico 625 obtiene el certificado, el proceso de interoperabilidad 970 continúa a la etapa 976, y realiza la acción o función criptográfica usando la clave pública, clave privada, o ambas que se corresponden con el certificado obtenido.

Cuando el usuario, en la etapa 982, no ha proporcionado al motor de confianza 110 con datos de autenticación de inscripción que cumplen los requisitos de la autoridad de certificación elegida, el módulo de manejo criptográfico 625 determina, en la etapa 986 si hay otras autoridades de certificación que tienen diferentes requisitos de autenticación. Por ejemplo, el módulo de manejo criptográfico 625 puede buscar autoridades de certificación que tengan requisitos de autenticación inferiores, pero que aún así expidan los certificados elegidos, o certificaciones cruzadas de los mismos.

Cuando existe la anterior autoridad de certificación que tiene requisitos inferiores, el proceso de interoperabilidad 970 continúa a la etapa 980 y elige esa autoridad de certificación. Como alternativa, cuando no existe tal autoridad de certificación, en la etapa 988, el motor de confianza 110 puede solicitar testigos de autenticación adicionales procedentes del usuario. Por ejemplo, el motor de confianza 110 puede solicitar nuevos datos de autenticación de inscripción que comprenden, por ejemplo, datos biométricos. Asimismo, el motor de confianza 110 puede solicitar al usuario que aparezca ante un tercero y proporcione credenciales de autenticación apropiados, tales como, por ejemplo, aparecer ante un notario con un permiso de conducir, una tarjeta de la seguridad social, una tarjeta bancaria, un certificado de nacimiento, una ID militar, o similares. Cuando el motor de confianza 110 recibe datos de autenticación actualizados, el proceso de interoperabilidad 970 continúa a la etapa 984 y obtiene el certificado elegido anterior.

A través del proceso de interoperabilidad 970 anterior, el módulo de manejo criptográfico 625 proporciona de forma ventajosa traducciones y conversiones transparentes sin interrupciones entre diferentes sistemas criptográficos. Un experto en la materia reconocerá a partir de la divulgación del presente documento, un amplio número de ventajas e implementaciones del sistema interoperable anterior. Por ejemplo, la etapa 986 anterior del proceso de interoperabilidad 970 puede incluir de forma ventajosa aspectos de arbitraje de confianza, analizados en mayor detalle a continuación, en donde la autoridad de certificación puede aceptar bajo circunstancias especiales niveles

inferiores de certificación cruzada. Además, el proceso de interoperabilidad 970 puede incluir asegurar la interoperabilidad entre y el empleo de revocaciones de certificados convencionales, tales como emplear listas de revocaciones de certificados (CRL, *certificate revocation list*), protocolos de estado de certificados en línea (OCSP, *online certificate status protocol*), o similares.

La figura 10 ilustra un flujo de datos de un proceso de autenticación 1000 de acuerdo con algunos aspectos de una forma de realización de la invención. De acuerdo con una forma de realización, el proceso de autenticación 1000 incluye recoger datos de autenticación actuales desde un usuario y comparar los mismos con los de los datos de autenticación de inscripción del usuario. Por ejemplo, el proceso de autenticación 1000 comienza en la etapa 1005 en donde un usuario desea realizar una transacción con, por ejemplo, un distribuidor. Tales transacciones pueden incluir, por ejemplo, seleccionar una opción de compra, solicitar acceso a un área o dispositivo restringidos del sistema de distribuidor 120, o similares. En la etapa 1010, un distribuidor proporciona al usuario con una ID de transacción y una solicitud de autenticación. La ID de transacción puede incluir de forma ventajosa una cantidad de 192 bits que tiene una indicación de 32 bits concatenada con una cantidad aleatoria de 128 bits, o un “nonce” (número aleatorio utilizado solo una vez), concatenado con una constante específica de distribuidor de 32 bits. Una ID de transacción de este tipo identifica de manera inequívoca la transacción de tal modo que las transacciones imitadas se puedan rechazar por el motor de confianza 110.

La solicitud de autenticación puede incluir de forma ventajosa qué nivel de autenticación es necesario para una transacción particular. Por ejemplo, el distribuidor puede especificar un nivel particular de confianza que se requiere para la transacción en la expedición. Si la autenticación no se puede realizar en este nivel de confianza, tal como se analizará a continuación, la transacción no tendrá lugar sin ninguna autenticación adicional por el usuario para elevarse al nivel de confianza, o sin un cambio en los términos de la autenticación entre el distribuidor y el servidor. Estas expediciones se analizan más completamente a continuación.

De acuerdo con una forma de realización, la ID de transacción y la solicitud de autenticación se pueden generar de forma ventajosa mediante una miniaplicación del lado del distribuidor u otro programa de soporte lógico. Además, la transmisión de la ID de transacción y los datos de autenticación pueden incluir uno o más documentos XML encriptados usando tecnología de SSL convencional, tal como, por ejemplo, ½ SSL, o, en otras palabras SSL autenticado en el lado del distribuidor.

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

Durante las etapas 1015 y 1020, el sistema de distribuidor 120, en la etapa 1025, reenvía la ID de transacción y la solicitud de autenticación al motor de confianza 110, usando la tecnología de SSL TOTAL preferida. Esta comunicación puede incluir también una ID de distribuidor, a pesar de que la identificación de distribuidor se puede comunicar también a través de una porción no aleatoria de la ID de transacción. En las etapas 1030 y 1035, el motor de transacción 205 recibe la comunicación, crea un registro en el recorrido de auditoría, y genera una solicitud para que se reensamblen los datos de autenticación de inscripción del usuario desde las instalaciones de almacenamiento de datos D1 a D4. En la etapa 1040, el sistema depósito 700 transfiere las porciones de los datos de autenticación de inscripción que se corresponden con el usuario al motor de autenticación 215. En la etapa 1045, el motor de autenticación 215 desencripta la transmisión usando su clave privada y compara los datos de autenticación de inscripción con los datos de autenticación actuales proporcionados por el usuario.

La comparación de la etapa 1045 puede aplicar de forma ventajosa autenticación sensible a contexto heurística, tal como se ha hecho referencia en lo que antecede, y se analiza en mayor detalle a continuación. Por ejemplo, si la información biométrica recibida no coincide perfectamente, resulta una coincidencia de confianza inferior. En formas de realización particulares, el nivel de confianza de la autenticación está equilibrado frente a la naturaleza de la transacción y los deseos de tanto el usuario como el distribuidor. De nuevo, esto se analiza en mayor detalle a continuación.

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

Basándose en lo que antecede, el proceso de autenticación 1000 mantiene de forma ventajosa los datos sensibles seguros y produce resultados configurados para mantener la integridad de los datos sensibles. Por ejemplo, los datos sensibles se reensamblan únicamente dentro del motor de autenticación 215. Por ejemplo, los datos de autenticación de inscripción son indescifrables hasta que se ensamblan en el motor de autenticación 215 mediante el módulo de ensamblaje de datos, y los datos de autenticación actuales son indescifrables hasta que se desempaquetan mediante la tecnología de SSL convencional y la clave privada del motor de autenticación 215. Además, el resultado de autenticación transmitido al distribuidor no incluye los datos sensibles, y el usuario incluso puede no conocer si él mismo produjo datos de autenticación válidos.

A pesar de que el proceso de autenticación 1000 se divulga con referencia a sus formas de realización preferida y alternativa, la invención no tiene por objeto estar limitada de esta manera. En su lugar, un experto en la materia reconocerá a partir de la divulgación del presente documento, un amplio número de alternativas para el proceso de autenticación 1000. Por ejemplo, el distribuidor se puede sustituir de forma ventajosa por casi cualquier aplicación solicitante, incluso las que residen con el sistema de usuario 105. Por ejemplo, una aplicación de cliente, tal como Microsoft Word, puede usar una interfaz de programa de aplicación (API, *application program interface*) o una API criptográfica (CAPI, *cryptographic API*) para solicitar autenticación antes de desbloquear un documento. Como alternativa, un servidor de correo, una red, un teléfono celular, un dispositivo informático personal o móvil, una estación de trabajo, o similares, pueden hacer, todos ellos, las solicitudes de autenticación que se pueden rellenar mediante el proceso de autenticación 1000. De hecho, después de proporcionar el proceso de autenticación de confianza 1000 anterior, la aplicación o dispositivo solicitantes pueden proporcionar acceso a o uso de un amplio número de dispositivos o sistemas electrónicos o informáticos.

Además, el proceso de autenticación 1000 puede emplear un amplio número de procedimientos alternativos en el caso de fallo de autenticación. Por ejemplo, el fallo de autenticación puede mantener la misma ID de transacción y solicitar que el usuario vuelva a introducir sus datos de autenticación actuales. Tal como se ha mencionado en lo que antecede, el uso de la misma ID de transacción permite al comparador del motor de autenticación 215 monitorizar y limitar el número de intentos de autenticación para una transacción particular, creando de esta manera un sistema criptográfico 100 más seguro.

Además, el proceso de autenticación 1000 se puede emplear de forma ventajosa para desarrollar soluciones de inicio de sesión únicas elegantes, tales como, desbloquear un almacén de datos sensibles. Por ejemplo, la autenticación satisfactoria o positiva puede proporcionar al usuario autenticado la capacidad para acceder de forma automática 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 acceder a contraseña, inicio de sesión, credenciales financieras, o similares, que están asociados con múltiples distribuidores en línea, una red de área local, diversos dispositivos informáticos personales, proveedores de servicio de Internet, proveedores de subastas, corredores de inversiones, o similares. Empleando un almacén de datos sensibles, los usuarios pueden elegir contraseñas verdaderamente grandes y aleatorias debido a que no necesitan recordarlas a través de asociación. En su lugar, el proceso de autenticación 1000 proporciona acceso a lo mismo. Por ejemplo, un usuario puede elegir una cadena alfanumérica aleatoria de más de veinte dígitos de longitud en lugar de algo que está asociado con un dato memorable, nombre, etc.

De acuerdo con una forma de realización, un almacén de datos sensibles que está asociado con un usuario dado se puede almacenar de forma ventajosa en las instalaciones de almacenamiento de datos del depósito 210, o dividirse y almacenarse en el sistema depósito 700. De acuerdo con esta forma de realización, después de autenticación de usuario positiva, el motor de confianza 110 sirve los datos sensibles solicitados, tales como, por ejemplo, a la contraseña apropiada a la aplicación solicitante. De acuerdo con otra forma de realización, el motor de confianza 110 puede incluir un sistema separado para almacenar el almacén de datos sensibles. Por ejemplo, el motor de confianza 110 puede incluir un motor de soporte lógico independiente que implementa la funcionalidad del almacén de datos y que reside de manera figurada “detrás” del sistema de seguridad de extremo frontal anterior del motor de confianza 110. De acuerdo con esta forma de realización, el motor de soporte lógico sirve los datos sensibles solicitados después de que el motor de soporte lógico recibe una señal que indica autenticación de usuario positiva desde el motor de confianza 110.

En otra forma de realización más, el almacén de datos se puede implementar por un sistema de terceros. Similar a la forma de realización del motor de soporte lógico, el sistema de terceros puede servir de forma ventajosa los datos sensibles solicitados después de que el sistema de terceros recibe una señal que indica autenticación de usuario positiva desde el motor de confianza 110. De acuerdo con otra forma de realización más, el almacén de datos se puede implementar en el sistema de usuario 105. Un motor de soporte lógico del lado del usuario puede servir de forma ventajosa los datos anteriores después de recibir una señal que indica autenticación de usuario positiva desde el motor de confianza 110.

A pesar de que los almacenes de datos anteriores se divulgan con referencia a formas de realización alternativas, un experto en la materia reconocerá a partir de la divulgación del presente documento, un amplio número de implementaciones adicionales de las mismas. Por ejemplo, un almacén de datos particular puede incluir aspectos de algunas o todas las formas de realización anteriores. Además, cualquiera de los almacenes de datos anteriores

puede emplear una o más solicitudes de autenticación a tiempos variables. Por ejemplo, cualquiera de los almacenes de datos puede requerir autenticación de cada una o más transacciones, de forma periódica, cada una o más sesiones, cada acceso a una o más páginas web o sitios web, a uno o más otros intervalos especificados, o similares.

La figura 11 ilustra un flujo de datos de un proceso de firma 1100 de acuerdo con algunos aspectos de una forma de realización de la invención. Tal 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 en lo que antecede con referencia a la figura 10. De acuerdo con una forma de realización de la invención, el proceso de firma 1100 autentica en primer lugar al usuario y a continuación realiza una o más de varias funciones de firma digital tal como se analizará en mayor detalle a continuación. De acuerdo con otra forma de realización, el proceso de firma 1100 puede almacenar de forma ventajosa datos relacionados con el mismo, tales como troceos de mensajes o documentos, o similares. Estos datos se pueden usar de forma ventajosa en una auditoria o cualquier otro evento, tal como por ejemplo, cuando una parte participante intenta rechazar una transacción.

Tal como se muestra en la figura 11, durante las etapas de autenticación, el usuario y el distribuidor se pueden poner, de forma ventajosa, de acuerdo en un mensaje, tal como, por ejemplo, un contrato. Durante la firma, el proceso de firma 1100 asegura de forma ventajosa que el contrato firmado por el usuario es idéntico al contrato suministrado por el distribuidor. Por lo tanto, de acuerdo con una forma de realización, durante la autenticación, el distribuidor y el usuario incluyen un troceo de sus respectivas copias del mensaje o contrato, en los datos transmitidos al motor de autenticación 215. Empleando únicamente un troceo de un mensaje o contrato, el motor de confianza 110 puede almacenar de forma ventajosa una cantidad significativamente reducida de datos, proporcionando un sistema criptográfico más eficaz y rentable. Además, el troceo almacenado se puede comparar de forma ventajosa con un troceo de un documento en cuestión para determinar si el documento en cuestión coincide con uno firmado por cualquiera de las partes. La capacidad para determinar que el documento es idéntico a uno relacionado con una transacción proporciona prueba adicional de que se puede usar frente a una repudiación por una parte a una transacción.

En la etapa 1103, el motor de autenticación 215 ensambla los datos de autenticación de inscripción y los compara con los datos de autenticación actuales proporcionados por el usuario. Cuando el comparador del motor de autenticación 215 indica que los datos de autenticación de inscripción coinciden con los datos de autenticación actuales, el comparador del motor de autenticación 215 compara también el troceo del mensaje suministrado por el distribuidor con el troceo del mensaje suministrado por el usuario. Por tanto, el motor de autenticación 215 asegura de forma ventajosa que el mensaje acordado para y por el usuario es idéntico al acordado para y por el distribuidor.

En la etapa 1105, el motor de autenticación 215 transmite una solicitud de firma digital al motor criptográfico 220. De acuerdo con una forma de realización de la invención, la solicitud incluye un troceo del mensaje o contrato. No obstante, un experto en la materia reconocerá a partir de la divulgación del presente documento que el motor criptográfico 220 puede encriptar virtualmente cualquier tipo de dato, incluyendo, pero sin limitación, vídeo, audio, biométrica, imágenes o texto para formar la firma digital deseada. Volviendo a la etapa 1105, la solicitud de firma digital comprende preferiblemente un documento XML que se comunicado a través de tecnologías de SSL convencionales.

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

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

ambos. De acuerdo con otra forma de realización, el motor de autenticación 215 puede solicitar de forma ventajosa ensamblaje de las claves criptográficas que se corresponden con el motor de confianza 110.

De acuerdo con otra forma de realización, el motor de confianza 110 realiza funciones similares a un poder legal. Por ejemplo, el motor de confianza 110 puede firmar de forma digital el mensaje en beneficio de un tercero. En tal caso, el motor de autenticación 215 solicita las claves criptográficas que están asociadas con el tercero. De acuerdo con esta forma de realización, el proceso de firma 1100 puede incluir de forma ventajosa autenticación del tercero, antes de permitir funciones similares a un poder legal. Además, el proceso de autenticación 1000 puede incluir una comprobación para restricciones de terceros, tales como, por ejemplo, lógica empresarial o similar que dictan cuándo y en qué circunstancias se puede usar una firma de terceros particular.

Basándose en lo que antecede, en la etapa 1110, el motor de autenticación solicita las claves criptográficas desde las instalaciones de almacenamiento de datos D1 a D4 que se corresponden con la parte firmante. En la etapa 1115, las instalaciones de almacenamiento de datos D1 a D4 transmiten sus respectivas porciones de la clave criptográfica que se corresponden con la parte firmante al motor criptográfico 220. De acuerdo con una forma de realización, las transmisiones anteriores incluyen tecnologías de SSL. De acuerdo con otra forma de realización, las transmisiones anteriores se pueden súperencriptar de forma ventajosa 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 encripta el mensaje con las mismas, formando de esta manera la firma o firmas digitales. En la etapa 1125 del proceso de firma 1100, el motor criptográfico 220 transmite la firma o firmas digitales al motor de autenticación 215. En la etapa 1130, el motor de autenticación 215 transmite la solicitud de autenticación rellenada junto con una copia del mensaje troceado y la firma o firmas digitales al motor de transacción 205. En la etapa 1135, el motor de transacción 205 transmite una recepción que comprende la ID de transacción, una indicación de si la autenticación fue satisfactoria, y la firma o firmas digitales, al distribuidor. De acuerdo con una forma de realización, la transmisión anterior puede incluir de forma ventajosa la firma digital del motor de confianza 110. Por ejemplo, el motor de confianza 110 puede encriptar el troceo de la recepción con su clave privada, formando de esta manera una firma digital para adjuntarse a la transmisión al distribuidor.

De acuerdo con una forma de realización, el motor de transacción 205 transmite también un mensaje de confirmación al usuario. A pesar de que el proceso de firma 1100 se divulga con referencia a sus formas de realización preferida y alternativa, la invención no tiene por objeto estar limitada de esta manera. En su lugar, un experto en la materia reconocerá a partir de la divulgación del presente documento, un amplio número de alternativas para el proceso de firma 1100. Por ejemplo, el distribuidor se puede sustituir con una aplicación de usuario, tal como una aplicación de correo electrónico. Por ejemplo, el usuario puede desear firmar de forma digital un correo electrónico particular con su firma digital. En una forma de realización de este tipo, la transmisión a lo largo de todo el proceso de firma 1100 puede incluir de forma ventajosa únicamente una copia de un troceo del mensaje. Además, un experto en la materia reconocerá a partir de la divulgación del presente documento que un amplio número de aplicaciones cliente pueden solicitar firmas digitales. Por ejemplo, las aplicaciones cliente pueden comprender procesadores de texto, hojas de cálculo, correos electrónicos, correo de voz, acceso a áreas de sistema restringidas o similares.

Además, un experto en la materia reconocerá a partir de la divulgación del presente documento que las etapas 1105 a 1120 del proceso de firma 1100 pueden emplear de forma ventajosa algunas o todas las etapas del proceso de interoperabilidad 970 de la figura 9B, proporcionando interoperabilidad de esta manera entre diferentes sistemas criptográficos que pueden necesitar procesar, por ejemplo, la firma digital bajo diferentes tipos de firma.

La figura 12 ilustra un flujo de datos de un proceso de encriptación / desencriptación 1200 de acuerdo con algunos aspectos de una forma de realización de la invención. Tal como se muestra en la figura 12, el proceso de desencriptación 1200 empieza autenticando al usuario usando el proceso de autenticación 1000. De acuerdo con una forma de realización, el proceso de autenticación 1000 incluye en la solicitud de autenticación, una clave de sesión síncrona. Por ejemplo, en tecnologías de PKI convencionales, se entiende por los expertos en la materia que encriptar o desencriptar datos usando claves públicas y privadas es matemáticamente intensivo y puede requerir recursos de sistema significativos. No obstante, en sistemas criptográficos de clave simétrica, o sistemas en donde el emisor y el receptor de un mensaje comparten una única clave común que se usa para encriptar y desencriptar un mensaje, las operaciones matemáticas son significativamente más sencillas y más rápidas. Por tanto, en las tecnologías de PKI convencionales, el emisor de un mensaje generará la clave de sesión síncrona, y encriptará el mensaje usando el sistema de clave simétrica más rápido y más simple. A continuación, el emisor encriptará la clave de sesión con la clave pública del receptor. La clave de sesión encriptada se adjuntará al mensaje encriptado de manera síncrona y ambos datos se envían al receptor. El receptor usa su clave privada para desencriptar la clave de sesión, y a continuación usa la clave de sesión para desencriptar el mensaje. Basándose en lo que antecede, el sistema de clave simétrica más sencillo y más rápido se usa para la mayoría del procesamiento de encriptación / desencriptación. Por tanto, en el proceso de desencriptación 1200, la desencriptación supone de forma ventajosa que se ha encriptado una clave síncrona con la clave pública del usuario. Por tanto, tal como se ha mencionado en lo que antecede, la clave de sesión encriptada se incluye en la solicitud de autenticación.

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

En la etapa 1220 del proceso de desencriptación 1200, el motor criptográfico 220 ensambla la clave criptográfica y desencripta la clave de sesión con la misma. En la etapa 1225, el motor criptográfico reenvía la clave de sesión al motor de autenticación 215. En la etapa 1227, el motor de autenticación 215 rellena la solicitud de autenticación que incluye la clave de sesión desencriptada, y transmite la solicitud de autenticación rellenada al motor de transacción 205. En la etapa 1230, el motor de transacción 205 reenvía la solicitud de autenticación junto con la clave de sesión a la aplicación o el distribuidor solicitante. A continuación, de acuerdo con una forma de realización, la aplicación o el distribuidor solicitante usa la clave de sesión para desencriptar el mensaje encriptado.

A pesar de que el proceso de desencriptación 1200 se divulga con referencia a sus formas de realización preferida y alternativa, un experto en la materia reconocerá a partir de la divulgación del presente documento, un amplio número de alternativas para el proceso de desencriptación 1200. Por ejemplo, el proceso de desencriptación 1200 puede renunciar a la encriptación de clave síncrona y basarse en tecnología de clave pública total. En una forma de realización de este tipo, la aplicación solicitante puede transmitir el mensaje completo al motor criptográfico 220, o puede emplear algún tipo de compresión o troceo reversible para transmitir el mensaje al motor criptográfico 220. Un experto en la materia reconocerá también a partir de la divulgación del presente documento que las comunicaciones anteriores pueden incluir de forma ventajosa documentos XML empaquetados en tecnología de SSL.

El proceso de encriptación / desencriptación 1200 proporciona también encriptación de documentos u otros datos. Por tanto, en la etapa 1235, una aplicación o un distribuidor solicitante puede transmitir de forma ventajosa al motor de transacción 205 del motor de confianza 110, una solicitud de la clave pública del usuario. La aplicación o el distribuidor solicitante realiza esta solicitud debido a que la aplicación o el distribuidor solicitante usa la clave pública del usuario, por ejemplo, para encriptar la clave de sesión que se usará para encriptar el documento o mensaje. Tal como se ha mencionado en el proceso de inscripción 900, el motor de transacción 205 almacena una copia del certificado digital del usuario, por ejemplo, en el almacenamiento masivo 225. Por tanto, en la etapa 1240 del proceso de encriptación 1200, el motor de transacción 205 solicita el certificado digital del usuario desde el almacenamiento masivo 225. En la etapa 1245, el almacenamiento masivo 225 transmite el certificado digital que se corresponde con el usuario, al motor de transacción 205. En la etapa 1250, el motor de transacción 205 transmite el certificado digital a la aplicación o el distribuidor solicitante. De acuerdo con una forma de realización, la porción de encriptación del proceso de encriptación 1200 no incluye la autenticación de un usuario. Esto es debido a que el distribuidor solicitante únicamente necesita la clave pública del usuario, y no está solicitando ningún dato sensible.

Un experto en la materia reconocerá a partir de la divulgación del presente documento que si un usuario particular no tiene un certificado digital, el motor de confianza 110 puede emplear alguno o todo el proceso de inscripción 900 para generar un certificado digital para ese usuario particular. A continuación, el motor de confianza 110 puede iniciar el proceso de encriptación / desencriptación 1200 y proporcionar de esta manera el certificado digital apropiado. Además, un experto en la materia reconocerá a partir de la divulgación del presente documento que las etapas 1220 y 1235 a 1250 del proceso de encriptación / desencriptación 1200 pueden emplear de forma ventajosa algunas o todas las etapas del proceso de interoperabilidad de la figura 9B, proporcionando interoperabilidad de esta manera entre diferentes sistemas criptográficos que pueden necesitar, por ejemplo, procesar la encriptación.

La figura 13 ilustra un diagrama de bloques simplificado de un sistema de motor de confianza 1300 de acuerdo con algunos aspectos de otra forma de realización más de la invención. Tal como se muestra en la figura 13, el sistema de motor de confianza 1300 comprende una pluralidad de distintos motores de confianza 1305, 1310, 1315 y 1320, de forma respectiva. 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 transacción, un depósito, y un motor de autenticación. No obstante, un experto en la materia reconocerá que cada motor de transacción puede comprender de forma ventajosa alguno, una combinación, o todos los elementos y canales de comunicación que se divulgan con referencia a las figuras 1 - 8. Por ejemplo, una forma de realización puede incluir de forma ventajosa 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 forma de realización de la invención, cada uno de los motores de confianza 1305, 1310, 1315 y 1320 están separados geográficamente, de tal modo que, por ejemplo, el motor de confianza 1305 puede residir en una primera localización, el motor de confianza 1310 puede residir en una segunda localización, el motor de confianza 1315 puede residir en una tercera localización, y el motor de confianza 1320 puede residir en una cuarta localización. La separación geográfica anterior reduce de forma ventajosa el tiempo de respuesta del sistema al tiempo que aumenta la seguridad del sistema de motor de confianza 1300 global.

Por ejemplo, cuando un usuario inicia sesión en el sistema criptográfico 100, el usuario puede estar cercano a la primera localización y puede desear autenticarse. Tal como se ha descrito con referencia a la figura 10, para autenticarse, el usuario proporciona datos de autenticación actuales, tales como biométrica o similares, y los datos de autenticación actuales se comparan con los datos de autenticación de inscripción del usuario. Por lo tanto, de acuerdo con un ejemplo, el usuario proporciona de forma ventajosa datos de autenticación actuales al motor de confianza 1305 geográficamente más cercano. El motor de transacción 1321 del motor de confianza 1305 a continuación reenvía los datos de autenticación actuales al motor de autenticación 1322 que reside también en la primera localización. De acuerdo con otra forma de realización, el motor de transacción 1321 reenvía los datos de autenticación actuales a uno o más de los motores de autenticación de los motores de confianza 1310, 1315, o 1320.

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

Basándose en lo que antecede, el sistema de motor de confianza 1300 emplea el más cercano de una pluralidad de motores de confianza separados geográficamente, 1305 a 1320, para realizar el proceso de autenticación. De acuerdo con una forma de realización de la invención, el encaminamiento de la información al motor de transacción más cercano se puede realizar de forma ventajosa en miniaplicaciones del lado de cliente que se ejecutan en uno o más del sistema de usuario 105, sistema de distribuidor 120, o autoridad de certificación 115. De acuerdo con una forma de realización alternativa, se puede emplear un proceso de decisión más sofisticado para seleccionar desde los motores de confianza 1305 a 1320. Por ejemplo, la decisión se puede basar en la disponibilidad, operabilidad, velocidad de las conexiones, carga, rendimiento, proximidad geográfica o una combinación de las mismas, de un motor de confianza dado.

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

De acuerdo con otra forma de realización, el sistema de motor de confianza 1300 puede incluir de forma ventajosa múltiples motores criptográficos dispuestos similares a los motores de autenticación. Los motores criptográficos pueden realizar de forma ventajosa funciones criptográficas tales como las que se divulgan con referencia a las figuras 1 - 8. De acuerdo con otra forma de realización más, el sistema de motor de confianza 1300 puede sustituir de forma ventajosa los múltiples motores de autenticación con múltiples motores criptográficos, realizando de esta manera funciones criptográficas tales como las que se divulgan con referencia a las figuras 1 - 8. De acuerdo con otra forma de realización más de la invención, el sistema de motor de confianza 1300 puede sustituir cada múltiple motor de autenticación con un motor que tenga alguna o toda la funcionalidad de los motores de autenticación, motores criptográficos, o ambos, tal como se ha que se divulga en lo que antecede.

A pesar de que el sistema de motor de confianza 1300 se divulga con referencia a sus formas de realización preferida y alternativa, un experto en la materia reconocerá que el sistema de motor de confianza 1300 puede comprender porciones de motores de confianza 1305 a 1320. Por ejemplo, el sistema de motor 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 motor de confianza 1400 de acuerdo con algunos aspectos de otra forma de realización más de la invención. Tal como se muestra en la figura 14, el sistema de motor de confianza 1400 incluye múltiples motores de confianza 1405, 1410, 1415 y 1420. De acuerdo con una forma de realización, cada uno de los motores de confianza 1405, 1410, 1415 y 1420, comprende alguno o todos los elementos del motor de confianza 110 que se divulga con referencia a las figuras 1 - 8. De acuerdo con esta forma de realización, cuando las miniaplicaciones del lado del cliente del sistema de usuario 105, del sistema de distribuidor 120, o de la autoridad de certificación 115, se comunican con el sistema de motor de confianza 1400, estas comunicaciones se envían a la dirección de IP de cada uno de los motores de confianza 1405 a 1420. Además, cada motor de transacción de cada uno de los motores de confianza, 1405, 1410, 1415 y 1420, se comporta similar al motor de transacción 1321 del motor de confianza 1305 que se divulga con referencia a la figura 13. Por ejemplo, durante un proceso de autenticación, cada motor de transacción de cada uno de los motores de confianza 1405, 1410, 1415 y 1420 transmite los datos de autenticación actuales a sus respectivos motores de

autenticación y transmite una solicitud para ensamblar los datos aleatorizados almacenados en cada uno de los depósitos de cada uno de los motores de confianza 1405 a 1420. La figura 14 no ilustra todas estas comunicaciones; ya que tal ilustración se haría demasiado compleja. Continuando con el proceso de autenticación, cada uno de los depósitos comunica a continuación su porción de los datos aleatorizados a cada uno de los motores de autenticación de cada uno de los motores de confianza 1405 a 1420. Cada uno de los motores de autenticación de cada uno de los motores de confianza emplea su comparador para determinar si los datos de autenticación actuales coinciden con los datos de autenticación de inscripción proporcionados mediante los depósitos de cada uno de los motores de confianza 1405 a 1420. De acuerdo con esta forma de realización, el resultado de la comparación mediante cada uno de los motores de autenticación se transmite a continuación a un módulo de redundancia de los otros tres motores de confianza. Por ejemplo, el resultado del motor de autenticación a partir del motor de confianza 1405 se transmite a los módulos de redundancia de los motores de confianza 1410, 1415 y 1420. Por tanto, el módulo de redundancia del motor de confianza 1405 recibe de forma análoga el resultado de los motores de autenticación a partir 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 a partir de tres motores de autenticación y transmitir ese resultado al motor de transacción el cuarto motor de confianza. El comparador compara el resultado de autenticación a partir de los tres motores de autenticación, y si dos de los resultados coinciden, el comparador concluye que el resultado de autenticación debería coincidir con el de los dos motores de autenticación que coinciden. Este resultado se transmite a continuación de vuelta al motor de transacción que se corresponde con el motor de confianza que no está asociado con los tres motores de autenticación.

Basándose en lo que antecede, el módulo de redundancia determina un resultado de autenticación a partir de los datos recibidos desde los motores de autenticación que, preferiblemente, se encuentran geográficamente remotos desde el motor de confianza del módulo de redundancia. Proporcionando tal funcionalidad de redundancia, el sistema de motor de confianza 1400 asegura que un compromiso del motor de autenticación de uno de los motores de confianza 1405 a 1420, es insuficiente para comprometer el resultado de autenticación del módulo de redundancia de ese motor de confianza particular. Un experto en la materia reconocerá que la funcionalidad de módulo de redundancia del sistema de motor de confianza 1400 se puede aplicar también al motor criptográfico de cada uno de los motores de confianza 1405 a 1420. No obstante, tal comunicación de motor criptográfico no se mostró en la figura 14 para evitar complejidad. Además, un experto en la materia reconocerá que un amplio número de algoritmos de resolución de conflictos de autenticación alternativos para el comparador de la figura 15 son adecuados para su uso en la presente invención.

De acuerdo con otra forma de realización más de la invención, el sistema de motor de confianza 1400 puede emplear de forma ventajosa el módulo de redundancia durante etapas de comparación criptográficas. Por ejemplo, alguna o toda la divulgación del módulo de redundancia anterior con referencia a las figuras 14 y 15 se puede implementar de forma ventajosa durante una comparación de troceo de documentos proporcionados mediante una o más partes durante una transacción particular.

A pesar de que la invención anterior se ha descrito en términos de ciertas formas de realización preferidas y alternativas, serán evidentes otras formas de realización para los expertos en la materia a partir de la divulgación del presente documento. Por ejemplo, el motor de confianza 110 puede expedir certificados a corto plazo, en donde la clave criptográfica privada se libera al usuario durante un periodo de tiempo predeterminado. Por ejemplo, las normas de certificados actuales incluyen un campo de validez que se puede establecer para expirar después de una cantidad de tiempo predeterminada Por tanto, el motor de confianza 110 puede liberar una clave privada a un usuario en donde la clave privada fuera válida durante, por ejemplo, 24 horas. De acuerdo con una forma de realización de este tipo, el motor de confianza 110 puede expedir de forma ventajosa un nuevo par de claves criptográficas para asociarse con un usuario particular y a continuación liberar la clave privada del nuevo par de claves criptográficas. A continuación, una vez que se libera la clave criptográfica privada, el motor de confianza 110 expira inmediatamente cualquier uso válido interno de tal clave privada, ya que ya no es asegurable por el motor de confianza 110.

Además, un experto en la materia reconocerá que el sistema criptográfico 100 o el motor de confianza 110 pueden incluir la capacidad de reconocer cualquier tipo de dispositivo, tal como, pero sin limitación, un portátil, un teléfono celular, una red, un dispositivo biométrico o similar. De acuerdo con una forma de realización, tal reconocimiento puede provenir de datos suministrados en la solicitud de un servicio particular, tal como, una solicitud de autenticación que conduce a acceso o uso, una solicitud de funcionalidad criptográfica, o similares. De acuerdo con una forma de realización, la solicitud anterior puede incluir un identificador de dispositivo único, tal como, por ejemplo, una ID de procesador. Como alternativa, la solicitud puede incluir datos en un formato de datos reconocible particular. Por ejemplo, los teléfonos móviles y satélites a menudo no incluyen la potencia de procesamiento para certificados de encriptación intensos X509.v3 completos, y por lo tanto no los solicitan. De acuerdo con esta forma de realización, el motor de confianza 110 puede reconocer el tipo de datos presentados, y responder únicamente de la misma manera.

En un aspecto adicional del sistema que se ha descrito en lo que antecede, se puede proporcionar autenticación sensible al contexto usando técnicas tal como se describirá a continuación. La autenticación sensible al contexto, por ejemplo tal como se muestra en la figura 16, proporciona la posibilidad de evaluar no únicamente los datos reales que se envían mediante el usuario cuando intenta autenticarse a sí mismo, sino también las circunstancias que rodean la generación y entrega de esos datos. Tales técnicas pueden soportar también arbitraje de confianza específico de transacción entre el usuario y motor de confianza 110 o entre el distribuidor y el motor de confianza 110, tal como se describirá a continuación.

Tal como se ha analizado en lo que antecede, la autenticación son los procesos de probar que un usuario es quien dice ser este. En 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 autenticar a sí mismo. El usuario debe demostrar al motor de confianza 110 que este es quien dice ser: conociendo algo que únicamente el usuario debería conocer (autenticación basada en conocimiento), que tiene algo que únicamente el usuario debería tener (autenticación basada en testigo), o siendo algo que únicamente el usuario debería ser (autenticación basada en biométrica).

Los ejemplos de autenticación basada en conocimiento incluyen sin limitación una contraseña, número PIN, o cerradura de combinación. Ejemplos de autenticación basada en testigo incluyen sin limitación una llave de casa, una tarjeta de crédito física, un permiso de conducir o un número de teléfono particular. Ejemplos de autenticación basada en biométrica incluyen sin limitación una huella digital, análisis de escritura, exploración facial, exploración de manos, exploración ocular, exploración de iris, patrón vascular, ADN, un análisis de voz o una exploración de retina.

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

Tal como se usa en el presente documento, “autenticación” hará referencia en términos generales al proceso global de verificar la identidad de alguien que es quien dice que es. Una “técnica de autenticación” se referirá a un tipo particular de autenticación basándose en un fragmento de conocimiento, un testigo físico o una lectura biométrica particular. “Datos de autenticación” se refieren a una información que se envía o se demuestra de otra manera a una autoridad de autenticación para establecer la identidad. “Datos de inscripción” harán referencia a los datos que se envíen inicialmente a una autoridad de autenticación para establecer una línea de base para comparación con los datos de autenticación. Una “instancia de autenticación” hará referencia a los datos que están asociados con un intento para autenticar mediante una técnica de autenticación.

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

Los datos de autenticación actuales proporcionados por el usuario y los datos de inscripción recuperados desde el depósito 210 se reciben mediante el 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 de autenticación separadas. El motor de autenticación 215 separa los datos de autenticación que están asociados con cada instancia de autenticación individual en la etapa 1605. Esto es necesario de tal modo que los datos de autenticación se comparen con el subconjunto apropiado de los datos de inscripción para el usuario (por ejemplo los datos de autenticación de huellas digitales se deberían comparar con datos de inscripción de huellas digitales, en lugar de los datos de inscripción de contraseña).

En general, autenticar a un usuario implica una o más instancias de autenticación, dependiendo de qué técnicas de autenticación estén disponibles para el usuario. Estos métodos están limitados por los datos de inscripción que se proporcionaron por el usuario durante su proceso de inscripción (si el usuario no proporcionó una exploración de retina cuando se inscribió, no se podrá autenticar a sí mismo usando una exploración de retina), así como los medios que pueden estar actualmente disponibles para el usuario (por ejemplo si el usuario no tiene un lector de huella digital en su localización actual, la autenticación de huella digital no será práctica). En algunos casos, una única instancia de autenticación puede ser suficiente para autenticar a un usuario; no obstante, en ciertas circunstancias se puede usar una combinación de múltiples instancias de autenticación para autenticar con más confianza a un usuario para una transacción particular.

Cada instancia de autenticación consiste en datos relacionados con una técnica de autenticación particular (por ejemplo, huella digital, contraseña, tarjeta inteligente, etc.) y las circunstancias que rodean la captación y entrega de

los datos para esa técnica particular. Por ejemplo, una instancia particular de intentar autenticar mediante contraseña generará no únicamente los datos relacionados con la propia contraseña, sino también datos circunstanciales, conocidos como “metadatos”, relacionados con ese intento de contraseña. Estos datos circunstanciales incluyen información tal como: el tiempo en el que tuvo lugar la instancia de autenticación particular, la dirección de red desde la que se entregó la información de autenticación, así como cualquier otra información tal como se conoce por los expertos en la materia que se puede determinar acerca del origen de los datos de autenticación (el tipo de conexión, el número de serie de procesador, etc.).

En muchos casos, únicamente estará disponible una pequeña cantidad de metadatos circunstanciales. Por ejemplo, si el usuario está localizado en una red que utiliza intermediarios o traducción de dirección de red u otra técnica que enmascara la dirección del ordenador de origen, únicamente se puede determinar la dirección del intermediario o encaminador. De manera similar, en muchos casos información tal como el número de serie de procesador no estará disponible debido a cualquiera de limitaciones de soporte físico o sistema operativo que se esté usando, desactivación de tales características mediante el operador del sistema, u otras limitaciones de la conexión entre el sistema de usuario y el motor de confianza 110.

Tal como se muestra en la figura 16, una vez que las instancias de autenticación individuales representadas en los datos de autenticación se extraen y se separan en la etapa 1605, el motor de autenticación 215 evalúa cada instancia para su fiabilidad al indicar que el usuario es quien reclama ser. La fiabilidad para una única instancia de autenticación se determinará en general basándose en varios factores. Estos se pueden agrupar como factores relacionados con la fiabilidad que está asociada con la técnica de autenticación, que se evalúan en la etapa 1610, y factores relacionados con los datos de autenticación particulares proporcionados, que se evalúan en la etapa 1815. El primer grupo incluye sin limitación la fiabilidad intrínseca de la técnica de autenticación que se está usando, y la fiabilidad de los datos de inscripción que se están usando con ese método. El segundo grupo incluye sin limitación el grado de coincidencia entre los datos de inscripción y los datos proporcionados con la instancia de autenticación, y los metadatos que están asociados con esa instancia de autenticación. Cada uno de estos factores puede variar con independencia de los otros.

La fiabilidad intrínseca de la técnica de autenticación está basada en cómo de difícil es para un impostor proporcionar datos correctos de otra persona, así como las tasas de errores globales para la técnica de autenticación. Para métodos de autenticación basados en contraseñas y conocimiento, esta fiabilidad a menudo es bastante baja debido a que 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 conocimiento más complejo puede tener únicamente fiabilidad moderada debido a que el conocimiento se puede transferir de persona a persona bastante fácilmente. La autenticación basada en testigo, tal como tener una tarjeta inteligente apropiada o usar un terminal particular para realizar la autenticación, es de manera similar de baja fiabilidad usada por sí misma, debido a que no hay garantía de que la persona correcta esté en posesión del testigo apropiado.

No obstante, las técnicas biométricas son intrínsecamente más fiables debido a que es en general más difícil de proporcionar a otra persona con la capacidad de usar tus huellas digitales de una manera conveniente, incluso de forma intencionada. Debido a que trastornar técnicas de autenticación biométricas es más difícil, la fiabilidad intrínseca de los métodos biométricos es en general más alta que la de técnicas de autenticación basadas puramente en conocimiento o en testigo. No obstante, incluso las técnicas biométricas pueden tener algunas ocasiones en las que se genera una falsa aceptación o un falso rechazo. Estas ocurrencias se pueden reflejar por diferentes fiabilidades para diferentes implementaciones de la misma técnica biométrica. Por ejemplo, un sistema de coincidencia de huella digital proporcionado por una compañía puede proporcionar una fiabilidad superior que uno proporcionado por una compañía diferente debido a que uno usa óptica de calidad superior o una resolución de exploración mejor o alguna otra mejora que reduce la aparición de falsas aceptaciones o falsos rechazos.

Obsérvese que esta fiabilidad se puede expresar de diferentes maneras. La fiabilidad se expresa de manera deseable en alguna métrica que se pueda usar mediante la heurística 530 y los algoritmos del motor de autenticación 215 para calcular el nivel de confianza de cada autenticación un modo preferido de expresar estas fiabilidades es un porcentaje o fracción. Por ejemplo, se puede asignar a las huellas digitales una fiabilidad intrínseca del 97 %, mientras que se puede asignar a las contraseñas únicamente una fiabilidad intrínseca del 50 %. Los expertos en la materia reconocerán que estos valores particulares son meramente a modo de ejemplo y pueden variar entre implementaciones específicas.

El segundo factor para el que se debe evaluar la fiabilidad es la fiabilidad de la inscripción. Esto es parte del proceso de “inscripción gradual” que se ha mencionado en lo que antecede. Este factor de fiabilidad refleja la fiabilidad de la identificación proporcionada durante el proceso de inscripción inicial. Por ejemplo, si el individuo se inscribe inicialmente de una manera en donde produce físicamente evidencia de su identidad a un notario u otro funcionario público, y los datos de inscripción se registran y certifican notarialmente en ese momento, los datos serán más fiables que los datos que se proporcionen a través de una red durante la inscripción y únicamente garantizados mediante una firma digital u otra información que no está verdaderamente ligada al individuo.

Otras técnicas de inscripción con niveles variables de fiabilidad incluyen sin limitación: inscripción en una oficina física del operador del motor de confianza 110; inscripción en un lugar de empleo del usuario; inscripción en una oficina postal u oficina de pasaportes; inscripción a través de un afiliado o parte de confianza para el operador del motor de confianza 110; inscripción anónima o con pseudónimo en la que la identidad inscrita no se identifica aún con un individuo real particular, así como otros medios que son conocidos en la técnica.

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

De manera similar, los datos adicionales que se envían a través de la red, pero que se autentican mediante otros datos de confianza proporcionados durante una inscripción anterior con el mismo motor de confianza 110 se pueden considerar tan fiables como eran los datos de inscripción original, incluso a pesar de que los últimos datos se enviaran a través de una red abierta. En tales circunstancias, una certificación notarial posterior aumentará de manera eficaz el nivel de fiabilidad que está asociado con los datos de inscripción originales. De esta manera por ejemplo, una inscripción anónima o seudónima se puede elevar a continuación a una inscripción completa demostrando alguna inscripción oficial de la identidad del individuo que coincide con los datos inscritos.

Los factores de fiabilidad que se han analizado en lo que antecede son en general valores que se pueden determinar con antelación de cualquier instancia de autenticación particular. Esto es debido a que están basados en la inscripción y en la técnica, en lugar de en la autenticación real. En una forma de realización, la etapa de generar fiabilidad basándose en estos factores implica buscar valores previamente determinados para esta técnica de autenticación particular y los datos de inscripción del usuario. En un aspecto adicional de una forma de realización ventajosa de la presente invención, tales fiabilidades se pueden incluir con los propios datos de inscripción. De esta manera, estos factores se entregan de forma automática al motor de autenticación 215 junto con los datos de inscripción enviados desde el depósito 210.

A pesar de que estos factores se pueden determinar en general con antelación de cualquier instancia de autenticación individual, aún tienen un efecto en cada instancia de autenticación que usa esa técnica de autenticación particular para ese usuario. Además, a pesar de que los valores pueden cambiar con el tiempo (por ejemplo si el usuario se vuelve a inscribir de una manera más fiable), no son dependientes de los propios datos de autenticación. En contraste, los factores de fiabilidad que están asociados con unos únicos datos de instancia específica pueden variar en cada ocasión. Estos factores, tal como se analizará a continuación, se deben evaluar para cada nueva autenticación para generar puntuaciones de fiabilidad en la etapa 1815.

La fiabilidad de los datos de autenticación refleja la coincidencia entre los datos proporcionados por el usuario en una instancia de autenticación particular y los datos proporcionados durante la inscripción de autenticación. Esto es la cuestión fundamental de si los datos de autenticación coinciden con los datos de inscripción para el usuario individual que está reclamando que es. Normalmente, cuando los datos no coinciden, el usuario se considera que no está autenticado de forma satisfactoria, y la autenticación falla. La manera en la que esto se evalúa puede cambiar dependiendo de la técnica de autenticación que se usa. La comparación de tales datos se realiza mediante la función del comparador 515 del motor de autenticación 215 tal como se muestra en la figura 5.

Por ejemplo, las coincidencias de contraseñas se evalúan en general de una manera binaria. En otras palabras, una contraseña es cualquiera de una coincidencia perfecta, o una coincidencia fallida. Normalmente no es deseable aceptar como incluso una coincidencia parcial una contraseña que está cercana a la contraseña correcta si no es exactamente correcta. Por lo tanto, cuando se evalúa una autenticación de contraseña, la fiabilidad de la autenticación devuelta por el comparador 515 es por lo general cualquiera de 100 % (correcta) o 0 % (errónea), sin posibilidad de valores intermedios.

Se aplican en general reglas similares a estas contraseñas a métodos de autenticación basados en testigo, tales como tarjetas inteligentes. Esto es debido a que tener una tarjeta inteligente que tiene un identificador similar o que es similar al correcto, es igualmente tan incorrecto como tener otro testigo incorrecto. Por lo tanto los testigos también tienden a ser autenticadores binarios: un usuario tiene el testigo correcto o no lo tiene.

No obstante, ciertos tipos de datos de autenticación, tales como cuestionarios y biométricas, en general no son autenticadores binarios. Por ejemplo, una huella digital puede coincidir con una huella digital de referencia a grados variables. Hasta cierto punto, esto se puede deber a variaciones en la calidad de los datos captados durante la inscripción inicial o en autenticaciones posteriores. (Una huella digital puede estar manchada o una persona puede tener una cicatriz o quemadura que se está aún curando en un dedo particular). En otros casos los datos pueden coincidir menos que perfectamente debido a que la propia información es un tanto variable y está basada en la coincidencia del patrón. (Un análisis de voz puede parecer bastante cercano pero no lo suficiente correcto debido a ruido de fondo, o la acústica del entorno en el que se graba la voz, o debido a que la persona puede tener un

resfriado). Por último, en situaciones en donde se están comparando grandes cantidades de datos, puede ser simplemente el caso de que muchas de las coincidencias de datos son buenas, pero algunas no. (Un cuestionario de diez preguntas puede haber dado como resultado ocho respuestas correctas a cuestiones personales, pero dos preguntas incorrectas). Por cualquiera de estas razones, la coincidencia entre los datos de inscripción y los datos para una instancia de autenticación particular se puede asignar de manera deseable un valor de coincidencia parcial mediante el comparador 515. De esta manera, se puede decir que la huella digital es un 85 % de coincidencia, la huella vocal es un 65 % de coincidencia y el cuestionario es un 80 % de coincidencia, por ejemplo.

Esta medida (grado de coincidencia) producida por el comparador 515 es el factor que representa la cuestión básica de si una autenticación es correcta o no. No obstante, tal como se ha analizado en lo que antecede, esto es únicamente uno de los factores que se pueden usar al determinar la fiabilidad de una instancia de autenticación dada. Obsérvese también que incluso a pesar de que se pueda determinar una coincidencia a algún grado parcial, que en última instancia, puede ser deseable proporcionar un resultado binario basándose en una coincidencia parcial. En un modo alternativo de operación, es también posible tratar coincidencias parciales como binarias, es decir, coincidencias perfectas (un 100 %) o fallidas (un 0 %), basándose en si el grado de coincidencia pasa o no un nivel de coincidencia umbral particular. Un proceso de este tipo se puede usar para proporcionar un nivel de paso / fallo sencillo de coincidencia para sistemas que podría producir de otra manera coincidencias parciales.

Otro factor que se ha de considerar al evaluar la fiabilidad de una instancia de autenticación dada se refiere a las circunstancias bajo las que se proporcionan los datos de autenticación para esta instancia particular. Tal como se ha analizado en lo que antecede, las circunstancias se refieren a los metadatos que están asociados con una instancia de autenticación particular. Esto puede incluir sin limitación información tal como: la dirección de red del autenticador, hasta el punto de que se puede determinar; la hora de la autenticación; el modo de transmisión de los datos de autenticación (línea de teléfono, 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 se solicita normalmente por el usuario. A continuación, esta información se puede usar para evaluar la fiabilidad en al menos dos maneras. Una manera es considerar si el usuario está solicitando autenticación de una manera que es coherente con el perfil normal de autenticación por este usuario. Si el usuario normalmente realiza solicitudes de autenticación a partir de una dirección de red durante sus días laborables (cuando está en el trabajo) y desde una dirección de red diferente durante las tardes o fines de semana (cuando está en casa), una autenticación que tiene lugar desde la dirección de casa durante el día laborable es menos fiable debido a que está fuera del perfil de autenticación normal. De manera similar, si el usuario se autentica normalmente usando una huella digital biométrica y por las noches, una autenticación que se origina durante el día usando únicamente una contraseña es menos fiable.

Una manera adicional en la 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 el individuo que reclama ser. Por ejemplo, si la autenticación proviene desde un sistema con un número de serie que se sabe que está asociado con el usuario, esto es un buen indicador circunstancial de que el usuario es quien reclama ser. A la inversa, si la autenticación proviene desde una dirección de red que se conoce que está en Los Ángeles cuando el usuario se sabe que reside en Londres, esto es una indicación de que esta autenticación es menos fiable basándose en sus circunstancias.

Es también posible que una cookie u otro dato electrónico se pueda poner en el sistema que se está usando por un usuario cuando interactúa con un sistema de distribuidor o con el motor de confianza 110. Estos datos se escriben en el almacenamiento del sistema del usuario y pueden contener una identificación que se puede leer mediante un explorador web u otro soporte lógico en el sistema de usuario. Si estos datos se permite que residan en el sistema de usuario entre sesiones (una “cookie persistente”), se pueden enviar con los datos de autenticación como evidencia adicional del uso pasado de este sistema durante la autenticación de un usuario particular. En efecto, los metadatos de una instancia dada, en particular una cookie persistente, pueden formar una clase de autenticador basado en testigo en sí mismo.

Una vez que se generan los factores de fiabilidad apropiados basándose en la técnica y los datos de la instancia de autenticación tal como se ha descrito en lo que antecede en las etapas 1610 y 1615, de forma respectiva, 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 a continuación multiplicarlos juntos.

Por ejemplo, suponiendo que los datos de autenticación se están enviando desde una dirección de red conocida que es del ordenador de la casa del usuario completamente de acuerdo con el perfil de autenticación pasado del usuario (un 100 %), y la técnica que se está usando es identificación por huella digital (un 97 %), y los datos de huella digital iniciales se registraron a través del empleador del usuario con el motor de confianza 110 (un 90 %), y la coincidencia entre los datos de autenticación y la muestra de la huella digital original en los datos de inscripción es muy buena (un 99 %). La fiabilidad global de esta instancia de autenticación se podría calcular a continuación como el producto de estas fiabilidades: 100 % * 97 % * 90 % * 99 % - 86,4 % fiabilidad.

Esta fiabilidad calculada representa la fiabilidad de una única instancia de autenticación. La fiabilidad global de una única instancia de autenticación se puede calcular también usando técnicas que tratan los diferentes factores de fiabilidad de manera diferente, por ejemplo usando fórmulas en donde se asignan diferentes pesos a cada factor de fiabilidad. Además, los expertos en la materia reconocerán que los valores reales que se usan pueden representar valores distintos de porcentajes y pueden usar sistemas no aritméticos. Una forma de realización puede incluir un módulo que es usado por un solicitante de la autenticación para establecer los pesos para 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, indicada como la etapa 1620. No obstante, puede ser útil en muchas situaciones de autenticación para múltiples instancias de autenticación que se proporcionen al mismo tiempo. Por ejemplo, mientras se intenta autenticar a sí mismo usando el sistema de la presente invención, un usuario puede proporcionar una identificación de usuario, datos de autenticación de huellas digitales, una tarjeta inteligente, y una contraseña. En un caso de este tipo, se están proporcionando tres instancias de autenticación independientes al motor de confianza 110 para evaluación. Continuando a la etapa 1625, si el motor de autenticación 215 determina que los datos proporcionados por el usuario incluyen más de una instancia de autenticación, entonces cada instancia a su vez se seleccionará tal como se muestra en la etapa 1630 y se evaluará tal como se ha descrito en lo que antecede en las etapas 1610, 1615 y 1620.

Obsérvese que muchos de los factores de fiabilidad analizados pueden variar de una de estas instancias a otra. Por ejemplo, la fiabilidad intrínseca de estas técnicas es probable que sea diferente, así como el grado de coincidencia proporcionado entre los datos de autenticación y los datos de inscripción. Además, el usuario puede haber proporcionado los datos de inscripción en diferentes momentos y bajo diferentes circunstancias para cada una de estas técnicas, proporcionando diferentes fiabilidades de inscripción para cada una de estas instancias también. Por último, incluso a pesar de que las circunstancias bajo las que los datos para cada una de estas instancias se estén enviando sean las mismas, el uso de tales técnicas puede ajustar cada uno de los perfiles de usuario de manera diferente, y así se pueden asignar diferentes fiabilidades circunstanciales. (Por ejemplo, el usuario puede usar normalmente su contraseña y huella digital, pero no su tarjeta inteligente).

Como resultado, la fiabilidad final para cada una de estas autenticaciones de instancias puede ser diferente entre sí. No obstante, usando múltiples instancias juntas, el nivel de confianza global para la autenticación tenderá a aumentar.

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

Un medio en el que el motor de autenticación 215 puede combinar las fiabilidades de múltiples instancias de autenticación concurrentes para generar un nivel de confianza final es multiplicar la no fiabilidad de cada instancia para llegar a una no fiabilidad total. La no fiabilidad es en general el porcentaje complementario de la fiabilidad. Por ejemplo, una técnica que es 84 % fiable es 16 % no fiable. Las tres instancias de autenticación que se han descrito en lo que antecede (huella digital, tarjeta inteligente, contraseña) producirán fiabilidades de 86 %, 75 %, y 72 % que se corresponderían con no fiabilidades de (100 - 86) %, (100 - 75) % y (100 - 72) %, o 14 %, 25 %, y 28 %, de forma respectiva. Multiplicando estas no fiabilidades, obtenemos una no fiabilidad acumulada de 14 % * 25 % * 28 % - .98 % no fiabilidad, que se corresponde con una fiabilidad del 99,02 %.

En un modo adicional de operación, se pueden aplicar factores adicionales y heurística 530 en el motor de autenticación 215 para tener en cuenta la interdependencia de diversas técnicas de autenticación. Por ejemplo, si alguien tiene acceso no autorizado a un ordenador doméstico particular, probablemente tenga acceso a la línea telefónica en esa dirección también. Por lo tanto, la autenticación basándose en un número de teléfono de origen así como en el número de serie del sistema de autenticación no añade mucho a la confianza global en la autenticación. No obstante, la autenticación basada en el conocimiento es enormemente independiente de la autenticación basada en testigo (es decir, si alguien roba tu teléfono celular o las llaves, no es más probable que conozcan tu PIN o contraseña que si no lo tuvieran).

Además, diferentes distribuidores u otros solicitantes de autenticación pueden desear ponderar diferentes aspectos de la autenticación de manera diferente. Esto puede incluir el uso de factores de ponderación o algoritmos que se usan al calcular las instancias de fiabilidad de individual así como el uso de diferentes medios para evaluar los eventos de autenticación con múltiples instancias.

Por ejemplo, los distribuidores para ciertos tipos de transacciones, por ejemplo sistemas de correo electrónico corporativos, pueden desear autenticar principalmente basándose en heurística y otros datos circunstanciales por defecto. Por lo tanto, pueden aplicar altos pesos a factores relacionados con los metadatos y otra información relacionada con el perfil que está asociada con las circunstancias que rodean los eventos de autenticación. Esta disposición se podría usar para facilitar la carga sobre los usuarios durante horas de operación normal, no requiriendo más del usuario que este inicie sesión en la máquina correcta durante las horas laborales. No obstante, otro distribuidor puede ponderar autenticaciones que provienen desde una técnica particular más fuertemente, por ejemplo coincidencia de huellas digitales, debido a una decisión de política de que una técnica de este tipo es más adecuada para autenticación para los fines del distribuidor particulares.

Tales diversos pesos se pueden definir mediante el solicitante de la autenticación al generar la solicitud de autenticación y enviar al motor de confianza 110 con la solicitud de autenticación en un modo de operación. Tales opciones se podrían establecer también como preferencias durante un proceso de inscripción inicial para el solicitante de la autenticación y almacenarse en el motor de autenticación en otro modo de operación.

Una vez que el motor de autenticación 215 produce un nivel de confianza de autenticación para los datos de autenticación proporcionados, este nivel de confianza se usa para completar la solicitud de autenticación en la etapa 1640, y esta información se reenvía desde el motor de autenticación 215 al motor de transacción 205 para inclusión en un mensaje al solicitante de la autenticación.

El proceso que se ha descrito en lo que antecede es meramente a modo de ejemplo, y los expertos en la materia reconocerán que las etapas no necesitan realizarse en el orden mostrado o que únicamente se desee realizar ciertas de las etapas, o que se puede desear una diversidad de combinación de etapas. Además, ciertas etapas, tales como la evaluación de la fiabilidad de cada instancia de autenticación proporcionada, se pueden llevar a cabo en paralelo entre sí si las circunstancias lo permiten.

En un aspecto adicional de esta invención, se proporciona un método para adaptar condiciones cuando el nivel de confianza de autenticación producido por el proceso que se ha descrito en lo que antecede no cumple el nivel de confianza requerido del distribuidor u otra parte que requiere la autenticación. En circunstancias tales como estas existe un hueco entre el nivel de confianza proporcionado y el nivel de confianza deseado, el operador del motor de confianza 110 está en una posición para proporcionar oportunidades para una o ambas partes para proporcionar datos o requisitos alternativos para cerrar este hueco de confianza. Este proceso se denominará como “arbitraje de confianza” en el presente documento.

El arbitraje de confianza puede tener lugar en una estructura de autenticación criptográfica tal como se ha descrito en lo que antecede con referencia a las figuras 10 y 11. Tal como se muestra en las mismas, un distribuidor u otra parte solicitará una autenticación de un usuario particular en asociación con una transacción particular. En una circunstancia, el distribuidor simplemente solicita una autenticación, positiva o negativa, y después de recibir datos apropiados procedentes del usuario, el motor de confianza 110 proporcionará una autenticación binaria de este tipo. En circunstancias tales como estas, el grado de confianza requerido para asegurar una autenticación positiva se determina basándose en preferencias establecidas en el motor de confianza 110.

No obstante, es posible también que el distribuidor pueda solicitar un nivel particular de confianza para completar una transacción particular. Este nivel requerido se puede incluir con la solicitud de autenticación (por ejemplo autenticar este usuario al 98 % de confianza) o se puede determinar mediante el motor de confianza 110 basándose en otros factores que están asociados con la transacción (es decir, autenticar a este usuario como apropiado para esta transacción). Un factor de este tipo puede ser el valor económico de la transacción. Para transacciones que tienen valor económico mayor, se puede requerir un grado más alto de confianza. De manera similar, para transacciones con grados altos de riesgo se puede requerir un alto grado de confianza. A la inversa, para transacciones que son de bajo riesgo o de bajo valor, se pueden requerir niveles de confianza inferiores por el distribuidor u otro solicitante de la autenticación.

El proceso de arbitraje de confianza tiene lugar entre las etapas del motor de confianza 110 que recibe los datos de autenticación en la etapa 1050 de la figura 10 y la devolución de un resultado de autenticación al distribuidor en la etapa 1055 de la figura 10. Entre estas etapas, el proceso que conduce a la evaluación de niveles de confianza y el arbitraje de confianza potencial tienen lugar tal como se muestra en la figura 17. En circunstancias en donde se realiza autenticación binaria sencilla, el proceso mostrado en la figura 17 reduce a tener el motor de transacción 205 que comparar directamente los datos de autenticación proporcionados con los datos de inscripción para el usuario identificado tal como se ha analizado en lo que antecede con referencia a la figura 10, etiquetando cualquier diferencia como una autenticación negativa.

Tal como se muestra en la figura 17, la primera etapa después de recibir los datos en la etapa 1050 es para que el motor de transacción 205 determine el nivel de confianza que se requiere para una autenticación positiva para esta transacción particular en la etapa 1710. Esta etapa se puede realizar mediante uno de varios modos diferentes. El nivel de confianza requerido se puede especificar al motor de confianza 110 mediante el solicitante de la autenticación en el momento cuando se realiza la solicitud de autenticación. El solicitante de la autenticación puede

establecer también una preferencia con antelación que se almacena en el depósito 210 u otro almacenamiento que es accesible mediante el motor de transacción 205. Esta preferencia se puede leer a continuación y usarse cada vez que se realiza una solicitud de autenticación mediante este solicitante de la autenticación. La preferencia se puede asociar también con un usuario particular y una medida de seguridad de tal modo que se requiera siempre un nivel de confianza particular para autenticar a ese usuario, almacenándose la preferencia de usuario en el depósito 210 u otro medio de almacenamiento accesible mediante el motor de transacción 205. El nivel requerido se puede obtener también mediante el motor de transacción 205 o el motor de autenticación 215 basándose en información proporcionada en la solicitud de autenticación, tal como el valor y el nivel de riesgo de la transacción para autenticarse.

En un modo de operación, un módulo de gestión de política u otro soporte lógico que se usa cuando se genera la solicitud de autenticación se usa para especificar el grado de confianza requerido para la autenticación de la transacción. Esto se puede usar para proporcionar una serie de reglas para seguirlas cuando se asigna el nivel requerido de confianza basándose en las políticas que se especifican en el módulo de gestión de política. Un modo ventajoso de operación es que se incorpore un módulo de este tipo con el servidor web de un distribuidor para determinar de forma apropiada el nivel requerido de confianza para transacciones indiciadas con el servidor web del distribuidor. De esta manera, las solicitudes de transacción desde los usuarios se pueden asignar a un nivel de confianza requerido de acuerdo con las políticas del distribuidor y tal información se puede reenviar al motor de confianza 110 junto con la solicitud de autenticación.

Este nivel de confianza requerido se correlaciona con el grado de certeza que el distribuidor desea tener de que el individuo que se está autenticando es de hecho quien dice ser al identificarse. Por ejemplo, si la transacción es una en donde el distribuidor desea bastante grado de certeza debido a que bienes se están cambiando de manos, el distribuidor puede requerir un nivel de confianza del 85 %. Para la situación en donde el distribuidor está autenticando meramente al usuario para permitirle ver contenido únicamente para miembros o privilegios para ejercer en una sala de conversaciones, el riesgo bajista puede ser lo suficientemente pequeño que el distribuidor requiera únicamente un 60 % de nivel de confianza. No obstante, para entrar en un contrato de producción con un valor de decenas de miles de dólares, el distribuidor puede requerir un nivel de confianza del 99 % o más.

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

Tal como se muestra en la figura 17, después de que el motor de transacción 205 recibe el nivel de confianza requerido, compara en la etapa 1720 el nivel de confianza requerido con el nivel de confianza de autenticación que el motor de autenticación 215 calculó para la autenticación actual (tal como se ha analizado con referencia a la figura 16). Si el nivel de confianza de autenticación es superior al nivel de confianza requerido para la transacción en la etapa 1730, entonces el proceso se mueve a la etapa 1740 en donde se produce una autenticación positiva para esta transacción mediante el motor de transacción 205. Un mensaje para este efecto se insertará a continuación en los resultados de autenticación y se devolverá al distribuidor mediante el motor de transacción 205 tal como se muestra en la etapa 1055 (véase la figura 10).

No obstante, si el nivel de confianza de autenticación no satisface el nivel de confianza requerido en la etapa 1730, entonces existe un hueco de confianza para la autenticación actual, y se realiza arbitraje de confianza en la etapa 1750. El arbitraje de confianza se describe más completamente con referencia a la figura 18 a continuación. Este proceso tal como se describe a continuación tiene lugar en el motor de transacción 205 del motor de confianza 110. Debido a que no es necesaria autenticación u otras operaciones criptográficas para ejecutar el arbitraje de confianza (distintas a las requeridas para la comunicación de SSL entre el motor de transacción 205 y otros componentes), el proceso se puede realizar fuera del motor de autenticación 215. No obstante, tal como se analizará a continuación, cualquier reevaluación de datos de autenticación u otros eventos criptográficos o de autenticación requerirá que el motor de transacción 205 vuelva a enviar los datos apropiados al motor de autenticación 215. Los expertos en la materia reconocerán que el proceso de arbitraje de confianza se podría estructurar como alternativa para tener lugar parcial o completamente en el propio motor de autenticación 215.

Tal como se ha mencionado en lo que antecede, el arbitraje de confianza es un proceso en donde el motor de confianza 110 media una negociación entre el distribuidor y el usuario en un intento de asegurar una autenticación positiva cuando sea apropiado. Tal como se muestra en la etapa 1805, el motor de transacción 205 determina en primer lugar si la situación actual es apropiada o no para arbitraje de confianza. Esto se puede determinar basándose en las circunstancias de la autenticación, por ejemplo si esta autenticación ya ha sido a través de múltiples ciclos de arbitraje, así como sobre las preferencias de cualquiera del distribuidor o usuario, tal como se analizará adicionalmente a continuación.

En tales circunstancias en donde el arbitraje no es posible, el proceso continúa a la etapa 1810 en donde el motor de transacción 205 genera una autenticación negativa, y a continuación la inserta en los resultados de autenticación que se envían al distribuidor en la etapa 1055 (véase la figura 10). Un límite que se puede usar de forma ventajosa para evitar que las autenticaciones estén pendientes de forma indefinida es establecer un periodo de límite de tiempo desde la solicitud de autenticación inicial. De esta manera, cualquier transacción que no se autentique positivamente en el límite de tiempo se deniega arbitraje adicional y se autentica negativamente. Los expertos en la materia reconocerán que un límite de tiempo de este tipo puede variar dependiendo de las circunstancias de la transacción y los deseos del usuario y el distribuidor. Se pueden poner también limitaciones tras el número de intentos que se pueden realizar al proporcionar una autenticación satisfactoria. Tales limitaciones se pueden manejar mediante un limitador de intentos 535 tal como se muestra en la figura 5.

Si no se prohíbe el arbitraje en la etapa 1805, el motor de transacción 205 participará a continuación en la negociación con una o ambas de las partes de la transacción. El motor de transacción 205 puede enviar un mensaje al usuario solicitando alguna forma de autenticación adicional para potenciar el nivel de confianza de autenticación producido tal como se muestra en la etapa 1820. En la forma más sencilla, esto puede indicar simplemente que la autenticación fue insuficiente. Se puede enviar también una solicitud para producir una o más instancias de autenticación adicionales para mejorar el nivel de confianza global de la autenticación.

Si el usuario proporciona alguna instancia de autenticación adicional en la etapa 1825, entonces el motor de transacción 205 añade estas instancias de autenticación a los datos de autenticación para la transacción y las reenvía al motor de autenticación 215 tal como se muestra en la etapa 1015 (véase la figura 10), y la autenticación se vuelve a evaluar basándose en las instancias de autenticación preexistentes para esta transacción y en las instancias de autenticación recién proporcionadas.

Un tipo adicional de autenticación puede ser una solicitud desde el motor de confianza 110 para hacer alguna forma de contacto de persona a persona entre el operador del motor de confianza 110 (o un asociado de confianza) y el usuario, por ejemplo, mediante llamada de teléfono. Esta llamada de teléfono u otra autenticación no informática se puede usar para proporcionar contacto personal con el individuo y también para realizar alguna forma de autenticación basada en cuestionario. Esto puede proporcionar también la oportunidad de verificar un número de teléfono de origen y potencialmente un análisis de voz del usuario cuando está en la llamada. Incluso a pesar de que no se puedan proporcionar datos de autenticación adicionales, el contexto adicional que está asociado con el número de teléfono del usuario puede mejorar el contexto de la fiabilidad de la autenticación. Cualquier dato o circunstancias revisadas basándose en esta llamada de teléfono se alimentan en el motor de confianza 110 para su uso en consideración de la solicitud de autenticación.

Además, en la etapa 1820 el motor de confianza 110 puede proporcionar una oportunidad para que el usuario compre una cobertura, comprando de manera eficaz una autenticación de mayor confianza. El operador del motor de confianza 110 puede desear, en ocasiones, únicamente hacer disponible una opción de este tipo si el nivel de confianza de la autenticación está por encima de un cierto umbral para empezar. En efecto, esta cobertura del lado del usuario es una manera para que el motor de confianza 110 garantice el usuario cuando la autenticación cumple el nivel de confianza requerido normal del motor de confianza 110 para autenticación, pero no cumple el nivel de confianza requerido del distribuidor para esta transacción. De esta manera, el usuario aún se puede autenticar de forma satisfactoria a un muy alto nivel como se puede requerir mediante el distribuidor, incluso a pesar de que este únicamente tenga instancias de autenticación que producen confianza suficiente para el motor de confianza 110.

Esta función del motor de confianza 110 permite al motor de confianza 110 garantizar a alguien que se autentica la satisfacción del motor de confianza 110, pero no del distribuidor. Esto es análogo a la función realizada por un notario añadiendo su firma a un documento para indicar que alguien que lee el documento en un momento posterior que la persona cuya firma aparece en el documento es de hecho la persona que lo firmó. La firma del notario testifica el acto de firma por el usuario. De la misma manera, el motor de confianza está proporcionando una indicación de que la persona que realiza la transacción es quien este dice que es.

No obstante, debido a que el motor de confianza 110 está potenciando de forma artificial el nivel de confianza proporcionado por el usuario, hay un riesgo superior para el operador del motor de confianza 110, debido a que el usuario no está cumpliendo realmente el nivel de confianza requerido del distribuidor. El coste de la cobertura está diseñado para desplazar el riesgo de una autenticación de falso positivo para el motor de confianza 110 (que puede estar certificando notarialmente, de forma eficaz, las autenticaciones del usuario). El usuario paga al operador del motor de confianza 110 para asumir el riesgo de autenticar a un nivel superior de confianza que el que realmente se ha proporcionado.

Debido a que un sistema de cobertura de este tipo permite a alguien comprar de forma eficaz una calificación de confianza superior desde el motor de confianza 110, ambos, distribuidores y usuarios pueden desear evitar el uso de cobertura del lado del usuario en ciertas transacciones. Los distribuidores pueden desear limitar autenticaciones positivas a circunstancias en donde conocen que los datos de autenticación reales soportan el grado de confianza que requieren y así pueden indicar al motor de confianza 110 que la cobertura del lado del usuario no se debe permitir. De manera similar, para proteger su identidad en línea, un usuario puede desear evitar el uso de su

cobertura del lado del usuario en su cuenta, o puede desear limitar su uso a situaciones en donde el nivel de confianza de autenticación sin la cobertura sea superior a un cierto límite. Esto se puede usar como una medida de seguridad para evitar que alguien escuche por casualidad una contraseña o robe una tarjeta inteligente y la use para autentificar de manera falsa en un nivel bajo de confianza, y a continuación comprar cobertura para producir un nivel muy alto de (falsa) confianza. Estos factores se pueden evaluar al determinar si se permite la cobertura del lado del usuario.

Si el usuario compra cobertura en la etapa 1840, entonces el nivel de confianza de autenticación se ajusta basándose en la cobertura comprada en la etapa 1845, y el nivel de confianza de autenticación y nivel de confianza requerido se comparan de nuevo en la etapa 1730 (véase la figura 17). El proceso continúa desde allí, y puede conducir a cualquiera de una autenticación positiva en la etapa 1740 (véase la figura 17), o de vuelta al proceso de arbitraje de confianza en la etapa 1750 para arbitraje adicional (si se permite) o una autenticación negativa en la etapa 1810 si se prohíbe el arbitraje adicional.

Además de enviar un mensaje al usuario en la etapa 1820, el motor de transacción 205 puede enviar también un mensaje al distribuidor en la etapa 1830 que indica que una autenticación pendiente está en la actualidad por debajo del nivel de confianza requerido. El mensaje puede ofrecer también diversas opciones sobre cómo continuar con el distribuidor. Una de estas opciones es simplemente informar al distribuidor de cuál es el nivel de confianza de autenticación actual y pedir si el distribuidor desea mantener su nivel de confianza requerido no satisfecho actual. Esto puede ser beneficioso debido a que en algunos casos, el distribuidor puede tener medios independientes para autenticar la transacción o puede haber usado un conjunto por defecto de requisitos que en general dan como resultado que se especifique inicialmente un nivel requerido superior que el que es realmente necesario para la transacción particular en cuestión.

Por ejemplo, puede ser una práctica convencional que todas las transacciones de órdenes de adquisición entrantes con el distribuidor se espere que cumplan un 98 % de nivel de confianza. No obstante, si se analizó una orden recientemente por teléfono entre el distribuidor y un cliente antiguo, e inmediatamente después a la transacción se autentica, pero únicamente a un 93 % de nivel de confianza, el distribuidor puede desear simplemente reducir el nivel de aceptación para esta transacción, debido a que la llamada de teléfono proporciona de forma eficaz autenticación adicional para el distribuidor. En ciertas circunstancias, el distribuidor puede desear reducir su nivel de confianza requerido, pero no todo hasta el nivel de la confianza de autenticación actual. Por ejemplo, el distribuidor en el ejemplo anterior puede considerar que la llamada telefónica antes de la orden puede merecer una reducción del 4 % en el grado de confianza necesaria; no obstante, esto es aún mayor que el 93 % de confianza producida por el usuario.

Si el distribuidor no ajusta su nivel de confianza requerido en la etapa 1835, entonces el nivel de confianza de autenticación producido por la autenticación y el nivel de confianza requerido se comparan en la etapa 1730 (véase la figura 17). Si el nivel de confianza ahora supera el nivel de confianza requerido, se puede generar una autenticación positiva en el motor de transacción 205 en la etapa 1740 (véase la figura 17). Si no, se puede intentar un arbitraje adicional tal como se ha analizado en lo que antecede si se permite.

Además de solicitar un ajuste al nivel de confianza requerido, el motor de transacción 205 puede ofrecer también cobertura del lado de distribuidor para el distribuidor que solicita la autenticación. Esta cobertura sirve para un fin similar al que se ha descrito en lo que antecede para la cobertura del lado del usuario. En este punto, no obstante, en lugar del coste que se corresponde con el riesgo que se está asumiendo por el motor de confianza 110 al autenticar por encima del nivel de confianza de autenticación real producido, el coste de la cobertura se corresponde con el riesgo que está siendo asumiendo por el distribuidor al aceptar un nivel de confianza inferior en la autenticación.

En lugar de solo reducir su nivel de confianza requerido actual, el distribuidor tiene la opción de comprar cobertura para protegerse asimismo del riesgo adicional que está asociado con un nivel inferior de confianza en la autenticación del usuario. Tal como se ha descrito en lo que antecede, puede ser ventajoso para el distribuidor considerar únicamente comprar tal cobertura para cubrir el hueco de confianza en condiciones en donde la autenticación existente ya esté por encima de un cierto umbral.

La disponibilidad de tal cobertura del lado del distribuidor permite al distribuidor la opción de: reducir su requisito de confianza directamente a ningún coste adicional para sí mismo, soportando él mismo el riesgo de una falsa autenticación (basándose en el nivel de confianza inferior requerido); o, comprando cobertura para el hueco de confianza entre el nivel de confianza de autenticación y su requisito, soportando el operador del motor de confianza 110 el riesgo del nivel de confianza inferior que se ha proporcionado. Comprando la cobertura, el distribuidor mantiene de forma eficaz su requisito de nivel de confianza alto: debido a que el riesgo de una falsa autenticación se desplaza al operador del motor de confianza 110.

Si el distribuidor compra cobertura en la etapa 1840, el nivel de confianza de autenticación y los niveles de confianza requeridos se comparan en la etapa 1730 (véase la figura 17), y el proceso continúa tal como se ha descrito en lo que antecede.

Obsérvese que es también posible que tanto el usuario como el distribuidor respondan a mensajes desde el motor de confianza 110. Los expertos en la materia reconocerán que hay múltiples maneras en las que se pueden manejar tales situaciones. Un modo ventajoso para manejar la posibilidad de múltiples respuestas es simplemente tratar las respuestas en una manera primero en entrar, primero en servir. Por ejemplo, si el distribuidor responde con un nivel de confianza requerido reducido e inmediatamente después el usuario compra también cobertura para elevar su nivel de autenticación, la autenticación se vuelve a evaluar en primer lugar basándose en el requisito de confianza reducido del distribuidor. Si la autenticación es ahora positiva, se ignora la adquisición de cobertura del usuario. En otro modo ventajoso de operación, se puede cobrar únicamente al usuario por el nivel de cobertura requerido para cumplir el nuevo requisito de confianza reducido del distribuidor (si incluso quedó un hueco de confianza con el requisito de confianza del distribuidor reducido).

Si no se recibe respuesta desde cualquier parte durante el proceso de arbitraje de confianza en la etapa 1850 en el límite de tiempo establecido para la autenticación, el arbitraje se vuelve a evaluar en la etapa 1805. Esto comienza de forma eficaz el proceso de arbitraje de nuevo. Si el límite de tiempo se finalizó u otras circunstancias evitan arbitraje adicional en la etapa 1805, se genera una autenticación negativa mediante el motor de transacción 205 en la etapa 1810 y se devuelve al distribuidor en la etapa 1055 (véase la figura 10). Si no, se pueden enviar nuevos mensajes al usuario y al distribuidor, y el proceso se puede repetir según se desee.

Obsérvese que para ciertos tipos de transacciones, por ejemplo, firma digital de documentos que no son parte de una transacción, puede no ser necesaria para un distribuidor u otra parte tercera; por lo tanto la transacción es principalmente entre el usuario y el motor de confianza 110. En circunstancias tales como estas, el motor de confianza 110 tendrá su propio nivel de confianza requerido que se debe satisfacer para generar una autenticación positiva. No obstante, en tales circunstancias, a menudo no será deseable que el motor de confianza 110 ofrezca cobertura al usuario para que se eleve la confianza de su propia firma.

El proceso que se ha descrito en lo que antecede y que se muestra en las figuras 16 - 18 se puede llevar a cabo usando diversos modos de comunicación tal como se ha descrito en lo que antecede con referencia al motor de confianza 110. Por ejemplo, los mensajes pueden estar basados en web y enviarse usando conexiones de SSL entre el motor de confianza 110 y miniaplicaciones descargadas en tiempo real a los exploradores que se ejecutan en el sistema del usuario o de los distribuidores. En un modo de operación alternativo, ciertas aplicaciones especializadas pueden estar en uso por el usuario y el distribuidor que facilitan tales transacciones de arbitraje y cobertura. En otro modo de operación alternativo, se pueden usar operaciones de correo electrónico seguras para mediar el arbitraje que se ha descrito en lo que antecede, permitiendo de esta manera evaluaciones diferidas y procesamiento en lotes de las autenticaciones. Los expertos en la materia reconocerán que se pueden usar diferentes modos de comunicaciones según sean apropiados para las circunstancias y requisitos de autenticación del distribuidor.

La siguiente descripción con referencia a la figura 19 describe una transacción de muestra que integra los diversos aspectos de la presente invención tal como se ha descrito en lo que antecede. Este ejemplo ilustra el proceso global entre un usuario y un distribuidor según median mediante el motor de confianza 110. A pesar de que las diversas etapas y componentes tal como se han descrito con detalle en lo que antecede se pueden usar para llevar a cabo la siguiente transacción, el proceso ilustrado se centra en la interacción entre el motor de confianza 110, el usuario y el distribuidor.

La transacción comienza cuando el usuario, mientras observa páginas web en línea, rellena un formulario de pedido en el sitio web del distribuidor en la etapa 1900. El usuario desea enviar su formulario de pedido al distribuidor, firmado con su firma digital. Para hacer esto, el usuario envía el formulario de pedido con su solicitud de una firma al motor de confianza 110 en la etapa 1905. El usuario proporcionará también datos de autenticación que se usarán tal como se ha descrito en lo que antecede para autenticar su identidad.

En la etapa 1910 los datos de autenticación se comparan con los datos de inscripción mediante el motor de confianza 110 tal como se ha analizado en lo que antecede, y si se produce una autenticación positiva, el troceo del formulario de pedido, firmado con la clave privada del usuario, se reenvía al distribuidor junto con el propio formulario de pedido.

El distribuidor recibe el formulario firmado en la etapa 1915, y a continuación el distribuidor generará una factura u otro contrato relacionado con la adquisición a realizar en la etapa 1920. Este contrato se envía de vuelta al usuario con una solicitud de una firma en la etapa 1925. El distribuidor envía también una solicitud de autenticación para esta transacción de contrato al motor de confianza 110 en la etapa 1930 que incluye un troceo del contrato que se firmará por ambas partes. Para permitir que se firme de forma digital el contrato por ambas partes, el distribuidor incluye también datos de autenticación por sí mismo de tal modo que la firma del distribuidor en el contrato se pueda verificar más tarde si fuera necesario.

Tal como se ha analizado en lo que antecede, el motor de confianza 110 a continuación verifica los datos de autenticación proporcionados mediante el distribuidor para confirmar la identidad del distribuidor, y si los datos producen una autenticación positiva en la etapa 1935, continúa con la etapa 1955 cuando se reciben los datos

procedentes del usuario. Si los datos de autenticación del distribuidor no coinciden con los datos de inscripción del distribuidor al grado deseado, se devuelve un mensaje al distribuidor que solicita autenticación adicional. Se puede realizar el arbitraje de confianza en este punto si fuera necesario, tal como se ha descrito en lo que antecede, para que el distribuidor se autentique de forma satisfactoria a sí mismo para el motor de confianza 110.

Cuando el usuario recibe el contrato en la etapa 1940, lo revisa, genera datos de autenticación para firmarlo si es aceptable en la etapa 1945, y a continuación envía un troceo del contrato y sus datos de autenticación al motor de confianza 110 en la etapa 1950. El motor de confianza 110 verifica los datos de autenticación en la etapa 1955 y si la autenticación es buena, continúa procesando el contrato tal como se describe a continuación. Tal como se ha analizado en lo que antecede con referencia a las figuras 17 y 18, se puede realizar el arbitraje de confianza según sea apropiado para cerrar cualquier hueco de confianza que exista entre el nivel de confianza de autenticación y el nivel de autenticación requerido para la transacción.

El motor de confianza 110 firma el troceo del contrato con la clave privada del usuario, y envía este troceo firmado al distribuidor en la etapa 1960, que firma el mensaje completo en su propio nombre, es decir, incluyendo un troceo del mensaje completo (incluyendo la firma del usuario) encriptado con la clave privada 510 del motor de confianza 110. Este mensaje se recibe mediante el distribuidor en la etapa 1965. El mensaje representa un contrato firmado (troceo de contrato encriptado usando la clave privada del usuario) y una recepción desde el motor de confianza 110 (el troceo del mensaje que incluye el contrato firmado, encriptado usando la clave privada del motor de confianza 110).

El motor de confianza 110 prepara de manera similar un troceo del contrato con la clave privada del distribuidor en la etapa 1970, y reenvía esta al usuario, firmado por el motor de confianza 110. De esta manera, el usuario también recibe una copia del contrato, firmado por el distribuidor, así como una recepción, firmada por el motor de confianza 110, de la entrega del contrato firmado en la etapa 1975.

Además de lo anterior, un aspecto adicional de la invención proporciona un Módulo de Proveedor de Servicio (SPM, *Service Provider Module*) criptográfico que puede estar disponible para una aplicación del lado del cliente como un medio para acceder a funciones proporcionadas por el motor de confianza 110 que se ha descrito en lo que antecede. Una manera ventajosa de proporcionar un servicio de este tipo es que el SPM criptográfico medie las comunicaciones entre una Interfaz de Programación de Aplicación (API, *application program interface*) de terceros y un motor de confianza 110 que es accesible mediante una red u otra conexión remota. Un SPM criptográfico de muestra se describe a continuación con referencia a la figura 20.

Por ejemplo, en un sistema habitual, está disponible un número de API para los programadores. Cada API proporciona un conjunto de llamadas de función que se pueden realizar mediante una aplicación 2000 que se ejecuta en el sistema. Ejemplos de API que pueden proporcionar interfaces de programación adecuadas para funciones criptográficas, funciones de autenticación y otra función de seguridad incluyen la API Criptográfica (CAPI, *cryptographic API*) 2010 proporcionada por Microsoft con sus sistemas operativos Windows, y la Arquitectura Común de Seguridad de Datos (CDSA, *Common Data Security Architecture*), patrocinada por IBM, Intel y otros miembros del Grupo Abierto. CAPI se usará como una API de seguridad a modo de ejemplo en el análisis que sigue. No obstante, el SPM criptográfico que se describe se podría usar con CDSA u otra API de seguridad tal como se conoce en la técnica.

Esta API se usa mediante un sistema de usuario 105 o sistema de distribuidor 120 cuando se realiza una llamada para una función criptográfica. Incluidas entre estas funciones pueden estar solicitudes que están asociadas con realizar diversas operaciones criptográficas, tales como encriptar un documento con una clave particular, firmar un documento, solicitar un certificado digital, verificar una firma en un documento firmado y tales otras funciones criptográficas tal como se describe en el presente documento o se conocen por los expertos en la materia.

Tales funciones criptográficas se realizan normalmente de forma local para el sistema en el que está localizada la CAPI 2010. Esto es debido a que en general las funciones solicitadas requieren el uso de cualquier recurso del sistema local de usuario 105, tal como un lector de huella digital, o funciones de soporte lógico que se programan usando bibliotecas que se ejecutan en la máquina local. El acceso a estos recursos locales se proporciona normalmente mediante uno o más Módulos de Proveedor de Servicios (SPM, *Service Provider Module*) 2015, 2020 tal como se ha hecho referencia en lo que antecede que proporcionan recursos con los que se llevan a cabo las funciones criptográficas. Tales SPM pueden incluir las bibliotecas de soporte lógico 2015 para realizar operaciones de encriptación o desencriptación, o controladores y aplicaciones 2020 que pueden acceder a soporte físico especializado 2025, tal como dispositivos de exploración biométricos. Así como CAPI 2010 proporciona funciones que se pueden usar mediante una aplicación 2000 del sistema 105, los SPM 2015, 2020 proporcionan CAPI con acceso a las funciones y recursos de nivel inferior que están asociados con los servicios disponibles en el sistema.

De acuerdo con la invención, es posible proporcionar un SPM criptográfico 2030 que puede acceder a las funciones criptográficas proporcionadas mediante el motor de confianza 110 y hacer disponibles estas funciones a una aplicación 2000 a través de CAPI 2010. A diferencia de las formas de realización en donde CAPI 2010 está únicamente disponible para acceder a recursos que están localmente disponibles a través de los SPM 2015, 2020, un SPM criptográfico 2030 tal como se describe en el presente documento podría enviar solicitudes de operaciones

criptográficas a una red localizada accesible de forma remota para el motor de confianza 110 para realizar las operaciones deseadas.

Por ejemplo, si una aplicación 2000 tiene una necesidad de una operación criptográfica, tal como firmar un documento, la aplicación 2000 hace una llamada de función a la función CAPI 2010 apropiada. CAPI 2010 a su vez ejecutará esta función, haciendo uso de los recursos que se ponen a disposición para la misma mediante los SPM 2015, 2020 y el SPM criptográfico 2030. En el caso de una función de firma digital, el SPM criptográfico 2030 generará una solicitud apropiada que 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 a disposición de manera eficaz para un sistema de usuario 105 a través de CAPI 2010 de tal modo que parecen estar localmente disponibles en el propio sistema de usuario 105. No obstante, a diferencia de los SPM convencionales 2015, 2020, las funciones se llevan a cabo en el motor de confianza remoto 110 y los resultados reenviados al SPM criptográfico 2030 en respuesta a solicitudes apropiadas a través del enlace de comunicación 125.

Este SPM criptográfico 2030 pone a disposición un número de operaciones para el sistema de usuario 105 o un sistema de distribuidor 120 que pueden no estar disponibles de otra manera. Estas funciones incluyen sin limitación: encriptación y desencriptación de documentos; cobertura de certificados digitales, firma digital de documentos; verificación de firmas digitales; y otras operaciones de este tipo tal como será evidente para los expertos en la materia.

En una forma de realización separada, la presente invención comprende un sistema completo para realizar los métodos de aseguración de datos de la presente invención en cualquier conjunto de datos. El sistema informático de esta forma de 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 punto. En una forma de realización de la presente invención, el módulo de división de datos, en ocasiones denominado en el presente documento como un analizador de datos seguro, comprende un programa o conjunto de soporte lógico analizador que comprende división de datos, encriptación y desencriptación, funcionalidad de reconstitución o reensamblaje. Esta forma de realización puede comprender adicionalmente una instalación de almacenamiento de datos o múltiples instalaciones de almacenamiento de datos, también. El módulo de división de datos, o analizador de datos seguro, comprende un conjunto de módulo de soporte lógico de plataforma cruzada que se integra en una infraestructura electrónica, o como un complemento a cualquier aplicación que requiere la seguridad final de sus elementos. Este proceso de análisis opera en cualquier tipo de conjunto de datos, y en cualquiera y todo tipo de ficheros, o en una base de datos en cualquier fila, columna o celda de datos en esa base de datos.

El proceso de análisis de la presente invención se puede diseñar, en una forma de realización, de una manera en niveles modulares, y cualquier proceso de encriptación es adecuado para su uso en los procesos de la presente invención. Los niveles modulares del proceso de análisis y división de la presente invención pueden incluir, pero sin limitación, 1) división criptográfica, almacenada dispersada y de manera segura en múltiples localizaciones; 2) encriptar, dividir de forma criptográfica, almacenada dispersada y de manera segura en múltiples localizaciones; 3) encriptar, dividir de forma criptográfica, encriptar cada compartición, a continuación almacenada dispersada y de manera segura en múltiples localizaciones; y 4) encriptar, dividir de forma criptográfica, encriptar cada compartición con un tipo diferente de encriptación que se usó en la primera etapa a continuación almacenada dispersada y de manera segura en múltiples localizaciones.

El proceso comprende, en una forma de realización, división de los datos de acuerdo con los contenidos de un número o clave aleatorios generados, y realizar la misma división criptográfica de la clave que se usa en la encriptación de la división de los datos para asegurarse en dos o más porciones, o comparticiones, de datos analizados y divididos, y en una forma de realización, preferiblemente en cuatro o más porciones de datos analizados y divididos, encriptar todas las porciones, a continuación distribuir y almacenar estas porciones de vuelta en la base de datos, o reubicarlas a cualquier dispositivo nombrado, fijo o extraíble, dependiendo de la necesidad del solicitante para privacidad y seguridad. Como alternativa, en otra forma de realización, la encriptación puede tener lugar antes de la división de los datos establecidos mediante el módulo de división o el analizador de datos seguro. Los datos originales procesados tal como se describe en esta forma de realización se encriptan y se ofuscan y se aseguran. La dispersión de los elementos encriptados, si se desea, puede ser virtualmente en cualquier lugar, incluyendo, pero sin limitación, un único servidor o dispositivo de almacenamiento de datos, o entre instalaciones de almacenamiento de datos o dispositivos separados. La gestión de la clave de encriptación en una forma de realización se puede incluir en el conjunto de soporte lógico, o en otra forma de realización puede integrase en una infraestructura existente o cualquier otra localización deseada.

Una división criptográfica (criptodivisión) divide en particiones los datos en N número de comparticiones. La división en particiones puede ser en cualquier tamaño de unidad de datos, incluyendo un bit individual, bits, bytes, kilobytes, megabytes, o unidades mayores, así como cualquier patrón o combinación de tamaños de unidades de datos ya estén predeterminados o generados de forma aleatoria. Las unidades pueden estar también con diferente tamaño,

basándose en cualquiera de un conjunto de valores aleatorios o predeterminados. Esto significa que los datos se pueden observar como una secuencia de estas unidades. De esta manera el tamaño de las propias unidades de datos puede presentar los datos más seguros, por ejemplo usando uno o más patrones, secuencias o combinaciones de tamaños de unidad de datos predeterminados o generados de forma aleatoria. Las unidades a continuación se distribuyen (de forma aleatoria o mediante un conjunto de valores predeterminado) en las N compartimentaciones. Esta distribución podría implicar también un mezclado del orden de las unidades en las compartimentaciones. Es inmediatamente evidente para los expertos en la materia que la distribución de las unidades de datos en las compartimentaciones se puede realizar de acuerdo con una amplia diversidad de posibles selecciones, incluyendo pero sin limitación tamaños predeterminados de tamaño fijo, o una o más combinaciones, patrón o secuencia de tamaños de unidades de datos que están predeterminados o generados de forma aleatoria.

Un ejemplo de este proceso de división criptográfico, o criptodivisión, sería considerar que los datos son de 23 bytes en tamaño, con el tamaño de la unidad de datos elegido para que sea un byte, y con el número de compartimentaciones seleccionado para que sea 4. Cada byte se distribuiría en una de las 4 compartimentaciones. Suponiendo una distribución aleatoria, se obtendría una clave para crear una secuencia de 23 números aleatorios (r1, r2, r3 a r23), cada una con un valor entre 1 y 4 que se corresponde con las cuatro compartimentaciones. Cada una de las unidades de datos (en este ejemplo 23 bytes individuales de datos) está asociada con uno de los 23 números aleatorios que se corresponden con una de las cuatro compartimentaciones. La distribución de los bytes de datos en las cuatro compartimentaciones tendría lugar colocando el primer byte de los datos en el número de compartición r1, el byte dos en la compartición r2, el byte tres en la compartición r3, hasta el 23º byte de datos en la compartición r23. Es inmediatamente evidente para los expertos en la materia que se puede usar una amplia diversidad de otras posibles etapas o combinación de secuencias de etapas, incluyendo el tamaño de las unidades de datos, en el proceso de criptodivisión de la presente invención, y el ejemplo anterior es una descripción no limitante de uno de los procesos para criptodividir datos. Para recrear los datos originales, se podría realizar la operación inversa.

En otra forma de realización del proceso de criptodivisión de la presente invención, una opción para el proceso de criptodivisión es proporcionar suficiente redundancia en las compartimentaciones de tal modo que únicamente sea necesario un subconjunto de las compartimentaciones para reensamblar o restaurar los datos a su forma original o utilizable. Como un ejemplo no limitante, la criptodivisión se puede hacer como una criptodivisión “3 de 4” de tal modo que únicamente tres de las cuatro compartimentaciones sean necesarias para reensamblar o restaurar los datos a su forma original o utilizable. Esto se denomina también como una “criptodivisión M de N” en el que N es el número total de compartimentaciones, y M es al menos uno menor que N. Es inmediatamente evidente para los expertos en la materia que puede haber muchas posibilidades para crear esta redundancia en el proceso de criptodivisión de la presente invención.

En una forma de realización del proceso de la criptodivisión de la presente invención, cada unidad de los datos se almacena en dos compartimentaciones, la primera compartición y la compartición de reserva. Usando el proceso de criptodivisión de “3 de 4” que se ha descrito en lo que antecede, una compartición cualquiera se puede perder, y esto es suficiente para reensamblar o restaurar los datos originales sin unidades de datos perdidos debido a que únicamente se requieren tres de las cuatro compartimentaciones totales. Tal como se describe en el presente documento, se genera un número aleatorio que se corresponde con una de las compartimentaciones. El número aleatorio está asociado con una unidad de datos, y se almacena en la compartición correspondiente, basándose en una clave. Se usa una clave, en esta forma de realización, para generar el número aleatorio de compartición principal y de reserva. Tal como se describe en el presente documento para el proceso de criptodivisión de la presente invención, se genera un conjunto de números aleatorios (también denominados como números de compartición primarios) de 0 a 3 iguales al número de unidades de datos. A continuación se genera otro conjunto de números aleatorios (también denominado como números de compartición de reserva) de 1 a 3 igual al número de unidades de datos. Cada unidad de datos se asocia a continuación con un número de compartición principal y un número de compartición de reserva. Como alternativa, se puede generar un conjunto de números aleatorios que es menor que el número de unidades de datos, y repetir el conjunto de números aleatorio, pero esto puede reducir la seguridad de los datos sensibles. El número de compartición principal se usa para determinar en qué compartición se almacena la unidad de datos. El número de compartición de reserva se combina con el número de compartición principal para crear un tercer número de compartición entre 0 y 3, y este número se usa para determinar en qué compartición se almacena la unidad de datos. En este ejemplo, la ecuación para determinar el tercer número es:

(número de compartición primario + número de compartición de reserva) MOD 4 = tercer número de compartición.

En la forma de realización que se ha descrito en lo que antecede en donde el número de compartición principal es entre 0 y 3, y el número de compartición de reserva es entre 1 y 3 asegura que el tercer número de compartición es diferente del número de compartición principal. Esto da como resultado que la unidad de datos se almacene en dos compartimentaciones diferentes. Es inmediatamente evidente para los expertos en la materia que puede haber muchas maneras de realizar criptodivisión redundante y criptodivisión no redundante además de las formas de realización que se divulgan en el presente documento. Por ejemplo, las unidades de datos en cada compartición se podrían mezclar utilizando un algoritmo diferente. Este mezclado de unidad de datos se puede realizar a medida que los datos originales se dividen en las unidades de datos, o después de que las unidades de datos se colocan en las particiones, o después de que la compartición está completa, por ejemplo.

Los diversos procesos de criptodivisión y procesos de mezclado de datos que se describen en el presente documento, y todas las otras formas de realización de la criptodivisión y métodos de mezclado de datos de la presente invención se pueden realizar en unidades de datos de cualquier tamaño, incluyendo pero sin limitación, tan pequeñas como un bit individual, bits, bytes, kilobytes, megabytes o mayores.

Un ejemplo de una forma de realización de código fuente que podría realizar el proceso de criptodivisión que se describe en el presente documento es:

```
DATA [1:24] - serie de bytes con los datos que se van a dividir
SHARES [0:3; 1:24] - serie bidimensional representando cada fila una de las comparticiones
RANDOM [1:24] - serie de números aleatorios en el intervalo de 0..3
S1 = 1;
S2 = 1;
S3 = 1;
S4 = 1;
For J = 1 to 24 do
    Begin
    IF RANDOM [J [== 0 then
        Begin
        SHARES [1,S1] = DATA [J];
        S1 = S1 + 1;
        End
    ELSE IF RANDOM [J [==1 then
        Begin SHARES [2,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 forma de realización de código fuente que realizaría el proceso de RAID de criptodivisión que se describe en el presente documento es:

Generar dos conjuntos de números, Compartición_Principal es de 0 a 3, Compartición_de_Reserva es de 1 a 3. A continuación poner cada unidad de datos en compartición[compartición_principal[1]] y compartición[(compartición_principal[1] + compartición_de_reserva[1]) mod 4, con el mismo proceso como en la criptodivisión que se ha descrito en lo que antecede. Este método será escalable a cualquier tamaño de N, en donde únicamente son necesarias N - 1 comparticiones para restaurar los datos.

La recuperación, la recombinación, el reensamblaje o la reconstitución de los elementos de datos encriptados puede utilizar cualquier número de técnicas de autenticación, incluyendo, pero sin limitación, biométrica, tal como reconocimiento de huellas digitales, exploración facial, exploración de manos, exploración de iris, exploración de retina, exploración ocular, reconocimiento de patrón vascular o análisis de ADN. La división de datos y / o módulos analizadores de la presente invención se pueden integrar en una amplia diversidad de productos de infraestructura o aplicaciones según se desee.

Las tecnologías de encriptación tradicionales en la técnica se basan en una o más claves que se usan para encriptar los datos y presentarlos no utilizables sin la clave. Los datos, no obstante, permanecen enteros e intactos y son objeto de ataque. El analizador de datos seguro de la presente invención, en una forma de realización, trata este problema realizando un análisis criptográfico y dividiendo el fichero encriptado en dos o más porciones o comparticiones, y en otra forma de realización, preferiblemente cuatro o más comparticiones, añadiendo otra capa de encriptación a cada compartición de los datos, almacenando a continuación las comparticiones en diferentes localizaciones físicas y / o lógicas. Cuando una o más comparticiones de datos se eliminan físicamente del sistema, usando un dispositivo extraíble, tal como un dispositivo de almacenamiento de datos, o colocando la partición bajo control de otra parte, cualquier posibilidad de compromiso de los datos asegurados se elimina de manera eficaz.

Un ejemplo de una forma de realización del analizador de datos seguro de la presente invención y un ejemplo de cómo se puede utilizar se muestra en la figura 21 y se describe a continuación. No obstante, es inmediatamente evidente para los expertos en la materia que el analizador de datos seguro de la presente invención se puede utilizar en una amplia diversidad de maneras además del ejemplo no limitante a continuación. Como una opción de

implantación, y en una forma de realización, el analizador de datos seguro se puede implementar con gestión de clave de sesión externa o almacenamiento interno seguro de claves de sesión. Tras la implementación, se generará una Clave Maestra de Analizador que se usará para asegurar la aplicación y para fines de encriptación. Se debería observar también que la incorporación de la Clave Maestra del Analizador en los datos asegurados resultantes permite una flexibilidad de compartición de datos asegurados para los individuos en un grupo de trabajo, empresa o público ampliado.

Tal como se muestra en la figura 21, esta forma de realización de la presente invención muestra las etapas de los procesos realizados mediante el analizador de datos seguro en datos para almacenar la clave maestra de sesión con los datos analizados:

1. Generar una clave maestra de sesión y encriptar los datos usando cifrado de flujo RS1.
2. Separar los datos encriptados resultantes en cuatro comparticiones o porciones de datos analizados de acuerdo con el patrón de la clave maestra de sesión.
3. En esta forma de realización del método, la clave maestra de sesión se almacenará junto con las comparticiones de datos aseguradas en un depósito de datos. Separar la clave maestra de sesión de acuerdo con el patrón de la Clave Maestra del Analizador y anexar los datos de la clave a los datos analizados encriptados.
4. Las resultantes cuatro comparticiones de datos contendrán porciones encriptadas de los datos originales y porciones de la clave maestra de sesión. Generar una clave de cifrado de flujo para cada una de las cuatro comparticiones de datos.
5. Encriptar cada compartición, a continuación almacenar las claves de encriptación en diferentes localizaciones de las porciones o comparticiones de datos encriptados: Compartición 1 obtiene la Clave 4, Compartición 2 obtiene la Clave 1, Compartición 3 obtiene la Clave 2, Compartición 4 obtiene la Clave 3.

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

Es inmediatamente evidente para los expertos en la materia que ciertas etapas de los métodos que se describen en el presente documento se pueden realizar en diferente orden, o repetirse múltiples veces, según sea necesario. Es también inmediatamente evidente para los expertos en la materia que las porciones de los datos se pueden manejar de manera diferente de unas a otras. Por ejemplo, se pueden realizar múltiples etapas de análisis en únicamente una porción de los datos analizados. Cada porción de datos analizados se puede asegurar de manera única en cualquier manera deseable con la condición únicamente de que los datos se puedan reensamblar, reconstituirse, reformarse, desencriptarse o restaurarse a su forma original o a otra forma utilizable.

Tal como se muestra en la figura 22 y se describe en el presente documento, otra forma de realización de la presente invención comprende las etapas del proceso realizado mediante el analizador de datos seguro en datos para almacenar los datos de clave maestra de sesión en una o más tablas de gestión de claves separadas:

1. Generar una clave maestra de sesión y encriptar los datos usando cifrado de flujo RS1.
2. Separar los datos encriptados resultantes en cuatro comparticiones o porciones de datos analizados de acuerdo con el patrón de la clave maestra de sesión.
3. En esta forma de realización del método de la presente invención, la clave maestra de sesión se almacenará en una tabla de gestión de claves separada en un depósito de datos. Generar una ID de transacción única para esta transacción. Almacenar la ID de transacción y clave maestra de sesión en una tabla de gestión de clave separada. Separar la ID de transacción de acuerdo con el patrón de la Clave Maestra del Analizador y anexar los datos a los datos analizados o separados encriptados.
4. Las resultantes cuatro comparticiones de datos contendrán porciones encriptadas de los datos originales y porciones de la ID de transacción.
5. Generar una clave de cifrado de flujo para cada una de las cuatro comparticiones de datos.
6. Encriptar cada compartición, a continuación almacenar las claves de encriptación en diferentes localizaciones de las porciones o comparticiones de datos encriptados: Compartición 1 obtiene la Clave 4, Compartición 2 obtiene la Clave 1, Compartición 3 obtiene la Clave 2, Compartición 4 obtiene la Clave 3.

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

Es inmediatamente evidente para los expertos en la materia que ciertas etapas del método que se describe en el presente documento se pueden realizar en diferente orden, o repetirse múltiples veces, según sea necesario. Es también inmediatamente evidente para los expertos en la materia que las porciones de los datos se pueden manejar de manera diferente de unas a otras. Por ejemplo, se pueden realizar múltiples etapas de separación o análisis en únicamente una porción de los datos analizados. Cada porción de datos analizados se puede asegurar de manera única en cualquier manera deseable con la condición únicamente de que los datos se puedan reensamblar, reconstituirse, reformarse, desencriptarse o restaurarse a su forma original o a otra forma utilizable.

Tal como se muestra en la figura 23, esta forma de realización de la presente invención muestra las etapas de los procesos realizados mediante el analizador de datos seguro en datos para almacenar la clave maestra de sesión con los datos analizados:

1. Acceder a la clave maestra del analizador que está asociada con el usuario autenticado
2. Generar una clave maestra de sesión única
3. Obtener una Clave Intermediaria a partir de una función O exclusiva de la Clave Maestra del Analizador y la clave maestra de sesión
4. Encriptación opcional de los datos usando un algoritmo de encriptación existente o nuevo con clave con la Clave Intermediaria.
5. Separar los datos resultantes opcionalmente encriptados en cuatro comparticiones o porciones de datos analizados de acuerdo con el patrón de la clave Intermediaria.
6. En esta forma de realización del método, la clave maestra de sesión se almacenará junto con las comparticiones de datos aseguradas en un depósito de datos. Separar la clave maestra de sesión de acuerdo con el patrón de la Clave Maestra del Analizador y anexar los datos de la clave en las comparticiones de datos analizadas opcionalmente encriptadas.
7. Las resultantes múltiples comparticiones de datos contendrán opcionalmente porciones de los datos originales encriptados y porciones de la clave maestra de sesión.
8. Generar opcionalmente una clave de encriptación para cada una de las cuatro comparticiones de datos.
9. Encriptar opcionalmente cada compartición con un algoritmo de encriptación existente o nuevo, a continuación almacenar las claves de encriptación en diferentes localizaciones de las porciones o comparticiones de datos encriptados: por ejemplo, Compartición 1 obtiene la Clave 4, Compartición 2 obtiene la Clave 1, Compartición 3 obtiene la Clave 2, Compartición 4 obtiene la Clave 3.

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

Es inmediatamente evidente para los expertos en la materia que ciertas etapas de los métodos que se describen en el presente documento se pueden realizar en diferente orden, o repetirse múltiples veces, según sea necesario. Es también inmediatamente evidente para los expertos en la materia que las porciones de los datos se pueden manejar de manera diferente de unas a otras. Por ejemplo, se pueden realizar múltiples etapas de análisis en únicamente una porción de los datos analizados. Cada porción de datos analizados se puede asegurar de manera única en cualquier manera deseable con la condición únicamente de que los datos se puedan reensamblar, reconstituirse, reformarse, desencriptarse o restaurarse a su forma original o a otra forma utilizable.

Tal como se muestra en la figura 24 y se describe en el presente documento, otra forma de realización de la presente invención comprende las etapas del proceso realizado mediante el analizador de datos seguro en datos para almacenar los datos de clave maestra de sesión en una o más tablas de gestión de claves separadas:

1. Acceder a la Clave Maestra del Analizador que está asociada con el usuario autenticado
2. Generar una Clave maestra de sesión única
3. Obtener una Clave Intermediaria a partir de una función O exclusiva de la Clave Maestra del Analizador y Clave maestra de sesión
4. Encriptar opcionalmente los datos usando un algoritmo de encriptación existente o nuevo con clave con la Clave Intermediaria.
5. Separar los datos resultantes opcionalmente encriptados en cuatro comparticiones o porciones de datos analizados de acuerdo con el patrón de la Clave Intermediaria.
6. En esta forma de realización del método de la presente invención, la clave maestra de sesión se almacenará en una tabla de gestión de claves separada en un depósito de datos. Generar una ID de transacción única para esta transacción. Almacenar la ID de transacción y clave maestra de sesión en una tabla de gestión de clave separada o pasar la clave maestra de sesión y la ID de transacción de vuelta al programa solicitante para la gestión externa. Separar la ID de transacción de acuerdo con el patrón de la Clave Maestra del Analizador y anexar los datos a los datos opcionalmente analizados encriptados o separados.
7. Las resultantes cuatro comparticiones de datos contendrán opcionalmente porciones de los datos originales encriptados y porciones de la ID de transacción.
8. Generar opcionalmente una clave de encriptación para cada una de las cuatro comparticiones de datos.
9. Encriptar opcionalmente cada compartición, a continuación almacenar las claves de encriptación en diferentes localizaciones de las porciones o comparticiones de datos encriptados. Por ejemplo: Compartición 1 obtiene la Clave 4, Compartición 2 obtiene la Clave 1, Compartición 3 obtiene la Clave 2, Compartición 4 obtiene la Clave 3.

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

Es inmediatamente evidente para los expertos en la materia que ciertas etapas del método que se describe en el presente documento se pueden realizar en diferente orden, o repetirse múltiples veces, según sea necesario. Es también inmediatamente evidente para los expertos en la materia que las porciones de los datos se pueden manejar de manera diferente de unas a otras. Por ejemplo, se pueden realizar múltiples etapas de separación o análisis en únicamente una porción de los datos analizados. Cada porción de datos analizados se puede asegurar de manera

única en cualquier manera deseable con la condición únicamente de que los datos se puedan reensamblar, reconstituirse, reformarse, desencriptarse o restaurarse a su forma original o a otra forma utilizable.

Es adecuada una amplia diversidad de metodologías para su uso en los métodos de la presente invención, como es inmediatamente evidente para los expertos en la materia. El algoritmo de Relleno de un Solo Uso, se considera en ocasiones uno de los métodos de encriptación más seguros, y es adecuado para su uso en el método de la presente invención. El uso del algoritmo de Relleno de un Solo Uso requiere que se genere una clave que es tan larga como los datos que se van a asegurar. El uso de este método puede ser menos deseable en ciertas circunstancias tales como las que dan como resultado la generación y gestión de claves muy largas debido al tamaño del conjunto de datos que se van a asegurar. En el algoritmo de Relleno de un Solo Uso (OTP, *One-Time Pad*), se usa la función o exclusiva sencilla, XOR. Para dos flujos binarios x e y de la misma longitud, x XOR y significa el o exclusivo a nivel de bits de x e y.

En el nivel de bits se genera:

0 XOR 0 = 0

0 XOR 1 = 1

1 XOR 0 = 1

1 XOR 1 = 0

Un ejemplo de este proceso se describe en el presente documento para un secreto de n bytes, *s*, (o conjunto de datos) a dividir. El proceso generará un valor aleatorio de n bytes, *a, y a continuación* establecerá:

b = a XOR s.

Obsérvese que se puede obtener “s” mediante la ecuación:

s = a XOR b.

Los valores a y b se denominan como comparticiones o porciones y se colocan en depósitos separados. Una vez que el secreto s se divide en dos o más comparticiones, se descarta de una manera segura.

El analizador de datos seguro de la presente invención puede utilizar esta función, realizar múltiples funciones XOR que incorporan múltiples valores de clave secreta distintas: K1, K2, K3, Kn, K5. En el comienzo de la operación, los datos que se van a asegurar se pasan a través de la primera operación de encriptación, datos seguros = datos XOR clave secreta 5:

S = D XOR K5

Con el fin de almacenar de manera segura los datos encriptados resultantes en, por ejemplo, cuatro comparticiones, S1, S2, S3, Sn, los datos se analizan y se dividen en “n” segmentos, o comparticiones, de acuerdo con el valor de K5. Esta operación da como resultado “n” comparticiones pseudoaleatorias de los datos encriptados originales. Las funciones XOR posteriores se pueden realizar en cada compartición con los valores de clave secreta restantes, por ejemplo: segmento de datos seguros 1 = compartición de datos encriptados 1 XOR clave secreta 1:

SD 1 = S1 XOR K1

SD2 = S2 XOR K2

SD3 = S3 XOR K3

SDn = Sn XOR Kn.

En una forma de realización, puede que no se desee tener un depósito cualquiera que contenga suficiente información para desencriptar la información mantenida en el mismo, por lo que la clave requerida para desencriptar la compartición se almacena en un depósito de datos diferente:

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

Además, anexada a cada compartición puede estar la información requerida para recuperar la clave de encriptación de sesión original, K5. Por lo tanto, en el ejemplo de gestión de clave que se describe en el presente documento, la clave maestra de sesión original se hace referencia mediante una ID de transacción dividida en "n" comparticiones de acuerdo con los contenidos de la Clave Maestra del Analizador dependiente de la instalación (TID1, TID2, TID3, TIDn):

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

En el ejemplo de clave de sesión incorporada que se describe en el presente documento, la clave maestra de sesión se divide en "n" comparticiones de acuerdo con los contenidos de la Clave Maestra del Analizador 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 recupere la totalidad de las cuatro comparticiones, los datos no se pueden reensamblar de acuerdo con este ejemplo. Incluso si se captara la totalidad de las cuatro comparticiones, no hay posibilidad de reensamblar o restaurar la información original sin acceso a la clave maestra de sesión y la Clave Maestra del Analizador.

Este ejemplo ha descrito una forma de realización del método de la presente invención, y describe asimismo, en otra forma de realización, el algoritmo que se usa para colocar particiones en depósitos de tal modo que las comparticiones desde todos los depósitos se pueden combinar para formar el material de autenticación secreto. Los cálculos necesarios son muy sencillos y rápidos. No obstante, con el algoritmo de Relleno de un Solo Uso (OTP, *One-Time Pad*) puede haber circunstancias que producen que sea menos deseable, tales como un gran conjunto de datos que se van a asegurar, debido a que el tamaño de clave es el mismo tamaño que los datos que se van a almacenar. Por lo tanto, habría una necesidad de almacenar y transmitir alrededor de dos veces la cantidad de los datos originales que puede ser menos deseable bajo ciertas circunstancias.

Cifrado de flujo RS1

La técnica de división de cifrado de flujo RS1 es muy similar a la técnica de división de OTP que se describe en el presente documento. En lugar de un valor aleatorio de n bytes, se genera un valor aleatorio n' = mín (n, 16) bytes y se usa para la clave del algoritmo de Cifrado de Flujo RS1. La ventaja del algoritmo de Cifrado de Flujo RS1 es que se genera una clave pseudoaleatoria desde un número de semilla mucho más pequeño. La velocidad de la ejecución de la encriptación de Cifrado de Flujo RS1 se considera también a aproximadamente 10 veces la velocidad de la encriptación Triple DES bien conocida en la técnica sin comprometer la seguridad. El algoritmo de Cifrado de Flujo RS1 es bien 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 su uso en los métodos de la presente invención.

Usando la notación de clave anterior, K1 a K5 son ahora unos valores aleatorios de n bytes y se establece:

$$SD1 = S1 \text{ XOR } E(K1)$$

$$SD2 = S2 \text{ XOR } E(K2)$$

$$SD3 = S3 \text{ XOR } E(K3)$$

$$SDn = Sn \text{ XOR } E(Kn)$$

en donde E(K1) a E(Kn) son los primeros n' bytes se salida del algoritmo de Cifrado de Flujo RS1 con clave por K1 a Kn. Las comparticiones se colocan ahora en depósitos de datos tal como se describe en el presente documento.

En este algoritmo RS1 de cifrado de flujo, los cálculos necesarios requeridos son casi tan sencillos y rápidos como el algoritmo OTP. El beneficio en este ejemplo usando el Cifrado de Flujo RS1 es que el sistema necesita almacenar y transmitir de media únicamente alrededor de 16 bytes más que el tamaño de los datos originales que se van a asegurar por compartición. Cuando el tamaño de los datos originales es más de 16 bytes, este algoritmo RS1 es más eficaz que el algoritmo OTP debido a que es sencillamente más corto. Es inmediatamente evidente para los expertos en la materia que son adecuados una amplia diversidad de métodos o algoritmos de encriptación para su uso en la presente invención, incluyendo, pero sin limitación RS1, OTP, RC4™, Triple DES y AES.

Se proporcionan ventajas principales mediante los métodos de seguridad de datos y sistemas informáticos de la presente invención sobre los métodos de encriptación tradicionales. Una ventaja es la seguridad obtenida de las compartimentaciones en movimiento de los datos a diferentes localizaciones en uno o más depósitos de datos o dispositivos de almacenamiento, que pueden estar en diferentes localizaciones lógicas, físicas o geográficas. Cuando las compartimentaciones de datos se dividen físicamente y bajo el control de diferente personal, por ejemplo, la posibilidad de comprometer los datos se reduce enormemente.

Otra ventaja proporcionada mediante los métodos y sistema de la presente invención es la combinación de las etapas del método de la presente invención para asegurar datos para proporcionar un proceso completo para mantener la seguridad de los datos sensibles. Los datos se encriptan con una clave segura y se dividen en una o más compartimentaciones, y en una forma de realización, cuatro compartimentaciones, de acuerdo con la clave segura. La clave segura se almacena de manera segura con un puntero de referencia que se asegura en cuatro compartimentaciones de acuerdo con una clave segura. Las compartimentaciones de datos se encriptan a continuación de forma individual y las claves se almacenan de manera segura con diferentes compartimentaciones encriptadas. Cuando se combina, el proceso completo para asegurar datos de acuerdo con los métodos que se divulgan en el presente documento se hace un paquete completo para la seguridad de datos.

Los datos asegurados de acuerdo con los métodos de la presente invención son fácilmente recuperables y se restauran, se reconstituyen, se reensamblan, se desencriptan o se devuelven de otra manera a su forma original o a otra forma adecuada para su uso. Para restaurar los datos originales, se pueden utilizar los siguientes elementos:

1. Todas las compartimentaciones o porciones del conjunto de datos.
2. Conocimiento de y capacidad para reproducir el flujo de proceso del método que se usa para asegurar los datos.
3. Acceso a la clave maestra de sesión.
4. Acceso a la Clave Maestra del Analizador.

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

La protección frente a una aplicación deshonesta que invoca la aplicación de métodos de aseguración de datos se puede aplicar mediante el uso de la Clave Maestra del Analizador. Se puede requerir una toma de contacto de autenticación mutua entre el analizador de datos seguro y la aplicación en esta forma de realización de la presente invención antes de cualquier acción emprendida.

La seguridad del sistema dicta que no hay método de “puerta trasera” para la recreación de los datos originales. Para instalaciones en donde pueden surgir problemas de recuperación de datos, el analizador de datos seguro se puede potenciar para proporcionar un reflejo de las cuatro compartimentaciones y el depósito de la clave maestra de sesión. Las opciones de soporte físico tales como RAID (*redundant array of inexpensive disks*, sistemas redundantes de discos de bajo coste, que se usan para dispersar la información a través de varios discos) y opciones de soporte lógico tales como replicación pueden ayudar así como en la planificación de recuperación de datos.

Gestión de clave

En una forma de realización de la presente invención, el método de aseguración de datos usa tres conjuntos de claves para una operación de encriptación. Cada conjunto de claves puede tener almacenamiento, recuperación, seguridad y opciones de recuperación de clave individuales basándose en la instalación. Las claves que se pueden usar, incluyen, pero sin limitación:

La clave maestra del analizador

Esta clave es una clave individual que está asociada con la instalación del analizador de datos seguro. Si se instala en el servidor en el que se ha implantado el analizador de datos seguro. Hay una diversidad de opciones adecuadas para asegurar esta clave incluyendo, pero sin limitación, una tarjeta inteligente, almacenamiento de clave de soporte físico separado, almacenamiento de claves convencionales, almacenamientos de claves personalizados o en una tabla de base de datos asegurada, por ejemplo.

La clave maestra de sesión

Una clave maestra de sesión se puede generar cada vez que se aseguran datos. La clave maestra de sesión se usa para encriptar los datos antes de las operaciones de análisis y división. Se puede incorporar también (si la clave maestra de sesión no está integrada en los datos analizados) como un medio para analizar los datos encriptados. La clave maestra de sesión se puede asegurar de una diversidad de maneras, incluyendo, pero sin limitación, un

almacenamiento de clave convencional, almacenamiento de clave personalizado, tabla de base de datos separada, o asegurarse en las comparticiones encriptadas, por ejemplo.

Las claves de encriptación de compartición

Para cada compartición o porciones de un conjunto de datos que se crea, se puede generar una Clave de Encriptación de Compartición individual para encriptar adicionalmente las comparticiones. Las claves de encriptación de compartición se pueden almacenar en diferentes comparticiones a la compartición que se encriptó.

Es inmediatamente evidente para los expertos en la materia que los métodos de aseguración de datos y sistema informático de la presente invención son ampliamente aplicables a cualquier tipo de datos en cualquier ajuste o entorno. Además de las aplicaciones comerciales realizadas a través de Internet o entre clientes y distribuidores, los métodos de aseguración de datos y sistemas informáticos de la presente invención son altamente aplicables a entornos o ajustes no comerciales o privados. Cualquier conjunto de datos que se desee mantener seguro de cualquier usuario no autorizado se puede asegurar usando los métodos y sistemas que se describen en el presente documento. Por ejemplo, acceder a una base de datos particular en una compañía u organización se puede restringir de forma ventajosa a únicamente usuarios seleccionados empleando los métodos y sistemas de la presente invención para asegurar datos. Otro ejemplo es la generación, modificación o acceso a documentos en los que se desea restringir acceso o evitar acceso no autorizado o accidental o divulgación fuera de un grupo de individuos, ordenadores o estaciones de trabajo seleccionados. Estos y otros ejemplos de las maneras en las que los métodos y sistemas de aseguración de datos de la presente invención son aplicables a cualquier entorno o ajuste no comercial o comercial para cualquier ajuste, incluyendo, pero sin limitación, cualquier organización, agencia gubernamental o corporación.

En otra forma de realización de la presente invención, el método de aseguración de datos usa tres conjuntos de claves para una operación de encriptación. Cada conjunto de claves puede tener almacenamiento, recuperación, seguridad y opciones de recuperación de clave individuales basándose en la instalación. Las claves que se pueden usar, incluyen, pero sin limitación:

1. La clave maestra del analizador

Esta clave es una clave individual que está asociada con la instalación del analizador de datos seguro. Si se instala en el servidor en el que se ha implantado el analizador de datos seguro. Hay una diversidad de opciones adecuadas para asegurar esta clave incluyendo, pero sin limitación, una tarjeta inteligente, almacenamiento de clave de soporte físico separado, almacenamiento de claves convencionales, almacenamientos de claves personalizados o en una tabla de base de datos asegurada, por ejemplo.

2. La clave maestra de sesión

Una clave maestra de sesión se puede generar cada vez que se aseguran datos. La clave maestra de sesión se usa en conjunto con la clave maestra del analizador para obtener la Clave Intermediaria. La clave maestra de sesión se puede asegurar de una diversidad de maneras, incluyendo, pero sin limitación, un almacenamiento de clave convencional, almacenamiento de clave personalizado, tabla de base de datos separada, o asegurarse en las comparticiones encriptadas, por ejemplo.

3. La clave intermediaria

Se puede generar una clave intermediaria cada vez que se aseguran datos. La clave intermediaria se usa para encriptar los datos antes de la operación de análisis y división. Se puede incorporar también como un medio para analizar los datos encriptados.

4. Las claves de encriptación de compartición

Para cada compartición o porciones de un conjunto de datos que se crea, se puede generar una Clave de Encriptación de Compartición individual para encriptar adicionalmente las comparticiones. Las claves de encriptación de compartición se pueden almacenar en diferentes comparticiones a la compartición que se encriptó.

Es inmediatamente evidente para los expertos en la materia que los métodos de aseguración de datos y sistema informático de la presente invención son ampliamente aplicables a cualquier tipo de datos en cualquier ajuste o entorno. Además de las aplicaciones comerciales realizadas a través de Internet o entre clientes y distribuidores, los métodos de aseguración de datos y sistemas informáticos de la presente invención son altamente aplicables a entornos o ajustes no comerciales o privados. Cualquier conjunto de datos que se desee mantener seguro de cualquier usuario no autorizado se puede asegurar usando los métodos y sistema tal como se describe en el presente documento. Por ejemplo, el acceso a una base de datos particular en una compañía u organización se puede restringir de forma ventajosa a únicamente usuarios seleccionados empleando los métodos y sistemas de la presente invención para asegurar datos. Otro ejemplo es la generación, modificación o acceso a documentos en los

que se desea restringir acceso o evitar acceso no autorizado o accidental o divulgación fuera de un grupo de individuos, ordenadores o estaciones de trabajo seleccionados. Estos y otros ejemplos de las maneras en las que los métodos y sistemas de aseguración de datos de la presente invención son aplicables a cualquier entorno o ajuste no comercial o comercial para cualquier ajuste, incluyendo, pero sin limitación a cualquier organización, agencia gubernamental o corporación.

Seguridad de datos de grupo de trabajo, de proyecto, de PC / portátil individual o de plataforma cruzada

Los métodos de aseguración de datos y sistemas informáticos de la presente invención son también útiles al asegurar datos por grupo de trabajo, proyecto, PC / portátil individual y cualquier otra plataforma que esté en uso en, por ejemplo, negocios, oficinas, agencias gubernamentales, o cualquier ajuste en el que se creen, manejen o almacenen datos sensibles. La presente invención proporciona métodos y sistemas informáticos para asegurar datos que se sabe que se deberían conocer después por organizaciones, tales como el Gobierno de los Estados Unidos, para implementación a través de toda la organización gubernamental o entre gobiernos a un nivel estatal o federal.

Los métodos de aseguración de datos y sistemas informáticos de la presente invención proporcionan la capacidad de no únicamente analizar y dividir ficheros planos sino también campos de datos, conjuntos y / o tablas de cualquier tipo. Además, todas las formas de datos que se pueden asegurar bajo este proceso, incluyendo, pero sin limitación, texto, vídeo, imágenes, biométrica y datos de voz. La escalabilidad, velocidad y rendimiento de datos de los métodos para asegurar datos de la presente invención están únicamente limitados al soporte físico que el usuario tiene a su disposición.

En una forma de realización de la presente invención, los métodos de aseguración de datos se utilizan tal como se describe a continuación en un entorno de grupo de trabajo. En una forma de realización, tal como se muestra en la figura 23 y se describe a continuación, el método de aseguración de datos a Escala de Grupo de Trabajo de la presente invención usa la funcionalidad de gestión de clave privada del TrustEngine para almacenar las relaciones del usuario / grupo y las claves privadas asociadas (Claves Maestras de Grupo de Analizador) necesarias para que un grupo de usuarios comparta datos seguros. El método de la presente invención tiene la capacidad de asegurar datos para una empresa, grupo de trabajo, o usuario individual, dependiendo de cómo se implantó la Clave Maestra del Analizador.

En una forma de realización, se pueden proporcionar programas de gestión de clave adicional y de gestión de usuarios / grupos, que posibilitan la implementación de grupos de trabajo a gran escala con un único punto de administración y gestión de clave. La generación de clave, gestión y revocación se manejan mediante el único programa de mantenimiento, que se hacen todos especialmente importantes a medida que el número de usuarios aumenta. En otra forma de realización, la gestión de clave se puede establecer también a través de uno o varios administradores de sistema diferentes, que pueden no permitir a una persona cualquiera o grupo controlar datos según sea necesario. Esto permite que se obtenga la gestión de datos asegurados por funciones, responsabilidades, afiliación, derechos, etc., tal como son definidos por una organización, y el acceso a datos asegurados se puede limitar a solo los que se requiere o permite tener acceso únicamente a la porción en la que están trabajando, mientras que otros, tales como gerentes o ejecutivos, pueden tener acceso a todos los datos asegurados. Esta forma de realización permite la compartición de datos asegurados entre diferentes grupos en una compañía u organización mientras que, al mismo tiempo, permite únicamente a ciertos individuos seleccionados, tales como aquellos con los papeles y responsabilidades autorizados y predeterminados, observar los datos como una totalidad. Además, esta forma de realización de los métodos y sistemas de la presente invención también permite la compartición de datos entre, por ejemplo, compañías separadas, o departamentos separados o divisiones de compañías, o cualquier departamento, grupo, agencia, u oficina o similar separado de cualquier gobierno u organización o cualquier tipo, en donde se requiera alguna compartición, pero no se pueda permitir a una parte cualquiera tener acceso a todos los datos. Ejemplos particularmente evidentes de la necesidad y utilidad para un método y sistema de este tipo de la presente invención son permitir la compartición, pero mantener seguridad, en áreas gubernamentales, agencias y oficinas y entre diferentes divisiones, departamentos u oficinas de una gran compañía, o cualquier otra organización, por ejemplo.

Un ejemplo de la aplicabilidad de los métodos de la presente invención a una escala más pequeña es tal como sigue. Se usa una clave Maestra de Analizador como una serialización o marca del analizador de datos seguro para una organización. A medida que la escala de uso de la clave maestra del analizador se reduce de la totalidad de la empresa a un grupo de trabajo más pequeño, los métodos de aseguración de datos que se describen en el presente documento se usan para compartir ficheros en grupos de usuarios.

En el ejemplo que se muestra en la figura 25 y que se describe a continuación, hay seis usuarios definidos junto con su título o papel en la organización. La barra lateral representa cinco posibles grupos a los que el usuario puede pertenecer de acuerdo con su papel. La flecha representa la afiliación por el usuario en uno o más de los grupos.

Cuando se configura el analizador de datos seguro para su uso en este ejemplo, el administrador de sistema accede a la información de usuario y grupo desde el sistema operativo mediante un programa de mantenimiento. Este

programa de mantenimiento genera y asigna Claves Maestras de Grupo de Analizador a usuarios basándose en su afiliación en grupos.

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

1. Acceder a la Clave Maestra del Grupo de Analizador para el grupo de Personal Senior (generar una clave si no está disponible);
2. Generar un certificado digital que asocia al Director General con el grupo de Personal Senior;
3. Generar un certificado digital que asocia al Director Financiero con el grupo de Personal Senior;
4. Generar un certificado digital que asocia al Vicepresidente de Marketing con el grupo de Personal Senior.

El mismo conjunto de acciones se harían para cada grupo, y cada miembro en cada grupo. Cuando el programa de mantenimiento está completo, la Clave Maestra del Grupo de Analizador se hace una credencial compartida para cada miembro del grupo. La revocación del certificado digital asignado se puede hacer de forma automática cuando un usuario se elimina de un grupo a través del programa de mantenimiento sin afectar a los miembros restantes del grupo.

Una vez que se han definido las credenciales compartidas, el proceso de análisis y división permanece igual. Cuando un fichero, documento o elemento de datos se ha de asegurar, se solicita al usuario el grupo objetivo que se va a usar cuando se aseguran los datos. Los datos asegurados resultantes son únicamente accesibles por otros miembros del grupo objetivo. Esta funcionalidad de los métodos y sistemas de la presente invención se puede usar con cualquier otro sistema informático o plataforma de soporte lógico y, por ejemplo, se puede integrar en programas de aplicación existentes o usarse de forma independiente para la seguridad de ficheros.

Es inmediatamente evidente para los expertos en la materia que una combinación cualquiera o combinación de algoritmos de encriptación son adecuadas para su uso en los métodos y sistemas de la presente invención. Por ejemplo, las etapas de encriptación se pueden repetir, en una forma de realización, para producir un esquema de encriptación de múltiples capas. Además, se puede usar un algoritmo de encriptación diferente, o combinación de algoritmos de encriptación, en etapas de encriptación repetidas de tal modo que se aplican diferentes algoritmos de encriptación a las diferentes capas del esquema de encriptación en múltiples capas. En este sentido, el propio esquema de encriptación se puede hacer un componente de los métodos de la presente invención para asegurar los datos sensibles de uso o acceso no autorizado.

El analizador de datos seguro puede incluir como un componente interno, como un componente externo, o como ambos un componente de comprobación de errores. Por ejemplo, en un enfoque adecuado, ya que las porciones de datos se crean usando el analizador de datos seguro de acuerdo con la presente invención, para asegurar la integridad de los datos en una porción, un valor de troceo se toma a intervalos preestablecidos en la porción y se anexa al final del intervalo. El valor de troceo es una representación numérica predecible y reproducible de los datos. Si cualquier bit de los datos cambia, el valor de troceo sería diferente. Un módulo de exploración (como un componente independiente externo al analizador de datos seguro o como un componente interno) puede a continuación explorar las porciones de datos generadas mediante el analizador de datos seguro. Cada porción de datos (o como alternativa, menos de todas las porciones de datos de acuerdo con algún intervalo o mediante muestreo aleatorio o pseudoaleatorio) se compara con el valor o valores anexados y se puede emprender una acción. Esta acción puede incluir un informe de valores que coinciden y no coinciden, una alerta para valores que no coinciden, o que invocan algún programa externo o interno para activar una recuperación de los datos. Por ejemplo, la recuperación de los datos se podría realizar invocando un módulo de recuperación basándose en el concepto de que pueden ser necesarias menos de todas las porciones para generar datos originales de acuerdo con la presente invención.

Cualquier otra comprobación de integridad adecuada se puede implementar usando cualquier información de integridad adecuada anexada en cualquier lugar en todas o en un subconjunto de las porciones de datos. La información de integridad puede incluir cualquier información adecuada que se pueda usar para determinar la integridad de porciones de datos. Ejemplos de información de integridad pueden incluir valores de troceo calculados basándose en cualquier parámetro adecuado (por ejemplo, basándose en respectivas porciones de datos), información de firma digital, información de código de autenticación de mensaje (MAC, *message authentication code*), cualquier otra información adecuada, o cualquier combinación de las mismas.

El analizador de datos seguro de la presente invención se puede usar en cualquier aplicación adecuada. En concreto, el analizador de datos seguro que se describe en el presente documento tiene una diversidad de aplicaciones en diferentes áreas de la informática y de la tecnología. Varias de tales áreas se analizan a continuación. Se entenderá que estas son meramente ilustrativas en su naturaleza y que cualquier otra aplicación adecuada puede hacer uso del analizador de datos seguro. Se entenderá adicionalmente que los ejemplos que se describen son meramente formas de realización ilustrativas que se pueden modificar de cualquier manera adecuada para satisfacer deseos adecuados. Por ejemplo, el análisis y división se puede basar en cualquier unidad adecuada, tal como en bits, en bytes, en kilobytes, en megabytes, mediante cualquier combinación de las mismas o mediante cualquier otra unidad adecuada.

El analizador de datos seguro de la presente invención se puede usar para implementar testigos físicos seguros, en los que los datos almacenados en un testigo físico se pueden requerir para acceder a datos adicionales almacenados en otro área de almacenamiento. En un enfoque adecuado, un testigo físico, tal como una unidad flash de USB compacta, un disco flexible, un disco óptico, una tarjeta inteligente, o cualquier otro testigo físico adecuado, se puede usar para almacenar una de al menos dos porciones de datos analizados de acuerdo con la presente invención. Para acceder los datos originales, necesitaría accederse a la unidad flash de USB. Por tanto, un ordenador personal que mantiene una porción de datos analizados necesitaría tener la unidad flash de USB, que tiene la otra porción de datos analizados, conectada antes de que se pueda acceder a los datos originales. La figura 26 ilustra esta aplicación. El área de almacenamiento 2500 incluye una porción de datos analizados 2502. El testigo físico 2504, que tiene una porción de datos analizados 2506 se necesitaría acoplar al área de almacenamiento 2500 usando cualquier interfaz de comunicaciones adecuada 2508 (por ejemplo, USB, serie, paralelo, Bluetooth, IR, IEEE 1394, Ethernet, o cualquier otra interfaz de comunicaciones adecuada) para acceder los datos originales. Esto es útil en una situación en donde, por ejemplo, los datos sensibles en un ordenador se dejan en solitario y se someten a intentos de acceso no autorizados. Retirando el testigo físico (por ejemplo, la unidad flash de USB), los datos sensibles son inaccesibles. Se entenderá que se puede usar cualquier otro enfoque para usar testigos físicos.

El analizador de datos seguro de la presente invención se puede usar para implementar un sistema de autenticación segura en el cual los datos de inscripción de usuario (por ejemplo, contraseñas, claves de encriptación privadas, muestras de huellas digitales, datos biométricos o cualquier otro dato de inscripción de usuario adecuado) se analizan y dividen usando el analizador de datos seguro. Los datos de inscripción del usuario se pueden analizar y dividirse, con lo que, una o más porciones se almacenan en una tarjeta inteligente, una Tarjeta de Acceso Común del Gobierno, cualquier dispositivo de almacenamiento físico adecuado (por ejemplo, disco magnético u óptico, unidad de llave de USB, etc.), o cualquier otro dispositivo adecuado. Una o más otras porciones de los datos de inscripción del usuario analizados se pueden almacenar en el sistema que realiza la autenticación. Esto proporciona un nivel añadido de seguridad al proceso de autenticación (por ejemplo, además de la información de autenticación biométrica obtenida desde la fuente biométrica, los datos de inscripción del usuario se deben obtener también mediante la porción de datos analizada y dividida apropiada).

El analizador de datos seguro de la presente invención se puede integrar en cualquier sistema existente adecuado para proporcionar el uso de su funcionalidad en cada entorno respectivo del sistema. La figura 27 muestra un diagrama de bloques de un sistema ilustrativo 2600, que puede incluir soporte lógico, soporte físico, o ambos para implementar cualquier aplicación adecuada. El sistema 2600 puede ser un sistema existente en el que el analizador de datos seguro 2602 se puede reacondicionar como un componente integrado. Como alternativa, el analizador de datos seguro 2602 se puede integrar en cualquier sistema 2600 adecuado desde, por ejemplo, su etapa de diseño más temprana. El analizador de datos seguro 2600 se puede integrar en cualquier nivel adecuado del sistema 2600. Por ejemplo, el analizador de datos seguro 2602 se puede integrar en el sistema 2600 a un nivel suficientemente de fondo de tal modo que la presencia del analizador de datos seguro 2602 puede ser sustancialmente transparente para un usuario final del sistema 2600. El analizador de datos seguro 2602 se puede usar para analizar y dividir datos entre uno o más dispositivos de almacenamiento 2604 de acuerdo con la presente invención. Algunos ejemplos ilustrativos de sistemas que tienen el analizador de datos seguro integrado en el mismo se analizan a continuación.

El analizador de datos seguro de la presente invención se puede integrar en un núcleo de sistema operativo (por ejemplo, Linux, Unix, o cualquier otro sistema operativo comercial o propietario adecuado). Esta integración se puede usar para proteger datos al nivel de dispositivo en el cual, por ejemplo, los datos que se almacenarían normalmente en uno o más dispositivos se separan en un cierto número de porciones mediante el analizador de datos seguro integrado en el sistema operativo y se almacenan entre el uno o más dispositivos. Cuando se intenta acceder a los datos originales, el soporte lógico apropiado, también integrado en el sistema operativo, puede recombinar las porciones de datos analizadas en los datos originales de una manera que puede ser transparente para el usuario final.

El analizador de datos seguro de la presente invención se puede integrar en un gestor de volumen o cualquier otro componente adecuado de un sistema de almacenamiento para proteger el almacenamiento de datos local y en red a través de cualquiera o todas las plataformas soportadas. Por ejemplo, con el analizador de datos seguro integrado, un sistema de almacenamiento puede hacer uso de la redundancia ofrecida por el analizador de datos seguro (es decir, que se usa para implementar la característica de necesitar menos de todas las porciones separadas de datos para reconstruir los datos originales) para protegerse frente a pérdida de datos. El analizador de datos seguro permite también que se escriban todos los datos a dispositivos de almacenamiento, se use redundancia o no, para que estén en forma de múltiples porciones que se generan de acuerdo con el análisis de la presente invención. Cuando se intenta acceder a los datos originales, el soporte lógico apropiado, también integrado en el gestor de volumen u otro componente adecuado del sistema de almacenamiento, puede recombinar las porciones de datos analizadas en los datos originales de una manera que puede ser transparente para el usuario final.

En un enfoque adecuado, el analizador de datos seguro de la presente invención se puede integrar en un controlador de RAID (como soporte físico o soporte lógico). Esto permite el almacenamiento seguro de datos a múltiples unidades al tiempo que se mantiene tolerancia a fallos en caso de fallo de unidad.

El analizador de datos seguro de la presente invención se puede integrar en una base de datos para proteger, por ejemplo, información de tabla sensible. Por ejemplo, en un enfoque adecuado, los datos que están asociados con celdas particulares de una tabla de base de datos (por ejemplo, celdas individuales, una o más columnas particulares, una o más filas particulares, cualquier combinación de las mismas, o una tabla de base de datos entera) se pueden analizar y separarse de acuerdo con la presente invención (por ejemplo, cuando se almacenan diferentes porciones en uno o más dispositivos de almacenamiento en una o más localizaciones o en un único dispositivo de almacenamiento). El acceso para recombinar las porciones para ver los datos originales se puede conceder mediante métodos de autenticación tradicionales (por ejemplo, consulta de nombre de usuario y contraseña).

El analizador seguro de la presente invención se puede integrar en cualquier sistema adecuado que implica datos en movimiento (es decir, transferencia de datos de una localización a otra). Tales sistemas incluyen, por ejemplo, correo electrónico, difusiones de datos de flujo continuo y comunicaciones inalámbricas (por ejemplo, WiFi). Con respecto a correo electrónico, en un enfoque adecuado, el analizador seguro se puede usar para analizar mensajes salientes (es decir, que contienen texto, datos binarios, o ambos (por ejemplo, ficheros adjuntos a un mensaje de correo electrónico)) y enviar las diferentes porciones de los datos analizados a lo largo de diferentes trayectorias creando de esta manera múltiples flujos de datos. Si uno cualquiera de estos flujos de datos está comprometido, el mensaje original permanece seguro debido a que el sistema puede requerir que se combine más de una de las porciones, de acuerdo con la presente invención, para generar los datos originales. En otro enfoque adecuado, las diferentes porciones de datos se pueden combinar a lo largo de una trayectoria de forma secuencial de tal modo que si se obtiene una porción, puede no ser suficiente para generar los datos originales. Las diferentes porciones llegan a la localización del receptor pretendido y se pueden combinar para generar los datos originales de acuerdo con la presente invención.

Las figuras 28 y 29 son diagramas de bloques ilustrativos de tales sistemas de correo electrónico. La figura 28 muestra un sistema de emisión 2700, que puede incluir cualquier soporte físico adecuado, tal como un terminal informático, un ordenador personal, un dispositivo portátil (por ejemplo, un PDA, una Blackberry), un teléfono celular, una red informática, cualquier otro soporte físico adecuado o cualquier combinación de los mismos. El sistema de emisión 2700 se usa para generar y / o almacenar un mensaje 2704, que puede ser, por ejemplo, un mensaje de correo electrónico, un fichero de datos binarios (por ejemplo, gráficos, voz, vídeo, etc.), o ambos. El mensaje 2704 se analiza y divide mediante el analizador de datos seguro 2702 de acuerdo con la presente invención. Las porciones resultantes de datos se pueden comunicar a través de una o más trayectorias de comunicaciones separadas 2706 a través de la red 2708 (por ejemplo, Internet, una intranet, una LAN, WiFi, Bluetooth, cualquier otro medio de comunicación de cableado permanente o inalámbrica adecuada o cualquier combinación de los mismos) al sistema de recepción 2710. Las porciones de datos se pueden comunicar paralelas en el tiempo o como alternativa, de acuerdo con cualquier retardo de tiempo adecuado entre la comunicación de las diferentes porciones de datos. El sistema de recepción 2710 puede ser cualquier soporte físico adecuado tal como se ha descrito en lo que antecede con respecto al sistema de emisión 2700. Las porciones de datos separadas llevadas a lo largo de las trayectorias de comunicación 2706 se recombinan en el sistema de recepción 2710 para generar el mensaje original o los datos de acuerdo con la presente invención.

La figura 29 muestra un sistema de emisión 2800, que puede incluir cualquier soporte físico adecuado, tal como un terminal informático, un ordenador personal, un dispositivo portátil (por ejemplo, un PDA), un teléfono celular, una red informática, cualquier otro soporte físico adecuado o cualquier combinación de los mismos. El sistema de emisión 2800 se usa para generar y / o almacenar un mensaje 2804, que puede ser, por ejemplo, un mensaje de correo electrónico, un fichero de datos binarios (por ejemplo, gráficos, voz, vídeo, etc.), o ambos. El mensaje 2804 se analiza y divide mediante el analizador de datos seguro 2802 de acuerdo con la presente invención. Las porciones resultantes de datos se pueden comunicar a través de una única trayectoria de comunicaciones 2806 a través de la red 2808 (por ejemplo, Internet, una intranet, una LAN, WiFi, Bluetooth, cualquier otro medio de comunicaciones adecuado, o cualquier combinación de los mismos) al sistema de recepción 2810. Las porciones de datos se pueden comunicar en serie a través de la trayectoria de comunicación 2806 con respecto entre sí. El sistema de recepción 2810 puede ser cualquier soporte físico adecuado tal como se ha descrito en lo que antecede con respecto al sistema de emisión 2800. Las porciones de datos separadas llevadas a lo largo de la trayectoria de comunicaciones 2806 se recombinan en el sistema de recepción 2810 para generar el mensaje original o los datos de acuerdo con la presente invención.

Se entenderá que la disposición de las figuras 28 y 29 es meramente ilustrativa. Cualquier otra disposición adecuada se puede usar. Por ejemplo, en otro enfoque adecuado, las características de los sistemas de las figuras 28 y 29 se pueden combinar con lo que se usa el enfoque de múltiple trayectoria de la figura 28 y en el que se usa una o más de las trayectorias de comunicaciones 2706 para llevar una porción de datos como hace la trayectoria de comunicaciones 2806 en el contexto de la figura 29.

El analizador de datos seguro se puede integrar en cualquier nivel adecuado de un sistema de datos en movimiento. Por ejemplo, en el contexto de un sistema de correo electrónico, el analizador seguro se puede integrar en el nivel de interfaz de usuario (por ejemplo, en Microsoft® Outlook), caso en el que el usuario puede tener control sobre el uso de las características del analizador de datos seguro cuando usa el correo electrónico. Como alternativa, el

analizador seguro se puede implementar en un componente de fondo tal como el servidor de intercambio, caso en el que los mensajes se pueden analizar, dividirse y comunicarse de forma automática a lo largo de diferentes trayectorias de acuerdo con la presente invención sin ninguna intervención del usuario.

De manera similar, en el caso de difusiones de flujo continuo de datos (por ejemplo, audio, vídeo), los datos de salida se pueden analizar y separarse en múltiples flujos conteniendo cada uno una porción de los datos analizados. Los múltiples flujos se pueden transmitir a lo largo de una o más trayectorias y recombinarse en la localización del receptor de acuerdo con la presente invención. Uno de los beneficios de este enfoque es que evita la tara relativamente grande que está asociada con la encriptación de datos tradicional seguido por la transmisión de los datos encriptados a través de un único canal de comunicaciones. El analizador seguro de la presente invención permite que se envíen datos en movimiento en múltiples flujos paralelos, aumentando la velocidad y eficacia.

Se entenderá que el analizador de datos seguro se puede integrar para la protección y la tolerancia a fallos de cualquier tipo de datos en movimiento a través de cualquier medio de transporte, incluyendo, por ejemplo, cableado, inalámbrico o físico. Por ejemplo, las aplicaciones de voz sobre el protocolo de Internet (VoIP, *voice over Internet protocol*) pueden hacer uso del analizador de datos seguro de la presente invención. El transporte de datos inalámbrico o cableado desde o a cualquier dispositivo de asistente digital personal (PDA, *personal digital assistant*) adecuado tal como Blackberries y teléfonos inteligentes se puede asegurar usando el analizador de datos seguro de la presente invención. Las comunicaciones usando protocolos 802.11 inalámbricos para redes inalámbricas entre iguales y basadas en concentrador, comunicaciones por satélite, comunicaciones inalámbricas punto a punto, comunicaciones cliente / servidor de Internet, o cualquier otra comunicación adecuada puede implicar las capacidades de los datos en movimiento del analizador de datos seguro de acuerdo con la presente invención. La comunicación de datos entre dispositivos periféricos informáticos (por ejemplo, una impresora, un escáner, un teclado, un encaminador de red, un dispositivo de autenticación biométrico (por ejemplo, un escáner de huellas digitales), o cualquier otro dispositivo periférico adecuado) entre un ordenador y un dispositivo periférico informático, entre un dispositivo periférico informático y cualquier otro dispositivo adecuado, o cualquier combinación de los mismos puede hacer uso de las características de los datos en movimiento de la presente invención.

Las características de los datos en movimiento de la presente invención se pueden aplicar también a transporte físico de comparticiones seguras usando por ejemplo, rutas separadas, vehículos, métodos, y cualquier otro transporte físico adecuado o cualquier combinación de los mismos. Por ejemplo, el transporte físico de datos puede tener lugar en cintas digitales / magnéticas, discos flexibles, discos ópticos, testigos físicos, unidades de USB, unidades de discos extraíbles, dispositivos de electrónica de consumo con memoria flash (por ejemplo, iPOD de Apple u otros reproductores de MP3), memoria flash, cualquier otro medio adecuado que se usa para transportar datos, o cualquier combinación de los mismos.

El analizador de datos seguro de la presente invención puede proporcionar seguridad con la capacidad para recuperación frente a desastres. De acuerdo con la presente invención, pueden ser necesarias menos de todas las porciones de los datos separados generados mediante el analizador de datos seguro para recuperar los datos originales. Es decir, de m porciones almacenadas, n puede ser el número mínimo de estas m porciones necesarias para recuperar los datos originales, en donde n <= m. Por ejemplo, si cada una de las cuatro porciones se almacena en una localización física diferente en relación con las otras tres porciones, entonces, si n = 2 en este ejemplo, dos de las localizaciones pueden estar comprometidas con lo que los datos están destruidos o son inaccesibles, y los datos originales aún se pueden recuperar desde las porciones en las otras dos localizaciones. Se puede usar cualquier valor adecuado para n o m.

Además, la característica n de m de la presente invención se puede usar para crear una “regla de los dos hombres” con lo que para evitar confiar a un único individuo o cualquier otra entidad con acceso completo a lo que podrían ser datos sensibles, dos o más entidades distintas, cada una con una porción de los datos separados analizados mediante el analizador seguro de la presente invención pueden necesitar ponerse de acuerdo para poner sus porciones juntas para recuperar los datos originales.

El analizador de datos seguro de la presente invención se puede usar para proporcionar a un grupo de entidades con una clave a nivel de grupo que permite a los miembros del grupo acceder a una información particular a la que está autorizado a acceder ese grupo particular. La clave de grupo puede ser una de las porciones de datos generadas mediante el analizador seguro de acuerdo con la presente invención que se puede requerir que se combine con otra porción almacenada de manera central, por ejemplo para recuperar la información solicitada. Esta característica permite, por ejemplo, asegurar la colaboración entre un grupo. Se puede aplicar en, por ejemplo, redes especializadas, redes privadas virtuales, intranets, o cualquier otra red adecuada.

Las aplicaciones específicas de este uso del analizador seguro incluyen, por ejemplo, compartición de información de coalición en la que, por ejemplo, fuerzas gubernamentales amigas multinacionales se les proporciona la capacidad de comunicar datos operacionales y de otra manera sensibles en un nivel de seguridad autorizado a cada país respectivo a través de una única red o una red dual (es decir, en comparación con las muchas redes que implican relativamente procesos sustancialmente manuales que se usan en la actualidad). Esta capacidad es aplicable también para compañías u otras organizaciones en las que la información que necesita ser conocida por

uno o más individuos específicos (en o sin la organización) se puede comunicar a través de una única red sin la necesidad de preocuparse acerca de qué individuos no autorizados vean la información.

Otra aplicación específica incluye una jerarquía de seguridad de múltiples niveles para sistemas gubernamentales. Es decir, el analizador seguro de la presente invención puede proporcionar la capacidad de operar un sistema gubernamental en diferentes niveles de información clasificada (por ejemplo, sin clasificar, clasificada, secreta, alto secreto) usando una única red. Si se desea, se pueden usar más redes (por ejemplo, una red separada para alto secreto), pero la presente invención permite sustancialmente menos de que en la disposición actual en la que se usa una red separada para cada nivel de clasificación.

Se entenderá que se puede usar cualquier combinación de las aplicaciones que se han descrito en lo que antecede del analizador seguro de la presente invención. Por ejemplo, la aplicación de clave de grupo se puede usar junto con la aplicación de seguridad de datos en movimiento (es decir, en la que se puede acceder a los datos que se comunican a través de una red únicamente por un miembro del respectivo grupo, y en donde, mientras los datos están en movimiento, se dividen entre múltiples trayectorias (o se envían en porciones secuenciales) de acuerdo con la presente invención).

El analizador de datos seguro de la presente invención se puede integrar en cualquier aplicación de soporte intermedio para posibilitar que las aplicaciones almacenen datos de manera segura a diferentes productos de bases de datos o a diferentes dispositivos sin modificación a cualquiera de las aplicaciones o las bases de datos. El soporte intermedio es una expresión general para cualquier producto que permite que dos programas separados y ya existentes se comuniquen. Por ejemplo, en un enfoque adecuado, el soporte intermedio que tiene el analizador de datos seguro integrado, se puede usar para permitir programas escritos para que una base de datos particular se comunique con otras bases de datos sin codificación personalizada.

El analizador de datos seguro de la presente invención se puede implementar teniendo cualquier combinación de cualquier capacidad adecuada, tales como las analizadas en el presente documento. En algunas formas de realización de la presente invención, por ejemplo, el analizador de datos seguro se puede implementar teniendo únicamente ciertas capacidades mientras que otras capacidades se pueden obtener a través del uso de soporte lógico, soporte físico externos o ambos interconectados directa o indirectamente con el analizador de datos seguro.

La figura 30, por ejemplo, muestra una implementación ilustrativa del analizador de datos seguro como el analizador de datos seguro 3000. El analizador de datos seguro 3000 se puede implementar con muy pocas capacidades integradas. Tal como se ilustra, el analizador de datos seguro 3000 puede incluir capacidades integradas para analizar y dividir datos en porciones (también denominadas en el presente documento como comparticiones) de datos usando el módulo 3002 de acuerdo con la presente invención. El analizador de datos seguro 3000 puede incluir también capacidades integradas para realizar redundancia para poder implementar, por ejemplo, la característica de m de n que se ha descrito en lo que antecede (es decir, recrear los datos originales usando menos de todas las comparticiones de datos analizados y divididos) usando el módulo 3004. El analizador de datos seguro 3000 puede incluir también capacidades de distribución de comparticiones usando el módulo 3006 para colocar las comparticiones de datos en memorias intermedias desde las que se envían para comunicación a una localización remota, para almacenamiento, etc., de acuerdo con la presente invención. Se entenderá que cualquier otra capacidad adecuada se puede integrar en el analizador de datos seguro 3000.

La memoria intermedia de datos ensamblada 3008 puede ser cualquier memoria adecuada que se usa para almacenar los datos originales (a pesar de que no necesariamente en su forma original) que se analizarán y dividirán mediante el analizador de datos seguro 3000. En una operación de división, la memoria intermedia de datos ensamblada 3008 proporciona entrada al analizador de datos seguro 3008. En una operación de restauración, la memoria intermedia de datos ensamblada 3008 se puede usar para almacenar la salida del analizador de datos seguro 3000.

Las memorias intermedias de comparticiones de división 3010 pueden ser uno o más módulos de memoria que se pueden usar para almacenar las múltiples comparticiones de datos que resultan del análisis y filtrado de datos originales. En una operación de división, las memorias intermedias de comparticiones de división 3010 soportan la salida del analizador de datos seguro. En una operación de restauración, las memorias intermedias de comparticiones de división soportan la entrada al analizador de datos seguro 3000.

Se entenderá que cualquier otra disposición adecuada de las capacidades puede estar integrada para el analizador de datos seguro 3000. Cualquier característica adicional se puede integrar y cualquiera de las características ilustradas se puede eliminar, hacerse más robusta, hacerse menos robusta, o se puede modificar de otra manera de cualquiera manera adecuada. Las memorias intermedias 3008 y 3010 son de manera análoga meramente ilustrativas y se pueden modificar, eliminarse o añadirse de cualquier manera adecuada.

Cualquier módulo adecuado implementado en soporte lógico, soporte físico o ambos puede llamar por o puede llamar al analizador de datos seguro 3000. Si se desea, incluso se pueden sustituir capacidades que están integradas en el analizador de datos seguro 3000 mediante uno o más módulos externos. Tal como se ilustra,

algunos módulos externos incluyen el generador de números aleatorios 3012, el generador de clave de realimentación de cifrado 3014, el algoritmo de troceo 3016, uno cualquiera o más tipos de encriptación 3018, y la gestión de claves 3020. Se entenderá que estos son módulos externos meramente ilustrativos. Se puede usar cualquier otro módulo adecuado además de o en lugar de los ilustrados.

El generador de clave de realimentación de cifrado 3014 puede generar, de forma externa al analizador de datos seguro 3000, para cada operación del analizador de datos seguro, una clave única, o número aleatorio (usando, por ejemplo, el generador de números aleatorios 3012), para usarse como un valor de semilla para una operación que extiende un tamaño de clave de sesión original (por ejemplo, un valor de 128, 256, 512, o 1024 bits) en un valor igual a la longitud de los datos que se van a analizar y a dividir. Se puede usar cualquier algoritmo adecuado para la generación de la clave de realimentación de cifrado, incluyendo, por ejemplo, el algoritmo de generación de clave de realimentación de cifrado AES.

Con el fin de facilitar la integración del analizador de datos seguro 3000 y sus módulos externos (es decir, la capa del analizador 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 de empaquetado que puede hacer uso de, por ejemplo, llamadas de función de API. Se puede usar cualquier otra disposición adecuada para facilitar la integración de la capa del analizador 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 se emite un comando de escritura (por ejemplo, a un dispositivo de almacenamiento), inserción (por ejemplo, en un campo de base de datos), o transmisión (por ejemplo, a través de una red) en la capa de aplicación 3024. En la etapa 3100 los datos que se van a asegurar se identifican y se realiza una llamada al analizador de datos seguro. La llamada se pasa a través de la capa de empaquetado 3022 en donde en la etapa 3102, la capa de empaquetado 3022 transmite los datos de entrada identificados en la etapa 3100 en la memoria intermedia de datos ensamblada 3008. También en la etapa 3102, se puede almacenar cualquier información de compartición adecuada, nombres de fichero, cualquier otra información adecuada, o cualquier combinación de los mismos (por ejemplo, como información 3106 en la capa de empaquetado 3022). El procesador de datos seguros 3000 a continuación analiza y divide los datos que toma como entrada desde la memoria intermedia de datos ensamblada 3008 de acuerdo con la presente invención. Emite las comparticiones de datos en las memorias intermedias de comparticiones de división 3010. En la etapa 3104, la capa de empaquetado 3022 obtiene desde la información almacenada 3106 cualquier información de compartición adecuada (es decir, almacenada mediante el empaquetamiento 3022 en la etapa 3102) y la localización o localizaciones de compartición (por ejemplo, desde uno o más ficheros de configuración). La capa de empaquetado 3022 a continuación escribe las comparticiones de salida (obtenidas desde las memorias intermedias de comparticiones de división 3010) de forma apropiada (por ejemplo, escritas en uno o más dispositivos de almacenamiento, comunicadas a una red, etc.).

La figura 32 muestra de manera ilustrativa cómo se puede usar la distribución de la figura 30 cuando tiene lugar una lectura (por ejemplo, desde un dispositivo de almacenamiento), selección (por ejemplo, desde un campo de base de datos), o recepción (por ejemplo, desde una red). En la etapa 3200, los datos que se van a restaurar se identifican y se realiza una llamada al analizador de datos seguro 3000 desde la capa de aplicación 3024. En la etapa 3202, desde la capa de empaquetado 3022, se obtiene cualquier información de compartición adecuada y se determina la localización de compartición. La capa de empaquetado 3022 carga las porciones de datos identificados en la etapa 3200 en las memorias intermedias de las comparticiones de división 3010. El analizador de datos seguro 3000 a continuación procesa estas comparticiones de acuerdo con la presente invención (por ejemplo, si únicamente están disponibles tres de cuatro comparticiones, entonces se pueden usar las capacidades de redundancia del analizador de datos seguro 3000 para restaurar los datos originales usando únicamente las tres comparticiones). Los datos reconstruidos a continuación se almacenan en la memoria intermedia de datos ensamblada 3008. En la etapa 3204, la capa de aplicación 3022 convierte los datos almacenados en la memoria intermedia de datos ensamblada 3008 en su formato de datos original (si fuera necesario) y proporciona los datos originales en su formato original a la capa de aplicación 3024.

Se entenderá que el análisis y filtrado de datos originales ilustrados en la figura 31 y la restauración de las porciones de datos en datos originales ilustrados en la figura 32 es meramente ilustrativo. Se puede usar cualquier otro proceso, componente o ambos adecuados además de o en lugar de los ilustrados.

La figura 33 es un diagrama de bloques de un flujo de proceso ilustrativo para analizar y dividir datos originales en dos o más porciones de datos de acuerdo con una forma de realización de la presente invención. Tal como se ilustra, los datos originales que se desean analizar y dividir son texto plano 3306 (es decir, se usa la palabra “ENVIAR” como un ejemplo). Se entenderá que se puede analizar y dividirse cualquier otro tipo de dato 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 datos originales 3306, entonces se puede generar la clave de sesión de realimentación de cifrado 3304.

En un enfoque adecuado, los datos originales 3306 se pueden encriptar antes del análisis, división o ambos. Por ejemplo, como ilustra la figura 33, a los datos originales 3306 se puede realizar la operación XOR con cualquier valor

adecuado (por ejemplo, con la clave de sesión de realimentación de cifrado 3304, o con cualquier otro valor adecuado). Se entenderá que se puede usar cualquier otra técnica de encriptación adecuada en lugar de o además de la técnica de XOR ilustrada. Se entenderá adicionalmente que a pesar de que la figura 33 se ilustra en términos de operaciones byte por byte, la operación puede tener lugar en el nivel de bits o en cualquier otro nivel adecuado. Se entenderá adicionalmente que, si se desea, no hay necesidad de ninguna encriptación de ningún modo de los datos originales 3306.

Los datos encriptados resultantes (o datos originales si no tuvo lugar encriptación) se trocen a continuación para determinar cómo dividir los datos encriptados (u originales) entre los cubos de salida (por ejemplo, de los cuales hay cuatro en el ejemplo ilustrado). En el ejemplo ilustrado, el troceo tiene lugar en bytes y es una función de clave de sesión de realimentación de cifrado 3304. Se entenderá que esto es meramente ilustrativo. El troceo se puede realizar en el nivel de bits, si se desea. El troceo puede ser una función de cualquier otro valor adecuado además de la clave de sesión de realimentación de cifrado 3304. En otro enfoque adecuado, no se necesita usar troceo. En su lugar, se puede emplear cualquier otra técnica adecuada para dividir datos.

La figura 34 es un diagrama de bloques de un flujo de proceso ilustrativo para restaurar datos originales 3306 desde dos o más porciones de datos originales 3306 analizadas y divididas de acuerdo con una forma de realización de la presente invención. El proceso implica trocear las porciones a la inversa (es decir, a los procesos de la figura 33) como una función de clave de sesión de realimentación de cifrado 3304 para restaurar los datos originales encriptados (o datos originales si no hubiera encriptación antes del análisis y división). La clave de encriptación se puede usar a continuación para restaurar los datos originales (es decir, en el ejemplo ilustrado, la clave de sesión de realimentación de cifrado 3304 se usa para desencriptar la encriptación XOR realizando la operación XOR con los datos encriptados). Esto restaura los datos originales 3306.

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

Se entenderá que cualquier referencia a funcionalidad de troceo realizada en el presente documento se puede realizar con respecto a cualquier algoritmo de troceo adecuado. Estos incluyen por ejemplo, MD5 y SHA-1. Se pueden usar diferentes algoritmos de troceo en diferentes momentos y por diferentes componentes de la presente invención.

Después de que se ha determinado un punto de división de acuerdo con el procedimiento ilustrativo anterior o a través de cualquier otro procedimiento o algoritmo, se puede realizar una determinación con respecto a qué porciones de datos anexar a cada uno de los segmentos izquierdo y derecho. Se puede usar cualquier algoritmo adecuado para realizar esta determinación. Por ejemplo, en un enfoque adecuado, se puede crear una tabla de todas las posibles distribuciones (por ejemplo, en forma de emparejamientos de destinos para el segmento izquierdo y para el segmento derecho), en las cuales se puede determinar un valor de compartición de destino para cada uno del segmento izquierdo y derecho usando cualquier función de troceo adecuada o dato correspondiente en la clave de sesión, clave de sesión de realimentación de cifrado, o cualquier otro valor aleatorio o pseudoaleatorio adecuado, que se puede generar y ampliarse al tamaño de los datos originales. Por ejemplo, se puede realizar una función de troceo de un byte correspondiente en el valor aleatorio o pseudoaleatorio. La salida de la función de troceo se usa para determinar qué emparejamientos de destinos (es decir, uno para el segmento izquierdo y uno para el segmento derecho) seleccionar desde la tabla de todas las combinaciones de destinos. Basándose en este resultado, cada segmento de la unidad de datos de división se anexa a las respectivas dos comparticiones indicadas mediante el valor de tabla seleccionado como resultado de la función de troceo.

Se puede anexar información de redundancia a las porciones de datos de acuerdo con la presente invención para permitir la restauración de los datos originales usando menos de todas las porciones de datos. Por ejemplo, si se desea que dos de cuatro porciones sean suficientes para la restauración de datos, entonces los datos adicionales desde las comparticiones se pueden anexar en consecuencia para cada compartición en, por ejemplo, una manera en orden cíclico (por ejemplo, en donde el tamaño de los datos originales es 4 MB, entonces la compartición 1 obtiene sus propias comparticiones así como las de las comparticiones 2 y 3; la compartición 2 obtiene su propia compartición así como las de las comparticiones 3 y 4; la compartición 3 obtiene su propia compartición así como las de las comparticiones 4 y 1; y la compartición 4 obtiene sus propias comparticiones así como las de las comparticiones 1 y 2). Se puede usar cualquier redundancia adecuada de acuerdo con la presente invención.

Se entenderá que se puede usar cualquier otro enfoque de análisis y división adecuado para generar porciones de datos desde un conjunto de datos originales de acuerdo con la presente invención. Por ejemplo, el análisis y división se puede procesar de forma aleatoria o pseudoaleatoria en una base bit a bit. Se puede usar un valor aleatorio o pseudoaleatorio (por ejemplo, clave de sesión, clave de sesión de realimentación de cifrado, etc.) en el cual para cada bit en los datos originales, el resultado de una función de troceo en los datos correspondientes en el valor aleatorio o pseudoaleatorio puede indicar a qué compartición anexar el bit respectivo. En un enfoque adecuado el

valor aleatorio o pseudoaleatorio se puede generar como, o ampliarse a, 8 veces el tamaño de los datos originales de tal modo que la función de troceo se puede realizar en un byte correspondiente del valor aleatorio o pseudoaleatorio con respecto a cada bit de los datos originales. Cualquier otro algoritmo adecuado para analizar y dividir datos en un nivel de bit a bit se puede usar de acuerdo con la presente invención. Se apreciará adicionalmente que los datos de redundancia se pueden anexar a las comparticiones de datos tal como, por ejemplo, de la manera que se ha descrito inmediatamente en lo que antecede de acuerdo con la presente invención.

En un enfoque adecuado, el análisis y división no necesita ser aleatorio o pseudoaleatorio. En su lugar, se puede usar cualquier algoritmo determinístico adecuado para analizar y dividir datos. Por ejemplo, se puede emplear descomponer los datos originales en comparticiones secuenciales como un algoritmo de análisis y división. Otro ejemplo es analizar y dividir los datos originales bit a bit, anexando cada bit respectivo a las comparticiones de datos de forma secuencial de una manera en orden cíclico. Se apreciará adicionalmente que los datos de redundancia se pueden anexar a las comparticiones de datos tal como, por ejemplo, de la manera que se ha descrito en lo que antecede de acuerdo con la presente invención.

En una forma de realización de la presente invención, después de que el analizador de datos seguro genera un número de porciones de datos originales, para restaurar los datos originales, pueden ser obligatorias ciertas una o más de las porciones generadas. Por ejemplo, si una de las porciones se usa como una compartición de autenticación (por ejemplo, grabada en un dispositivo de testigo físico), y se está usando la característica de tolerancia a fallos del analizador de datos seguro (es decir, en donde son necesarias menos de todas las porciones para restaurar los datos originales), entonces incluso a pesar de que el analizador de datos seguro pueda tener acceso a un número suficiente de porciones de los datos originales para restaurar los datos originales, puede requerir la compartición de autenticación almacenada en el dispositivo de testigo físico antes de que restauren los datos originales. Se entenderá que cualquier número y tipos de comparticiones particulares se pueden requerir basándose en, por ejemplo, aplicación, tipo de datos, usuario, cualquier otro factor adecuado o cualquier combinación de los mismos.

En un enfoque adecuado, el analizador de datos seguro o algún componente externo al analizador de datos seguro puede encriptar una o más porciones de los datos originales. Se puede requerir que se proporcionen y desencripten las porciones encriptadas para restaurar los datos originales. Las diferentes porciones encriptadas se pueden encriptar con diferentes claves de encriptación. Por ejemplo, esta característica se puede usar para implementar una “regla de los dos hombres” más segura en la que un primer usuario necesitaría tener una compartición particular encriptada usando una primera encriptación y un segundo usuario necesitaría tener una compartición particular encriptada usando una segunda clave de encriptación. Para acceder los datos originales, ambos usuarios necesitarían tener sus respectivas claves de encriptación y proporcionar sus respectivas porciones de los datos originales. En un enfoque adecuado, se puede usar una clave pública para encriptar una o más porciones de datos que pueden ser una compartición obligatoria requerida para restaurar los datos originales. Se puede usar a continuación una clave privada para desencriptar la compartición para usarse para restaurar los datos originales.

Se puede usar cualquier paradigma adecuado de este tipo que haga uso de comparticiones obligatorias en donde sean necesarias menos de todas las comparticiones para restaurar los datos originales.

En una forma de realización adecuada de la presente invención, la distribución de datos en un número finito de comparticiones de datos se puede procesar de forma aleatoria o pseudoaleatoria de tal modo que desde una perspectiva estadística, la probabilidad de que una compartición particular de datos reciba una unidad de datos particular es igual a la probabilidad de que una cualquiera de las restantes comparticiones reciba la unidad de datos. Como resultado, cada compartición de datos tendrá una cantidad aproximadamente igual de bits de datos.

De acuerdo con otra forma de realización de la presente invención, cada uno del número finito de comparticiones de datos no necesita tener una probabilidad igual de recibir unidades de datos desde la división y análisis de los datos originales. En su lugar ciertas una o más comparticiones pueden tener una probabilidad superior o inferior que las restantes comparticiones. Como resultado, ciertas comparticiones pueden ser mayores o menores en términos de tamaño de bit en relación con otras comparticiones. Por ejemplo, en un escenario de dos comparticiones, una compartición puede tener una probabilidad del 1 % de recibir una unidad de datos mientras que la segunda compartición tiene una probabilidad del 99 %. Se debería deducir, por lo tanto que una vez que las unidades de datos se han distribuido mediante el analizador de datos seguro entre las dos comparticiones, la primera compartición debería tener aproximadamente el 1 % de los datos y la segunda compartición el 99 %. Se puede usar cualquier probabilidad adecuada de acuerdo con la presente invención.

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

De acuerdo con otra forma de realización de la presente invención, el analizador de datos seguro puede generar comparticiones de datos, una o más de las cuales tienen tamaños predefinidos. Por ejemplo, el analizador de datos

seguro puede dividir datos originales en porciones de datos en donde una de las porciones es exactamente 256 bits. En un enfoque adecuado, si no es posible generar una porción de datos que tiene el tamaño requerido, entonces el analizador de datos seguro puede rellenar la porción para hacerla al tamaño correcto. Se puede usar cualquier tamaño adecuado.

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

Tal como se ha analizado en lo que antecede, el analizador de datos seguro puede usar claves en el análisis y división de los datos. Por fines de claridad y brevedad, estas claves se denominarán en el presente documento como “claves de división”. Por ejemplo, la clave maestra de sesión, anteriormente introducida, es un tipo de clave de división. Asimismo, tal como se ha analizado en lo que antecede, las claves de división se pueden asegurar en comparticiones de datos generadas mediante el analizador de datos seguro. Se puede usar cualquier algoritmo adecuado para asegurar las claves de división para asegurarlas entre las comparticiones de datos. Por ejemplo, se puede usar el algoritmo de Shamir para asegurar las claves de división con las que la información que se puede usar para reconstruir una clave de división se genera y anexa a las comparticiones de datos. Se puede usar cualquier otro algoritmo adecuado de este tipo de acuerdo con la presente invención.

De manera similar, cualquier clave de encriptación adecuada se puede asegurar en una o más comparticiones de datos de acuerdo con cualquier algoritmo adecuado tal como el algoritmo de Shamir. Por ejemplo, las claves de encriptación que se usan para encriptar un conjunto de datos antes de análisis y división, las claves de encriptación que se usan para encriptar unas porciones de datos después de análisis y división, o ambas se pueden asegurar usando, por ejemplo, el algoritmo de Shamir o cualquier otro algoritmo adecuado.

De acuerdo con una forma de realización de la presente invención, una Transformación Todo o Nada (AoNT, *All or Nothing Transform*), tal como una Transformación de Paquete Completo, se puede usar para asegurar adicionalmente los datos transformando claves de división, claves de encriptación, cualquier otro elemento de datos adecuado, o cualquier combinación de los mismos. Por ejemplo, una clave de encriptación que se usa para encriptar un conjunto de datos antes de análisis y división de acuerdo con la presente invención se puede transformar mediante un algoritmo de AoNT. La clave de encriptación transformada se puede distribuir a continuación entre las comparticiones de datos de acuerdo con, por ejemplo, el algoritmo de Shamir o cualquier otro algoritmo adecuado. Para reconstruir la clave de encriptación, el conjunto de datos encriptados se debe restaurar (por ejemplo, no necesariamente usando todas las comparticiones de datos si se usó redundancia de acuerdo con la presente invención) para acceder a la información necesaria con respecto a la transformación de acuerdo con AoNT como es bien conocido por un experto en la materia. Cuando se recupera la clave de encriptación original, se puede usar para desencriptar el conjunto de datos encriptados para recuperar el conjunto de datos original. Se entenderá que las características de tolerancia a fallos de la presente invención se pueden usar junto con la característica AoNT. En concreto, los datos de redundancia se pueden incluir en las porciones de datos de tal modo que son necesarias menos de todas las porciones de datos para restaurar el conjunto de datos encriptados.

Se entenderá que AoNT se puede aplicar a las claves de encriptación que se usan para encriptar las porciones de datos después del análisis y división en lugar de o además de la encriptación y AoNT de la respectiva clave de encriptación que se corresponde con el conjunto de datos antes del análisis y división. De forma análoga, AoNT se puede aplicar a las claves de división.

En una forma de realización de la presente invención, las claves de encriptación, claves de división, o ambas que se usan de acuerdo con la presente invención se pueden encriptar adicionalmente usando, por ejemplo, una clave de grupo de trabajo para proporcionar un nivel adicional de seguridad a un conjunto de datos asegurado.

En una forma de realización de la presente invención, se puede proporcionar un módulo de auditoría que rastrea cada vez que el analizador de datos seguro se invoca para dividir datos.

La figura 36 ilustra posibles opciones 3600 para usar los componentes del analizador de datos seguro de acuerdo con la invención. Cada combinación de opciones se resume a continuación y se etiqueta con los números de etapa apropiados desde la figura 36. El analizador de datos seguro puede ser modular en su naturaleza, permitiendo que se use cualquier algoritmo conocido en cada uno de los bloques de función mostrados en la figura 36. Por ejemplo, se pueden usar otros algoritmos de división de clave (por ejemplo, compartición secreta) tales como Blakely en lugar de Shamir, o la encriptación AES se podría sustituir por cualquier otro algoritmo de encriptación conocido tal como Triple DES. Las etiquetas mostradas en el ejemplo de la figura 36 representan meramente una posible combinación de algoritmos para su uso en una forma de realización de la invención. Se debería entender que cualquier algoritmo adecuado o combinación de algoritmos se puede usar en lugar de los algoritmos etiquetados.

1) 3610, 3612, 3614, 3615, 3616, 3617, 3618, 3619
Usando los datos previamente encriptados en la etapa 3610, los datos se pueden dividir con el tiempo en un número predefinido de comparticiones. Si el algoritmo de división requiere una clave, se puede generar una clave de encriptación de división en la etapa 3612 usando un generador de números pseudoaleatorios

criptográficamente seguro. La clave de encriptación de división se puede transformar opcionalmente usando una Transformación Todo o Nada (AoNT, *All or Nothing Transform*) en una clave de división de transformación en la etapa 3614 antes de que la clave se divida en el número predefinido de comparticiones con tolerancia a fallos en la etapa 3615. Los datos se pueden dividir a continuación en el número predefinido de comparticiones en la etapa 3616. Se puede usar un esquema tolerante a fallos en la etapa 3617 para permitir la regeneración de los datos desde menos del número total de comparticiones. Una vez que se han creado las comparticiones, se puede embeber información de autenticación / integridad en las comparticiones en la etapa 3618. De forma opcional, cada compartición se puede postencriptar en la etapa 3619.

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

En algunas formas de realización, los datos de entrada se pueden encriptar usando una clave de encriptación proporcionada por un usuario o un sistema externo. La clave externa se proporciona en la etapa 3611. Por ejemplo, la clave se puede proporcionar desde un almacenamiento de clave externo. Si el algoritmo de división requiere una clave, la clave de encriptación de división se puede generar usando un generador de números pseudoaleatorios criptográficamente seguro en la etapa 3612. La clave de división se puede transformar opcionalmente usando una Transformación Todo o Nada (AoNT) en una clave de encriptación de división de transformación en la etapa 3614 antes de que la clave se divida en el número predefinido de comparticiones con tolerancia a fallos en la etapa 3615. Los datos se dividen a continuación en un número predefinido de comparticiones en la etapa 3616. Se puede usar un esquema tolerante a fallos en la etapa 3617 para permitir la regeneración de los datos desde menos del número total de comparticiones. Una vez que se han creado las comparticiones, se puede embeber información de autenticación / integridad en las comparticiones en la etapa 3618. De forma opcional, cada compartición se puede postencriptar en la etapa 3619.

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

En algunas formas de realización, se puede generar una clave de encriptación usando un generador de números pseudoaleatorios criptográficamente seguro en la etapa 3612 para transformar los datos. La encriptación de los datos usando la clave de encriptación generada puede tener lugar en la etapa 3613. La clave de encriptación se puede transformar opcionalmente usando una Transformación Todo o Nada (AoNT) en una clave de encriptación de transformación en la etapa 3614. La clave de encriptación de transformación y / o la clave de encriptación generada se pueden dividir a continuación en el número predefinido de comparticiones con tolerancia a fallos en la etapa 3615. Si el algoritmo de división requiere una clave, la generación de la clave de encriptación de división usando un generador de números pseudoaleatorios criptográficamente seguro puede tener lugar en la etapa 3612. La clave de división se puede transformar opcionalmente usando una Transformación Todo o Nada (AoNT) en una clave de encriptación de división de transformación en la etapa 3614 antes de que la clave se divida en el número predefinido de comparticiones con tolerancia a fallos en la etapa 3615. Los datos se pueden dividir a continuación en un número predefinido de comparticiones en la etapa 3616. Se puede usar un esquema tolerante a fallos en la etapa 3617 para permitir la regeneración de los datos desde menos del número total de comparticiones. Una vez que se han creado las comparticiones, se embeberá la información de autenticación / integridad en las comparticiones en la etapa 3618. Cada compartición se puede postencriptar opcionalmente a continuación en la etapa 3619.

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

En algunas formas de realización, los datos se pueden dividir en un número predefinido de comparticiones. Si el algoritmo de división requiere una clave, la generación de la clave de encriptación de división usando un generador de números pseudoaleatorios criptográficamente seguro puede tener lugar en la etapa 3612. La clave de división se puede transformar opcionalmente usando una Transformación Todo o Nada (AoNT) en una clave de división transformada en la etapa 3614 antes de que la clave se divida en el número predefinido de comparticiones con tolerancia a fallos en la etapa 3615. Los datos se pueden dividir a continuación en la etapa 3616. Se puede usar un esquema tolerante a fallos en la etapa 3617 para permitir la regeneración de los datos desde menos del número total de comparticiones. Una vez que se han creado las comparticiones, se puede embeber información de autenticación / integridad en las comparticiones en la etapa 3618. De forma opcional, cada compartición se puede postencriptar en la etapa 3619.

A pesar de que las cuatro combinaciones anteriores de opciones se usan preferiblemente en algunas formas de realización de la invención, se puede usar cualquier otra combinación de características, etapas u opciones adecuadas con el analizador de datos seguro en otras formas de realización.

El analizador de datos seguro puede ofrecer protección de datos flexible facilitando la separación física. Los datos se pueden encriptar en primer lugar, a continuación dividirse en comparticiones con tolerancia a fallos “m de n”. Esto permite la regeneración de la información original cuando están disponibles menos del número total de comparticiones. Por ejemplo, algunas particiones se pueden perder o corromperse en la transmisión. Las comparticiones perdidas o corrompidas se pueden recrear a partir de la tolerancia a fallos o la información de integridad anexada a las comparticiones, tal como se analiza con más detalle a continuación.

Con el fin de crear las comparticiones, se utilizan opcionalmente un número de claves por el analizador de datos seguro. Estas claves pueden incluir uno o más de lo siguiente:

Clave de preencriptación: cuando se selecciona la preencriptación de las comparticiones, se puede pasar una clave externa al analizador de datos seguro. Esta clave se puede generar y almacenarse de forma externa en un

almacenamiento de claves (u otra localización) y se puede usar para encriptar opcionalmente datos antes de la división de datos.

Clave de encriptación de división: esta clave se puede generar de forma interna y usarse mediante el analizador de datos seguro para encriptar los datos antes de la división. Esta clave se puede almacenar a continuación de manera segura en las comparticiones usando un algoritmo de división de clave.

Clave de sesión de división: esta clave no se usa con un algoritmo de encriptación; en su lugar, se puede usar para aplicar claves los algoritmos de división en particiones de datos cuando se selecciona división aleatoria. Cuando se usa una división aleatoria, se puede generar una clave de sesión de división de forma interna y usarse mediante el analizador de datos seguro para dividir en particiones los datos en comparticiones. Esta clave se puede almacenar de manera segura en las comparticiones usando un algoritmo de división de clave.

Clave de postencriptación: cuando se selecciona la postencriptación de las comparticiones, se puede pasar una clave externa al analizador de datos seguro y usarse para post encriptar las comparticiones individuales. Esta clave se puede generar y almacenarse de forma externa en un almacenamiento de claves u otra localización adecuada.

En algunas formas de realización, cuando se aseguran los datos usando el analizador de datos seguro de esta manera, la información únicamente se puede reensamblar con la condición de que las comparticiones requeridas y claves de encriptación externas estén presentes.

La figura 37 muestra la vista general ilustrativa del proceso 3700 para usar el analizador de datos seguro de la presente invención en algunas formas de realización. Tal como se ha descrito en lo que antecede, dos funciones bien adecuadas para el analizador de datos seguro 3706 pueden incluir encriptación 3702 y respaldo 3704. En este sentido, el analizador de datos seguro 3706 se puede integrar con un sistema RAID o de respaldo o un motor de encriptación de soporte físico o soporte lógico en algunas formas de realización.

Los procesos de clave principal que están asociados con el analizador de datos seguro 3706 pueden incluir uno o más de proceso de preencriptación 3708, proceso de encriptación / transformación 3710, proceso de clave segura 3712, proceso de analizar / distribuir 3714, proceso de tolerancia a fallos 3716, proceso de autenticación de compartición 3716, y proceso de postencriptación 3720. Estos procesos se pueden ejecutar en varios órdenes o combinaciones adecuados, tal como se detalla en la figura 36. La combinación y orden de los procesos puede depender de la aplicación o uso particular, el nivel de seguridad deseado, si se desea preencriptación, postencriptación, o ambas, la redundancia deseada, las capacidades o rendimiento de un sistema subyacente o integrado, o cualquier otro factor o combinación de factores adecuados.

La salida del proceso 3700 ilustrativo pueden ser dos o más comparticiones 3722. Tal como se ha descrito en lo que antecede, los datos se pueden distribuir a cada una de estas comparticiones de forma aleatoria (o pseudoaleatoria) en algunas formas de realización. En otras formas de realización, se puede usar un algoritmo determinístico (o alguna combinación de aleatoriedad adecuada, pseudoaleatoriedad, y algoritmos determinísticos).

Además de los activos de protección de información individual, existe en ocasiones un requisito de compartir información entre diferentes grupos de usuarios o comunidades de interés. Puede ser necesario a continuación controlar el acceso a las comparticiones individuales en ese grupo de usuario o compartir credenciales entre esos usuarios que permitiría únicamente a los miembros del grupo reensamblar las comparticiones. Para este fin, se puede implantar una clave de grupo de trabajo a miembros de grupo en algunas formas de realización de la invención. La clave de grupo de trabajo se debería proteger y mantenerse confidencial, ya que el compromiso de la clave de grupo de trabajo puede permitir potencialmente a aquellos fuera del grupo acceder a información. Algunos sistemas y métodos para el desarrollo y protección de clave de grupo de trabajo se analizan a continuación.

El concepto de clave de grupo de trabajo permite protección mejorada de activos de información encriptando información de clave almacenada en las comparticiones. Una vez que se realiza esta operación, incluso si se descubrieran todas las comparticiones y claves externas requeridas, un atacante no tiene esperanza de recrear la información sin acceder a la clave de grupo de trabajo.

La figura 38 muestra el diagrama de bloques ilustrativo 3800 para almacenar componentes de clave y datos en las comparticiones. En el ejemplo del diagrama 3800, se omiten las etapas de preencriptación y postencriptación, a pesar de que estas etapas se pueden incluir en otras formas de realización.

El proceso simplificado para dividir los datos incluye encriptar los datos usando la clave de encriptación 3804 en la etapa de encriptación 3802. Las porciones de la clave de encriptación 3804 se pueden dividir a continuación y almacenarse en las comparticiones 3810 de acuerdo con la presente invención. Las porciones de división de la clave de encriptación 3806 se pueden almacenar también en las comparticiones 3810. Usando la clave de encriptación de división, los datos 3808 se dividen a continuación y se almacenan en las comparticiones 3810.

Con el fin de restaurar los datos, la clave de encriptación de división 3806 se puede recuperar y restaurarse de acuerdo con la presente invención. La operación de división se puede invertir a continuación para restaurar el texto de cifrado. La clave de encriptación 3804 también se puede recuperar y restaurarse, y el texto de cifrado se puede desencriptar a continuación usando la clave de encriptación.

Cuando se utiliza una clave de grupo de trabajo, el proceso anterior se puede cambiar para proteger ligeramente la clave de encriptación con la clave de grupo de trabajo. La clave de encriptación se puede encriptar a continuación con la clave de grupo de trabajo antes de almacenarse en las comparticiones. Las etapas modificadas se muestran en diagrama de bloque ilustrativo 3900 de la figura 39.

El proceso simplificado para dividir los datos usando una clave de grupo de trabajo incluye encriptar en primer lugar los datos usando la clave de encriptación en la etapa 3902. La clave de encriptación se puede encriptar a continuación con la clave de grupo de trabajo en la etapa 3904. La clave de encriptación encriptada con la clave de grupo de trabajo se puede dividir a continuación en porciones y almacenarse con las comparticiones 3912. La clave de división 3908 también se puede dividir y almacenarse en las comparticiones 3912. Por último, las porciones de datos 3910 se dividen y almacenan en las comparticiones 3912 usando la clave de división 3908.

Para restaurar los datos, la clave de división se puede recuperar y restaurarse de acuerdo con la presente invención. La operación de división se puede invertir a continuación para restaurar el texto de cifrado de acuerdo con la presente invención. La clave de encriptación (que se encriptó con la clave de grupo de trabajo) se puede recuperar y restaurarse. La clave de encriptación se puede desencriptar a continuación usando la clave de grupo de trabajo. Por último, el texto de cifrado se puede desencriptar usando la clave de encriptación.

Hay varios métodos seguros para implantar y proteger las claves del grupo de trabajo. La selección de qué método usar para una aplicación particular depende de un número de factores. Estos factores pueden incluir nivel de seguridad requerido, coste, conveniencia, y el número de usuarios en el grupo de trabajo. Algunas técnicas que se usan comúnmente en algunas formas de realización se proporcionan a continuación:

Almacenamiento de clave basado en soporte físico

Las soluciones basadas en soporte físico proporcionan en general las garantías más fuertes para la seguridad de claves de encriptación / desencriptación en un sistema de encriptación. Ejemplos de soluciones de almacenamiento basadas en soporte físico incluyen los dispositivos de testigo de clave resistentes a manipulación que almacenan claves en un dispositivo portátil (por ejemplo, tarjeta inteligente / mochila), o periféricos de almacenamiento de clave no portátiles. Estos dispositivos están diseñados para evitar la fácil duplicación de material de clave por partes no autorizadas. Las claves se pueden generar mediante una autoridad de confianza y distribuirse a los usuarios, o generarse en el soporte físico. Además, muchos sistemas de almacenamiento de claves proporcionan autenticación de múltiples factores, en donde el uso de las claves requiere acceso tanto a un objeto físico (testigo) como una frase de paso o biométrica.

Almacenamiento de clave basado en soporte lógico

A pesar de que el almacenamiento basado en soporte físico especializado puede ser deseable para implantaciones o aplicaciones de alta seguridad, otras implantaciones pueden elegir almacenar las claves directamente en soporte físico local (por ejemplo, discos, almacenamientos de RAM o RAM no volátil tales como unidades de USB). Esto proporciona un nivel inferior de protección frente a atacantes internos, o en casos en donde un atacante puede acceder directamente a la máquina de encriptación.

Para asegurar claves en disco, la gestión de claves basada en soporte lógico a menudo protege las claves almacenándolas en forma encriptada bajo una clave obtenida desde una combinación de otras métricas de autenticación, incluyendo: contraseñas y frases de paso, presencia de otras claves (por ejemplo, desde una solución basada en soporte físico), biométricas o cualquier combinación adecuada de lo anterior. El nivel de seguridad proporcionado mediante tales técnicas puede variar desde los mecanismos de protección de claves relativamente débiles proporcionados mediante algunos sistemas operativos (por ejemplo, MS Windows y Linux), a soluciones más robustas implementadas usando autenticación de múltiples factores.

El analizador de datos seguro de la presente invención se puede usar de forma ventajosa en un número de aplicaciones y tecnologías. Por ejemplo, sistema de correo electrónico, sistemas RAID, sistemas de difusión de vídeo, sistemas de base de datos, sistemas de respaldo de cinta, o cualquier otro sistema adecuado puede tener el analizador de datos seguro integrado en cualquier nivel adecuado. Tal como se ha analizado en lo que antecede, se entenderá que el analizador de datos seguro se puede integrar también para la protección y la tolerancia a fallos de cualquier tipo de datos en movimiento a través de cualquier medio de transporte, incluyendo, por ejemplo, medios de transporte cableado, inalámbrico o físico. Como un ejemplo, las aplicaciones de voz sobre el protocolo de Internet (VoIP, *voice over Internet protocol*) pueden hacer uso del analizador de datos seguro de la presente invención para resolver problemas relacionados con ecos y retardos que se encuentran comúnmente en VoIP. La necesidad de los reintentos de red en paquetes interrumpidos se puede eliminar usando tolerancia a fallos, que garantiza la entrega

de paquetes incluso con la pérdida de un número predeterminado de comparticiones. Los paquetes de datos (por ejemplo, paquetes de red) también se pueden dividir y restaurarse de forma eficaz “al vuelo” con un retardo y un almacenamiento en memoria intermedia mínimos, dando como resultado una solución completa para diversos tipos de datos en movimiento. El analizador de datos seguro puede actuar en paquetes de datos de red, paquetes de voz de red, bloques de datos de sistema de ficheros, o cualquier otra unidad de información adecuada. Además de integrarse con una aplicación de VoIP, el analizador de datos seguro se puede integrar con una aplicación de compartición de ficheros (por ejemplo, una aplicación de compartición de ficheros entre pares), una aplicación de difusión de vídeo, una aplicación de voto o encuesta electrónica (que puede implementar un protocolo de voto electrónico y firmas ciegas, tales como el protocolo Sensus), una aplicación de correo electrónico, o cualquier otra aplicación de red que pueda requerir o desear comunicación segura.

En algunas formas de realización, el soporte para datos en red en movimiento se puede proporcionar mediante el analizador de datos seguro de la presente invención en dos fases distintas -- una fase de generación de encabezamiento y una fase de división en particiones de datos. El proceso de generación de encabezamiento simplificado 4000 y el proceso de partición de datos simplificado 4010 se muestran en las figuras 40A y 40B, de forma respectiva. Uno o ambos de estos procesos se pueden realizar en paquetes de red, bloques de sistema de ficheros, o cualquier otra información adecuada.

En algunas formas de realización, el proceso de generación de encabezamientos 4000 se puede realizar una vez en el inicio de un flujo de paquete de paquetes de red. En la etapa 4002, se puede generar una clave de encriptación de división, K, aleatoria (o pseudoaleatoria). La clave de encriptación de división, K, se puede encriptar opcionalmente a continuación (por ejemplo, usando la clave de grupo de trabajo que se ha descrito en lo que antecede) en la etapa de empaquetado de clave AES 4004. A pesar de que se puede usar un empaquetado de clave AES en algunas formas de realización, se puede usar cualquier algoritmo de encriptación de clave o de empaquetado de clave adecuado en otras formas de realización. La etapa de empaquetado de clave AES 4004 puede operar en toda la clave de encriptación de división, K, o la clave de encriptación de división se puede analizar en varios bloques (por ejemplo, bloques de 64 bits). La etapa de compresión de clave AES 4004 puede a continuación operar en bloques de la clave de encriptación de división, si se desea.

En la etapa 4006, se puede usar un algoritmo de compartición secreta (por ejemplo, Shamir) para la clave de encriptación de división de división, K, en comparticiones de clave. Cada compartición de clave se puede embeber a continuación en una de las comparticiones de salida (por ejemplo, en los encabezamientos de compartición). Por último, se puede anexar un bloque de integración de compartición y (opcionalmente) una etiqueta de postautenticación (por ejemplo, MAC) al bloque de encabezamiento de cada compartición. Cada bloque de encabezamiento se puede diseñar para ajustarse en un único paquete de datos.

Después de que la generación de encabezamientos está completa (por ejemplo, usando el proceso de generación de encabezamientos simplificado 4000), el analizador de datos seguro puede entrar en la fase de división en particiones de datos usando el proceso de división de datos simplificado 4010. Cada paquete de datos entrante o bloque de datos en el flujo se encripta usando la clave de encriptación de división, K, en la etapa 4012. En la etapa 4014, la información de integridad de compartición (por ejemplo, un troceo H) se puede calcular en el texto de cifrado resultante desde la etapa 4012. Por ejemplo, se puede calcular un troceo de SHA-256. En la etapa 4106, los paquetes de datos o bloques de datos se pueden dividir en particiones a continuación en dos o más comparticiones de datos usando uno de los algoritmos de división de datos que se han descrito en lo que antecede de acuerdo con la presente invención. En algunas formas de realización, los paquetes de datos o bloques de datos se pueden dividir de tal modo que cada compartición de datos contiene una distribución sustancialmente aleatoria de los paquetes de datos o bloques de datos encriptados. La información de integridad (por ejemplo, troceo de H) se puede anexar a continuación a cada compartición de datos. Se puede calcular también una etiqueta de postautenticación opcional (por ejemplo, MAC) y anexarse a cada compartición de datos en algunas formas de realización.

Cada compartición de datos puede incluir metadatos, que pueden ser necesarios para permitir la reconstrucción correcta de los bloques de datos o paquetes de datos. Esta información se puede incluir en el encabezamiento de compartición. Los metadatos pueden incluir información tal como comparticiones de clave criptográfica, identidades de clave, números aleatorios utilizados solo una vez de compartición, firmas / valores de MAC, y bloques de integridad. Para maximizar la eficacia del ancho de banda, los metadatos se pueden almacenar en un formato binario compacto.

Por ejemplo, en algunas formas de realización, el encabezamiento de compartición incluye un fragmento de encabezamiento de texto limpio, que no está encriptado y puede incluir tales elementos como la compartición de clave Shamir, número aleatorio utilizado solo una vez por sesión, número aleatorio utilizado solo una vez por compartición, identificadores de clave (por ejemplo, un identificador de clave de grupo de trabajo y un identificador de clave post20 autenticación). El encabezamiento de compartición puede incluir también un fragmento de encabezamiento encriptado que está encriptado con la clave de encriptación de división. Un fragmento de encabezamiento de integridad, que puede incluir comprobaciones de integridad para cualquier número de los bloques anteriores (por ejemplo, los dos bloques anteriores) se puede incluir también en el encabezamiento. Cualquier otro valor adecuado o información se puede incluir también en el encabezamiento de compartición.

Tal como se muestra en el formato de compartición ilustrativo 4100 de la figura 41, el bloque de encabezamiento 4102 se puede asociar con dos o más bloques de salida 4104. Cada bloque de encabezamiento, tal como el bloque de encabezamiento 4102, se puede diseñar para ajustarse en un único paquete de datos de red. En algunas formas de realización, después de que se transmite el bloque de encabezamiento 4102 desde una primera localización a una segunda localización, los bloques de salida se pueden transmitir a continuación. Como alternativa, el bloque de encabezamiento 4102 y los bloques de salida 4104 se pueden transmitir al mismo tiempo en paralelo. La transmisión puede tener lugar a través de una o más trayectorias de comunicaciones similares o no similares.

Cada bloque de salida puede incluir la porción de datos 4106 y la porción de integridad / autenticidad 4108. Tal como se ha descrito en lo que antecede, cada compartición de datos se puede asegurar usando una porción de integridad de compartición que incluye información de integridad de compartición (por ejemplo, un troceo de SHA-256) de los datos encriptados prediviididos en particiones. Para verificar la integridad de los bloques de salida en el momento de recuperación, el analizador de datos seguro puede comparar los bloques de integridad de compartición de cada compartición y a continuación invertir el algoritmo de división. El troceo de los datos recuperados se puede verificar a continuación frente al troceo de compartición.

Tal como se ha mencionado en lo que antecede, en algunas formas de realización de la presente invención, el analizador de datos seguro se puede usar conjuntamente con un sistema de respaldo de cinta. Por ejemplo, se puede usar una cinta individual como un nodo (es decir, porción / compartición) de acuerdo con la presente invención. Cualquier otra disposición adecuada se puede usar. Por ejemplo, una biblioteca o subsistema de cintas, que está compuesto de dos o más cintas, se puede tratar como un único nodo.

Se puede usar también la redundancia con las cintas de acuerdo con la presente invención. Por ejemplo, si un conjunto de datos se reparte entre cuatro cintas (es decir, porciones / comparticiones), entonces dos de las cuatro cintas pueden ser necesarias para restaurar los datos originales. Se entenderá que cualquier número adecuado de nodos (es decir, menos del número total de nodos) se puede requerir para restaurar los datos originales de acuerdo con las características de redundancia de la presente invención. Esto aumenta sustancialmente la probabilidad de restauración cuando expira una o más cintas.

Cada cinta también puede estar protegida de forma digital con un valor de troceo HMAC de SHA-256, cualquier otro valor adecuado, o cualquier combinación de los mismos para asegurar frente a manipulación. Si cambiara algún dato en la cinta o el valor del troceo, esta cinta no sería una candidata para restauración y cualquier número mínimo requerido de cintas de las restantes cintas se usaría para restaurar los datos.

En sistemas de respaldo de cintas convencionales, cuando un usuario solicita que se escriban o se lean datos desde una cinta, el sistema de gestión de cinta (TMS, *tape management system*) presenta un número que se corresponde con un montaje de cinta físico. Esta cinta monta puntos en una unidad física en donde se montarán los datos. La cinta se carga mediante un operador de cintas humano o mediante un robot de cintas en un silo de cintas.

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

Para un rendimiento aumentado de los nodos de cinta se puede usar o incluirse un conjunto de discos RAID que se usa para almacenar imágenes de cinta. Esto permite la restauración a alta velocidad debido a que los datos pueden estar siempre disponibles en el RAID protegido.

En cualquiera de las formas de realización anteriores, los datos que se van a asegurar se pueden distribuir en una pluralidad de comparticiones usando técnicas de distribución de datos determinísticas, probabilísticas o tanto determinísticas como probabilísticas. Para evitar que un atacante comience un ataque criptográfico en cualquier bloque de cifrado, los bits desde los bloques de cifrado se pueden distribuir de manera determinística en las comparticiones. Por ejemplo, la distribución se puede realizar usando la rutina BitSegment, o la rutina BlockSegment se puede modificar para permitir distribución de porciones de bloques a múltiples comparticiones. Esta estrategia puede defender frente a un atacante que ha acumulado menos de “M” comparticiones.

En algunas formas de realización, se puede emplear una rutina de compartición secreta con clave usando dispersión de información con clave (por ejemplo, a través del uso de un algoritmo de dispersión de información con clave o “IDA”). La clave para el IDA con clave se puede proteger también mediante una o más claves de grupo de trabajo externas, una o más claves compartidas, o cualquier combinación de claves de grupo de trabajo y claves compartidas. De esta manera, se puede emplear un esquema de compartición secreta de múltiples factores. Para reconstruir los datos, se pueden requerir al menos “M” comparticiones más la clave o claves de grupo de trabajo (y / o clave o claves compartidas) en algunas formas de realización. El IDA (o la clave para el IDA) se puede introducir también en el proceso de encriptación. Por ejemplo, la transformación se puede introducir en el texto limpio (por ejemplo, durante la capa de preprocesamiento antes de la encriptación) y puede proteger adicionalmente el texto limpio antes de que se encripte.

Por ejemplo, en algunas formas de realización, la dispersión de información con clave se usa para distribuir porciones únicas de datos desde un conjunto de datos en dos o más compartimentos. La dispersión de información con clave puede usar una clave de sesión para encriptar en primer lugar el conjunto de datos, para distribuir porciones únicas de datos encriptados desde el conjunto de datos en dos o más compartimentos de conjuntos de datos encriptados, o tanto encriptar el conjunto de datos como distribuir porciones únicas de datos encriptados desde el conjunto de datos en las dos o más compartimentos de conjunto de datos encriptados. Por ejemplo, para distribuir porciones únicas del conjunto de datos o conjunto de datos encriptados, se puede usar la compartición secreta (o los métodos que se han descrito en lo que antecede, tales como BitSegment o BlockSegment). La clave de sesión se puede transformar a continuación opcionalmente (por ejemplo, usando una transformación de paquete completo o AoNT) y compartirse usando, por ejemplo, compartición secreta (o la dispersión de información con clave y clave de sesión).

En algunas formas de realización, la clave de sesión se puede encriptar usando una clave compartida (por ejemplo, una clave de grupo de trabajo) antes de que se distribuyan o compartan las porciones únicas de la clave en dos o más compartimentos de clave de sesión. A continuación se pueden formar y combinarse dos o más compartimentos de usuario combinando al menos un conjunto de datos encriptados y al menos una compartición de clave de sesión. Al formar una compartición de usuario, en algunas formas de realización, la al menos una compartición de clave de sesión se puede intercalar en una compartición de conjunto de datos encriptados. En otras formas de realización, la al menos una compartición de clave de sesión se puede insertar en una compartición de conjunto de datos encriptados en una localización basada al menos en parte en la clave de grupo de trabajo compartida. Por ejemplo, la dispersión de información con clave se puede usar para distribuir cada compartición de clave de sesión en una compartición de conjunto de datos encriptados única para formar una compartición de usuario. Intercalar o insertar una compartición de clave de sesión en una compartición de conjunto de datos encriptados en una localización basada al menos en parte en el grupo de trabajo compartido puede proporcionar seguridad aumentada frente a los ataques criptográficos. En otras formas de realización, se puede anexar una o más compartimentos de clave de sesión al comienzo o al final de una compartición de conjunto de datos encriptados para formar una compartición de usuario. La colección de compartimentos de usuario se puede almacenar a continuación de manera separada en al menos un depósito de datos. El depósito o depósitos de datos se pueden localizar en la misma localización física (por ejemplo, en el mismo dispositivo de almacenamiento magnético o cinta) o separarse geográficamente (por ejemplo, en servidores físicamente separados en diferentes localizaciones geográficas). Para reconstruir el conjunto de datos original, se puede requerir un conjunto autorizado de compartimentos de usuario y la segunda clave de grupo de trabajo compartida.

La dispersión de información con clave puede ser segura incluso frente a oráculos de recuperación de clave. Por ejemplo, tomando un bloque de cifrado E y una recuperación de clave de oráculo para E que toma una lista (X_1, Y_1), ... , (X_c, Y_c) de pares de entrada / salida en el bloque de cifrado, 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 distinguido $\perp$ si no hay clave coherente. Este oráculo puede modelar un ataque de análisis criptográfico que puede recuperar una clave desde una lista de ejemplos de entrada / salida.

Los esquemas basados en bloques de cifrado convencionales pueden fallar en la presencia de un oráculo de recuperación de clave. Por ejemplo, encriptación de CBC o MAC de CBC se pueden volver completamente inseguras en presencia de un oráculo de recuperación de clave.

Si $\prod^{IDA}$ es un esquema de IDA y $\prod^{Enc}$ es un esquema de encriptación dado por un modo de operación de algún bloque de cifrado E, entonces ($\prod^{IDA}$, $\prod^{Enc}$) proporciona seguridad frente a un ataque de recuperación de clave si los dos esquemas, cuando se combinan con un esquema de compartición secreto perfecto arbitrario (PSS, *perfect secret-sharing*) al igual que para HK1 o HK2, consiguen el objetivo de compartición secreta computacional robusta (RCSS, *robust computational secret sharing*), excepto en el modelo en el que el adversario tiene un oráculo de recuperación de clave.

Si existe un esquema de IDA $\prod^{IDA}$ y un esquema de encriptación $\prod^{Enc}$ de tal modo que el par de esquemas proporciona seguridad frente a ataques de recuperación de clave, entonces una manera de conseguir este par puede ser tener un IDA “listo” y un esquema de encriptación “tonto”. Otra manera para conseguir este par de esquemas puede ser tener un IDA “tonto” y un esquema de encriptación “listo”.

Para ilustrar el uso de un IDA listo y un esquema de encriptación tonto, en algunas formas de realización, el esquema de encriptación puede ser CBC y el IDA puede tener una propiedad de “privacidad débil”. La propiedad de privacidad débil significa, por ejemplo, que si la salida al IDA es una secuencia aleatoria de bloques $M = M_1 ... M_1$ y el adversario obtiene compartimentos desde una colección no autorizada, entonces hay algún índice de bloque i de tal modo que es factible que el adversario calcule M_i. Se puede crear y en primer lugar un IDA débilmente privado de este tipo aplicando a M una información teórica AoNT, tal como AoNT de Stinson, y a continuación aplicar un IDA sencillo tal como BlockSegment, o un IDA eficaz en bits como el esquema de Rabin (por ejemplo, codificación de Reed - Solomon).

Para ilustrar el uso de un IDA tonto y un esquema de encriptación listo, en algunas formas de realización, se puede usar un modo de CBC con doble encriptación en lugar de única encriptación. Ahora se puede usar cualquier IDA, incluso replicación. Tener el oráculo de recuperación de clave para el bloque de cifrado sería inútil para un adversario, ya que se denegaría al adversario cualquier ejemplo de entrada / salida cifrado de manera sencilla.

A pesar de que un IDA listo tiene un valor, puede ser no esencial en algunos contextos, en el sentido que las "inteligencias" necesarias para proporcionar seguridad frente a un ataque de recuperación de clave se podrían haber "impulsado" en cualquier lugar. Por ejemplo, en algunas formas de realización, no importa cuánto de inteligente sea IDA, y para cualquier el objetivo que se está intentando conseguir con el IDA en el contexto de HK1 / HK2, las inteligencias se pueden impulsar fuera del IDA y en el esquema de encriptación, dejarlo fuera con un IDA fijo y tonto.

Basándose en lo que antecede, en algunas formas de realización, se puede usar un IDA $\prod^{IDA}$ listo "universalmente sólido". Por ejemplo, se proporciona un IDA de tal modo que, para todos los esquemas de encriptación $\prod^{Enc}$, el par ($\prod^{IDA}$, $\prod^{Enc}$) proporciona seguridad universalmente frente a ataques de recuperación de clave.

En algunas formas de realización, un esquema de encriptación se proporciona que es RCSS seguro frente a un oráculo de recuperación de clave. El esquema se puede integrar con HK1 / HK2, con cualquier IDA, para conseguir seguridad frente a la recuperación de clave. Usar el nuevo esquema puede ser particularmente útil, por ejemplo, para hacer los esquemas de encriptación simétrica más seguros frente a ataques de recuperación de clave.

Tal como se ha mencionado en lo que antecede, las nociones de compartición secreta clásicas son por lo general sin claves. Por tanto, un secreto se descompone en comparticiones, o se reconstruye desde las mismas, de tal modo que requiere que ni el repartidor ni la parte que reconstruye el secreto mantenga cualquier tipo de clave simétrica o asimétrica. El analizador de datos seguro que se describe en el presente documento, no obstante, opcionalmente está con clave. El repartidor puede proporcionar una clave simétrica que, si se usa para compartición de datos, se puede requerir para recuperación de datos. El analizador de datos seguro puede usar la clave simétrica para dispersar o distribuir porciones únicas del mensaje que se va a asegurar en dos o más comparticiones.

La clave compartida puede posibilitar compartición de secreto de múltiples factores o de dos factores (2FSS, *two-factor secret sharing*). Se puede requerir a continuación al adversario que navegue a través de dos tipos fundamentalmente diferentes de seguridad para romper el mecanismo de seguridad. Por ejemplo, para violar los objetivos de compartición secreta, el adversario (1) puede necesitar obtener las comparticiones de un conjunto de operadores autorizado, *y* (2) puede necesitar obtener una clave secreta que no debería poder obtener (o romper el mecanismo criptográfico que está con clave mediante esa clave).

En algunas formas de realización, se añade un conjunto nuevo de requisitos adicionales al objetivo RCSS. Los requisitos adicionales pueden incluir la posesión de la clave del "segundo factor". Estos requisitos adicionales se pueden añadir sin disminuir 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 suficientes comparticiones (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 se las arregla para obtener soporte de todas las comparticiones (por ejemplo, los requisitos nuevos o de segundo factor).

En algunas formas de realización, puede haber dos requisitos de segundo factor: un requisito de privacidad y un requisito de autenticidad. En el requisito de privacidad, puede estar implicado un juego en donde se selecciona una clave secreta *K* y un bit *b* mediante el entorno. El adversario ahora suministra un par de mensajes de igual longitud en el dominio del esquema de compartición secreta, $M_1^{\ 0}$ y $M_1^{\ 1}$. El entorno calcula las comparticiones de $M_1^{\ b}$ para obtener un vector de comparticiones, $S_1 = (S_1[1], \ldots, S_1[n])$, y proporciona las comparticiones S_1 (todas ellas) al adversario. El adversario puede ahora elegir otro par de mensajes ($M_2^{\ 0}$, $M_2^{\ 1}$) y todo continúa tal como en lo que antecede, usando la misma clave *K* y el bit oculto *b.* El trabajo del adversario es emitir el bit *b'* que cree que es *b.* La ventaja de privacidad del adversario es una menos de dos veces la probabilidad de que *b = b'.* Este juego capta la noción de que, incluso aprendiendo todas las comparticiones, el adversario aún no puede aprender nada acerca del secreto compartido si carece de la clave secreta.

En el requisito de autenticidad, puede estar implicado un juego en donde el entorno elige una clave secreta *K* y usa esta en las posteriores solicitudes de *Compartir* y *Recuperar. Compartir* y *Recuperar* pueden tener su sintaxis modificada, en algunas formas de realización, para reflejar la presencia de esta clave. A continuación el adversario realiza solicitud de *Compartir* para cualquier mensaje $M_1, \ldots, M_q$ que elige en el dominio del esquema de compartición secreto. En respuesta a cada solicitud de *Compartir* obtiene el vector-*n* de comparticiones correspondiente, $S_1, \ldots, S_q$. El objetivo del adversario es *forjar* un nuevo texto plano; gana si emite un vector de comparticiones *S'* de tal modo que, cuando alimenta el algoritmo de *Recuperar*, da como resultado algo que *no* se encuentra en $\{M_1, \ldots, M_q\}$. Esto es una noción de "integridad de texto plano".

Existen dos enfoques para conseguir compartición de secreto de múltiples factores. El primero es un enfoque genérico -- genérico en el sentido de usar un esquema de (R)CSS subyacente en una manera de caja negra. Se usa un esquema de encriptación autenticada para encriptar el mensaje que se ha de compartir por CSS, y a continuación

el texto de cifrado resultante se puede compartir, por ejemplo, usando un algoritmo de compartición secreta, tal como Blakely o Shamir.

Un enfoque potencialmente más eficaz es permitir que la clave compartida sea la clave de grupo de trabajo. En concreto, (1) la clave de sesión generada de forma aleatoria del esquema (R)CSS se puede encriptar usando la clave compartida, y (2) el esquema de encriptación aplicado al mensaje (por ejemplo, el fichero) se puede sustituir por un esquema de encriptación autenticada. Este enfoque puede implicar únicamente una degradación mínima en rendimiento.

A pesar de que algunas aplicaciones del analizador de datos seguro se describen a continuación, se debería entender de manera evidente que la presente invención se puede integrar con cualquier aplicación de red para aumentar la seguridad, la tolerancia a fallos, la anonimidad, o cualquier combinación adecuada de lo anterior.

El analizador de datos seguro de la presente invención se puede usar para implementar una solución de seguridad de datos informáticos en la nube. La informática en la nube es informática basada en red, almacenamiento, o ambos en donde se pueden proporcionar recursos informáticos y de almacenamiento a sistemas informáticos y otros dispositivos a través de una red. Los recursos de la informática en la nube se acceden en general a través de Internet, pero la informática en la nube se puede realizar 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 soporte físico subyacentes (por ejemplo, servidores, dispositivos de almacenamiento, redes), posibilitando acceso remoto a un grupo de recursos informáticos. Estos recursos de la informática en la nube se pueden denominar de manera colectiva como la “nube”. La informática en la nube se puede usar para proporcionar recursos escalables de forma dinámica y a menudo virtualizados como un servicio a través de Internet o cualquier otra red adecuada o combinación de redes.

La seguridad es un asunto importante con la informática en la nube debido a que los datos privados (por ejemplo, desde una red privada de empresas) se pueden transferir a través de redes públicas y se pueden procesar y almacenarse en sistemas públicamente accesibles o compartidos (por ejemplo, Google (por ejemplo, Google Apps Storage), Dropbox, o Amazon (por ejemplo, instalación de almacenamiento de Amazon S3)). Estos sistemas públicamente accesibles no proporcionan necesariamente espacio de almacenamiento encriptado, no obstante, proporcionan al usuario con la capacidad de almacenar un conjunto de ficheros en sus servidores. El analizador de datos seguro se puede usar para proteger los recursos de informática en la nube y los datos que se comunican entre la nube y un usuario final o dispositivo. Por ejemplo, el analizador de datos seguro se puede usar para almacenamiento de datos seguro en la nube, datos en movimiento a / desde la nube, acceso de 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 en la nube informática. El sistema 4200, que incluye el analizador de datos seguro 4210, está acoplado a la nube 4250 que incluye los recursos de la nube 4260. El sistema 4200 puede incluir cualquier soporte físico adecuado, tal como un terminal informático, un ordenador personal, un dispositivo portátil (por ejemplo, un PDA, una Blackberry, un teléfono inteligente, un dispositivo de tipo tableta), un teléfono celular, una red informática, cualquier otro soporte físico adecuado o cualquier combinación de los mismos. El analizador de datos seguro 4210 se puede integrar en cualquier nivel adecuado del sistema 4200. Por ejemplo, analizador de datos seguro 4210 se puede integrar en el soporte físico y / o soporte lógico del sistema 4200 en un nivel suficientemente de fondo de tal modo que la presencia del analizador de datos seguro 4210 puede ser sustancialmente transparente para un usuario final del sistema 4200. La integración del analizador de datos seguro en sistemas adecuados se ha descrito en mayor detalle en lo que antecede con respecto a, por ejemplo, las figuras 27 y 28. La nube 4250 incluye múltiples recursos de la nube ilustrativos 4260 que incluye, los recursos de almacenamiento de datos 4260a y 4260e, los recursos de servicios de datos 4260b y 4260g, recursos de control de acceso de red 4260c y 4260h, y recursos informáticos de alto rendimiento 4260d y 4260f. Los recursos de la nube se pueden proporcionar mediante una pluralidad de proveedores de recursos de la nube, por ejemplo, Amazon, Google o Dropbox. Cada uno de estos recursos de informática en la nube se describirá en mayor detalle a continuación respecto a las figuras 43 - 56. Estos recursos de informática en la nube son meramente ilustrativos. Se debería entender que cualquier número adecuado y tipo de recursos de informática en la nube pueden ser accesibles desde el sistema 4200.

Una ventaja de la informática en la nube es que el usuario del sistema 4200 puede poder acceder a múltiples recursos de informática en la nube sin tener que invertir en soporte físico de almacenamiento especializado. El usuario puede tener la capacidad de controlar de forma dinámica el número y tipo de los recursos de informática en la nube accesibles para el sistema 4200. Por ejemplo, el sistema 4200 se puede proporcionar con recursos de almacenamiento a petición en la nube que tienen capacidades que son ajustables de forma dinámica basándose en las necesidades actuales. En algunas formas de realización, una o más aplicaciones de soporte lógico ejecutadas en el sistema 4200 pueden acoplar el sistema 4200 a recursos de la nube 4260. Por ejemplo, se puede usar un explorador web de Internet para acoplar el sistema 4200 a uno o más recursos en la nube 4260 a través de Internet. En algunas formas de realización, el soporte físico integrado con o conectado al sistema 4200 puede acoplar el sistema 4200 a recursos de la nube 4260. En ambas formas de realización, el analizador de datos seguro 4210 se

puede comunicar de manera segura con los recursos de la nube 4260 y / o los datos almacenados en los recursos de la nube 4260. El acoplamiento de los recursos de la nube 4260 al sistema 4200 puede ser transparente para el sistema 4200 o los usuarios del sistema 4200 de tal modo que los recursos de la nube 4260 aparezcan para el sistema 4200 como recursos de soporte físico locales. Además, pueden aparecer recursos de la nube 4260 compartidos para el sistema 4200 como recursos de soporte físico especializado.

En algunas formas de realización, el analizador de datos seguro 4210 puede encriptar y dividir datos de tal modo que ningún dato discernible de manera forense atravesará o se almacenarán en la nube. Los componentes soporte físico subyacentes de la nube (por ejemplo, servidores, dispositivos de almacenamiento, redes) se pueden distribuir geográficamente para asegurar la continuidad de los recursos de la nube en caso de un fallo de la red eléctrica, evento climático u otro evento hecho por el hombre o natural. Como resultado, incluso si alguno de los componentes del soporte físico en la nube sufre un fallo catastrófico, los recursos de la nube pueden seguir estando accesibles. Los recursos de la nube 4260 se pueden diseñar con redundancia para proporcionar servicio ininterrumpido a pesar de uno o más fallos de soporte físico.

En algunas formas de realización, el analizador seguro de la presente invención puede aleatorizar en primer lugar los datos originales y a continuación dividir los datos de acuerdo con una técnica aleatorizada o determinística. Por ejemplo, si se aleatoriza en el nivel de bits, el analizador seguro de la presente invención puede mezclar los bits de datos originales de acuerdo con una técnica aleatorizada (por ejemplo, de acuerdo con una clave de sesión aleatoria o pseudoaleatoria) para formar una secuencia de bits aleatorizados. El analizador seguro puede a continuación dividir los bits en un número predeterminado de comparticiones mediante cualquier técnica adecuada (por ejemplo, un algoritmo de dispersión de información (IDA, *information dispersal algorithm*) adecuado) tal como se ha analizado en lo que antecede.

La figura 43 es un diagrama de bloques ilustrativo de una solución de seguridad de informática en la nube para asegurar datos en movimiento (es decir, durante la transferencia de datos desde una localización a otra) a través de la nube. La figura 43 muestra un sistema de emisión 4300, que puede incluir cualquier soporte físico adecuado, tal como un terminal informático, un ordenador personal, un dispositivo portátil (por ejemplo, un PDA, una Blackberry), un teléfono celular, una red informática, cualquier otro soporte físico adecuado o cualquier combinación de los mismos. El sistema de emisión 4300 se usa para generar y / o almacenar datos, que pueden ser, por ejemplo, un mensaje de correo electrónico, un fichero de datos binarios (por ejemplo, gráficos, voz, vídeo, etc.), o ambos. Los datos se analizan y dividen mediante el analizador de datos seguro 4310 de acuerdo con la presente invención. Las porciones resultantes de datos se pueden comunicar a través de la nube 4350 al sistema de recepción 4370.

La nube 4350 puede incluir cualquier combinación adecuada de almacenamiento en la nube público y privado mostrado de manera ilustrativa como las nubes 4350a, 4350b y 4350c. Por ejemplo, las nubes 4350a y 4350c pueden ser recursos de almacenamiento en la nube que son públicamente accesibles, tales como los proporcionados mediante Amazon, Google o Dropbox. La nube 4350b puede ser una nube privada que es inaccesible a cualquier individuo o grupo fuera de una organización particular, por ejemplo, una empresa o una institución educacional. En otras formas de realización, una nube podría ser un híbrido de una nube pública y privada.

El sistema de recepción 4370 del sistema 4300 puede ser cualquier soporte físico adecuado tal como se ha descrito en lo que antecede con respecto al sistema de emisión 4300. Las porciones de datos separadas se pueden recombinar en el sistema de recepción 4370 para generar los datos originales de acuerdo con la presente invención. Cuando viajan a través de la nube 4310 las porciones de datos se pueden comunicar a través de una o más trayectorias de comunicaciones incluyendo Internet y / o una o más intranets, LAN, WiFi, Bluetooth, cualquier otras redes de comunicaciones de cableado permanente o inalámbricas adecuadas, o cualquier combinación de las mismas. Tal como se ha descrito en lo que antecede con respecto a las figuras 28 y 29, los datos originales se aseguran mediante el analizador de datos seguro incluso si algunas de las porciones de datos están comprometidas.

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 forma de realización, un usuario 4400 puede proporcionar servicios de datos 4420 a un usuario final 4440 a través de la nube 4430. El analizador seguro 4410 puede asegurar los servicios de datos de acuerdo con las formas de realización que se divulgan. El servicio de datos 4420 puede ser cualquier aplicación o servicio de soporte lógico adecuado que es accesible a través de la nube 4430. Por ejemplo, el servicio de datos 4420 puede ser una aplicación basada en web implementada como parte de un sistema de arquitectura orientada a servicio (SOA, *service-oriented architecture*). El servicio de datos 4420 se puede almacenar y ejecutarse en uno o más sistemas en la nube 4430. La abstracción proporcionada mediante esta implementación informática en la nube permite al servicio de datos 4420 aparecer como un recurso virtualizado para el usuario final 4440 con independencia de los recursos de soporte físico subyacentes. El analizador seguro 4410 puede asegurar datos en movimiento entre el servicio de datos 4420 y usuario final 4440. El analizador seguro 4410 puede asegurar también datos almacenados que están asociados con el servicio de datos 4420. Los datos almacenados que están asociados con el servicio de datos 4420 se pueden asegurar en el sistema o sistemas que implementan el servicio de datos 4420 y / o en dispositivos de almacenamiento en la nube seguros separados, que se describirán en mayor

detalle a continuación. A pesar de que el servicio de datos 4420 y otras porciones de la figura 44 se muestran fuera de la nube 4430, se debería entender que cualquiera de estos elementos se puede incorporar 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 el analizador de datos seguro 4510, está acoplado a la nube 4550 que incluye los recursos de almacenamiento de datos 4560. El analizador de datos seguro 4510 se puede usar para analizar y dividir datos entre uno o más recursos de almacenamiento de datos 4560. Cada recurso de almacenamiento de datos 4560 puede representar a uno o más dispositivos de almacenamiento en red. Estos dispositivos de almacenamiento se pueden asignar a un único usuario / sistema que se puede compartir mediante múltiples usuarios / sistemas. La seguridad proporcionada mediante el analizador de datos seguro 4510 puede permitir que coexistan de manera segura datos desde múltiples usuarios / sistemas en los mismos dispositivos de almacenamiento o recursos de proveedores de almacenamiento en la nube. La abstracción proporcionada mediante esta implementación de informática en la nube permite a los recursos de almacenamiento de datos 4560 aparecer como un único recurso de almacenamiento virtualizado para el sistema 4500 con independencia del número y localización de los recursos de almacenamiento de datos subyacentes. Cuando se escriben o leen datos desde los recursos de almacenamiento de datos 4560, el analizador de datos seguro 4510 puede dividir y recombinar los datos de una manera que pueden ser transparentes para el usuario final. De esta manera, un usuario final puede poder acceder a almacenamiento escalable de forma dinámica a petición.

El almacenamiento de datos en la nube usando el analizador de datos seguro 4510 es seguro, resistente, persistente, y privado. El analizador de datos seguro 4510 asegura los datos asegurando que no atraviesan datos discernibles de manera forense en la nube o se almacenan en un único dispositivo de almacenamiento. El sistema de almacenamiento en la nube es resistente debido a la redundancia ofrecida mediante el analizador de datos seguro (es decir, son necesarias menos de todas las porciones de los datos separadas para reconstruir los datos originales). Almacenar las porciones separadas en múltiples dispositivos de almacenamiento y / o en múltiples recursos de almacenamiento de datos 4560 asegura que los datos se puedan reconstruir incluso si uno o más de los dispositivos de almacenamiento falla o está inaccesible. El sistema de almacenamiento en la nube es persistente debido a que la pérdida de un dispositivo de almacenamiento en los recursos de almacenamiento de datos 4560 no tiene impacto en el usuario final. Si un dispositivo de almacenamiento falla, las porciones de datos que se almacenaron en ese dispositivo de almacenamiento se pueden reconstruir en otro dispositivo de almacenamiento sin tener que exponer los datos. Además, los recursos de almacenamiento 4560 (o incluso los múltiples dispositivos de almacenamiento en red que componen un recurso de almacenamiento de datos 4560) pueden estar dispersados 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. Tal como se ha descrito en lo que antecede, los datos se pueden asignar a un usuario o a una comunidad de interés mediante claves únicas de tal modo que únicamente ese usuario o comunidad tendrán acceso a los datos.

El almacenamiento de datos en la nube usando el analizador de datos seguro puede proporcionar también un aumento del rendimiento sobre el almacenamiento local tradicional o en red. El rendimiento del sistema se puede mejorar escribiendo y leyendo porciones de datos separadas en múltiples dispositivos de almacenamiento en paralelo. Este aumento en rendimiento puede permitir que se usen dispositivos de almacenamiento menos caros sin afectar sustancialmente la velocidad global del sistema de almacenamiento.

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

Además de proporcionar seguridad para datos en reposo almacenados en una red de comunicaciones y seguridad para datos en movimiento a través de la red de comunicaciones, el bloque de control de acceso de red 4620 se puede usar con el analizador de datos seguro 4620 para compartir información entre diferentes grupos de usuarios o comunidades de interés. Los grupos de colaboración se pueden establecer para participar como comunidades seguras de interés en redes virtuales seguras. Se puede implantar una clave de grupo de trabajo a miembros de grupo para proporcionar a los miembros del grupo acceso a la red y recursos en red. Los sistemas y métodos para implantaciones de clave de grupo de trabajo se han analizado en lo que antecede.

La figura 47 es un diagrama de bloques ilustrativo para asegurar acceso a recursos informáticos de alto rendimiento usando un analizador de datos seguro de acuerdo con las formas de realización que se divulgan. El analizador de datos seguro 4710 se puede usar para proporcionar acceso seguro a recursos informáticos de alto rendimiento 4720. Tal como se ilustra en la figura 47 el usuario final 4740 puede acceder a recursos informáticos de alto rendimiento 4720. En algunas formas de realización, el analizador de datos seguro 4710 puede proporcionar acceso seguro a recursos de alto rendimiento en la nube (por ejemplo, la nube 4250, Figura 42). Los recursos informáticos de alto rendimiento pueden ser grandes servidores informáticos o granjas de servidores. Estos recursos informáticos de alto rendimiento pueden proporcionar servicios de datos flexibles, escalables y configurables y servicios de almacenamiento de datos a los usuarios.

El analizador de datos seguro de la presente invención puede configurase para implementar una solución de datos segura basada en servidor. La solución basada en servidor del analizador seguro de la presente invención se refiere a una solución de Datos en Reposo (DAR, *Data at Rest*) basada en servidor de fondo. El servidor puede ser cualquiera basado en Windows, basado en Linux, basado en Solaris, o cualquier otro sistema operativo adecuado. Esta solución basada en servidor presenta un sistema de ficheros transparente para un usuario, es decir, un usuario no observa ninguna indicación de las divisiones de datos. Cuando los datos se presentan al servidor de fondo del analizador de datos seguro de la presente invención, los datos se dividen en N comparticiones y se envían a N localizaciones de almacenamiento de datos accesibles (por lo tanto, disponibles) montadas / conectadas al servidor. No obstante, únicamente se requiere algún número M de estas comparticiones para reconstruir los datos. En algunas formas de realización, la solución basada en servidor del analizador seguro de la presente invención puede aleatorizar en primer lugar los datos originales y a continuación dividir los datos de acuerdo con cualquiera de una técnica aleatorizada o determinística. Por ejemplo, si se aleatoriza en el nivel de bits, el analizador seguro de la presente invención puede mezclar los bits de datos originales de acuerdo con una técnica aleatorizada (por ejemplo, de acuerdo con una clave de sesión aleatoria o pseudoaleatoria) para formar una secuencia de bits aleatorizados. La solución basada en servidor del analizador seguro de la presente invención puede a continuación dividir los bits en un número predeterminado de comparticiones mediante cualquier técnica adecuada (por ejemplo, orden cíclico) tal como se ha analizado en lo que antecede. Para las formas de realización de las figuras 42 - 47 anteriores, y las formas de realización de las figuras a continuación, se supondrá que el analizador seguro de la presente invención puede dividir en primer lugar los datos de acuerdo con cualquier técnica aleatorizada o determinística. Además, en las formas de realización que se describen a continuación, la división de datos puede incluir dividir datos usando cualquier algoritmo de dispersión de información (IDA, *information dispersal algorithm*) adecuado, incluyendo orden cíclico o división de bits aleatoria, tal como se ha descrito en lo que antecede.

Las soluciones que se han descrito en lo que antecede posibilitan la recuperación de datos desde almacenamiento local o almacenamiento remoto tal como nubes únicas y múltiples debido a que los datos se pueden reconstruir desde cualquiera de M de las N comparticiones de datos, incluso cuando los datos se aleatorizan en primer lugar y a continuación se dividen de acuerdo con cualquiera de una técnica aleatorizada o determinística. Las descripciones adicionales de la solución basada en servidor del analizador seguro de la presente invención se proporcionan a continuación, en particular con respecto a las figuras 48 - 56. En algunas formas de realización, la solución basada en servidor se puede usar en conjunto con las formas de realización de informática en la nube que se han descrito en lo que antecede con respecto a las figuras 42 - 47.

En las formas de realización de las figuras 48 - 50, las formas de realización de la solución basada en servidor del analizador seguro de la presente invención se describirán en relación con su implementada en conexión con nubes públicas (por ejemplo, Dropbox), así como otras nubes privadas, públicas e híbridas o recursos informáticos en la nube.

La figura 48 es un diagrama esquemático de una disposición ilustrativa en la que se usa el analizador de datos seguro para almacenamiento de datos seguro en una pluralidad de dispositivos de almacenamiento en una nube privada y una pública de acuerdo con una forma de realización de la presente invención. La nube privada 4804 incluye un procesador 4808 que está configurado para implementar la solución basada en servidor de un analizador seguro de la presente invención y generar comparticiones de datos encriptadas 4816b, 4818b, 4814b, 4812b, 4820b y 4822b. La nube privada 4804 puede ser opcionalmente accesible, por ejemplo, mediante una conexión de Internet, para un dispositivo de usuario final 4800. Los usuarios remotos pueden acceder a sus datos almacenados en la nube privada 4804 mediante el dispositivo de usuario final 4800, y pueden transmitir también comandos relacionados con la generación y gestión de compartición de datos desde el dispositivo de usuario final 4800 al procesador 4804 de la nube 4804. Un subconjunto de estas comparticiones de datos encriptadas se almacenan en dispositivos de almacenamiento en la nube privada 4804. En particular, la compartición de datos 4814b se almacena en el dispositivo de almacenamiento 4814a, mientras que la compartición de datos 4812b se almacena en el dispositivo de almacenamiento 4812a. El procesador 4808 está también configurado para almacenar otros subconjuntos de las comparticiones de datos encriptadas en otras nubes públicas, privadas o híbridas 4802, 4806, o 4810. Por ejemplo, la nube 4806 puede incluir recursos en la nube públicos proporcionados mediante Amazon, mientras que la nube 4802 puede incluir recursos en la nube públicos proporcionados mediante Dropbox. En esta forma de realización ilustrativa, las comparticiones 4818b y 4816b se almacenan en los dispositivos de almacenamiento 4818a y 4816a, de forma respectiva, en la nube 4802, la compartición 4822b se almacena en el dispositivo de almacenamiento 4822a en la nube 4806, y la compartición 4820b se almacena en el dispositivo de

almacenamiento 4820a en la nube 4810. De esta manera, el proveedor de la nube privada 4804 puede aprovechar los recursos de almacenamiento de los otros proveedores de almacenamiento en la nube para almacenar compartimentos de datos, reduciendo de esta manera la carga de almacenamiento en los dispositivos de almacenamiento con la nube 4804. El analizador seguro de la nube privada 4804 asegura datos de forma simultánea al tiempo que proporciona supervivencia contra desastres de datos robusta debido a que únicamente M de N compartimentos analizadas se requerirán para reconstruir los datos, en donde M < N. Por ejemplo, si el acceso a una de las nubes pública o privada 4806, 4810, o 4802 se interrumpe o pierde, se puede acceder aún a los datos y recuperarse usando el subconjunto disponible de compartimentos de datos encriptadas. En general, únicamente M de N compartimentos analizadas se requerirán para reconstruir los datos, en donde M < N. Por ejemplo, si el acceso a una de las nubes pública o privada 4806, 4810, o 4802 se interrumpe o pierde, se puede acceder aún a los datos y recuperarse usando el subconjunto disponible de compartimentos de datos encriptadas. Como un ejemplo ilustrativo adicional, si un recurso de almacenamiento en una o más de las nubes públicas o privadas 4806, 4810, o 4802 está caído o se encuentra por lo demás inaccesible, se puede acceder aún a los datos y recuperarse usando el subconjunto accesible de las compartimentos de datos encriptadas en la nube o nubes.

La figura 49 es un diagrama esquemático de una disposición ilustrativa en la que se usa el analizador de datos seguro para almacenamiento de datos seguro en una pluralidad de nubes privadas y públicas similar a la disposición de la figura 48, de acuerdo con una forma de realización de la presente invención. La figura 49 ilustra una nube privada 4904 que está acoplada, por ejemplo, mediante una conexión de Internet, a un dispositivo de usuario final tal como el portátil 4902, y a nubes públicas 4906 y 4908, por ejemplo, mediante una conexión de Internet. Las nubes públicas incluyen recursos de almacenamiento en la nube que son públicamente accesibles, tales como los proporcionados por Dropbox y Amazon (por ejemplo, la instalación de almacenamiento de Amazon S3). Las conexiones de Internet que se han descrito en lo que antecede pueden ser seguras o inseguras. En la forma de realización ilustrativa de la figura 49, la nube pública 4906 se proporciona mediante Dropbox, mientras que la nube pública 4908 se proporciona mediante Amazon. Los datos desde el dispositivo de usuario final 4902 se pueden transmitir a la nube privada 4904. El procesador 4905 de la nube privada 4904 se puede configurar para implementar la solución basada en servidor de un analizador seguro de la presente invención y generar las compartimentos de datos encriptadas 4910a, 4910b, 4910c y 4910d. Las compartimentos 4910a y 4910b se almacenan en dispositivos de almacenamiento en la nube privada 4904, mientras que las compartimentos 4910c y 4910d se transmiten a y se almacenan en las nubes públicas 4906 y 4908, de forma respectiva. Al igual que con la disposición de la figura 48, el proveedor de la nube privada 4904 puede aprovechar los recursos de almacenamiento de los otros proveedores de almacenamiento en la nube para almacenar compartimentos de datos, reduciendo de esta manera la carga de almacenamiento en los dispositivos de almacenamiento con la nube 4904. El analizador seguro de la nube privada 4904 asegura datos de forma simultánea al tiempo que proporciona supervivencia contra desastres de datos robusta debido a que únicamente M de N compartimentos analizadas se requerirán para reconstruir los datos, en donde M < N. Por ejemplo, si el acceso a una de las nubes pública o privada 4906 o 4908 se interrumpe o pierde, se puede acceder aún a los datos y recuperarse usando el subconjunto disponible de compartimentos de datos encriptadas.

La figura 50 es un diagrama esquemático de otra disposición ilustrativa en la que se usa el analizador de datos seguro para almacenamiento de datos seguro en una pluralidad de nubes privadas y públicas mediante Internet 5006 de acuerdo con una forma de realización de la presente invención. En la disposición de la figura 50, similar a la de las figuras 48 y 49, un dispositivo de usuario final 5002 está acoplado a una nube privada 5008 mediante Internet accesible públicamente 5006. La nube privada 5008 incluye un procesador 5001 que está configurado para implementar la solución basada en servidor del analizador seguro de la presente invención y generar dos conjuntos de compartimentos de datos encriptados: 5014a - d y 5016a - d. Algunas de estas compartimentos de datos encriptados se almacenan en el mismo dispositivo de almacenamiento, por ejemplo, las compartimentos 5014b y 5016a, y las compartimentos 5014c y 5016b, mientras que otras compartimentos se almacenan en diferentes dispositivos de almacenamiento, por ejemplo, las compartimentos 5016c y 5016d. Las compartimentos 5014a y 5014d se transmiten a y se almacenan en las nubes públicas 5010 y 5012, de forma respectiva, proporcionadas mediante los proveedores de almacenamiento en la nube públicos Google, Amazon, y Dropbox, que se han descrito en lo que antecede, de forma respectiva. Al igual que con la disposición de las figuras 48 y 49, el proveedor de la nube privada 5008 puede aprovechar los recursos de almacenamiento de los otros proveedores de almacenamiento en la nube para almacenar compartimentos de datos, reduciendo de esta manera la carga de almacenamiento en los dispositivos de almacenamiento en la nube privada 5008. El analizador seguro de la nube privada 5008 por lo tanto asegura datos de forma simultánea al tiempo que proporciona supervivencia contra desastres de datos robusta debido a que únicamente M de N compartimentos analizadas se requerirán para reconstruir los datos, en donde M < N. Por tanto, si el acceso a una de las nubes pública o privada 5010 o 5012 se interrumpe o pierde, se puede acceder aún a los datos y recuperarse usando el subconjunto disponible de compartimentos de datos encriptadas. En algunas formas de realización, se puede requerir un dispositivo de almacenamiento extraíble tal como la clave de acceso de USB 5004 en el dispositivo de usuario final 5002 para autenticar la identidad de un usuario remoto que desea ver, encriptar, o desencriptar datos que se gestionan mediante el procesador 5001 de la nube privada 5008. En algunas formas de realización, un dispositivo de almacenamiento extraíble tal como un testigo de USB 5004 se puede requerir en el dispositivo de usuario final 5002 para iniciar la encriptación, desencriptación o división de datos mediante el procesador 5001 de la nube privada 5008. En algunas formas de realización, los datos se dividen usando cualquier algoritmo de dispersión de información (IDA, *information dispersal algorithm*) adecuado. En

algunas formas de realización, en primer lugar se aleatorizan los datos antes de la división. En algunas formas de realización, un usuario puede gestionar sus claves criptográficas por sí mismo. En estas formas de realización, las claves de un usuario se pueden almacenar en un dispositivo final del usuario tal como un testigo de USB 5004 o dispositivo de usuario final 5002. En otras formas de realización, se puede usar cualquier sistema de gestión de claves centralizado o dispersado adecuado para gestionar unas claves criptográficas de grupos de trabajo.

En algunas formas de realización, para permitir la visualización y / o reconstrucción de datos en cada una de una pluralidad de distintos dispositivos de usuario final, se pueden almacenar una o más claves criptográficas y / o una o más comparticiones de datos en el dispositivo de memoria de USB 5004. Además, se pueden almacenar también uno o más de las comparticiones de datos en una nube 5010 y / o 5012. Por tanto, un usuario en posesión del dispositivo de usuario portátil puede acceder al dispositivo de memoria de USB 5004 desde un dispositivo de usuario final diferente al dispositivo 5002 para ver y / o reconstruir los datos desde las comparticiones dispersadas a través del dispositivo de memoria de USB 5004 y si fuera necesario, la nube. Por ejemplo, se pueden almacenar dos comparticiones de datos en el dispositivo de memoria de USB 5004 y se pueden almacenar dos comparticiones de datos en cada una de las nubes 5010 y 5012. Un usuario en posesión de un dispositivo de memoria de USB 5004 puede usar cualquier dispositivo informático con el analizador seguro de la presente invención acoplado al dispositivo de memoria de USB 5004 para acceder a las dos comparticiones de datos almacenadas en el dispositivo 5004. Por ejemplo, un usuario puede usar un primer ordenador portátil para crear y dispersar las comparticiones a través del dispositivo de memoria de USB 5004 y la nube, y puede a continuación usar un segundo diferente ordenador portátil para recuperar las comparticiones desde el dispositivo de memoria de USB 5004 y / o las nubes 5010 y 5012, y a continuación reconstruir / recrear los datos desde las comparticiones recuperadas.

En algunas formas de realización, el analizador seguro de la presente invención puede proporcionar confidencialidad, disponibilidad e integridad de los datos almacenados asegurando que unos datos perdidos o de dispositivo robado permanecen seguros e indescifrables. En algunas formas de realización, la presente invención puede incluir soporte lógico que se ejecuta en el nivel de núcleo en segundo plano de cualquier PC o dispositivo de usuario final posibilitado con Windows o Linux (por ejemplo, un teléfono móvil, un ordenador portátil, un ordenador personal, un ordenador de tipo tableta, un teléfono inteligente, un decodificador de salón, etc.). En algunas formas de realización, un analizador seguro tal como FIPS 140-2 certificado, compatible con Suit B, SecureParser Extended (SPχ) de Security First Corp. se puede usar para dividir los datos que se van a asegurar. En algunas formas de realización, se realiza encriptación de FIPS 140-2 AES 256, división de datos de bits aleatoria, comprobación de integridad y reencriptación de las comparticiones de división. En algunas formas de realización, los datos se dividen usando cualquier algoritmo de dispersión de información (IDA, *information dispersal algorithm*) adecuado. En algunas formas de realización, la división es determinística. En algunas formas de realización, los datos se pueden aleatorizar también antes de la división. En algunas formas de realización, cualquier fichero almacenado en una localización segura (por ejemplo la unidad “C:”) en un dispositivo final del usuario son invisibles sin las credenciales y acceso apropiados. En algunas formas de realización, incluso los nombres de fichero no se pueden ver o recuperarse sin la clave criptográfica y proceso de autenticación requeridos.

En algunas formas de realización, se crea un conjunto de N comparticiones y el analizador seguro de la presente invención almacena estas N comparticiones en N localizaciones de almacenamiento separadas posiblemente dispersadas geográficamente. Por ejemplo, se pueden crear cuatro (4) comparticiones encriptadas y el analizador seguro de la presente invención a continuación almacena estas cuatro comparticiones encriptadas en cuatro (4) localizaciones de almacenamiento separadas. Las figuras 51 - 53 ilustran dos de tales formas de realización, que se crean cuatro comparticiones encriptadas, del analizador seguro de la presente invención.

La figura 51 es un diagrama esquemático de una disposición ilustrativa en la que se usa el analizador de datos seguro para almacenamiento de datos seguro en un dispositivo de almacenamiento extraíble del usuario 5104 y en el dispositivo de almacenamiento masivo 5106 de acuerdo con una forma de realización de la presente invención. La figura 51 muestra un dispositivo de usuario final tal como un ordenador portátil 5102 que ha generado cuatro comparticiones encriptadas 5108a, 5108b, 5108c y 5108d. Cada una de estas comparticiones encriptadas 5108a - d se almacena en un sector de almacenamiento diferente en el almacenamiento masivo 5106 del dispositivo de usuario final 5102. El analizador seguro del dispositivo de usuario final asegura datos de forma simultánea al tiempo que proporciona supervivencia contra desastres de datos robusta debido a que únicamente M de N comparticiones analizadas se requerirán para reconstruir los datos, en donde M < N. En la forma de realización de la figura 51, hay 4 comparticiones, y 2 o 3 de estar comparticiones se requerirían para reconstruir los datos. Suponiendo que únicamente dos de las cuatro, o tres de las cuatro, comparticiones encriptadas se requieren para reconstruir los datos, el proceso de recuperación de desastres se acelera si se pierde una o dos de las comparticiones encriptadas, por ejemplo, si uno de los sectores del almacenamiento masivo 5106 está corrupto. El dispositivo de almacenamiento extraíble 5104 se puede usar almacenar una o más claves de acceso criptográfico que se pueden requerir para ver y / o desencriptar y / o encriptar datos en el almacenamiento masivo 5106 del dispositivo de usuario final 5102. En algunas formas de realización, sin la clave criptográfica en el dispositivo de almacenamiento extraíble 5104, las comparticiones de datos encriptados 5108a - d no se pueden desencriptar y / o reconstruirse. En algunas formas de realización, un usuario puede gestionar sus propias claves criptográficas. En estas formas de realización, se pueden almacenar unas claves del usuario en un dispositivo final del usuario tal como el dispositivo de almacenamiento extraíble (por ejemplo, memoria de USB) 5104 o dispositivo de usuario final 5102. En otras formas

de realización, cualquier sistema de gestión de claves centralizado o dispersado adecuado se puede usar para gestionar unas claves criptográficas del usuario o grupos de trabajo.

En algunas formas de realización, para permitir visualización y / o reconstrucción de datos en cada uno de una pluralidad de distintos dispositivos de usuario final, se puede almacenar una o más claves criptográficas y / o una o más comparticiones de datos en el dispositivo de memoria de USB 5104. Además, una o más de las comparticiones de datos se pueden almacenar también en una nube. Por tanto, un usuario en posesión del dispositivo de usuario portátil puede acceder al dispositivo de memoria de USB 5104 desde un dispositivo de usuario final diferente al dispositivo 5102 para ver y / o reconstruir los datos desde las comparticiones dispersadas a través del dispositivo de memoria de USB 5104 y si fuera necesario, la nube. Por ejemplo, se pueden almacenar dos comparticiones de datos en el dispositivo de memoria de USB 5104 y se pueden almacenar dos comparticiones de datos en el dispositivo de usuario final 5102. Un usuario en posesión del dispositivo de memoria de USB 5104 puede usar cualquier dispositivo informático con el analizador seguro de la presente invención acoplado al dispositivo de memoria de USB 5104 para acceder a las dos comparticiones de datos almacenadas en el dispositivo de memoria de USB 5104. Por ejemplo, un usuario puede usar un primer ordenador portátil para crear y dispersar las comparticiones a través del dispositivo de memoria de USB 5104 y el dispositivo de usuario final 5102, y puede a continuación usar un segundo ordenador portátil diferente para recuperar las comparticiones desde el dispositivo de memoria de USB 5104 y, suponiendo que estas dos comparticiones son suficientes para reconstruir los datos, reconstruir / recrear los datos desde estas dos comparticiones.

La figura 52 es un diagrama esquemático de una disposición ilustrativa en la que se usa el analizador de datos seguro para almacenamiento de datos seguro en una pluralidad de dispositivos de almacenamiento de usuario de acuerdo con una forma de realización de la presente invención. La figura 52 muestra un dispositivo de usuario final tal como un ordenador portátil 5202 que ha generado cuatro comparticiones encriptadas 5208a, 5208b, 5208c y 5208d. Cada una de estas comparticiones encriptadas 5208a - d se almacena en la localización de almacenamiento dispersada geográficamente y / o diferentes partes de la misma localización de almacenamiento. En particular, las comparticiones encriptadas 5208c y 5208d se almacenan en dos sectores diferentes en el dispositivo de almacenamiento masivo 5206 del ordenador portátil 5202, mientras que las comparticiones encriptadas 5308a y 5308b se almacena cada una en un dispositivo de almacenamiento extraíble tal como el dispositivo de memoria de USB 5204. El analizador seguro del dispositivo de usuario final asegura datos de forma simultánea al tiempo que proporciona supervivencia contra desastres de datos robusta debido a que únicamente M de N comparticiones analizadas se requerirán para reconstruir los datos, en donde M < N. En la forma de realización de la figura 52, hay 4 comparticiones, y 2 o 3 de estar comparticiones se requerirían para reconstruir los datos. Por tanto, las comparticiones encriptadas están geográfica y físicamente dispersadas, y suponiendo que únicamente dos de las cuatro, o tres de las cuatro comparticiones encriptadas se requieren para reconstruir los datos, el proceso de recuperación de desastres se acelera si se pierde una o dos de las comparticiones encriptadas. Una pérdida de este tipo puede tener lugar, por ejemplo, si uno de los sectores del almacenamiento masivo 5202 está corrupto, o si el dispositivo de almacenamiento extraíble tal como el dispositivo de memoria de USB 5204 se pierde, o cualquier combinación de los mismos.

En algunas formas de realización, en lugar de o además de almacenar las comparticiones encriptadas en el dispositivo de memoria de USB 5204, una o más claves (por ejemplo, la clave de encriptación, la clave de división, o la clave de autenticación) se almacenan en el dispositivo de memoria de USB 5204. Estas claves se pueden usar para dividir, encriptar / desencriptar, o autenticar comparticiones de datos almacenadas en el propio dispositivo de memoria de USB 5204, o en otra parte, por ejemplo, en el almacenamiento masivo de dispositivo de usuario final 5202 o en un almacenamiento en la nube pública o privada. Por ejemplo, un usuario puede almacenar una clave en el dispositivo de memoria de USB 5204 y usar esta clave para desencriptar comparticiones de datos encriptadas almacenadas en el dispositivo de almacenamiento masivo 5202. Como un ejemplo ilustrativo adicional, se pueden almacenar dos comparticiones de datos en el dispositivo de memoria de USB 5204 y se pueden almacenar dos comparticiones de datos en el dispositivo de usuario final almacenamiento masivo 5202. Un usuario en posesión del dispositivo de memoria de USB 5204 puede usar cualquier dispositivo informático con el analizador seguro de la presente invención acoplado al dispositivo de memoria de USB 5204 para acceder a la clave almacenada en el dispositivo de memoria de USB 5204. Por ejemplo, un usuario puede usar un primer ordenador portátil para almacenar la clave en el dispositivo de memoria de USB 5204, y puede usar a continuación un segundo ordenador portátil diferente para recuperar la clave desde el dispositivo de memoria de USB 5204. Esta clave se puede usar a continuación para encriptar / desencriptar, dividir, o autenticar datos.

En algunas formas de realización, para permitir visualización y / o reconstrucción de datos en cada una de una pluralidad de distintos dispositivos de usuario final, una o más claves criptográficas y / o una o más comparticiones de datos se pueden almacenar en el dispositivo de memoria de USB 5204. Además, uno o más de las comparticiones de datos se pueden almacenar también en una nube. Por tanto, un usuario en posesión del dispositivo de usuario portátil puede acceder al dispositivo de memoria de USB 5204 desde un dispositivo de usuario final diferente al dispositivo 5202 para ver y / o reconstruir los datos desde las comparticiones dispersadas a través del dispositivo de memoria de USB 5204 y si fuera necesario, la nube. Por ejemplo, se pueden almacenar dos comparticiones de datos en el dispositivo de memoria de USB 5204 y se pueden almacenar dos comparticiones de datos en el dispositivo de usuario final 5202. Un usuario en posesión del dispositivo de memoria de USB 5204 puede

usar cualquier dispositivo informático con el analizador seguro de la presente invención acoplado al dispositivo de memoria de USB 5204 para acceder a las dos comparticiones de datos almacenadas en el dispositivo de memoria de USB 5204. Por ejemplo, un usuario puede usar un primer ordenador portátil para crear y dispersar las comparticiones a través del dispositivo de memoria de USB 5204 y el dispositivo de usuario final 5202, y puede a continuación usar un segundo ordenador portátil diferente para recuperar las comparticiones desde el dispositivo de memoria de USB 5204 y, suponiendo que estas dos comparticiones son suficientes para reconstruir los datos, reconstruir / recrear los datos desde estas dos comparticiones.

La figura 53 es un diagrama esquemático de una disposición ilustrativa en la que se usa el analizador de datos seguro para almacenamiento de datos seguro en una pluralidad de nubes públicas y privadas y al menos un dispositivo de almacenamiento de usuario de acuerdo con una forma de realización de la presente invención. La figura 53 muestra un dispositivo de usuario final tal como un ordenador portátil 5302 que ha generado cuatro comparticiones encriptadas 5306a, 5306b, 5306c y 5306d. Cada una de estas comparticiones encriptadas 5306a - d se almacena en la localización de almacenamiento dispersada geográficamente y / o diferentes partes de la misma localización de almacenamiento. En particular, las comparticiones encriptadas 5306a y 5306b se almacenan en dos sectores diferentes en el dispositivo de almacenamiento masivo 5308 del ordenador portátil 5302, mientras que la compartición encriptada 5306c se almacena, mediante transmisión a través de una conexión de red segura, en un almacenamiento en la nube accesible públicamente tal como el almacenamiento en la nube de Amazon S3 5310, y la compartición encriptada 5306d se almacena, mediante transmisión a través de una conexión de red segura, en un almacenamiento en la nube accesible públicamente tal como el almacenamiento en la nube de Dropbox 5312. De esta manera, las comparticiones encriptadas están geográfica y físicamente dispersadas, y suponiendo que únicamente dos de las cuatro, o tres de las cuatro, comparticiones encriptadas se requieren para reconstruir los datos, el proceso de recuperación de desastres se acelera si se pierde una o dos de las comparticiones encriptadas. Una pérdida de este tipo puede tener lugar, por ejemplo, si uno de los sectores del almacenamiento masivo 5308 está corrupto, o si la conexión de Internet entre el dispositivo de usuario final 5302 y las nubes 5310 y 5312 se pierde.

En cada una de las formas de realización de las figuras 51 - 53, el proceso de división del proceso de generación de compartición de datos encriptados es transparente para el usuario. Además, el analizador seguro de la presente invención asegura datos de forma simultánea al tiempo que proporciona supervivencia contra desastres de datos robusta debido a que únicamente M de N comparticiones analizadas se requerirán para reconstruir los datos, en donde M < N. Por ejemplo, en algunas de las formas de realización que se han descrito en lo que antecede, únicamente dos (2) o tres (3) de las cuatro (4) comparticiones analizadas se necesitarían para reconstruir o recrear los datos. Si un sector de disco duro falla, o un dispositivo de USB extraíble se pierde, o una localización de almacenamiento remota está caída o inaccesible, aún se puede acceder a los datos y recuperarse los mismos. Además, si se recupera una compartición de unidad fallada, o si se roba una compartición, se desconecta o se piratea, los datos pueden permanecer seguros y protegidos debido a que una única compartición analizada no contiene información discernible de manera forense. En otras palabras, una única compartición analizada no se puede reconstruir, desencriptarse, piratearse o recuperarse sin tener en primer lugar la segunda y / o tercera comparticiones correspondientes, autenticación de usuario apropiada, el analizador seguro de la presente invención, y en algunos casos, la llave de USB o el dispositivo de memoria de USB.

En algunas formas de realización, el analizador seguro de la presente invención se puede usar en un dispositivo móvil tal como un iPad de Apple, una Blackberry de RIM, un iPhone de Apple, un teléfono Droid de Motorola, o cualquier dispositivo adecuado. Los expertos en la materia se darán cuenta de que los sistemas y métodos que se divulgan en el presente documento son de aplicación a una diversidad de los dispositivos de usuario final, incluyendo pero sin limitación dispositivos móviles, ordenadores personales, ordenadores de tipo tableta, teléfonos inteligentes y similares.

El analizador seguro de la presente invención se puede implementar usando uno o más procesadores, cada uno de los cuales realiza una o más de las funciones del analizador seguro tales como generación de clave, encriptación de datos, generación de compartición, desencriptación de datos, etc. En algunas formas de realización, la división de datos incluye dividir datos de forma criptográfica, por ejemplo, división de bits aleatoria. En algunas formas de realización, los datos se dividen usando cualquier algoritmo de dispersión de información (IDA, *information dispersal algorithm*) adecuado. El procesador o procesadores pueden ser cualquier procesador adecuado, por ejemplo, Intel o AMD, y pueden ejecutar un fondo para una plataforma basada en servidor. En algunas formas de realización, se puede usar uno o más coprocesadores especializados para acelerar la operación del analizador seguro de la presente invención. En las formas de realización de las figuras 54 - 56 que se han descrito en lo que antecede, se implementan una o más funciones del analizador seguro de la presente invención en uno o más coprocesadores especializados, que permite la aceleración de las funciones del analizador seguro. En algunas formas de realización, los coprocesadores se pueden incluir una placa madre principal o en una placa hija, o cualquier combinación adecuada de las mismas, de la plataforma de soporte físico del analizador seguro.

La figura 54 es un diagrama esquemático de un dispositivo de aceleración de coprocesador 5400 para el analizador de datos seguro de acuerdo con una forma de realización de la presente invención. El dispositivo 5400 incluye dos procesadores: la unidad de procesamiento central (CPU, *central processing unit*) o procesador principal 5402 y la

unidad de procesamiento rápido (RPU, *rapid processing unit*) o procesador auxiliar 5404. Los procesadores 5402 y 5404 están acoplados entre sí, y acoplados también a un dispositivo de memoria 5406 y dispositivo de almacenamiento masivo 5408. El acoplamiento de estos dispositivos puede incluir el uso de un bus de interconexión. Cada uno de la CPU y RPU puede incluir un único microprocesador o una pluralidad de microprocesadores para configurar la CPU y / o RPU como un sistema multiprocesador. La memoria 5406 puede incluir Memoria de Acceso Aleatorio Dinámica (DRAM, *dynamic random access memory*) y / o memoria caché de alta velocidad. La memoria 5406 puede incluir al menos dos dispositivos de memoria, uno para cada CPU 5402 y RPU 5404. El dispositivo de almacenamiento masivo 5408 puede incluir una o más unidades de disco o cinta magnética, para almacenar datos e instrucciones para su uso mediante la CPU 5402 y / o RPU 5406. El dispositivo de almacenamiento masivo 5408 puede incluir también una o más unidades para diversos medios portátiles, tales como un disco flexible, una memoria de solo lectura de disco compacto (CD-ROM, *compact disc read only memory*), DVD, una unidad FLASH o un adaptador de memoria no volátil de circuito integrado (es decir, un adaptador de PC-MCIA) para entrada y salida de datos y código a y desde la CPU 5402 y / o RPU 5406. La CPU 5402 y / o RPU 5406 puede cada una incluir también una o más interfaces de entrada / salida para comunicaciones, mostradas a modo de ejemplo, como el bus de comunicaciones 5410. El bus de comunicaciones puede incluir también una interfaz para comunicaciones de datos mediante la red 5412. La red 5412 puede incluir uno o más dispositivos de almacenamiento, por ejemplo, dispositivos de almacenamiento en la nube, NAS, SAN, etc. La interfaz a la red 5412 mediante el bus de comunicaciones 5410 puede ser un módem, una tarjeta de red, un puerto serie, un adaptador de bus, o cualquier otro mecanismo de comunicaciones de datos adecuado para comunicarse con uno o más sistemas a bordo de la aeronave o en la superficie. El enlace de comunicación a la red 5412 puede ser, por ejemplo, óptico, cableado, o inalámbrico (por ejemplo, mediante red satélite o celular).

En algunas formas de realización, la RPU puede incluir una unidad de procesamiento de sistemas redundantes de discos independientes (RAID, *redundant array of independent disks*) que implementa una o más funciones de RAID para uno o más dispositivos de almacenamiento que están asociados con el dispositivo de aceleración de coprocesador 5400. En algunas formas de realización, la RPU 5404 puede incluir un circuito integrado (CI) de fin general o especial para realizar cálculos de creación de series y / o cálculos de RAID. En algunas formas de realización, la RPU 5404 puede estar acoplada a la CPU 5402 mediante una conexión PCIe tal como un bus PCIe acoplado a la RPU. Si la RPU incluye una unidad de procesamiento de RAID, entonces la conexión PCIe puede incluir un adaptador de RAID especializado. En algunas formas de realización, la tarjeta PCIe puede correr a 10 Gigabits / s (Gb / s) o más. En algunas formas de realización, la RPU 5404 puede estar acoplada a la CPU 5402 mediante una conexión HT, tal como una RPU en zócalo conectada a un bus HT. Los procesadores 5402 y 5404 accederán tipo a la misma memoria y dispositivos de almacenamiento masivo de tal modo que los mismos datos son accesibles a ambos de estos procesadores. El coprocesador puede realizar funciones aceleradas de análisis seguro especializado incluyendo, pero sin limitación, división de datos, encriptación, y desencriptación. Estas funciones son independientes entre sí, y se pueden realizar usando diferentes algoritmos. Por ejemplo, la encriptación se puede realizar usando cualquiera de las técnicas que se han descrito en lo que antecede, mientras que la división se puede realizar usando cualquier algoritmo de dispersión de información (IDA, *information dispersal algorithm*) adecuado, tal como los que se han descrito en lo que antecede. En algunas formas de realización, la RPU puede estar acoplada a un dispositivo de Matriz de Puertas Programables en Campo (FPGA, *Field Programmable Gate Array*) que podría realizar también funciones aceleradas especializadas del analizador seguro de la presente invención externo al dispositivo de aceleración de coprocesador 5400.

La figura 55 es un primer diagrama de flujo de proceso de un proceso de aceleración ilustrativo que usa el dispositivo de aceleración de coprocesador 5400 de la figura 54 para el analizador de datos seguro de acuerdo con una forma de realización de la presente invención. Con referencia continuada a las figuras 54 y 55, en esta forma de realización ilustrativa, la RPU 5510 puede estar acoplada a la CPU 5520 mediante una conexión HT, tal como una RPU en zócalo mediante un bus HT. El lado izquierdo de la figura 55 ilustra que ciertas funciones del analizador seguro tal como la división de datos y funciones de generación de compartición (3910 y 3912 en la figura 39) se pueden realizar mediante la CPU, mientras que otras funciones tales como la encriptación (por ejemplo, los algoritmos AES, IDA, SHA) (3902, 3904, 3906 en la figura 39) se pueden realizar mediante la RPU. Estas funciones de encriptación y generación de compartición de encriptación se muestran en el lado derecho de la figura 55, en el que hay una indicación de si la CPU o RPU realiza una función de analizador seguro particular.

La figura 56 es un segundo diagrama de flujo de proceso de un proceso de aceleración ilustrativo que usa el dispositivo de aceleración de coprocesador 5400 de la figura 54 para el analizador de datos seguro de acuerdo con una forma de realización de la presente invención. Con referencia continuada a las figuras 54 y 56, en esta forma de realización ilustrativa, la RPU 5610 puede estar acoplada a la CPU 5620 mediante una conexión HT, tal como una RPU en zócalo mediante un bus HT. El lado izquierdo de la figura 56 ilustra que ciertas funciones del analizador seguro tal como la división de datos y funciones de generación de compartición (3910 y 3912 en la figura 39) se pueden realizar mediante la CPU, mientras que otras funciones tales como la encriptación (por ejemplo, los algoritmos AES, IDA, SHA) (3902, 3904, 3906 en la figura 39) se pueden realizar mediante la RPU. Estas funciones de encriptación y generación de compartición de encriptación se muestran en el lado derecho de la figura 55, en el que hay una indicación de si la CPU o RPU realiza una función de analizador seguro particular.

Con respecto a las formas de realización en las figuras 48 - 56 que describen la solución basada en servidor del analizador seguro de la presente invención, hay varias funciones y características adicionales del analizador seguro de la presente invención que se pueden activar o proporcionarse mediante la solución basada en servidor. Además de realizar una división criptográfica y la reconstrucción de compartición de datos, se puede incluir otra funcionalidad tal como actualizaciones de nivel de bloque de comparticiones de datos encriptados y gestión de clave criptográfica. La descripción que sigue describirá cada una de estas funciones. Los expertos en la materia se darán cuenta de que esta funcionalidad se puede incorporar fácilmente en cualquiera de las formas de realización que se describen con respecto a las figuras 48 - 56.

En algunas formas de realización, la solución basada en servidor del analizador seguro de la presente invención permite actualizaciones / cambios de nivel de bloque a ficheros, en lugar de actualizaciones / cambios a todo el fichero de datos. En algunas formas de realización, una vez que se ha enviado una compartición de datos desde el analizador seguro a un dispositivo de almacenamiento en la nube, para operar de forma más eficaz, cuando los datos subyacentes se actualizan por un usuario o grupo de trabajo, en lugar de restaurar todo el fichero de datos, únicamente se pueden transmitir las actualizaciones a nivel de bloque de fichero de particular comparticiones de datos particulares al dispositivo de almacenamiento en la nube que usa los sistemas criptográficos de la presente invención. Por tanto, no se realiza la restauración de un fichero de datos entero ni se requiere cuando únicamente se realizan cambios menores a los ficheros de datos.

En algunas formas de realización, la solución basada en servidor del analizador seguro de la presente invención genera una sección para cada una de las comparticiones de datos. En algunas formas de realización, una sección puede incluir una lista de atributos para sus comparticiones de datos asociadas, y se almacena junto con las comparticiones de datos. En algunas formas de realización, una sección puede incluir información acerca de las comparticiones de datos incluyendo, por ejemplo, el nombre de una compartición de datos, la fecha en que se creó la compartición de datos, la última vez que se modificó la compartición de datos, una indicación a la localización de la compartición de datos en el sistema de fichero de un dispositivo de almacenamiento, etc. Tal información se podría usar para proporcionar con rapidez a un usuario con información con respecto a las comparticiones de datos. En algunas formas de realización, un usuario puede designar un directorio de sección que almacena las secciones. Por ejemplo, un usuario puede designar una unidad virtual o física particular en su dispositivo de almacenamiento en el que se debería almacenar el directorio de sección. Por ejemplo, se puede crear un directorio de sección para un usuario, en el que cada una de las secciones en el directorio apunta al usuario a datos seguros almacenados mediante el analizador seguro en un dispositivo de almacenamiento masivo, un dispositivo de almacenamiento extraíble, una nube pública, una nube privada, o cualquier combinación de los mismos. De esta manera, se pueden utilizar secciones para generar un sistema de ficheros virtual de comparticiones de datos para un usuario.

En algunas formas de realización, las secciones se pueden almacenar en una localización separada de las comparticiones de datos, en la misma localización que las comparticiones de datos, o ambas. En algunas formas de realización, cuando un usuario desea ver alguna información en las comparticiones de datos, puede acceder al directorio sección. En algunas formas de realización, en lugar de ver directamente el directorio sección, las secciones se recuperan desde el directorio sección, se procesan mediante la solución basada en servidor del analizador seguro de la presente invención, y se usan posteriormente para proporcionar la información que se ha mencionado en lo que antecede para el usuario. De esta manera, se pueden utilizar las secciones para generar un sistema de ficheros virtual de comparticiones de datos para un usuario.

En algunas formas de realización, las secciones se almacenan en los respectivos encabezamientos de las comparticiones de datos. Por tanto, si un usuario desea ver la información en una sección, la sección se recupera desde el encabezamiento, se procesa mediante la solución basada en servidor del analizador seguro de la presente invención, y posteriormente se genera un directorio de sección y se proporciona al usuario.

En algunas formas de realización, la solución basada en servidor del analizador seguro de la presente invención comprueba frecuentemente la sección o secciones y / o comparticiones de datos encriptados para integridad de datos usando las técnicas que se han descrito en lo que antecede. El analizador seguro de la presente invención es esencialmente proactivo al recuperar y examinar comparticiones de datos para integridad de datos, incluso cuando no se inició o solicitó por un usuario. Si una compartición de datos o sección se pierde o daña, el analizador seguro de la presente invención intenta recrear y restaurar la sección o la compartición de datos.

La solución basada en servidor del analizador seguro de la presente invención se puede configurar para proporcionar una instalación de gestión de clave criptográfica centralizada. En particular, las claves criptográficas que se usan para encriptar / desencriptar datos, comparticiones de datos y sesiones de comunicación a través de una pluralidad de dispositivos de almacenamiento y sistemas se pueden almacenar en una localización central en una instalación de almacenamiento de la empresa, por ejemplo, una nube privada de la empresa. Esta instalación de gestión de claves centralizada puede interconectar también con soluciones de gestión de claves basadas en soporte físico tales como las proporcionadas por SafeNet, Inc., Belcamp, MD, o con sistemas de gestión de claves basada en soporte lógico. Por ejemplo, una nube privada existente puede controlar acceso a comparticiones de datos encriptados mediante un sistema de autenticación / acceso / autorización, y la solución basada en servidor puede usar la información de autenticación para permitir acceso a las claves criptográficas que se usan para encriptar esas

comparticiones, permitiendo de esta manera a un usuario dividir datos de forma criptográfica, o restaurar las comparticiones de datos encriptadas. En otras palabras, la solución basada en servidor del analizador seguro de la presente invención puede actuar en conjunto con un sistema de autenticación / acceso / autorización existente. De esta manera, una empresa no se ve forzada a cambiar su manera actual de gestionar el acceso de los usuarios y de los grupos de trabajo a los datos.

En algunas formas de realización, la solución basada en servidor del analizador seguro de la presente invención puede realizar reconstrucción de compartición sin desencriptar ninguna de las comparticiones de datos encriptadas. En algunas formas de realización, la solución basada en servidor del analizador seguro de la presente invención puede regenerar divisiones de datos usando una o más nuevas claves sin desencriptar ninguna de las comparticiones de datos encriptadas. La figura 57 ilustra un proceso 5700 mediante el cual los datos se dividen en N comparticiones y se almacenan, de acuerdo con una forma de realización ilustrativa de la presente invención. La figura 58 ilustra un proceso mediante el cual las comparticiones de datos se reconstruyen y / o se vuelven a aplicar claves, de acuerdo con una forma de realización ilustrativa de la presente invención. En cada una de las figuras 57 y 58 cada una de las etapas de los procesos puede ser opcional. Por ejemplo, si no es necesario encriptar datos antes de dividir los datos.

Con referencia a la figura 57, el analizador seguro encripta en primer lugar los datos usando una clave de encriptación (5702). La clave de encriptación se puede generar de forma interna en el analizador seguro de la presente invención. La clave de encriptación se puede generar basándose al menos en parte en una clave de grupo de trabajo externa. El analizador seguro a continuación divide los datos en N comparticiones usando una clave de división (5704). La clave de división se puede generar de forma interna en el analizador seguro de la presente invención. La clave de división se puede generar basándose al menos en parte en una clave de grupo de trabajo externa. El analizador seguro a continuación asegura que únicamente M de N comparticiones se requerirán para reconstruir los datos (5706) y autentica las N comparticiones usando una clave de autenticación (5708). La clave de autenticación se puede generar de forma interna en el analizador seguro de la presente invención. La clave de autenticación se puede generar basándose al menos en parte en una clave de grupo de trabajo externa. Las claves de autenticación, división, y de encriptación se empaquetan cada una usando una clave de la clave de encriptación (5710). La KEK a continuación se divide y almacena en los encabezamientos de las N comparticiones (5712). Las N comparticiones a continuación se dispersan a través de las N localizaciones de almacenamiento.

En algunos casos, es deseable para un usuario o una empresa usar una nueva clave de división y / o una nueva clave de autenticación para un conjunto de comparticiones de datos. Con la solución basada en servidor del analizador seguro de la presente invención, esta reasignación de la clave de los datos se puede realizar sin desencriptar ninguno de las comparticiones de datos. En otros casos, es deseable para un usuario o una empresa que regenere un conjunto de nuevas comparticiones de datos debido a que una o más comparticiones de datos existentes se han corrompido, se han perdido o se encuentran por lo demás inaccesibles. Con la solución basada en servidor del analizador seguro de la presente invención, esta reconstrucción de las comparticiones de datos perdidas se puede realizar sin desencriptar ninguna de las comparticiones de datos disponibles restantes. Con referencia a la figura 58, suponiendo que se corrompen N - M comparticiones de datos o son inaccesibles de otra manera, el analizador seguro recupera las restantes M de N comparticiones desde sus localizaciones de almacenamiento (5802). Estas M comparticiones se autentican usando una clave de autenticación (5804). Usando las M comparticiones autenticadas, los datos encriptados se reconstruyen mediante el analizador seguro (5806). La clave de división se usa a continuación para regenerar las N comparticiones (5808), y la clave de autenticación se usa para autenticar las N comparticiones (5810). Si se usara una diferente clave de división o clave de autenticación (5812) para las etapas 5808 o 5810, entonces los encabezamientos de cada una de las M comparticiones se recuperan (5816), la clave de la clave de encriptación se reconstruye (5818), y similar a los procesos de las etapas 5710 y 5712 (Figura 57), la nueva clave de división y / o clave de autenticación se empaquetan / encriptan usando la clave de la clave de encriptación (5820). Las N comparticiones se almacenan a continuación en uno o más dispositivos de almacenamiento del analizador seguro de la presente invención (5822). Si no se usó una diferente la clave de división o de autenticación (5812) en las etapas 5808 o 5810, entonces las N - M comparticiones perdidas / inaccesibles se almacenan en uno o más dispositivos de almacenamiento del analizador seguro de la presente invención (5814).

La solución basada en servidor del analizador seguro de la presente invención se puede configurar para asegurar el nombre de fichero de una compartición de datos, tal como las comparticiones de datos que se describen en relación con las formas de realización de las figuras 42 - 58 anteriores. En algunas formas de realización, cuando se divide un fichero en N comparticiones de datos, por ejemplo, usando un IDA, las comparticiones de datos generadas se almacenan en una o más localizaciones de compartición en una red de almacenamiento. La red de almacenamiento puede incluir una nube privada, una nube pública, una nube híbrida, un dispositivo de almacenamiento extraíble, un dispositivo de almacenamiento masivo, o cualquier combinación de los mismos. En muchas aplicaciones, habrá más de un fichero que se divida y almacene en una localización de compartición en la red de almacenamiento. En otras palabras, pueden haber varios ficheros, cada uno de los cuales se puede dividir en N comparticiones de datos (por ejemplo, usando un IDA), en donde cada una de las comparticiones de datos generadas se puede almacenar como ficheros en las localizaciones de compartición. En estas aplicaciones, es ventajoso tener un identificador único tal

como un nombre de fichero que asocie una compartición de datos en una localización de compartición con el fichero desde el que se generó.

En algunas formas de realización, el analizador seguro de la presente invención se puede configurar para usar una porción del nombre de fichero del fichero original (es decir, el fichero que se ha de dividir) para nombrar las comparticiones de datos con el mismo nombre que el fichero original. Como un ejemplo ilustrativo, si un fichero original “2010Budget.xls” se divide en 4 comparticiones de datos, estas comparticiones de datos se pueden nombrar “2010Budget.xls.1”, “2010Budget.xls.2”, “2010Budget.xls.3” y “2010Budget.xls.4”, asociando de esta manera cada compartición de datos generada con el fichero original. Mediante este proceso, el analizador seguro de la presente invención podría localizar de forma eficaz las comparticiones de datos y asociarlas con el fichero original. La desventaja de este proceso, no obstante, es que puede exponer información tal como el hecho de que la información del presupuesto es para el año 2010 a un tercero. En muchas aplicaciones, exponer el nombre de fichero de esta manera no es aceptable, y por lo tanto el nombre de fichero de una compartición de datos no se puede asociar fácilmente con el nombre de fichero del fichero original.

En algunas formas de realización, el analizador seguro de la presente invención se puede configurar para asegurar en primer lugar el nombre de fichero que usaría un algoritmo de autenticación tal como HMAC-SHA256 para trocear el nombre de fichero del fichero original en un valor que no se pueda invertir. El analizador seguro de la presente invención procesaría por lo tanto el nombre de fichero del fichero original con el algoritmo HMAC-SHA256 para obtener un nombre de fichero “troceado” y recibir un valor de autenticación que es seguro y no se puede invertir al nombre de fichero del fichero original. Los nombres de fichero de las comparticiones de datos que están asociados con el fichero original se generan a continuación usando este nombre de fichero troceado en lugar del nombre de fichero del fichero original. En estas formas de realización, para localizar las comparticiones de datos (en una red de almacenamiento) que están asociadas con el nombre de fichero del fichero original, el analizador seguro de la presente invención usaría una vez más el algoritmo HMAC-SHA256 en el nombre de fichero original y regeneraría el valor de autenticación. En algunas formas de realización, el valor de autenticación para el nombre de fichero original y los nombres de fichero de las comparticiones generadas son sustancialmente iguales. El analizador seguro de la presente invención buscaría a continuación las localizaciones de compartición en la red de almacenamiento para los nombres de fichero de la compartición de datos que coinciden con este valor de autenticación. La red de almacenamiento puede incluir una nube privada, una nube pública, una nube híbrida, un dispositivo de almacenamiento extraíble, un dispositivo de almacenamiento masivo, o cualquier combinación de los mismos. En algunas formas de realización, la ruta completa del nombre del fichero original se usa de tal modo que el valor de autenticación generado para un fichero con la ruta completa, por ejemplo, “\Marketing\2010Budget.xls” es diferente del valor de autenticación generado para el fichero con la ruta completa, por ejemplo, “\Sales\2010Budget.xls”. En algunas formas de realización, la compartición de datos nombres de fichero resultante que se corresponde con cada localización de compartición de datos se hace diferente troceando la ruta completa para un fichero, incluyendo la ruta completa la localización de compartición. Por ejemplo, anexando el número de compartición de una compartición de datos a la ruta completa del fichero original, por ejemplo “\.Sales\2010Budget.xls.1”, los nombres de fichero de la compartición de datos resultante son diferentes para cada localización de compartición de datos.

En algunas formas de realización, el analizador seguro de la presente invención asegura el nombre de fichero de un fichero encriptando la ruta completa del nombre del fichero original usando un algoritmo de encriptación tal como AES, tal como se ha descrito en lo que antecede. Tal encriptación asegura que el nombre de fichero del fichero original es seguro hasta que se desencripte por el analizador seguro de la presente invención basándose en acceso autenticado a las localizaciones de compartición en una red de almacenamiento, las comparticiones de datos recuperadas y la clave de encriptación. La red de almacenamiento puede incluir una nube privada, una nube pública, una nube híbrida, un dispositivo de almacenamiento extraíble, un dispositivo de almacenamiento masivo, o cualquier combinación de los mismos. Al igual que con los ejemplos que se han descrito en lo que antecede, los nombres de fichero de compartición de datos únicos para cada localización de compartición se puede crear anexando en primer lugar información adicional tal como el número de compartición para una compartición de datos a la ruta completa del fichero original.

En algunas formas de realización, se puede usar un servicio de registro diario para proteger frente a fallos de E / S, tales como fallos de lectura y escritura a un disco. En estas formas de realización, el servicio de registro diario se puede usar para identificar y registrar cada uno de las operaciones de almacenamiento de datos, tales como solicitudes de lectura y escritura, que están asociadas con una o más comparticiones de datos almacenadas en una o más localizaciones de compartición. La una o más comparticiones de datos se pueden crear desde un conjunto de datos originales usando cualquier algoritmo de dispersión de información adecuado, tal como un IDA con clave. Las comparticiones de datos pueden incluir datos mezclados y a continuación dividir usando cualquier técnica aleatorizada o determinística adecuada que se ha divulgado en lo que antecede. Las localizaciones de compartición pueden incluir cualquier instalación de almacenamiento de datos adecuada o combinaciones de instalaciones de almacenamiento de datos que se han descrito en lo que antecede, tales como un disco duro en local o en red, almacenamiento extraíble tal como una llave de USB, o los recursos de un proveedor de almacenamiento en la nube tal como DropBox o Amazon S3. Además, las localizaciones de compartición pueden almacenar cualquier número adecuado de ficheros que están asociados con comparticiones de datos. En algunas formas de realización, el servicio de registro diario se puede integrar con un analizador de datos seguro, tal como el analizador de datos

seguro 3706 del proceso de vista general ilustrativo 3700 de la figura 37, para mantener la salud de datos en localizaciones de compartición que el analizador de datos seguro usa para almacenar datos. En algunas formas de realización, el servicio de registro diario se puede implementar en un ordenador de fin general que tiene uno o más microprocesadores o un conjunto de circuitos de procesamiento.

En algunas formas de realización, el servicio de registro diario puede usar uno o más registros para registrar cada una de las solicitudes de lectura y escritura a las localizaciones de compartición. Este registro se puede gestionar de manera central en las instalaciones que ejecutan el servicio de registro diario, o se puede localizar en las propias localizaciones de compartición. En algunas formas de realización, el registro puede ser una estructura de datos en cola que almacena información que está asociada con operaciones de almacenamiento de datos fallidas, tales como operaciones de lectura y escritura, que están asociadas con una localización de compartición particular. En algunas formas de realización, se puede mantener una cola de registro diario para cada localización de compartición que está asociada con el servicio de registro diario. Las colas de registro diario pueden almacenar información para operaciones de almacenamiento de datos fallidas en el nivel de fichero, el nivel de bloque, el nivel de bit o cualquier nivel de granularidad adecuado. En algunas formas de realización, la cola de registro diario se puede mantener en una memoria que está asociada con el servicio de registro diario, tal como la RAM de un servidor que ejecuta el servicio de registro diario. En algunas formas de realización, la cola de registro diario se puede mantener en almacenamiento en disco que está asociado con el servicio de registro diario. Por ejemplo, la cola de registro diario se puede mantener en una configuración almacenada en ficheros en un disco en un servidor que ejecuta el servicio de registro diario. Tal como se describirá a continuación con respecto a la figura 60, en algunas formas de realización el servicio de registro diario puede aprovechar tanto el almacenamiento de memoria y de disco para mantener la cola de registro diario.

La figura 59 es un proceso ilustrativo 5900 para operar un servicio de registro diario en una forma de realización de la presente invención. El proceso 5900 comienza en la etapa 5910. En la etapa 5910, una o más comparticiones de datos se pueden almacenar en localizaciones de compartición. Tal como se ha analizado en lo que antecede, la una o más comparticiones de datos se pueden crear usando cualquier IDA adecuado, y pueden incluir datos que se han mezclado y dividido usando cualquier técnica aleatorizada o determinística adecuada. El proceso 5900 a continuación continúa a la etapa 5920. En la etapa 5920, el servicio de registro diario puede determinar si una localización de compartición particular está fuera de línea o no disponible para operaciones de almacenamiento de datos. Esta determinación puede resultar de una operación de almacenamiento de datos intentada que está asociada con la localización de compartición particular. Por ejemplo, el servicio de registro diario puede intentar escribir una compartición de datos a una localización de compartición particular. Si la operación de escritura es insatisfactoria, el servicio de registro diario puede recibir una notificación de que la operación de escritura ha fallado. Por consiguiente, el servicio de registro diario marcará la localización de compartición particular como que no está disponible, o fuera de línea, para futuras operaciones de escritura o lectura. En algunas formas de realización, la indicación de que una localización de compartición está fuera de línea se puede almacenar en cualquier bandera de datos adecuada mantenida en memoria o disco central para el servicio de registro diario, o en la propia compartición de datos. El proceso 5900 a continuación continúa a la etapa 5930.

En la etapa 5930, una cola de registro diario se puede establecer y mantenerse para la localización de compartición particular que se ha designado como fuera de línea. En algunas formas de realización, siempre que la localización de compartición se haya designado como fuera de línea, el servicio de registro diario puede almacenar información que está asociada con operaciones de almacenamiento de datos entrantes relacionadas con la localización de compartición en la cola de registro diario. Por ejemplo, si una localización de compartición se ha marcado como fuera de línea, las futuras operaciones de lectura y escritura relacionadas con esa localización de compartición se almacenan en la cola de registro diario que se ha establecido para esa localización de compartición. En algunas formas de realización, cada cola de registro diario mantenida mediante el servicio de registro diario se puede asociar con una localización de compartición única. Además, cada cola de registro diario mantenida mediante el servicio de registro diario se puede gestionar mediante un hilo de procesamiento separado. El proceso 5900 a continuación continúa a la etapa 5940.

En la etapa 5940, el servicio de registro diario puede determinar si una localización de almacenamiento fuera de línea se ha hecho disponible. En algunas formas de realización, esta determinación se puede realizar mediante el servicio de registro diario que monitoriza constantemente la localización de compartición fuera de línea para una indicación de que la localización de compartición se ha restaurado. Esta indicación puede ser un cambio en una bandera de datos que está asociada con la localización de compartición que se produce por, por ejemplo, la reparación de la localización de compartición mediante el servicio de registro diario o un administrador del servicio de registro diario. El proceso 5900 a continuación continúa a la etapa 5950.

En la etapa 5950, el servicio de registro diario puede reproducir las operaciones de almacenamiento de datos fallidas almacenadas en la cola de registro diario para la localización de compartición que se ha hecho disponible. En algunas formas de realización, reproducir las operaciones fallidas puede incluir ejecutar las operaciones de lectura y escritura fallidas que se han almacenado en la cola de registro diario. Una vez que las operaciones fallidas almacenadas en la cola de registro diario se han ejecutado, el servicio de registro diario puede opcionalmente limpiar o vaciar la cola de registro diario. Al vaciar la cola de registro diario, el servicio de registro diario puede liberar

cualquier recurso de memoria o de disco que está asociado con la cola de registro diario. Una vez que se reproducen las operaciones fallidas almacenadas en la cola de registro diario, el proceso 5900 a continuación finaliza.

La figura 60 es un proceso ilustrativo 6000 para operar un servicio de registro diario en una forma de realización de la presente invención. El proceso 6000 comienza en la etapa 6010. En la etapa 6010, el servicio de registro diario puede establecer un límite de cola para cada localización de compartición que tiene una cola de registro diario asociada. Este límite de cola puede especificar el número máximo de mensajes (por ejemplo, operaciones de lectura o escritura fallidas) que está asociado con una cola de registro diario que se puede almacenar en una memoria que está asociada con el servicio de registro diario. El servicio de registro diario puede a continuación rastrear el número de mensajes en cada cola de registro diario manteniendo, por ejemplo, un registro del número de mensajes en cada cola de registro diario. El proceso 6000 a continuación continúa a la etapa 6020. En la etapa 6020, el servicio de registro diario puede determinar que el límite de cola se ha superado para una cola de registro diario particular. Por ejemplo, el servicio de registro diario puede determinar que el número de operaciones fallidas almacenadas en la cola particular supera un número máximo preconfigurado. Si el servicio de registro diario determina que el límite de cola se ha superado, el proceso 6000 continúa a la etapa 6030.

En la etapa 6030, la cola de registro diario se puede vaciar, o almacenarse, en un fichero mantenido en el almacenamiento en disco que está asociado con el servicio de registro diario. En algunas formas de realización, el fichero se puede mantener en almacenamiento en disco hasta que la localización de compartición se hace disponible. Por ejemplo, después de que la localización de compartición se hace disponible, el servicio de registro diario puede reproducir cada operación almacenada en el fichero, y a continuación eliminar el fichero desde el almacenamiento en disco. De esta manera, el número de operaciones fallidas registradas mediante el servicio de registro diario se permiten superar las limitaciones de memoria del sistema que ejecuta el servicio de registro diario. En algunas formas de realización, los contenidos de la cola de registro diario que se almacenan en memoria se pueden vaciar en el fichero en el caso de un cierre de sistema (por ejemplo, una pérdida de potencia para el sistema que ejecuta el servicio de registro diario). De esta manera, el servicio de registro diario puede recuperar las operaciones sin una pérdida de integridad de datos una vez que se restaura el sistema que ejecuta el servicio de registro diario. El proceso 6000 a continuación finaliza. Si el servicio de registro diario determina que el límite de cola no se ha superado, el proceso 6000 continúa a la etapa 6040. En la etapa 6040, el servicio de registro diario puede continuar para escribir operaciones fallidas en la cola de la memoria. El proceso 6000 a continuación finaliza.

En algunas formas de realización, si se registran demasiadas operaciones de almacenamiento de datos fallidas para una localización de compartición, el servicio de registro diario registrará un estado de “fallo crítico”. Este estado de fallo crítico puede indicar que la integridad de los datos en la localización de compartición ya no puede ser de confianza y se requiere una operación de restauración o reconstrucción. Tal como se describirá con respecto a la figura 61, marcar una localización de compartición como que está en un estado de fallo crítico puede colocar de forma eficaz un límite superior en la cantidad de memoria y / o espacio de disco que son usados por el sistema que ejecuta el servicio de registro diario. La figura 61 es un proceso ilustrativo 6100 para operar un servicio de registro diario usando un estado de fallo crítico en una forma de realización de la presente invención. El proceso 6100 comienza en la etapa 6110. En la etapa 6110, el servicio de registro diario establece un recuento de fallo máximo. En algunas formas de realización, este recuento de fallo máximo puede ser un número preconfigurado de operaciones fallidas que el servicio de registro diario está permitido a registrar en una cola de registro diario que está asociada con una localización de datos antes de que esa localización se marque como que está en un estado de fallo crítico. El proceso 6100 a continuación continúa a la etapa 6120. En la etapa 6120, el servicio de registro diario monitoriza el número de operaciones fallidas para cada localización de compartición. En algunas formas de realización, esta monitorización puede incluir el servicio de registro diario que mantiene un recuento actualizado del número de operaciones fallidas almacenadas en la cola de registro diario para cada localización de compartición. El proceso 6100 a continuación continúa a la etapa 6130.

En la etapa 6130, el servicio de registro diario puede determinar si el recuento de fallo máximo se ha superado para una localización de compartición particular. En algunas formas de realización, el servicio de registro diario puede realizar esta determinación comparando un recuento actualizado del número de operaciones de almacenamiento de datos fallidas almacenadas en una cola de registro diario que está asociada con la localización de compartición particular para el recuento de fallo máximo. Si el recuento de fallo máximo se ha superado, el proceso 6100 continúa a la etapa 6140. En algunas formas de realización, si el recuento de fallo máximo se ha superado para una localización de compartición particular, el servicio de registro diario puede marcar esa localización de compartición como que está en un estado de fallo crítico. En algunas formas de realización, una indicación de que una localización de compartición está en un estado de fallo crítico se puede almacenar en cualquier bandera de datos adecuada mantenida en memoria o disco central al servicio de registro diario, o en la propia compartición de datos.

En la etapa 6140, el servicio de registro diario puede descartar cualquier operación de almacenamiento de datos fallida almacenada en la cola de registro diario que está asociada con la localización de compartición que está en un estado de fallo crítico. En algunas formas de realización, el servicio de registro diario puede descartar estas operaciones fallidas limpiando la cola de registro diario que está asociada con la localización de compartición que está en un estado de fallo crítico. Como alternativa, el servicio de registro diario puede borrar toda la cola de registro

diario que está asociada con la localización de compartición que está en un estado de fallo crítico. Además, en la etapa 6140 el servicio de registro diario puede dejar de registrar operaciones fallidas que están asociadas con la localización de compartición que está en un estado de fallo crítico. Por ejemplo, el servicio de registro diario puede ya no actualizar la cola de registro diario que está asociada con la localización de compartición que está en un estado de fallo crítico. El proceso 6100 a continuación continúa a la etapa 6150.

En la etapa 6150, el servicio de registro diario puede recrear una localización de compartición que está en un estado de fallo crítico. En algunas formas de realización, la funcionalidad de restauración de un analizador de datos seguro se puede usar para recrear una localización de compartición. Por ejemplo, los datos almacenados en la localización de compartición que está en un estado de fallo crítico se pueden asociar con datos originales que se dividieron usando cualquier algoritmo de dispersión de información adecuado en cualquier número de compartimentos de datos. Cada una de estas compartimentos de datos se puede almacenar en dos o más compartimentos de datos, tales como cualquier combinación adecuada de una nuble pública o privada, un dispositivo de almacenamiento extraíble o un dispositivo de almacenamiento masivo. Siempre que el analizador seguro pueda recuperar estos datos desde al menos una de las otras localizaciones de compartición que están en línea (en otras palabras, no en un estado de fallo crítico), entonces el analizador de datos seguro puede recrear la localización de compartición. En algunas formas de realización, la localización de compartición se puede recrear a partir de cero. Por ejemplo, todos los ficheros que se vayan a restaurar en la localización de compartición se pueden eliminar antes de que se ejecute inicialmente el proceso de recreación en la localización de compartición. En algunas formas de realización, se pueden requerir permisos administrativos para leer y escribir en la localización de compartición para que el proceso de reconstrucción se ejecute en la localización de compartición.

Tal como se describirá a continuación con respecto a la figura 62, en algunas formas de realización las localizaciones de compartición que están en los procesos que se están reconstruyendo se pueden marcar como que están en un “estado de reconstrucción crítico”. Este estado de reconstrucción crítico puede indicar al servicio de registro diario que se deberían registrar ciertas operaciones fallidas. Estas operaciones pueden ser a nivel de fichero, nivel de bloque, nivel de bit o cualquier nivel adecuado de granularidad de fichero. En algunas formas de realización, la etapa 6150 puede ser opcional. El proceso 6100 a continuación continúa a la etapa 6160. En la etapa 6160, el servicio de registro diario puede reanudar manteniendo una cola de registro diario para la localización de compartición que se reconstruyó en la etapa 6150. En algunas formas de realización, la etapa 6150 puede ser opcional. El proceso 6100 puede a continuación finalizar.

Si el servicio de registro diario determina que el recuento de fallo máximo para una localización de compartición particular no se supera en la etapa 6130, el proceso 6100 puede continuar a la etapa 6170. En la etapa 6170, el servicio de registro diario puede continuar para registrar operaciones fallidas para la localización de compartición particular. El proceso 6100 a continuación finaliza.

En algunas formas de realización, el proceso 6100 puede usar un máximo tiempo de expiración además del recuento de fallo máximo en las etapas 6110, 6120 y 6130 para determinar si una localización de compartición está en un estado de fallo catastrófico. En algunas formas de realización, el tiempo de expiración máximo puede ser la cantidad de tiempo preconfigurada que una localización de compartición particular puede permanecer fuera de línea antes de que la localización de compartición se marque como que está en un estado de fallo catastrófico. El estado de fallo catastrófico puede indicar al servicio de registro diario que todas las operaciones de lectura y escritura para la compartición se deberían rechazar hasta que la compartición se restaure o que esté en el proceso de restaurarse. En algunas formas de realización, la compartición se puede restaurar de acuerdo con el proceso de reconstrucción que se describe con respecto a la etapa 6150. En otras formas de realización, la localización de compartición se puede restaurar mediante un administrador del servicio de registro diario restaurando de forma manual la localización de compartición. Por ejemplo, un administrador del servicio de registro diario puede sustituir o remapear la instalación de almacenamiento de datos que están asociados con la localización de compartición.

En algunas formas de realización, el servicio de registro diario puede registrar un estado de reconstrucción crítico para una localización de compartición que está en el proceso de reconstruirse. En algunas formas de realización, el servicio de registro diario puede registrar un estado de reconstrucción crítico para una localización de compartición particular tan pronto como el proceso de reconstrucción empieza. En algunas formas de realización, este proceso de reconstrucción puede ser similar al que se describe con respecto a la etapa 6150 de la figura 61. Tal como se describirá a continuación con respecto a la figura 62, este estado de reconstrucción crítico puede indicar al servicio de registro diario que debería registrar operaciones fallidas para ficheros que ya se han restaurado en la localización de compartición que se está reconstruyendo.

La figura 62 es un proceso ilustrativo 6200 para operar un servicio de registro diario usando un estado de reconstrucción crítico en una forma de realización de la presente invención. A pesar de que el proceso 6200 se describe como operando en el nivel de fichero, se reconocerá que el servicio de registro diario puede ejecutar el proceso 6200 en cualquier nivel adecuado de granularidad, tal como en el nivel de bloque o el nivel de bit. El proceso 6200 comienza en la etapa 6210. En la etapa 6210, el servicio de registro diario recibe una solicitud para realizar una operación de almacenamiento de datos en un fichero que está asociado con una localización de compartición que está en un estado de reconstrucción crítico. En algunas formas de realización, esta operación de

almacenamiento de datos puede ser una solicitud de lectura o escritura en el fichero. Debido a que la localización de compartición está en un estado de reconstrucción crítico, la solicitud de lectura o escritura para la localización de compartición fallará. Por ejemplo, el servicio de registro diario puede recibir una solicitud para escribir en un fichero que contiene una presentación de diapositivas. Las comparticiones de datos que están asociadas con el fichero que contiene la presentación de diapositivas se pueden almacenar en una localización de compartición que se está reconstruyendo y está en un estado de reconstrucción crítico, así como tres otras localizaciones de compartición que están en un estado en línea. La solicitud para escribir en el fichero fallará con respecto a la localización de compartición que está en un estado de reconstrucción crítico, pero tendrá éxito con respecto a las localizaciones de compartición que están en un estado en línea. El proceso 6200 continúa a la etapa 6220.

En la etapa 6220, el servicio de registro diario determina si el fichero existe en la localización de compartición que está en un estado de reconstrucción crítico. En algunas formas de realización, el servicio de registro diario puede mantener una lista de ficheros que se han restaurado en la localización de compartición que está en un estado de reconstrucción crítico. Si el fichero que está asociado con la operación de almacenamiento de datos está en la lista, el servicio de registro diario puede determinar que el fichero existe en la localización de compartición. El proceso 6200 a continuación continúa a la etapa 6240. En la etapa 6240, el servicio de registro diario registra la operación de almacenamiento de datos, tal como una solicitud de lectura o escritura, que falló en la etapa 6210. En algunas formas de realización, esta operación fallida se puede almacenar en una cola de registro diario similar a la que se describe con respecto un proceso 5900 de la figura 59. El proceso 6200 a continuación continúa a la etapa 6250. En la etapa 6250, el servicio de registro diario reproduce la operación fallida una vez que el proceso de reconstrucción está completo. En algunas formas de realización, se puede notificar al servicio de registro diario que el proceso de reconstrucción está completo con respecto a una localización de compartición cuando todos los ficheros que están asociados con la localización de compartición se restauran. Cuando todos los ficheros que están asociados con la localización de compartición se restauran, la localización de compartición se puede marcar como que está disponible para operaciones de almacenamiento de datos (es decir, está en un estado en línea). De esta manera, el estado de reconstrucción crítico permite al servicio de registro diario continuar manteniendo la salud del sistema de ficheros con una o más localizaciones de compartición mientras una o más localizaciones en el sistema de ficheros se están reconstruyendo. El proceso 6200 a continuación finaliza.

Si el servicio de registro diario determina en la etapa 6220 que el fichero desde la solicitud para realizar una operación en la etapa 6210 no existe (es decir, no se ha restaurado aún) en la localización de compartición que se está reconstruyendo, el proceso 6200 continúa a la etapa 6230. En la etapa 6230, la operación que falló en la etapa 6210 se descarta mediante el servicio de registro diario. En algunas formas de realización, el servicio de registro diario puede descartar estas operaciones fallidas no escribiéndolas en la cola de registro diario que está asociada con la localización de compartición que está en un estado de reconstrucción crítico. En tales formas de realización, el servicio de registro diario se puede basar en la operación del fichero que es satisfactorio con respecto a otros almacenamientos de datos que están asociados con el servicio de registro diario. Por ejemplo, una actualización para un fichero que contiene una presentación de diapositivas se puede descartar con respecto a una localización de compartición que está en un estado de reconstrucción crítico y no ha restaurado aún el fichero que contiene la presentación de diapositivas. No obstante, la operación de actualización puede ser satisfactoria con respecto a otras tres localizaciones de compartición que están en un estado en línea y contienen el fichero. El proceso 6200 a continuación finaliza.

A pesar de que se han descrito en lo que antecede algunas aplicaciones del analizador de datos seguro, se debería entender claramente que la presente invención se puede integrar con cualquier aplicación de red para aumentar la seguridad, la tolerancia a fallos, la anonimidad, cualquier combinación adecuada de lo anterior.

Además, otras combinaciones, adiciones, sustituciones y modificaciones serán evidentes para los expertos en la materia en vista de la divulgación del presente documento.

REIVINDICACIONES

1. Un método para leer y escribir un conjunto de datos, que comprende:

dividir el conjunto de datos en una o más comparticiones de datos usando un algoritmo de dispersión de información;
transmitir las una o más comparticiones de datos para almacenamiento a localizaciones de compartición;
identificar e intentar operaciones de almacenamiento de datos para las una o más comparticiones de datos, en donde cada una de las operaciones de almacenamiento de datos comprende una solicitud de lectura o una solicitud de escritura para una compartición de datos almacenada respectiva;
determinar que al menos una de las localizaciones de compartición se encuentra no disponible para las operaciones de almacenamiento de datos; y
almacenar las operaciones de almacenamiento de datos entrantes que están asociadas con cada una de las localizaciones de compartición no disponibles en colas respectivas únicas para cada una de las localizaciones de compartición no disponibles.

2. El método de la reivindicación 1, que comprende adicionalmente:

determinar que al menos una de las localizaciones de compartición no disponibles se ha hecho disponible; y
ejecutar las operaciones de almacenamiento de datos que están almacenadas en la cola única para la al menos una localización de compartición no disponible que se ha hecho disponible.

3. El método de la reivindicación 2, que comprende adicionalmente vaciar las operaciones de almacenamiento de datos ejecutadas.

4. El método de una cualquiera de las reivindicaciones 1 a 3, que comprende adicionalmente:

almacenar las colas en memoria;
establecer un límite de cola que está asociado con una cantidad de operaciones de almacenamiento de datos;
determinar que se supera el límite de cola para al menos una de las colas; y
para cada una de las colas que superan el límite de cola, vaciar la cola de la memoria en el almacenamiento en disco.

5. El método de una cualquiera de las reivindicaciones 1 a 4, que comprende adicionalmente:

establecer una cantidad máxima de tiempo que una localización de compartición se encuentra no disponible para las operaciones de almacenamiento de datos;
determinar que se supera la cantidad máxima de tiempo para al menos una de las localizaciones de compartición no disponibles;
para cada una de las localizaciones de compartición no disponibles que superan la cantidad máxima de tiempo, rechazar las operaciones de almacenamiento de datos entrantes.

6. El método de una cualquiera de las reivindicaciones 1 a 5, que comprende adicionalmente:

establecer un número máximo de operaciones de almacenamiento de datos fallidas;
determinar que las operaciones de almacenamiento de datos que están almacenadas en al menos una de las colas superan el número máximo establecido de operaciones de almacenamiento de datos fallidas; y
descartar las operaciones de almacenamiento de datos que están almacenadas en la al menos una de las colas que superan el número máximo establecido de operaciones de almacenamiento de datos fallidas.

7. El método de la reivindicación 6, que comprende adicionalmente descartar las operaciones de almacenamiento de datos entrantes que están asociadas con cada una de las colas respectivas que superan el número máximo establecido de operaciones de almacenamiento de datos fallidas.

8. El método de la reivindicación 6, que comprende adicionalmente:
reconstruir comparticiones que están almacenadas en cada localización de compartición que está asociada con la al menos una de las colas que supera el número máximo establecido de operaciones de almacenamiento de datos fallidas usando al menos una de las localizaciones de compartición que están en línea.

9. El método de una cualquiera de las reivindicaciones 1 a 8,
en donde al menos una de las localizaciones de compartición se está reconstruyendo;
en donde determinar que al menos una de las localizaciones de compartición se encuentra no disponible para las operaciones de almacenamiento de datos comprende determinar que al menos una de las localizaciones de compartición se está reconstruyendo; y que comprende adicionalmente:

recibir una solicitud para realizar una operación de almacenamiento de datos sobre un archivo que está asociado con la al menos una localización de compartición que se está reconstruyendo;
determinar que el archivo se restaura en aquella de las localizaciones de compartición que se está reconstruyendo; y
basándose en la determinación, almacenar la operación de almacenamiento de datos en una cola que está asociada con la al menos una localización de compartición que se está reconstruyendo.

10. El método de la reivindicación 9, que comprende adicionalmente:

determinar que el archivo no se restaura en la al menos una localización de compartición que se está reconstruyendo; y
basándose en la determinación, descartar la operación de almacenamiento de datos.

11. El método de la reivindicación 9, que comprende adicionalmente:

determinar que la al menos una localización de compartición que se está reconstruyendo se encuentra disponible para las operaciones de almacenamiento de datos; y
basándose en la determinación, ejecutar las operaciones de almacenamiento de datos que están almacenadas en la cola que está asociada con la al menos una localización de compartición que se está reconstruyendo.

12. Un sistema que está adaptado para realizar el método de una cualquiera de las reivindicaciones 1 a 11.

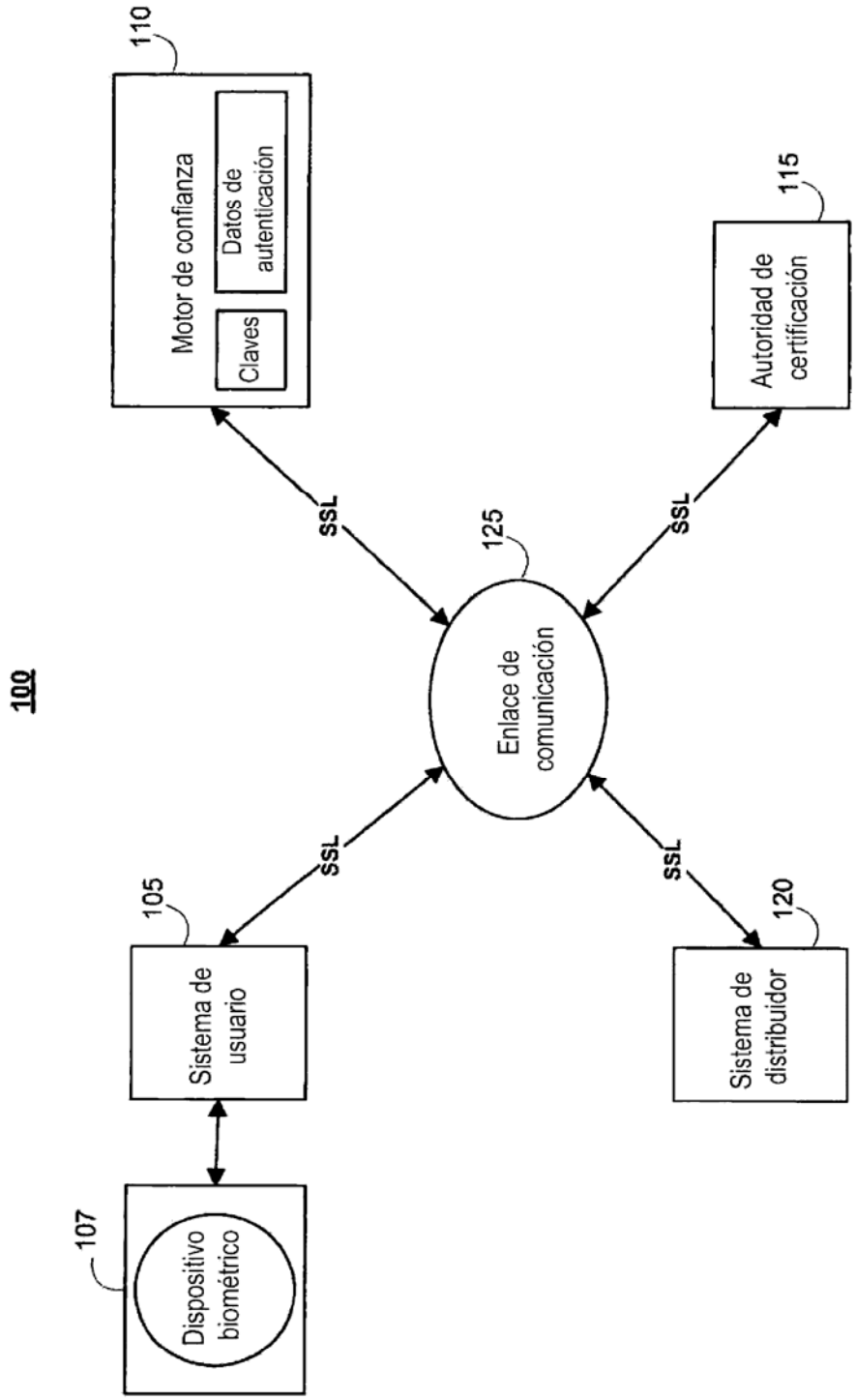

100
110
Motor de confianza
Datos de autenticación
Claves
115
Autoridad de certificación
SSL
SSL
125
Enlace de comunicación
SSL
SSL
105
Sistema de usuario
120
Sistema de distribuidor
107
Dispositivo biométrico

FIG. 1

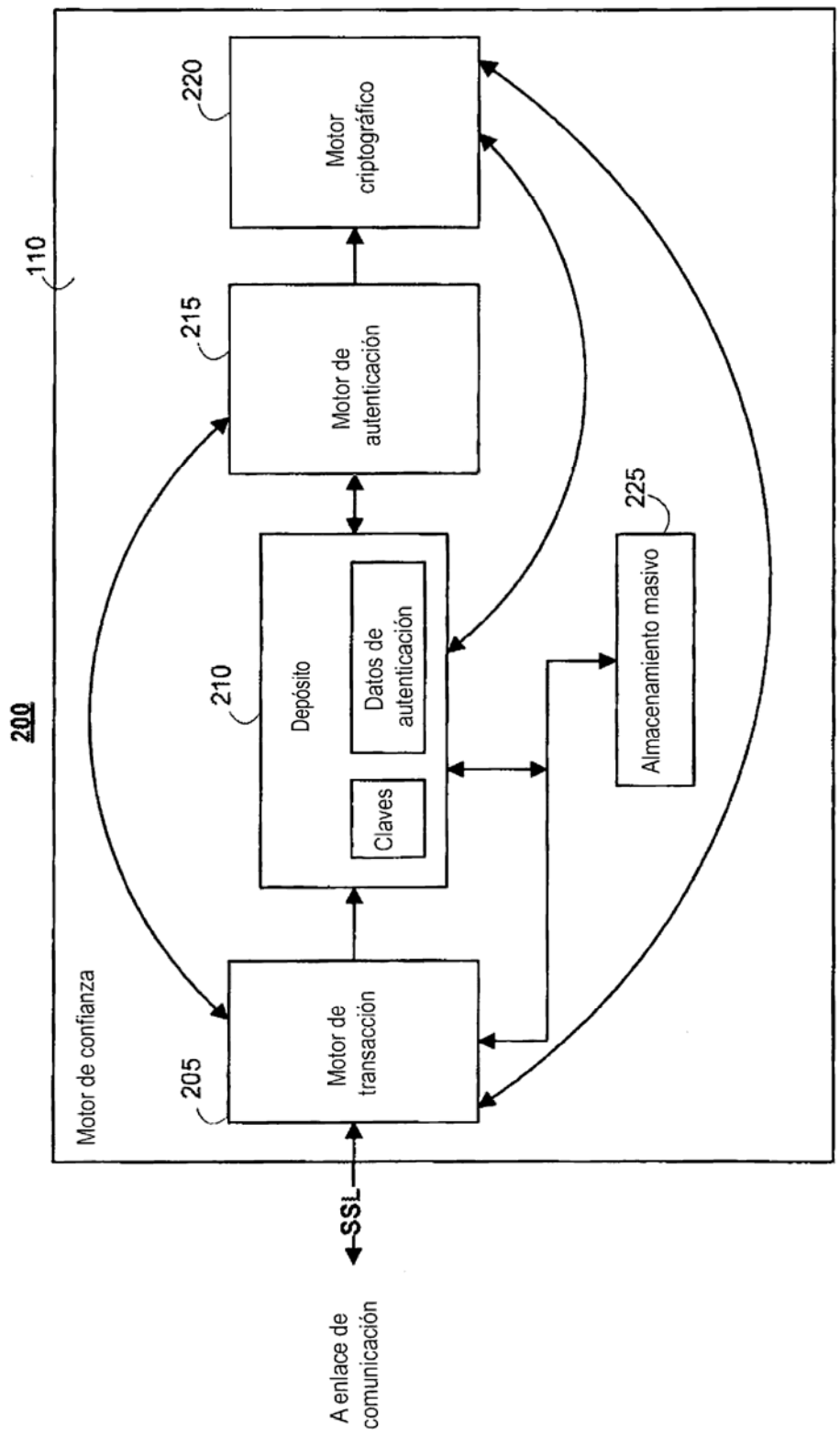

200
110
Motor de confianza
205
Motor de transacción
210
Depósito
Datos de autenticación
Claves
215
Motor de autenticación
220
Motor criptográfico
225
Almacenamiento masivo
SSL
A enlace de comunicación

FIG. 2

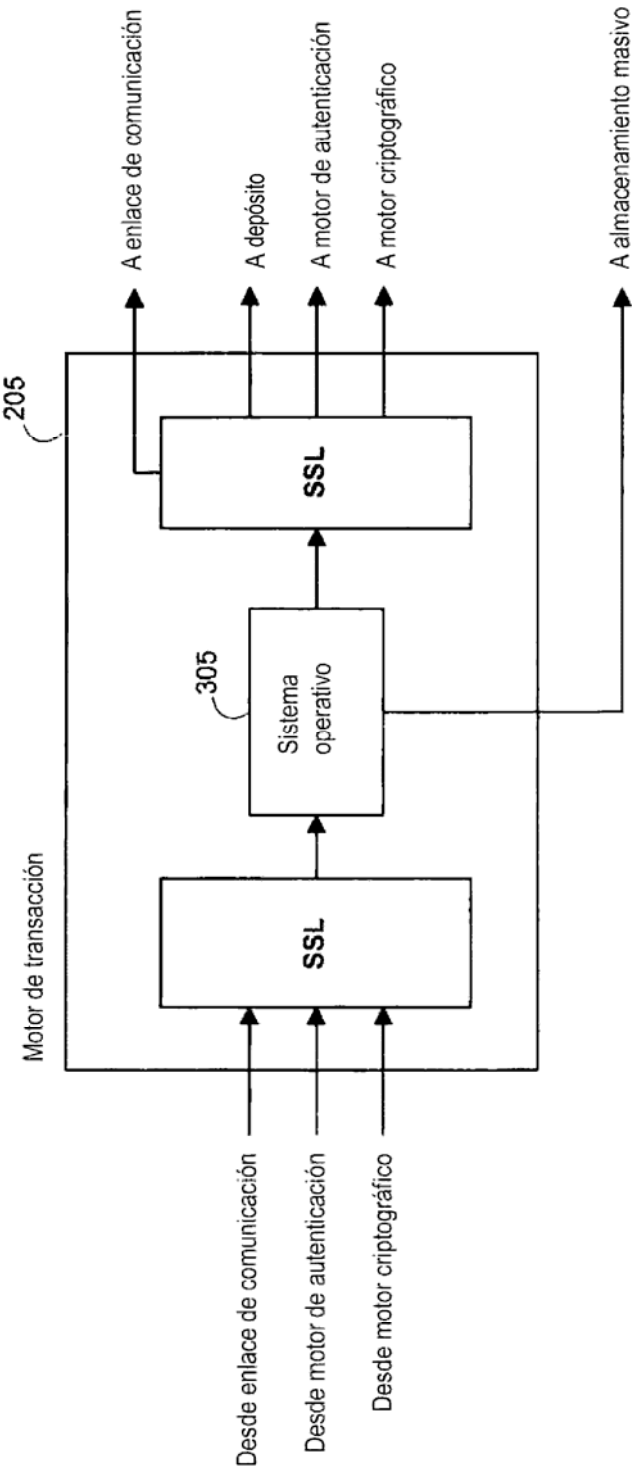

Motor de transacción
205
SSL
SSL
305
Sistema operativo
Desde enlace de comunicación
Desde motor de autenticación
Desde motor criptográfico
A enlace de comunicación
A depósito
A motor de autenticación
A motor criptográfico
A almacenamiento masivo

FIG. 3

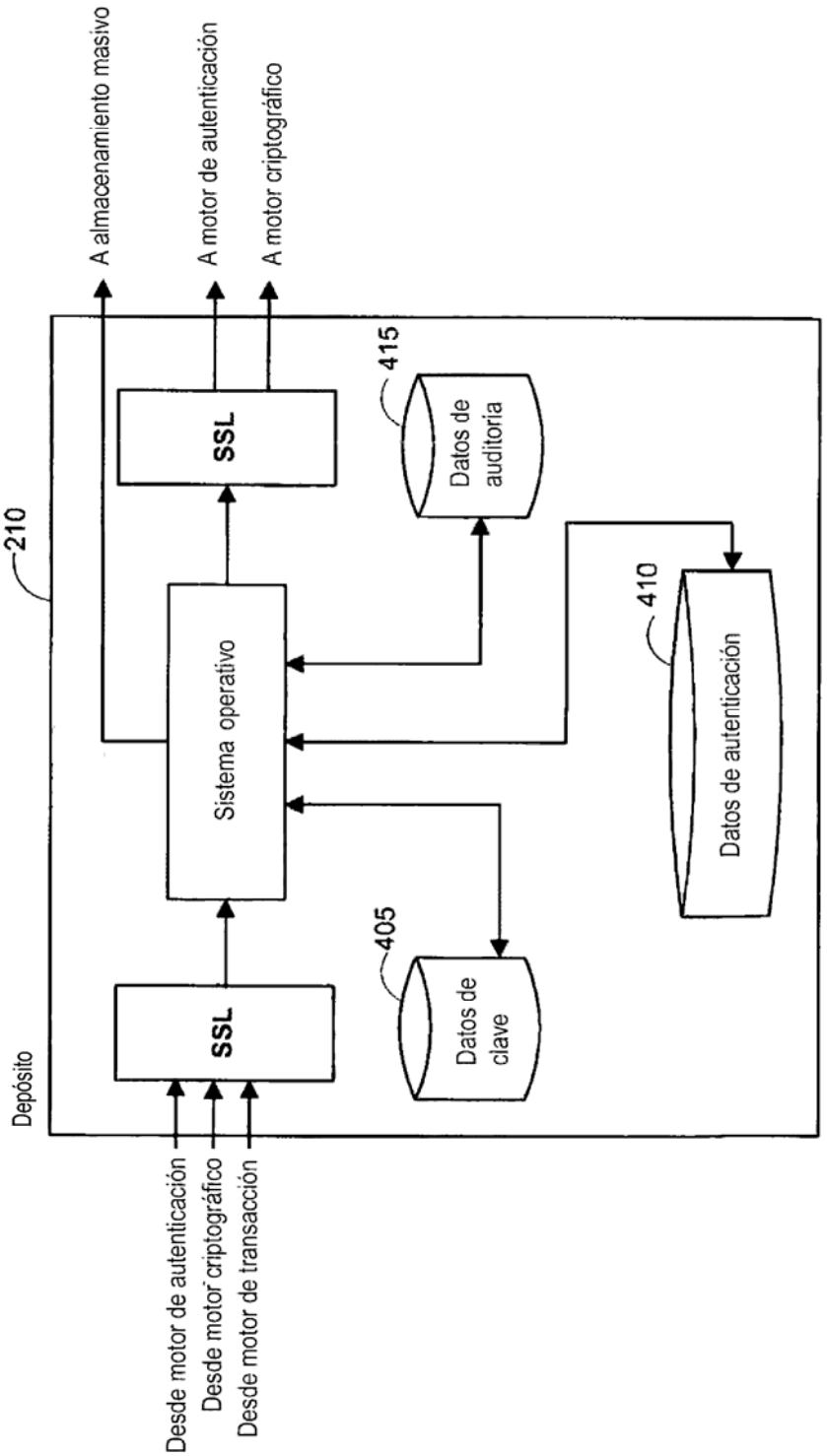

A almacenamiento masivo
A motor de autenticación
A motor criptográfico
210
SSL
415
Datos de auditoria
Sistema operativo
410
Datos de autenticación
405
Datos de clave
SSL
Depósito
Desde motor de autenticación
Desde motor criptográfico
Desde motor de transacción

FIG. 4

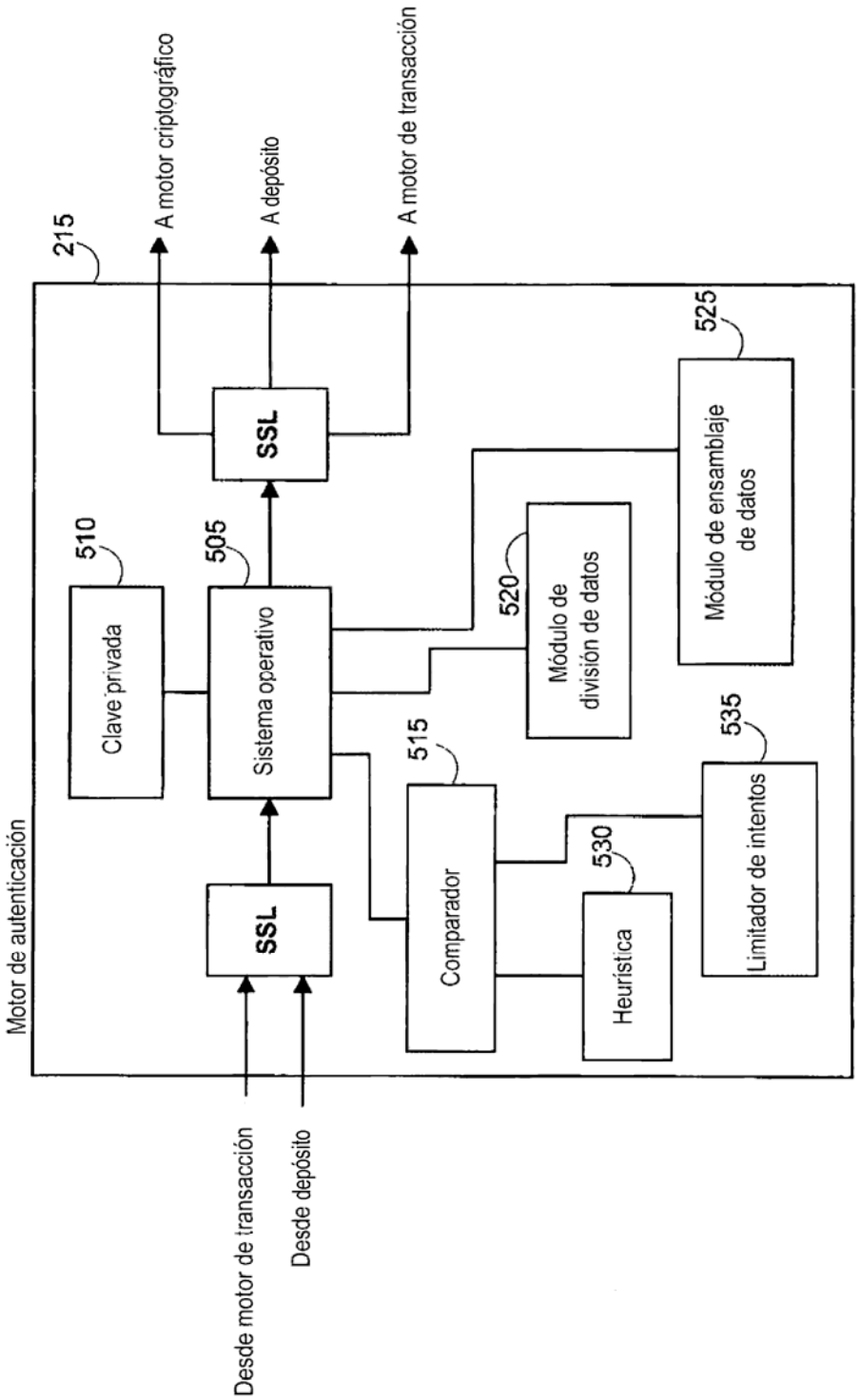

Motor de autenticación
215
A motor criptográfico
A depósito
A motor de transacción
SSL
SSL
Clave privada
510
Sistema operativo
505
Módulo de división de datos
520
Módulo de ensamblaje de datos
525
Comparador
515
Heurística
530
Limitador de intentos
535
Desde motor de transacción
Desde depósito

FIG. 5

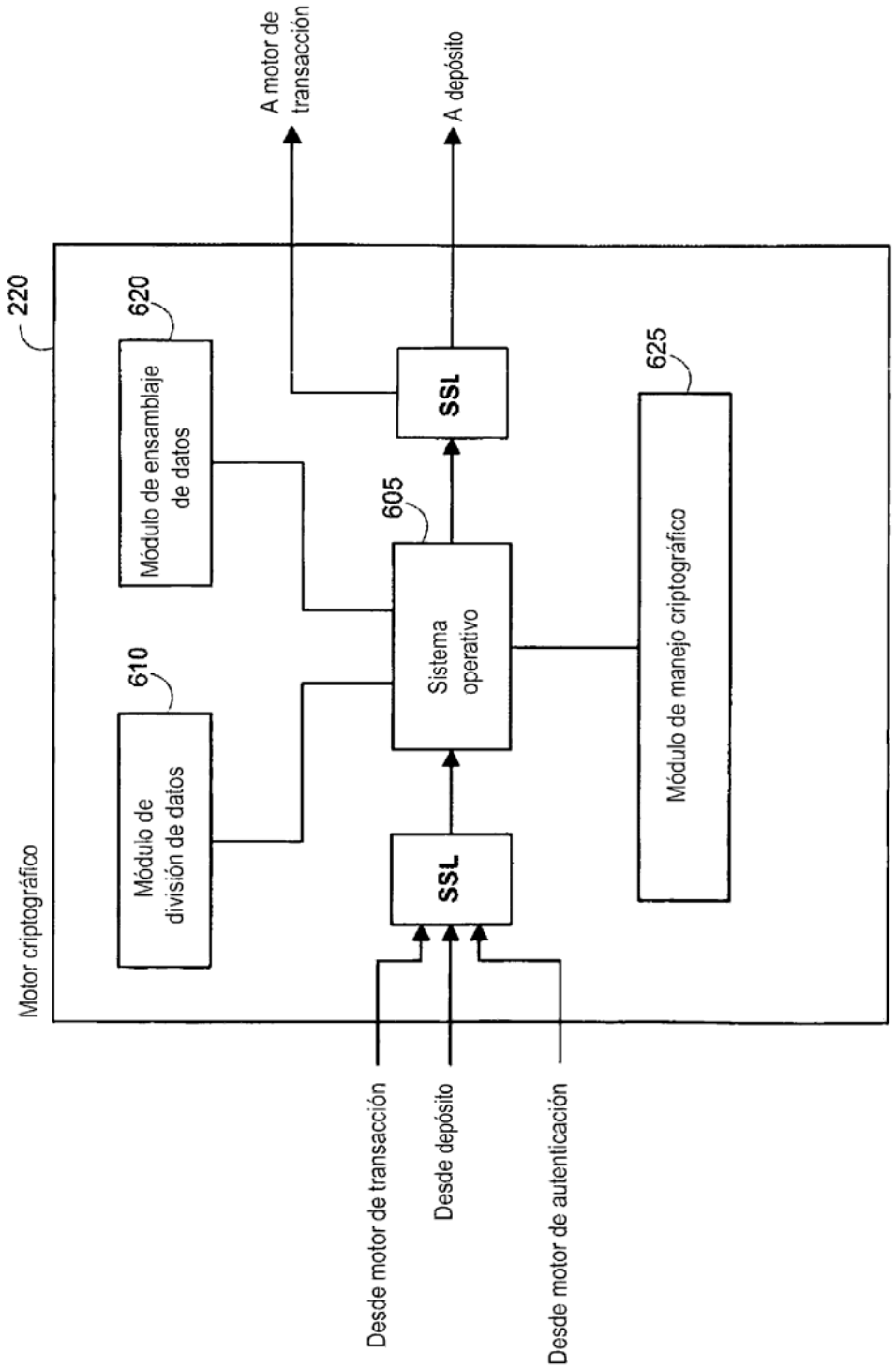

A motor de transacción
A depósito
220
620
Módulo de ensamblaje de datos
SSL
625
605
Sistema operativo
Módulo de manejo criptográfico
610
Módulo de división de datos
SSL
Motor criptográfico
Desde motor de transacción
Desde depósito
Desde motor de autenticación

FIG. 6

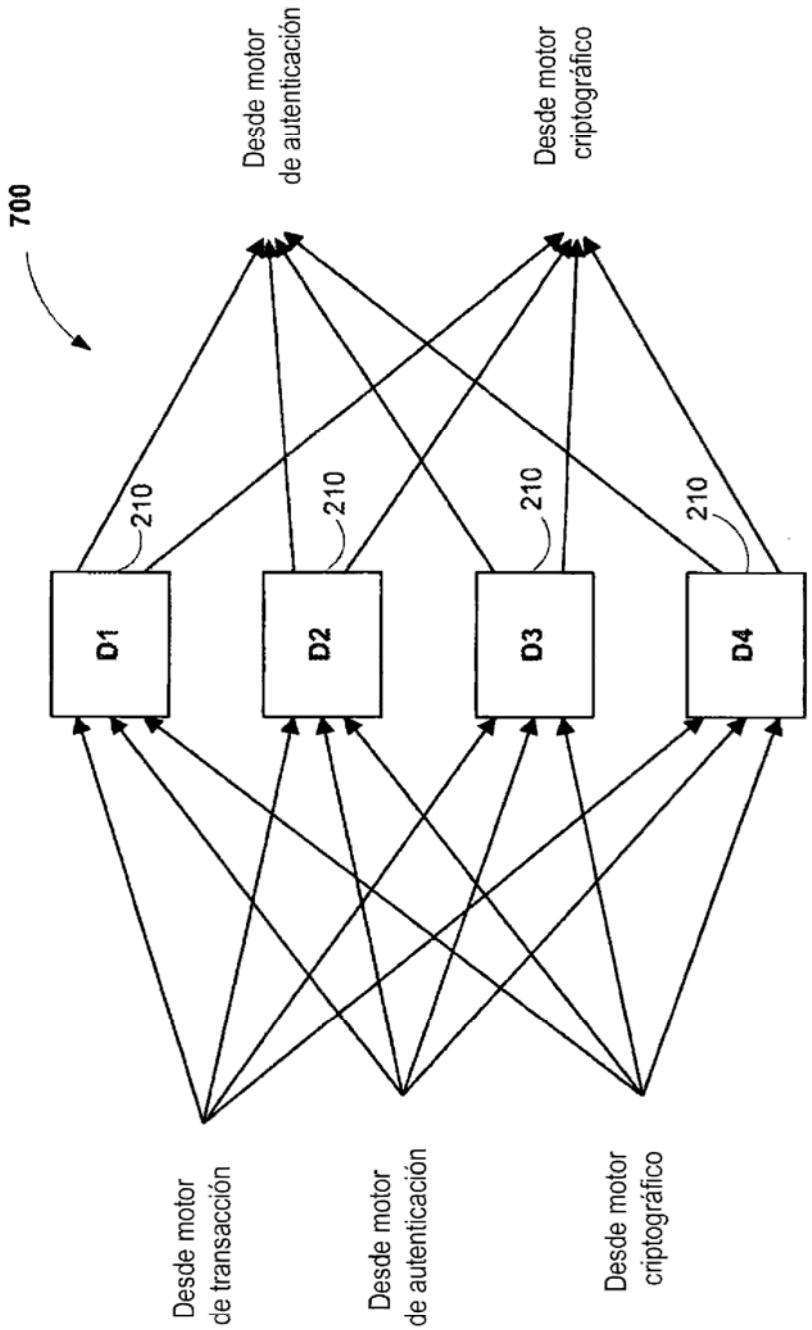

700
Desde motor de autenticación
Desde motor criptográfico
210
210
210
210
D1
D2
D3
D4
Desde motor de transacción
Desde motor de autenticación
Desde motor criptográfico

FIG. 7

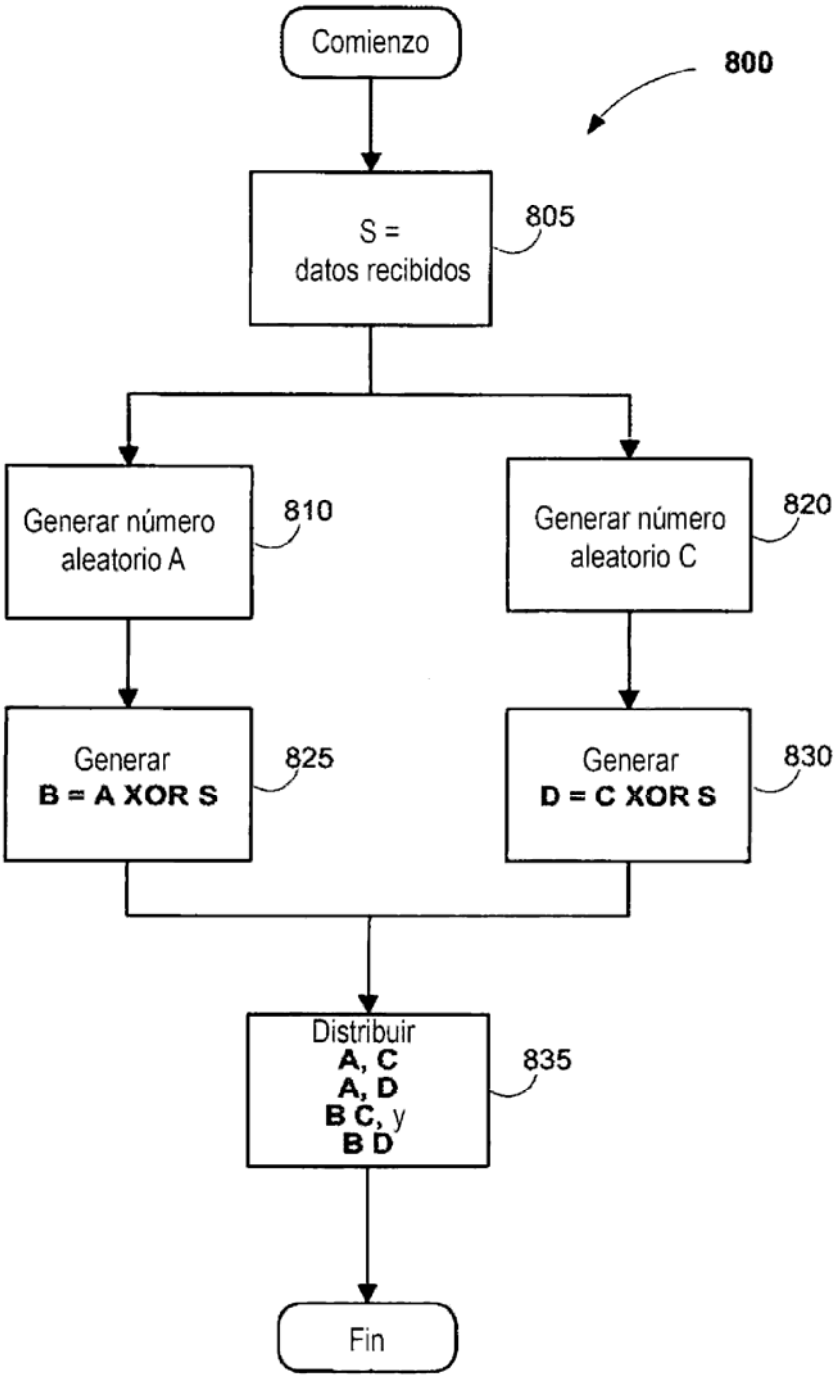
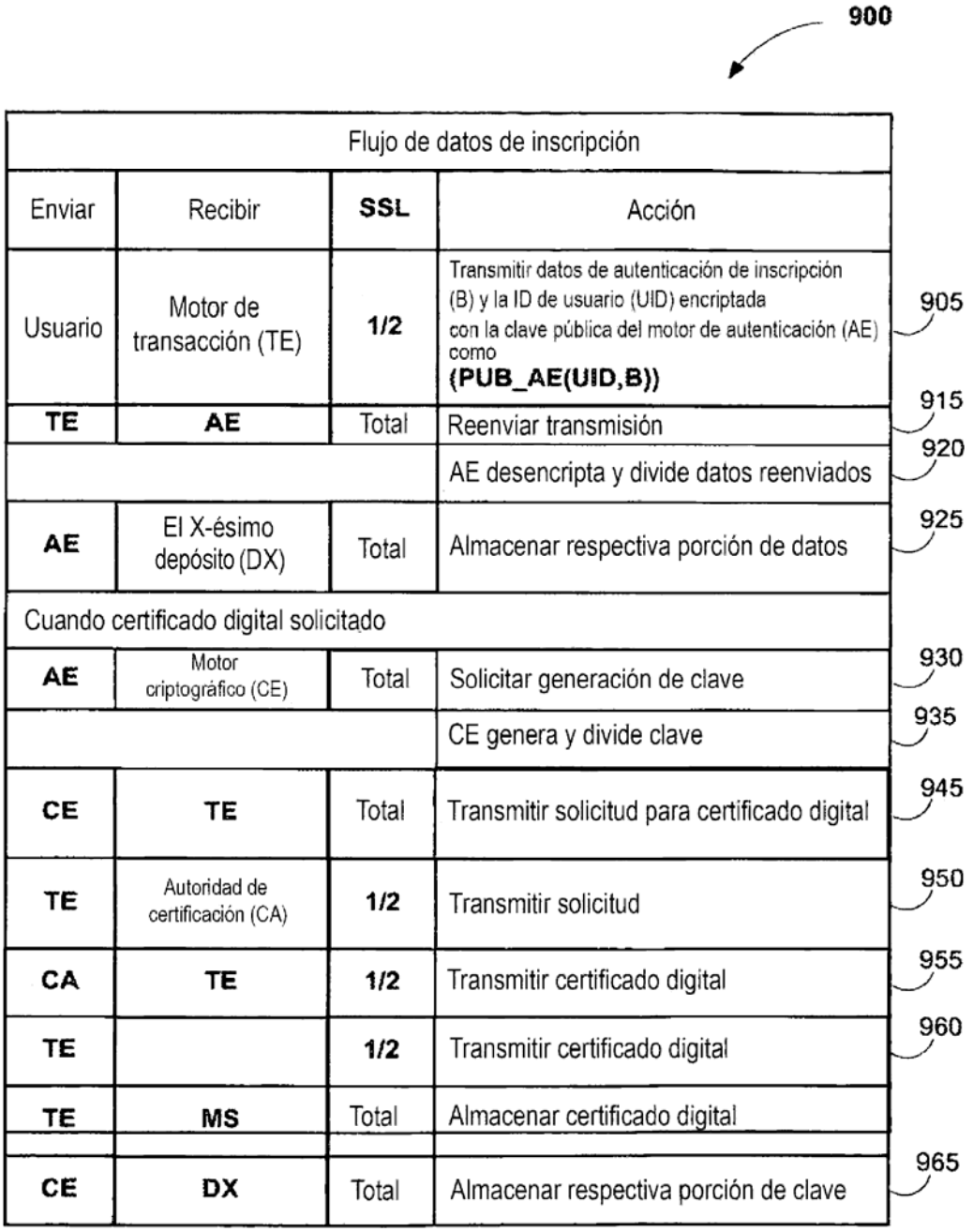

Comienzo
800
S =
datos recibidos
805
Generar número
aleatorio A
810
Generar número
aleatorio C
820
Generar
B = A XOR S
825
Generar
D = C XOR S
830
Distribuir
A, C
A, D
B C, y
B D
835
Fin

FIG. 8



900

Flujo de datos de inscripción				
Enviar	Recibir	SSL	Acción	
Usuario	Motor de transacción (TE)	1/2	Transmitir datos de autenticación de inscripción (B) y la ID de usuario (UID) encriptada con la clave pública del motor de autenticación (AE) como **(PUB_AE(UID,B))**	905
TE	**AE**	Total	Reenviar transmisión	915
			AE desencripta y divide datos reenviados	920
AE	El X-ésimo depósito (DX)	Total	Almacenar respectiva porción de datos	925
Cuando certificado digital solicitado				
AE	Motor criptográfico (CE)	Total	Solicitar generación de clave	930
			CE genera y divide clave	935
CE	**TE**	Total	Transmitir solicitud para certificado digital	945
TE	Autoridad de certificación (CA)	1/2	Transmitir solicitud	950
CA	**TE**	1/2	Transmitir certificado digital	955
TE		1/2	Transmitir certificado digital	960
TE	**MS**	Total	Almacenar certificado digital	
CE	**DX**	Total	Almacenar respectiva porción de clave	965

FIG. 9, Panel A

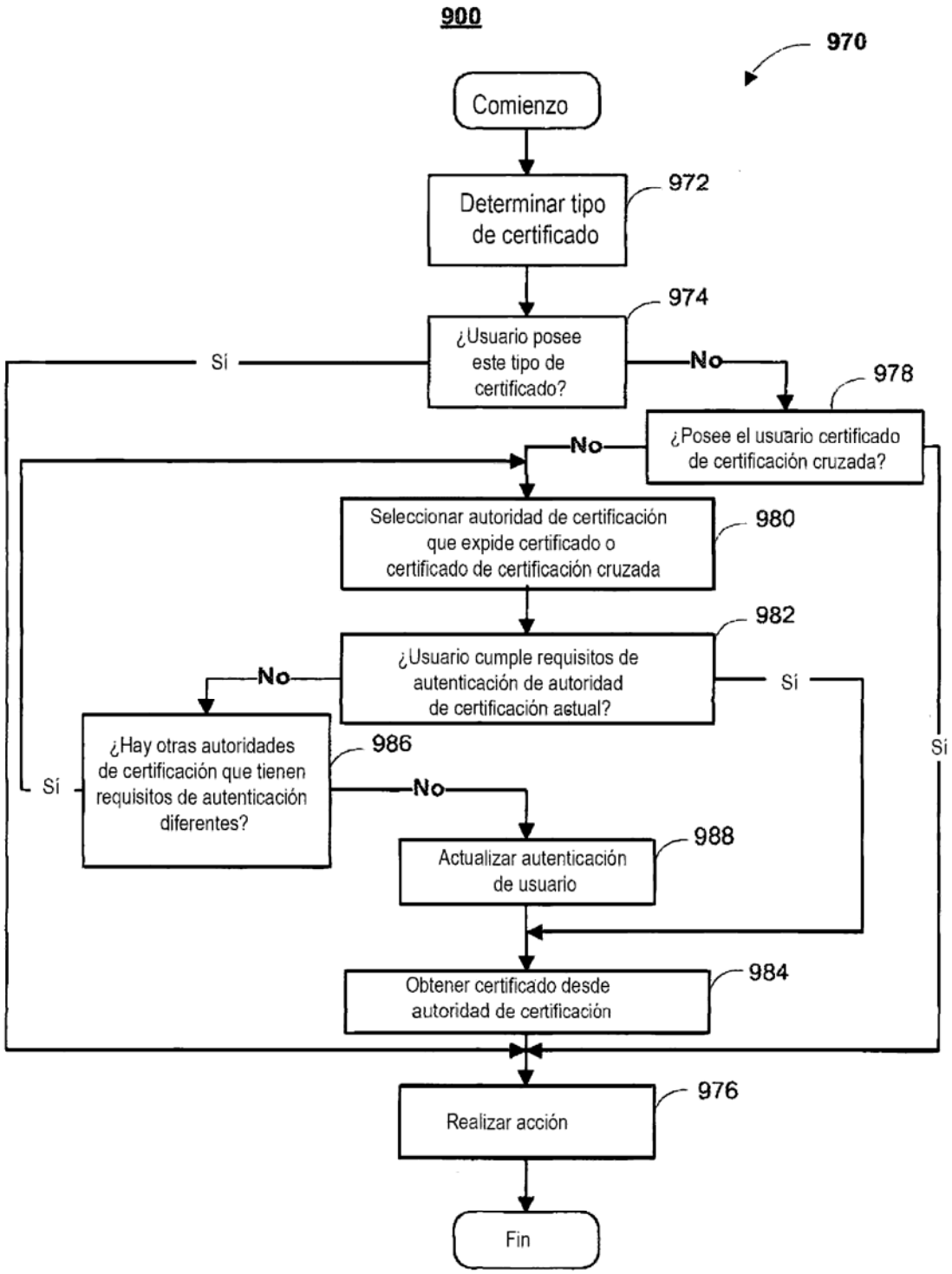

900
970
Comienzo
Determinar tipo de certificado
972
¿Usuario posee este tipo de certificado?
974
Sí
No
¿Posee el usuario certificado de certificación cruzada?
978
No
Seleccionar autoridad de certificación que expide certificado o certificado de certificación cruzada
980
¿Usuario cumple requisitos de autenticación de autoridad de certificación actual?
982
No
Sí
¿Hay otras autoridades de certificación que tienen requisitos de autenticación diferentes?
986
Sí
No
Actualizar autenticación de usuario
988
Obtener certificado desde autoridad de certificación
984
Sí
Realizar acción
976
Fin

FIG. 9, Panel B

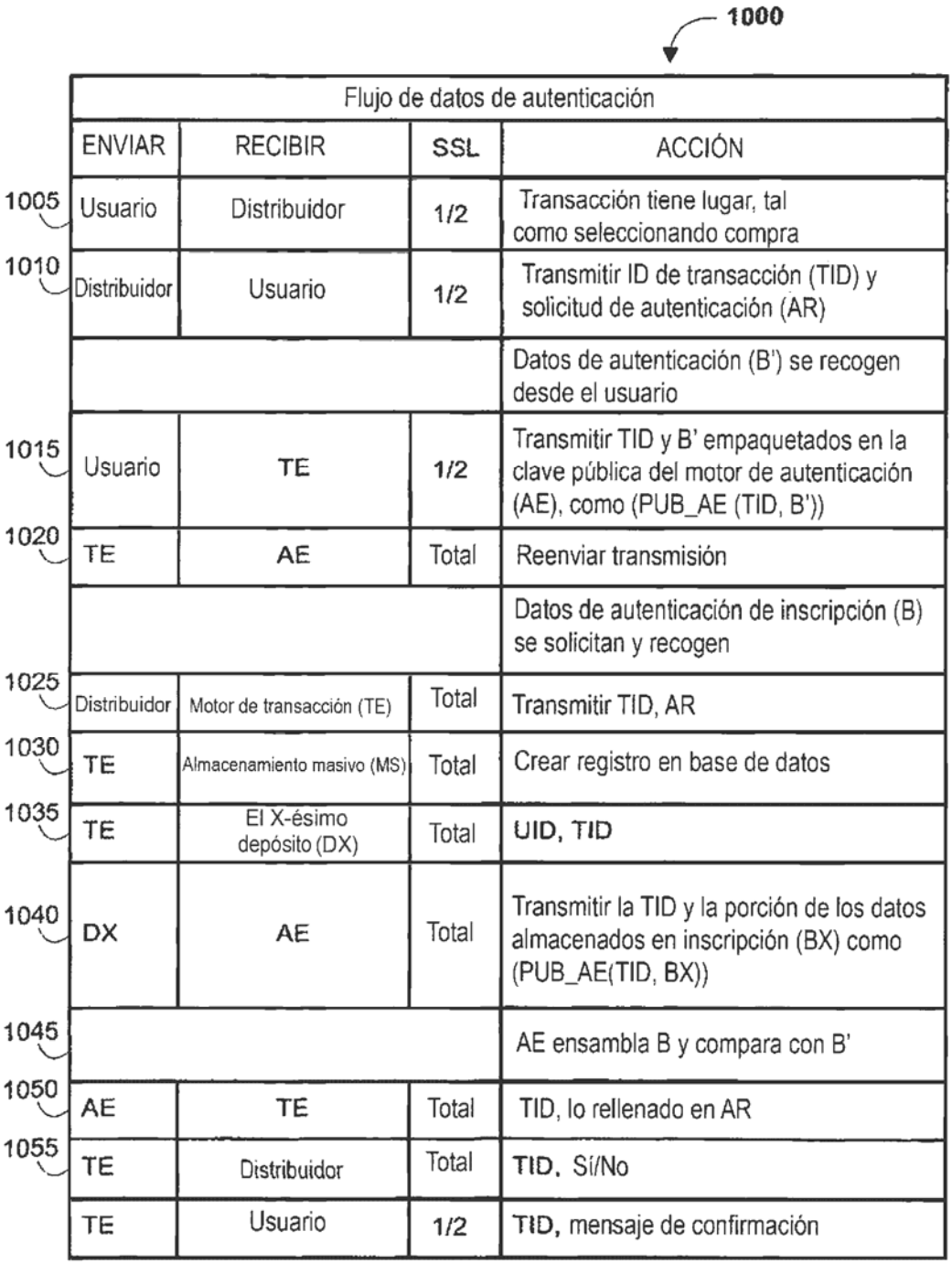

1000
Flujo de datos de autenticación
ENVIAR
RECIBIR
SSL
ACCIÓN
1005
Usuario
Distribuidor
1/2
Transacción tiene lugar, tal como seleccionando compra
1010
Distribuidor
Usuario
1/2
Transmitir ID de transacción (TID) y solicitud de autenticación (AR)
Datos de autenticación (B') se recogen desde el usuario
1015
Usuario
TE
1/2
Transmitir TID y B' empaquetados en la clave pública del motor de autenticación (AE), como (PUB_AE (TID, B'))
1020
TE
AE
Total
Reenviar transmisión
Datos de autenticación de inscripción (B) se solicitan y recogen
1025
Distribuidor
Motor de transacción (TE)
Total
Transmitir TID, AR
1030
TE
Almacenamiento masivo (MS)
Total
Crear registro en base de datos
1035
TE
El X-ésimo depósito (DX)
Total
UID, TID
1040
DX
AE
Total
Transmitir la TID y la porción de los datos almacenados en inscripción (BX) como (PUB_AE(TID, BX))
1045
AE ensambla B y compara con B'
1050
AE
TE
Total
TID, lo rellenado en AR
1055
TE
Distribuidor
Total
TID, Sí/No
TE
Usuario
1/2
TID, mensaje de confirmación

FIG. 10

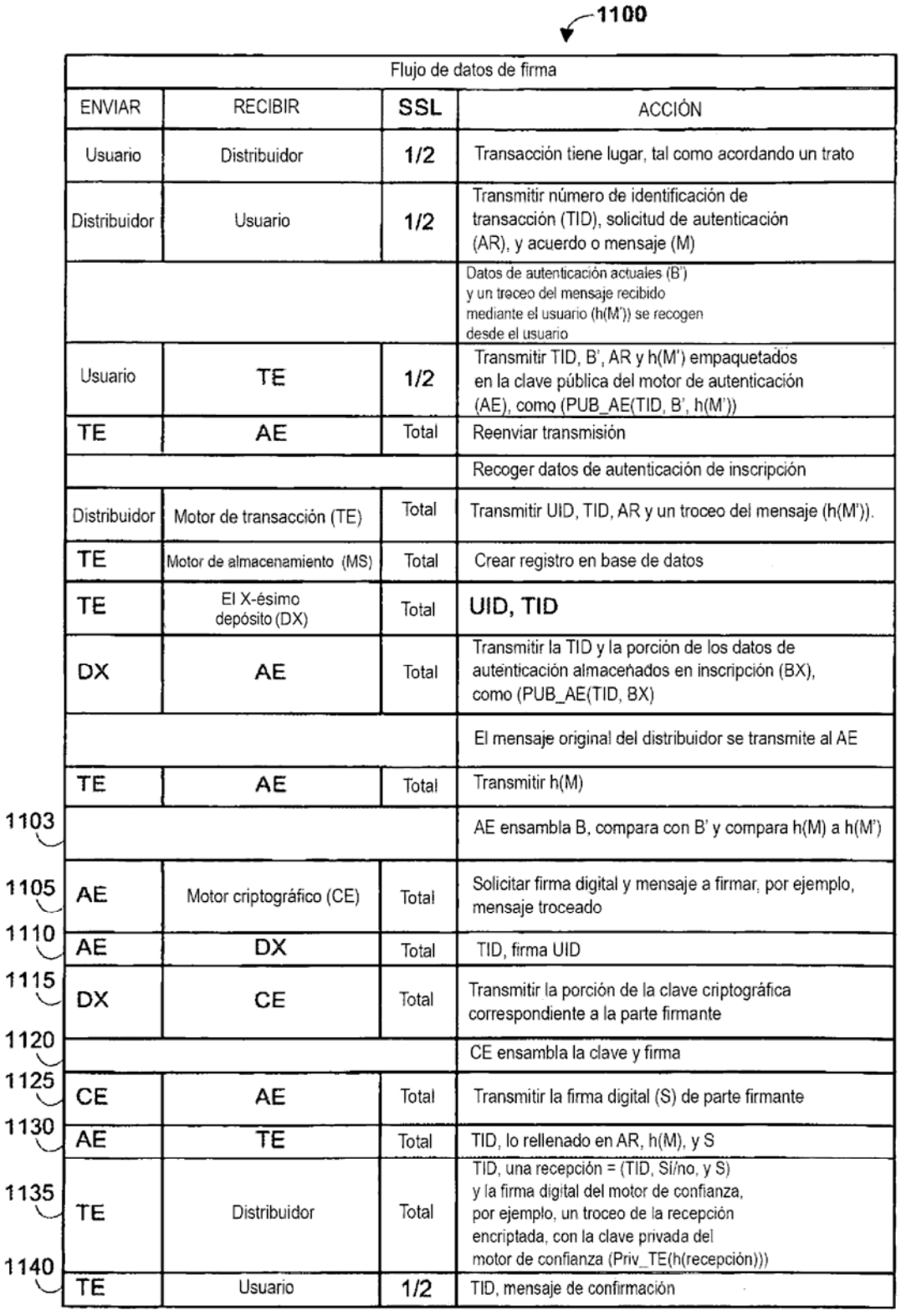

1100
Flujo de datos de firma
ENVIAR
RECIBIR
SSL
ACCIÓN
Usuario
Distribuidor
1/2
Transacción tiene lugar, tal como acordando un trato
Distribuidor
Usuario
1/2
Transmitir número de identificación de transacción (TID), solicitud de autenticación (AR), y acuerdo o mensaje (M)
Datos de autenticación actuales (B') y un troceo del mensaje recibido mediante el usuario (h(M')) se recogen desde el usuario
Usuario
TE
1/2
Transmitir TID, B', AR y h(M') empaquetados en la clave pública del motor de autenticación (AE), como (PUB_AE(TID, B', h(M'))
TE
AE
Total
Reenviar transmisión
Recoger datos de autenticación de inscripción
Distribuidor
Motor de transacción (TE)
Total
Transmitir UID, TID, AR y un troceo del mensaje (h(M')).
TE
Motor de almacenamiento (MS)
Total
Crear registro en base de datos
TE
El X-ésimo depósito (DX)
Total
UID, TID
DX
AE
Total
Transmitir la TID y la porción de los datos de autenticación almacenados en inscripción (BX), como (PUB_AE(TID, BX)
El mensaje original del distribuidor se transmite al AE
TE
AE
Total
Transmitir h(M)
1103
AE ensambla B, compara con B' y compara h(M) a h(M')
1105
AE
Motor criptográfico (CE)
Total
Solicitar firma digital y mensaje a firmar, por ejemplo, mensaje troceado
1110
AE
DX
Total
TID, firma UID
1115
DX
CE
Total
Transmitir la porción de la clave criptográfica correspondiente a la parte firmante
1120
CE ensambla la clave y firma
1125
CE
AE
Total
Transmitir la firma digital (S) de parte firmante
1130
AE
TE
Total
TID, lo rellenado en AR, h(M), y S
1135
TE
Distribuidor
Total
TID, una recepción = (TID, Sí/no, y S) y la firma digital del motor de confianza, por ejemplo, un troceo de la recepción encriptada, con la clave privada del motor de confianza (Priv_TE(h(recepción)))
1140
TE
Usuario
1/2
TID, mensaje de confirmación

FIG. 11

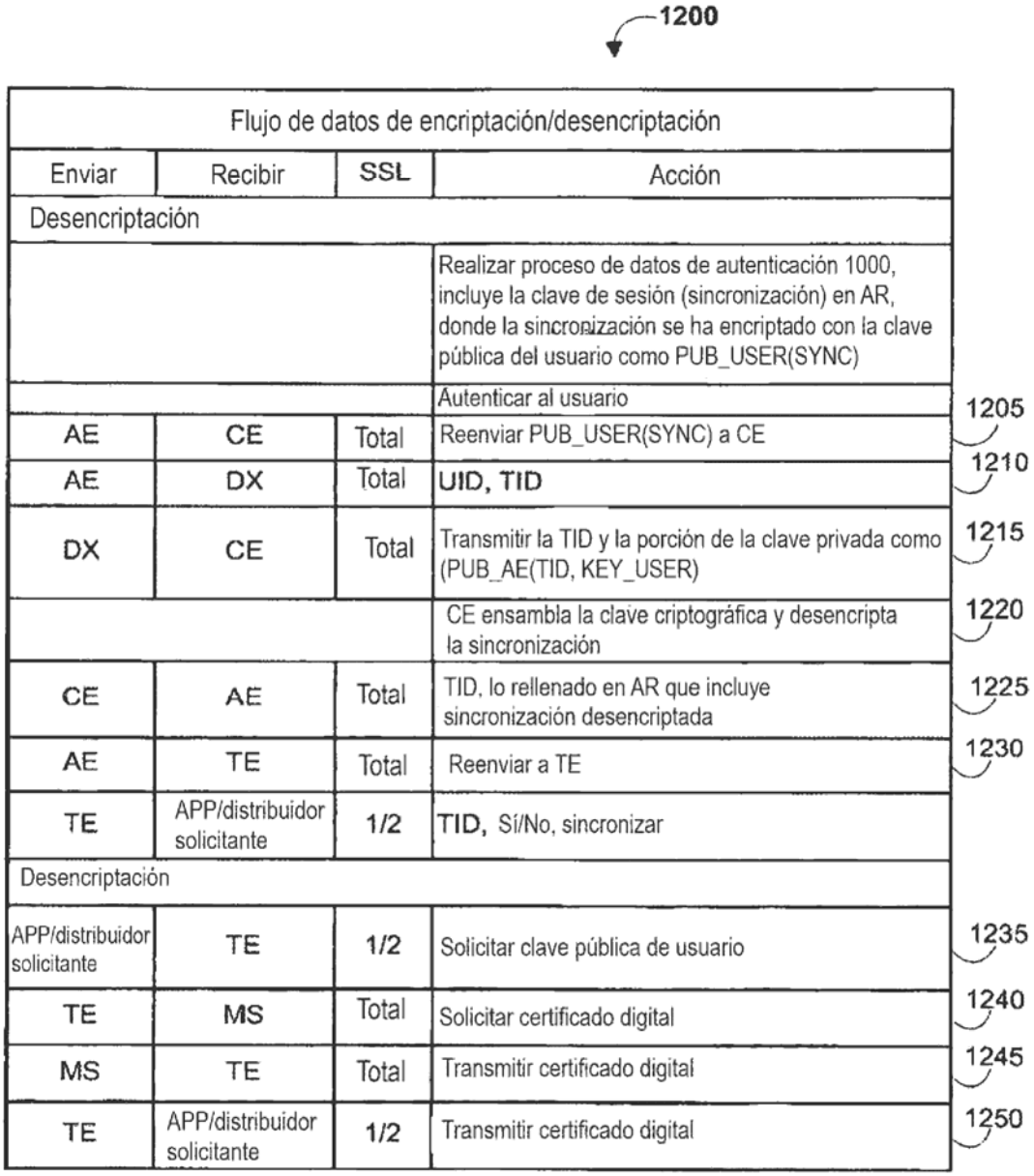

1200
Flujo de datos de encriptación/desencriptación
Enviar
Recibir
SSL
Acción
Desencriptación
Realizar proceso de datos de autenticación 1000, incluye la clave de sesión (sincronización) en AR, donde la sincronización se ha encriptado con la clave pública del usuario como PUB_USER(SYNC)
Autenticar al usuario
AE
CE
Total
Reenviar PUB_USER(SYNC) a CE
1205
AE
DX
Total
UID, TID
1210
DX
CE
Total
Transmitir la TID y la porción de la clave privada como (PUB_AE(TID, KEY_USER)
1215
CE ensambla la clave criptográfica y desencripta la sincronización
1220
CE
AE
Total
TID, lo rellenado en AR que incluye sincronización desencriptada
1225
AE
TE
Total
Reenviar a TE
1230
TE
APP/distribuidor solicitante
1/2
TID, Sí/No, sincronizar
Desencriptación
APP/distribuidor solicitante
TE
1/2
Solicitar clave pública de usuario
1235
TE
MS
Total
Solicitar certificado digital
1240
MS
TE
Total
Transmitir certificado digital
1245
TE
APP/distribuidor solicitante
1/2
Transmitir certificado digital
1250

FIG. 12

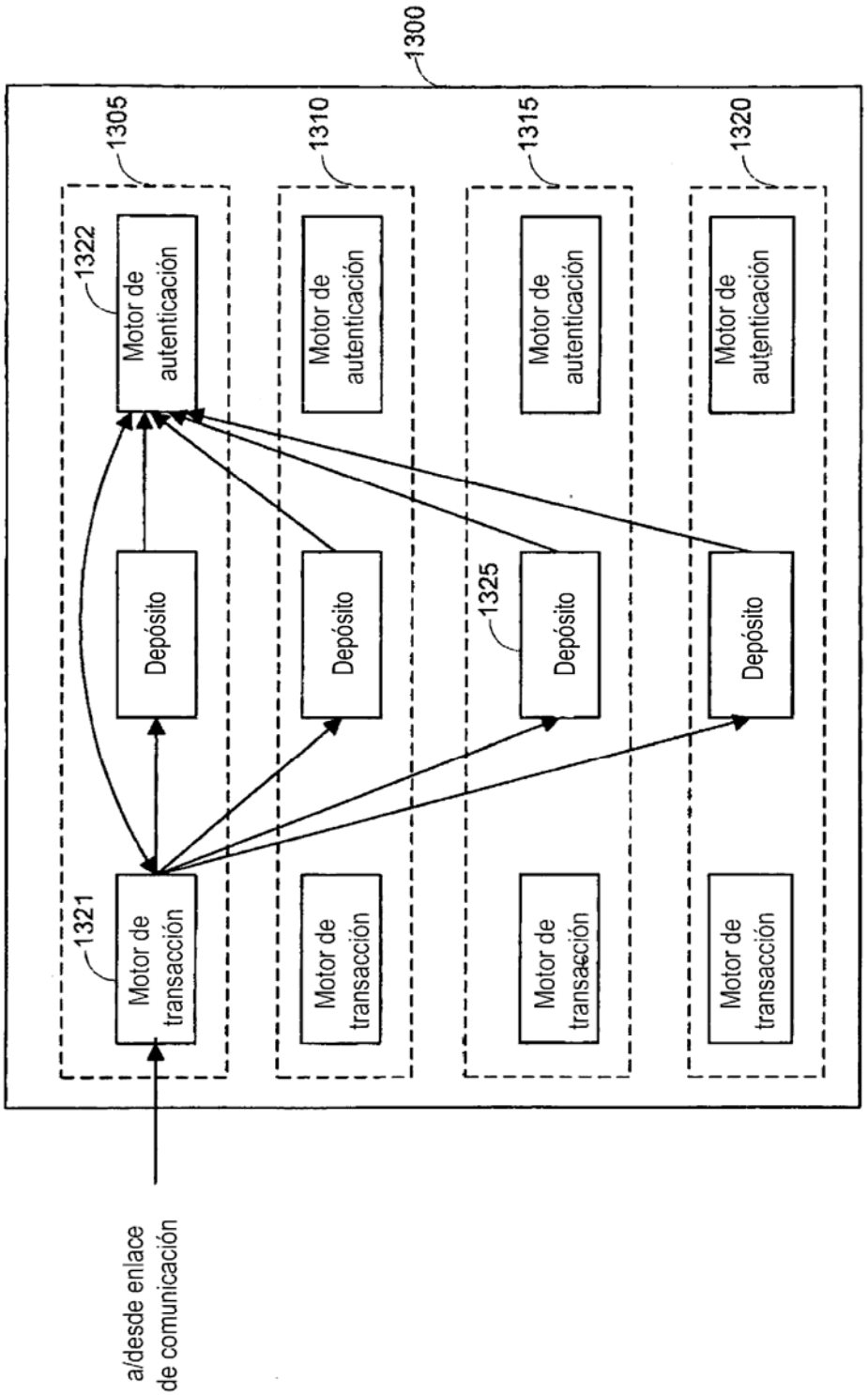

1300
1305
1310
1315
1320
1322
Motor de autenticación
Motor de autenticación
Motor de autenticación
Motor de autenticación
Depósito
Depósito
1325
Depósito
Depósito
1321
Motor de transacción
Motor de transacción
Motor de transacción
Motor de transacción
a/desde enlace de comunicación

FIG. 13

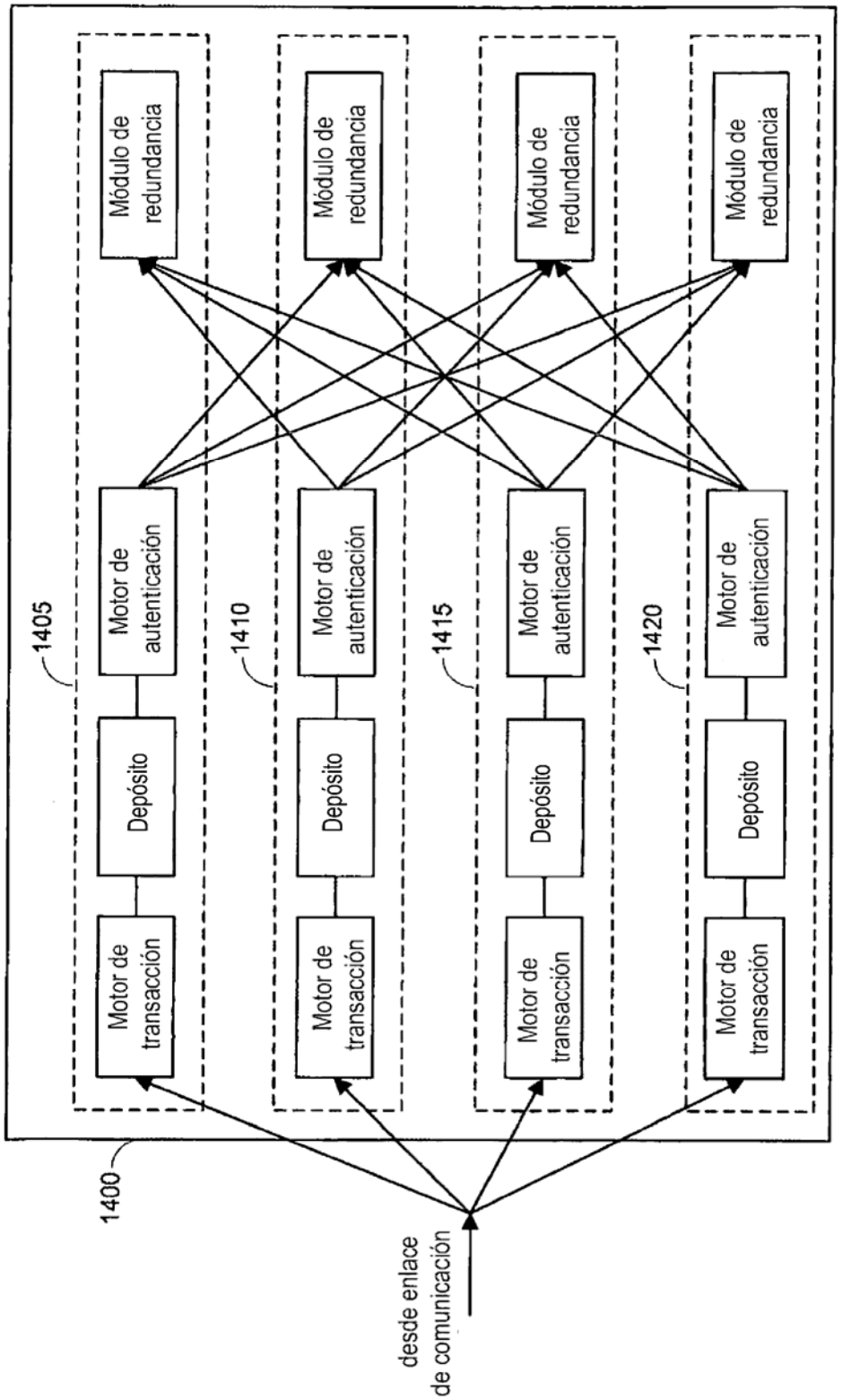

1400
desde enlace de comunicación
1405
1410
1415
1420
Motor de transacción
Depósito
Motor de autenticación
Módulo de redundancia

FIG. 14

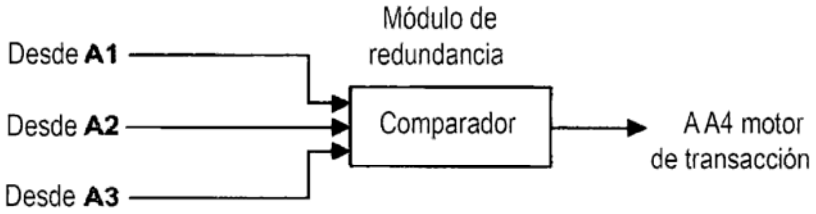

Módulo de
redundancia
Desde A1
Desde A2
Desde A3
Comparador
A A4 motor
de transacción

FIG. 15

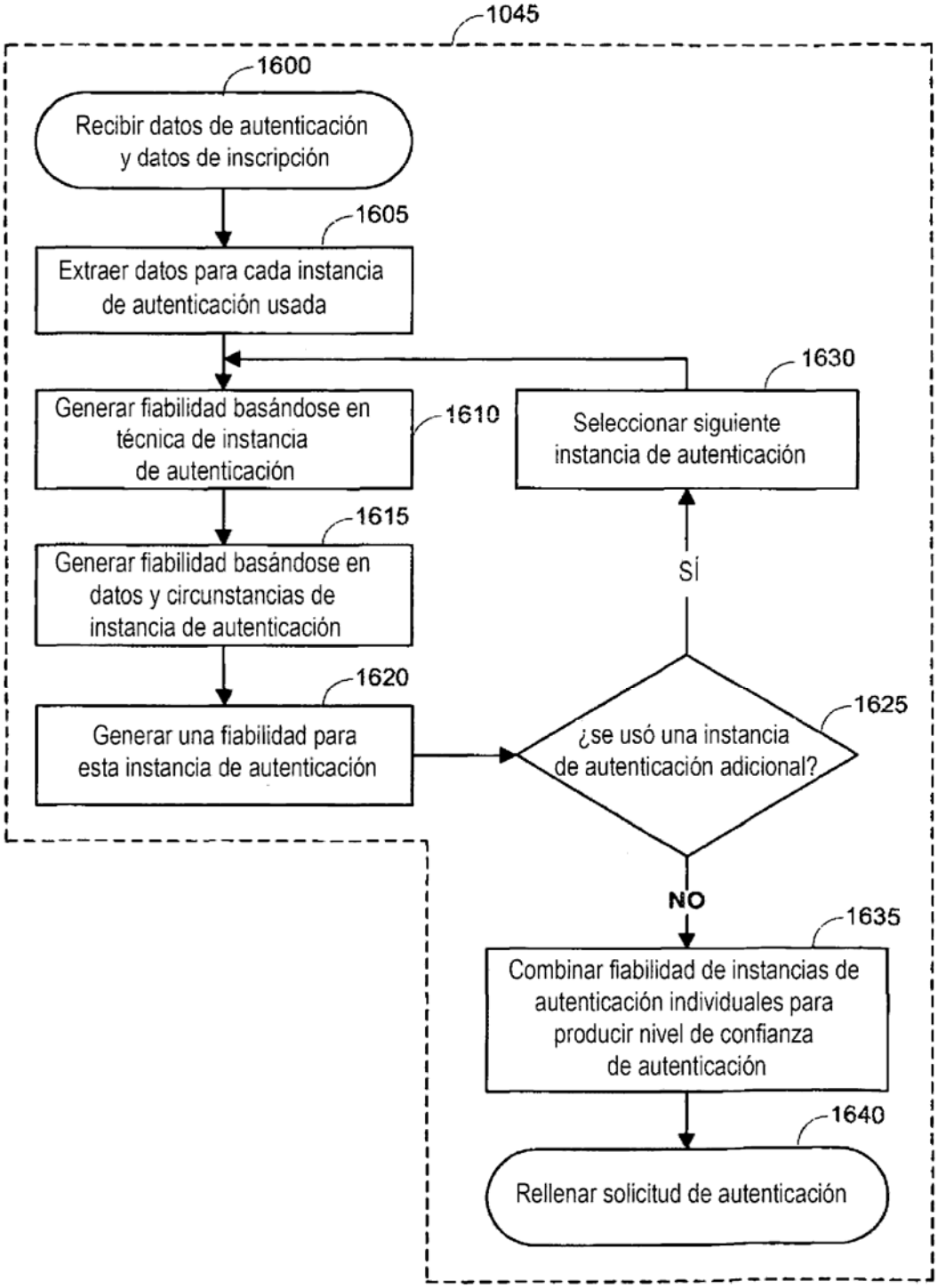

1045
1600
Recibir datos de autenticación y datos de inscripción
1605
Extraer datos para cada instancia de autenticación usada
1610
Generar fiabilidad basándose en técnica de instancia de autenticación
1615
Generar fiabilidad basándose en datos y circunstancias de instancia de autenticación
1620
Generar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

FIG. 16

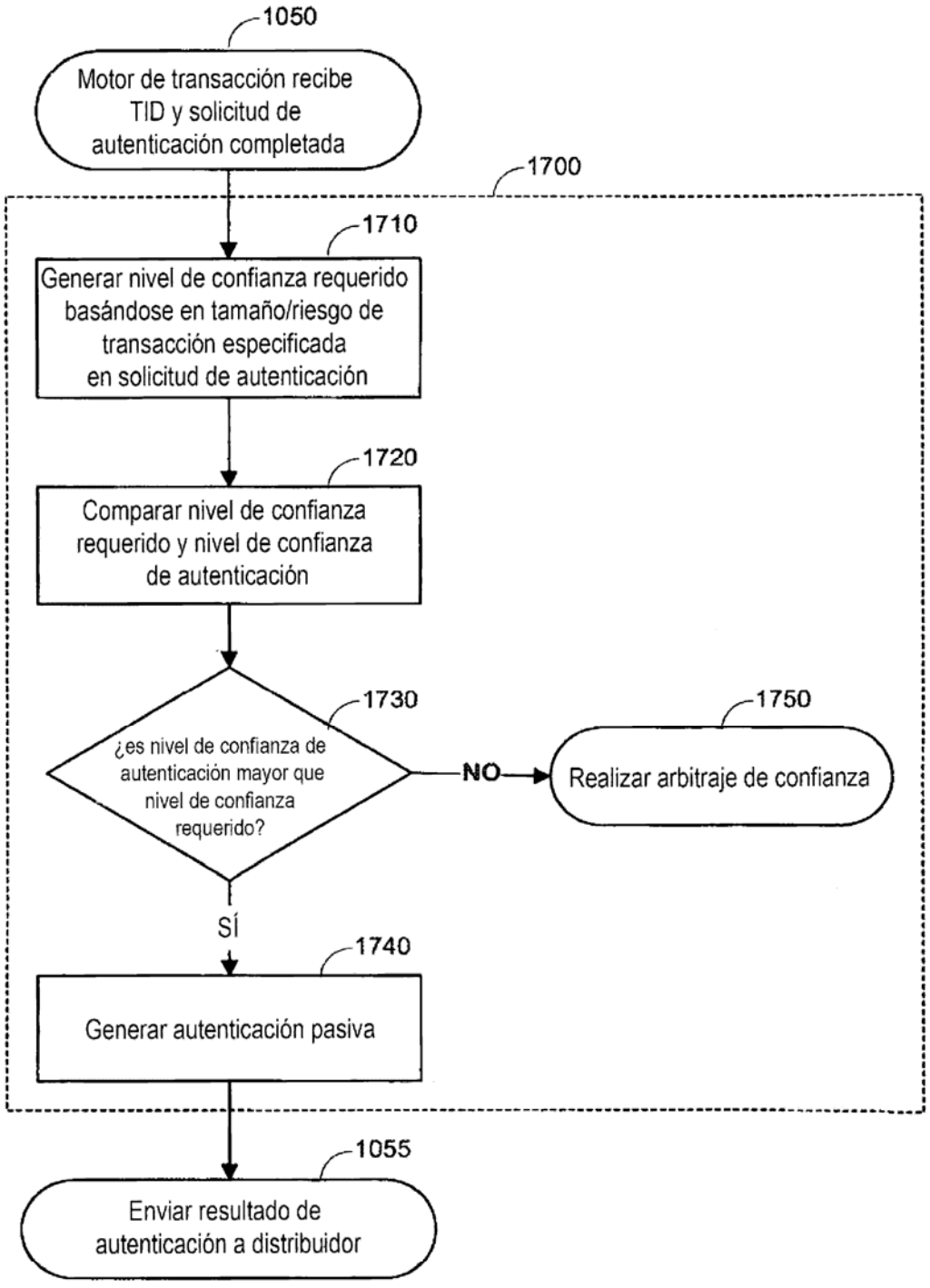

1050
Motor de transacción recibe TID y solicitud de autenticación completada
1700
1710
Generar nivel de confianza requerido basándose en tamaño/riesgo de transacción especificada en solicitud de autenticación
1720
Comparar nivel de confianza requerido y nivel de confianza de autenticación
1730
¿es nivel de confianza de autenticación mayor que nivel de confianza requerido?
NO
1750
Realizar arbitraje de confianza
SÍ
1740
Generar autenticación pasiva
1055
Enviar resultado de autenticación a distribuidor

FIG. 17

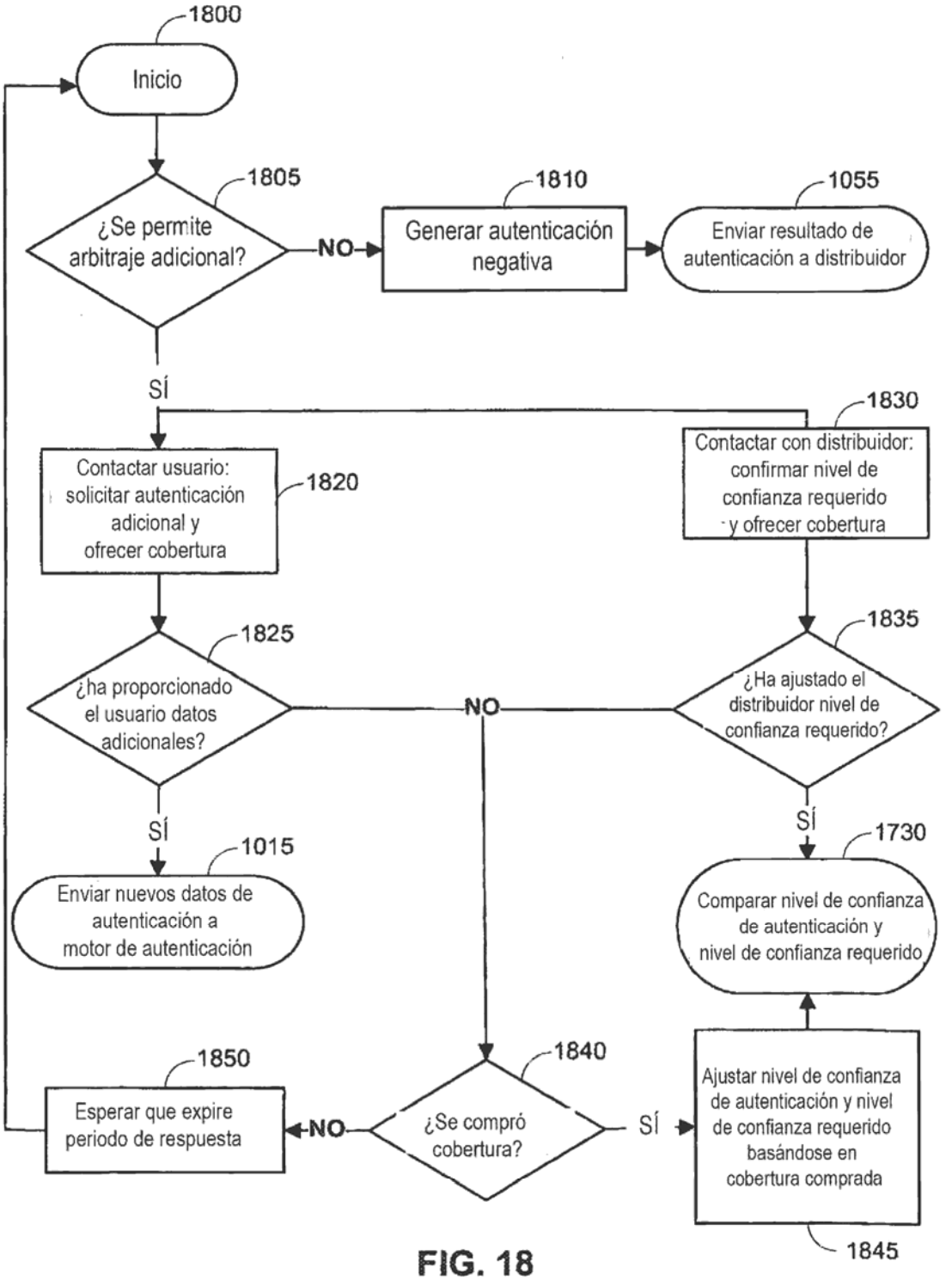

1800
Inicio
1805
¿Se permite arbitraje adicional?
NO
1810
Generar autenticación negativa
1055
Enviar resultado de autenticación a distribuidor
SÍ
1830
Contactar con distribuidor: confirmar nivel de confianza requerido y ofrecer cobertura
Contactar usuario: solicitar autenticación adicional y ofrecer cobertura
1820
1835
¿Ha ajustado el distribuidor nivel de confianza requerido?
1825
¿ha proporcionado el usuario datos adicionales?
NO
SÍ
SÍ
1730
1015
Enviar nuevos datos de autenticación a motor de autenticación
Comparar nivel de confianza de autenticación y nivel de confianza requerido
1840
1850
Esperar que expire periodo de respuesta
NO
¿Se compró cobertura?
SÍ
Ajustar nivel de confianza de autenticación y nivel de confianza requerido basándose en cobertura comprada
1845

FIG. 18

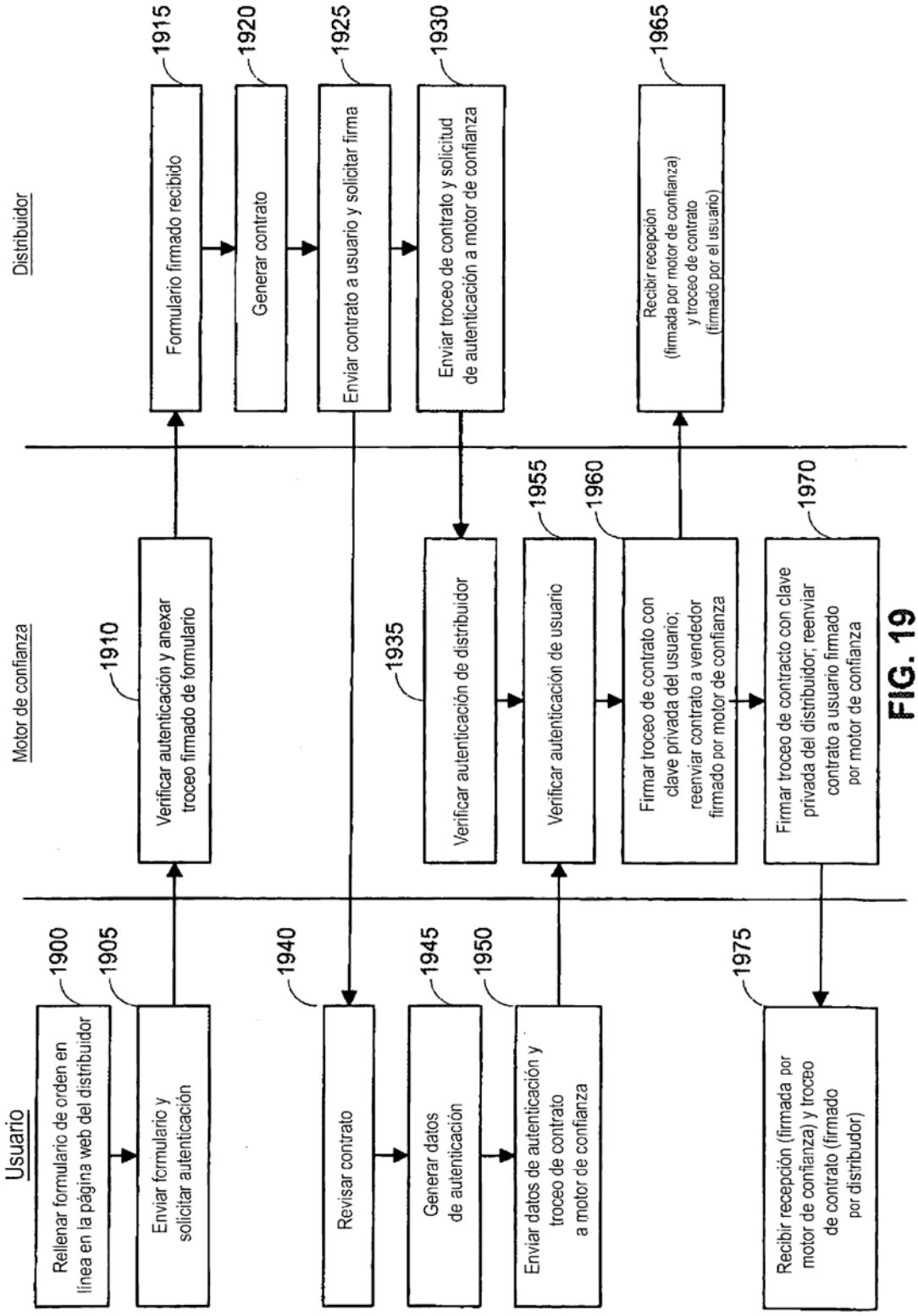

Usuario
Motor de confianza
Distribuidor
1900
Rellenar formulario de orden en línea en la página web del distribuidor
1905
Enviar formulario y solicitar autenticación
1910
Verificar autenticación y anexar troceo firmado de formulario
1915
Formulario firmado recibido
1920
Generar contrato
1925
Enviar contrato a usuario y solicitar firma
1930
Enviar troceo de contrato y solicitud de autenticación a motor de confianza
1935
Verificar autenticación de distribuidor
1940
Revisar contrato
1945
Generar datos de autenticación
1950
Enviar datos de autenticación y troceo de contrato a motor de confianza
1955
Verificar autenticación de usuario
1960
Firmar troceo de contrato con clave privada del usuario; reenviar contrato a vendedor firmado por motor de confianza
1965
Recibir recepción (firmada por motor de confianza) y troceo de contrato (firmado por el usuario)
1970
Firmar troceo de contracto con clave privada del distribuidor; reenviar contrato a usuario firmado por motor de confianza
1975
Recibir recepción (firmada por motor de confianza) y troceo de contrato (firmado por distribudor)

FIG. 19

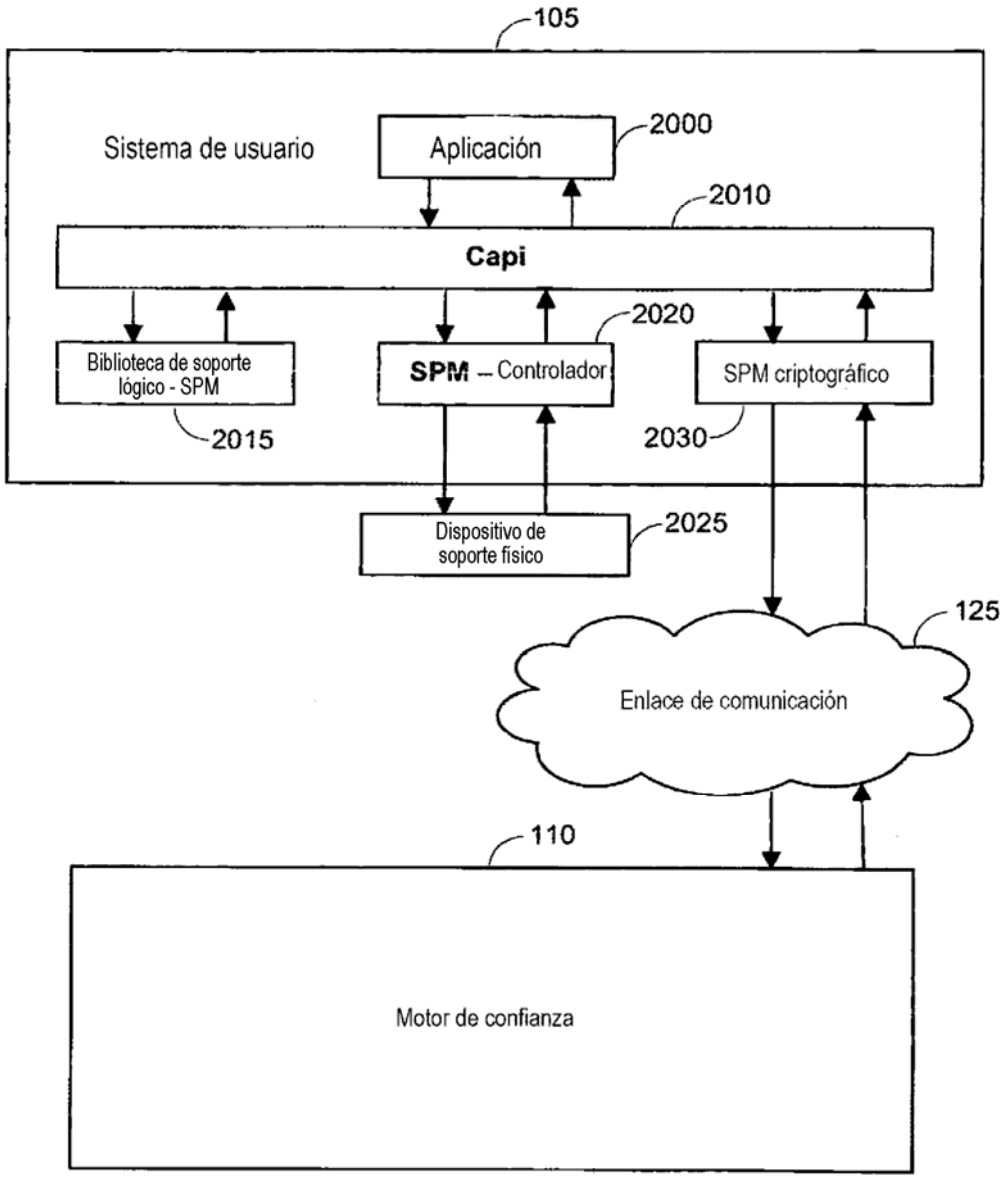

105
Sistema de usuario
Aplicación
2000
2010
Capi
2020
Biblioteca de soporte lógico - SPM
SPM – Controlador
SPM criptográfico
2015
2030
Dispositivo de soporte físico
2025
125
Enlace de comunicación
110
Motor de confianza

FIG. 20

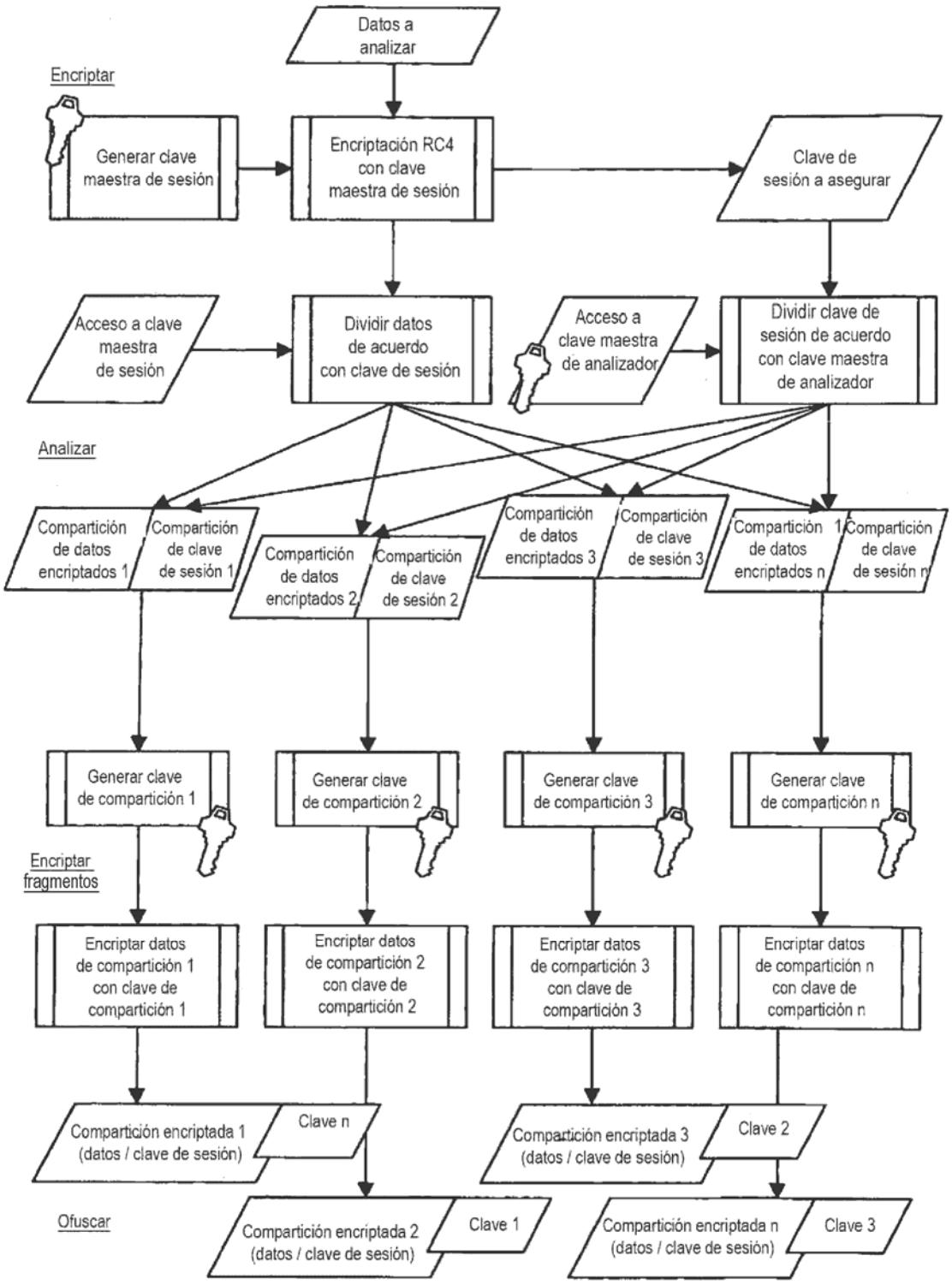

Datos a analizar
Encriptar
Generar clave maestra de sesión
Encriptación RC4 con clave maestra de sesión
Clave de sesión a asegurar
Acceso a clave maestra de sesión
Dividir datos de acuerdo con clave de sesión
Acceso a clave maestra de analizador
Dividir clave de sesión de acuerdo con clave maestra de analizador
Analizar
Compartición de datos encriptados 1
Compartición de clave de sesión 1
Compartición de datos encriptados 2
Compartición de clave de sesión 2
Compartición de datos encriptados 3
Compartición de clave de sesión 3
Compartición de datos encriptados n
Compartición de clave de sesión n
Generar clave de compartición 1
Generar clave de compartición 2
Generar clave de compartición 3
Generar clave de compartición n
Encriptar fragmentos
Encriptar datos de compartición 1 con clave de compartición 1
Encriptar datos de compartición 2 con clave de compartición 2
Encriptar datos de compartición 3 con clave de compartición 3
Encriptar datos de compartición n con clave de compartición n
Compartición encriptada 1 (datos / clave de sesión)
Clave n
Compartición encriptada 3 (datos / clave de sesión)
Clave 2
Ofuscar
Compartición encriptada 2 (datos / clave de sesión)
Clave 1
Compartición encriptada n (datos / clave de sesión)
Clave 3

FIG. 21

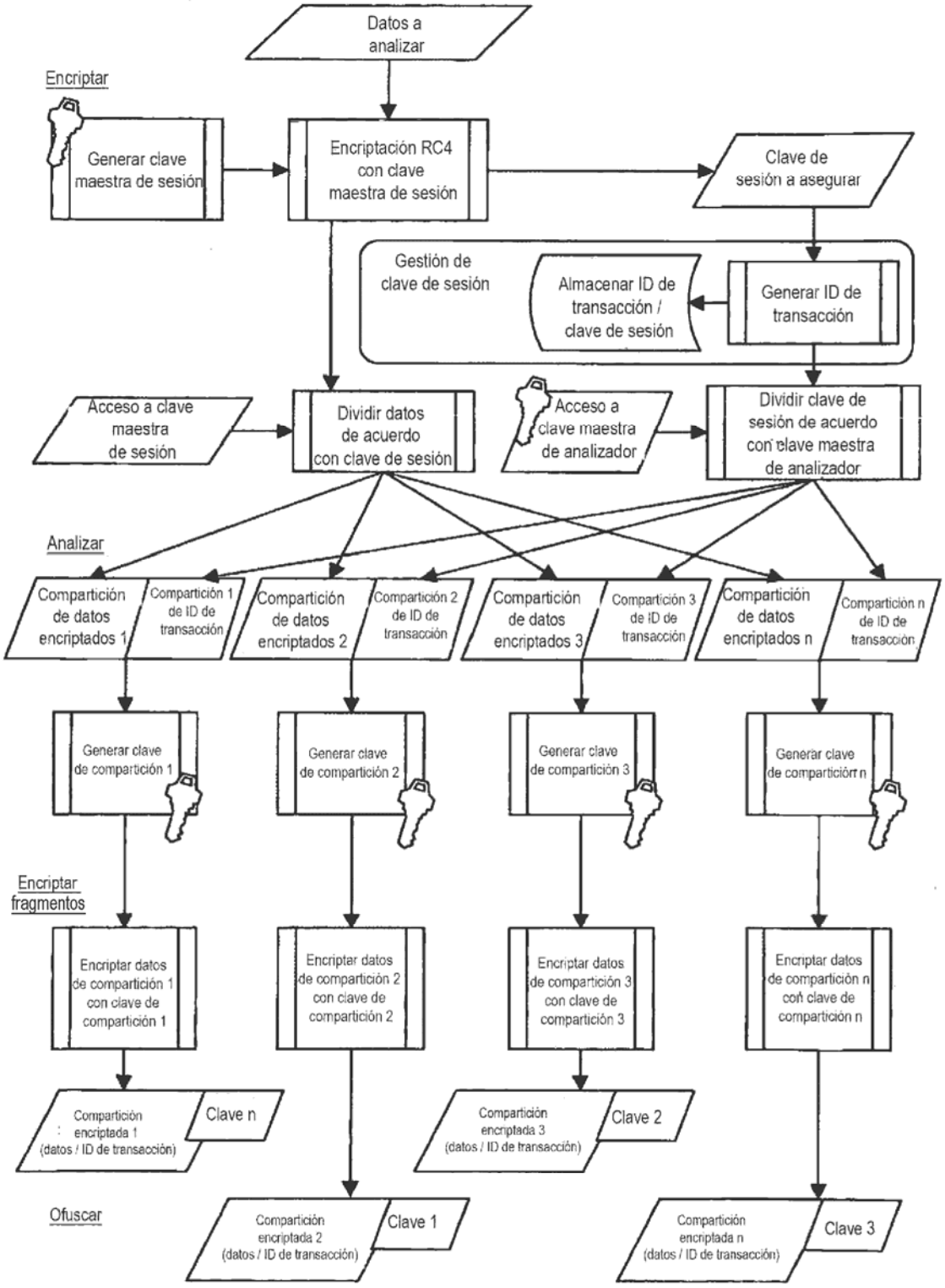

Datos a analizar
Encriptar
Generar clave maestra de sesión
Encriptación RC4 con clave maestra de sesión
Clave de sesión a asegurar
Gestión de clave de sesión
Almacenar ID de transacción / clave de sesión
Generar ID de transacción
Acceso a clave maestra de sesión
Dividir datos de acuerdo con clave de sesión
Acceso a clave maestra de analizador
Dividir clave de sesión de acuerdo con clave maestra de analizador
Analizar
Compartición de datos encriptados 1
Compartición 1 de ID de transacción
Compartición de datos encriptados 2
Compartición 2 de ID de transacción
Compartición de datos encriptados 3
Compartición 3 de ID de transacción
Compartición de datos encriptados n
Compartición n de ID de transacción
Generar clave de compartición 1
Generar clave de compartición 2
Generar clave de compartición 3
Generar clave de compartición n
Encriptar fragmentos
Encriptar datos de compartición 1 con clave de compartición 1
Encriptar datos de compartición 2 con clave de compartición 2
Encriptar datos de compartición 3 con clave de compartición 3
Encriptar datos de compartición n con clave de compartición n
Compartición encriptada 1 (datos / ID de transacción)
Clave n
Compartición encriptada 3 (datos / ID de transacción)
Clave 2
Ofuscar
Compartición encriptada 2 (datos / ID de transacción)
Clave 1
Compartición encriptada n (datos / ID de transacción)
Clave 3

FIG. 22

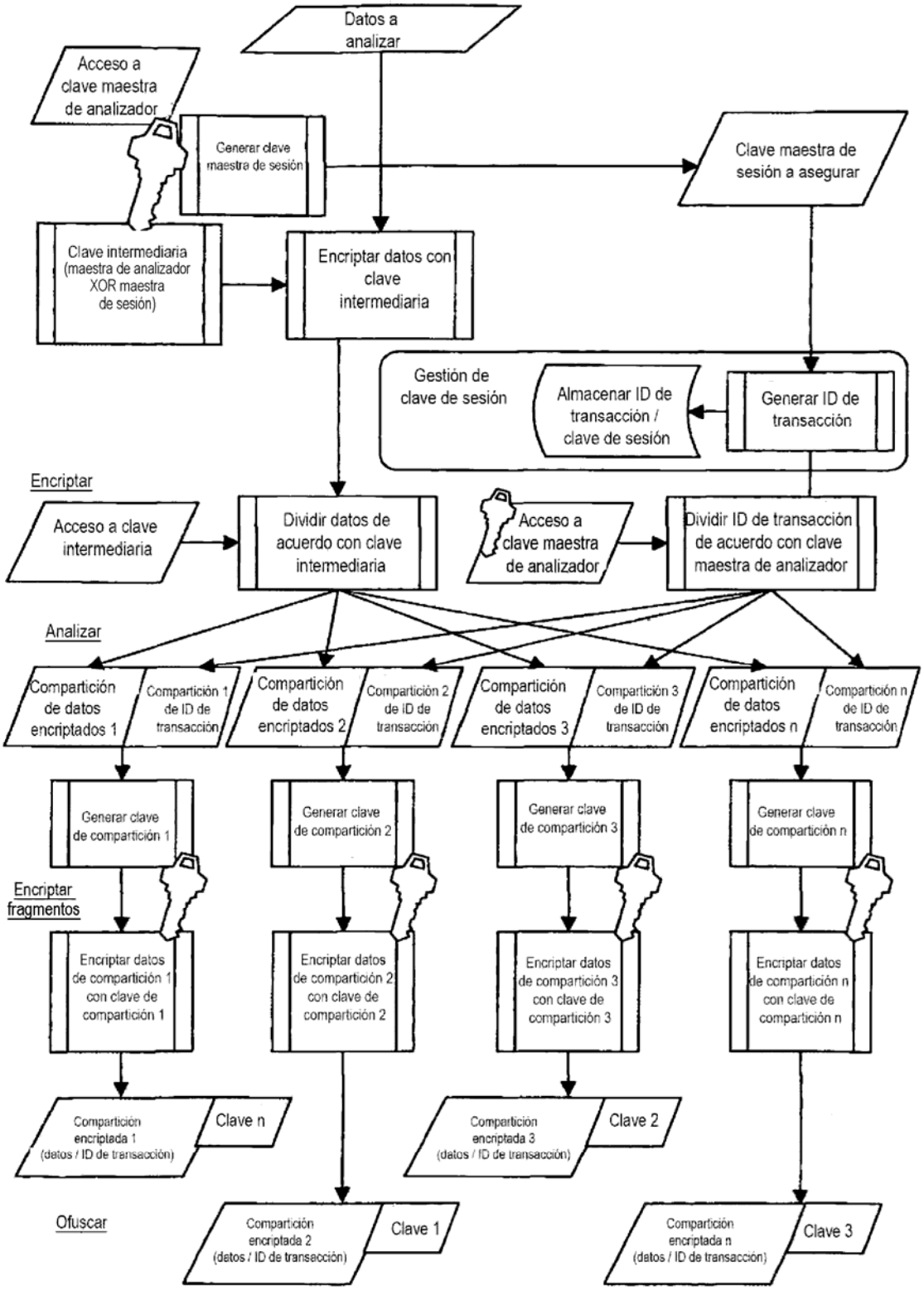

Datos a analizar
Acceso a clave maestra de analizador
Generar clave maestra de sesión
Clave maestra de sesión a asegurar
Clave intermediaria (maestra de analizador XOR maestra de sesión)
Encriptar datos con clave intermediaria
Gestión de clave de sesión
Almacenar ID de transacción / clave de sesión
Generar ID de transacción
Encriptar
Acceso a clave intermediaria
Dividir datos de acuerdo con clave intermediaria
Acceso a clave maestra de analizador
Dividir ID de transacción de acuerdo con clave maestra de analizador
Analizar
Compartición de datos encriptados 1
Compartición 1 de ID de transacción
Compartición de datos encriptados 2
Compartición 2 de ID de transacción
Compartición de datos encriptados 3
Compartición 3 de ID de transacción
Compartición de datos encriptados n
Compartición n de ID de transacción
Generar clave de compartición 1
Generar clave de compartición 2
Generar clave de compartición 3
Generar clave de compartición n
Encriptar fragmentos
Encriptar datos de compartición 1 con clave de compartición 1
Encriptar datos de compartición 2 con clave de compartición 2
Encriptar datos de compartición 3 con clave de compartición 3
Encriptar datos de compartición n con clave de compartición n
Compartición encriptada 1 (datos / ID de transacción)
Clave n
Compartición encriptada 3 (datos / ID de transacción)
Clave 2
Ofuscar
Compartición encriptada 2 (datos / ID de transacción)
Clave 1
Compartición encriptada n (datos / ID de transacción)
Clave 3

FIG. 23

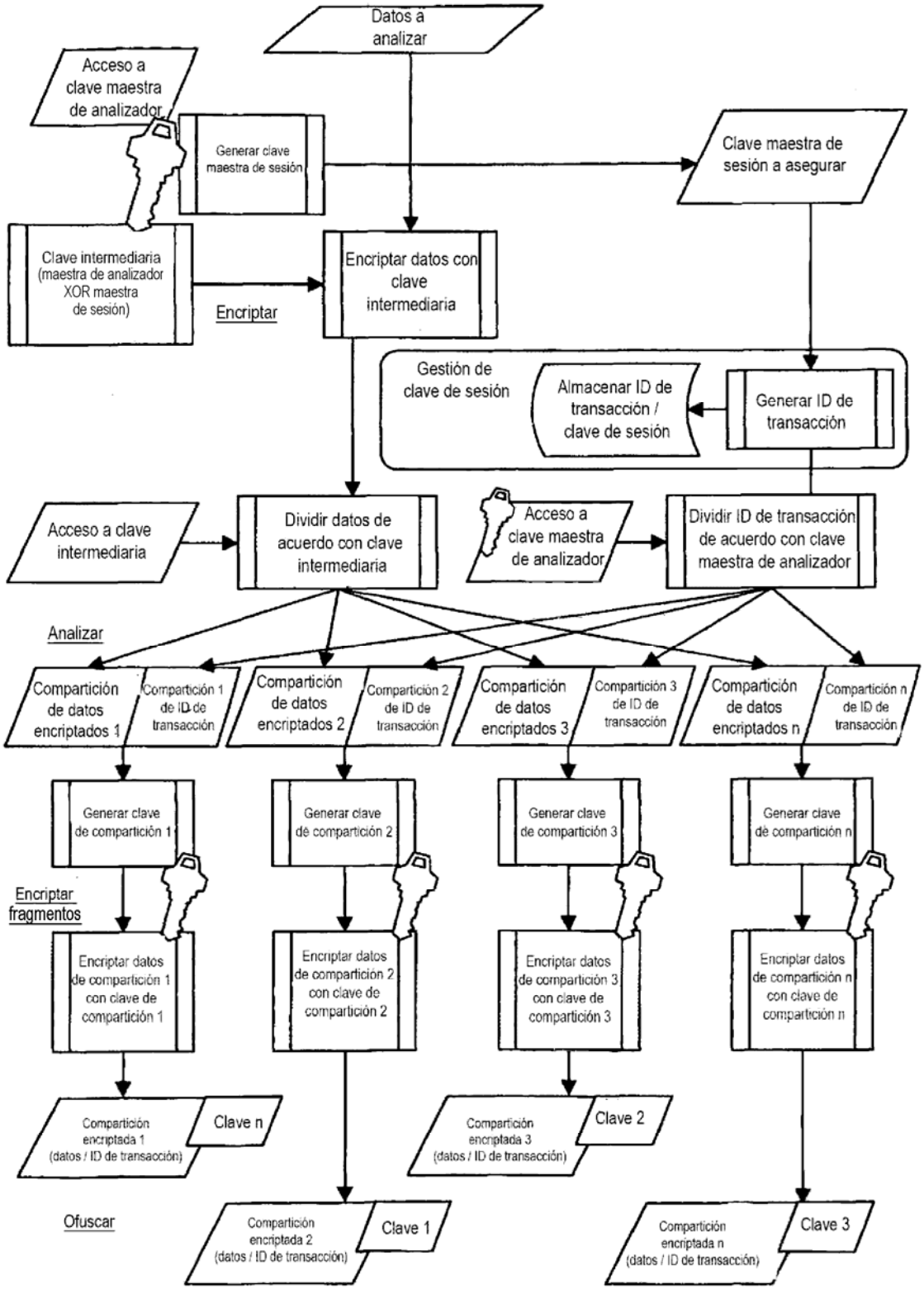

Datos a analizar
Acceso a clave maestra de analizador
Generar clave maestra de sesión
Clave maestra de sesión a asegurar
Clave intermediaria (maestra de analizador XOR maestra de sesión)
Encriptar
Encriptar datos con clave intermediaria
Gestión de clave de sesión
Almacenar ID de transacción / clave de sesión
Generar ID de transacción
Acceso a clave intermediaria
Dividir datos de acuerdo con clave intermediaria
Acceso a clave maestra de analizador
Dividir ID de transacción de acuerdo con clave maestra de analizador
Analizar
Compartición de datos encriptados 1
Compartición 1 de ID de transacción
Compartición de datos encriptados 2
Compartición 2 de ID de transacción
Compartición de datos encriptados 3
Compartición 3 de ID de transacción
Compartición de datos encriptados n
Compartición n de ID de transacción
Generar clave de compartición 1
Generar clave de compartición 2
Generar clave de compartición 3
Generar clave de compartición n
Encriptar fragmentos
Encriptar datos de compartición 1 con clave de compartición 1
Encriptar datos de compartición 2 con clave de compartición 2
Encriptar datos de compartición 3 con clave de compartición 3
Encriptar datos de compartición n con clave de compartición n
Compartición encriptada 1 (datos / ID de transacción)
Clave n
Compartición encriptada 3 (datos / ID de transacción)
Clave 2
Ofuscar
Compartición encriptada 2 (datos / ID de transacción)
Clave 1
Compartición encriptada n (datos / ID de transacción)
Clave 3

FIG. 24

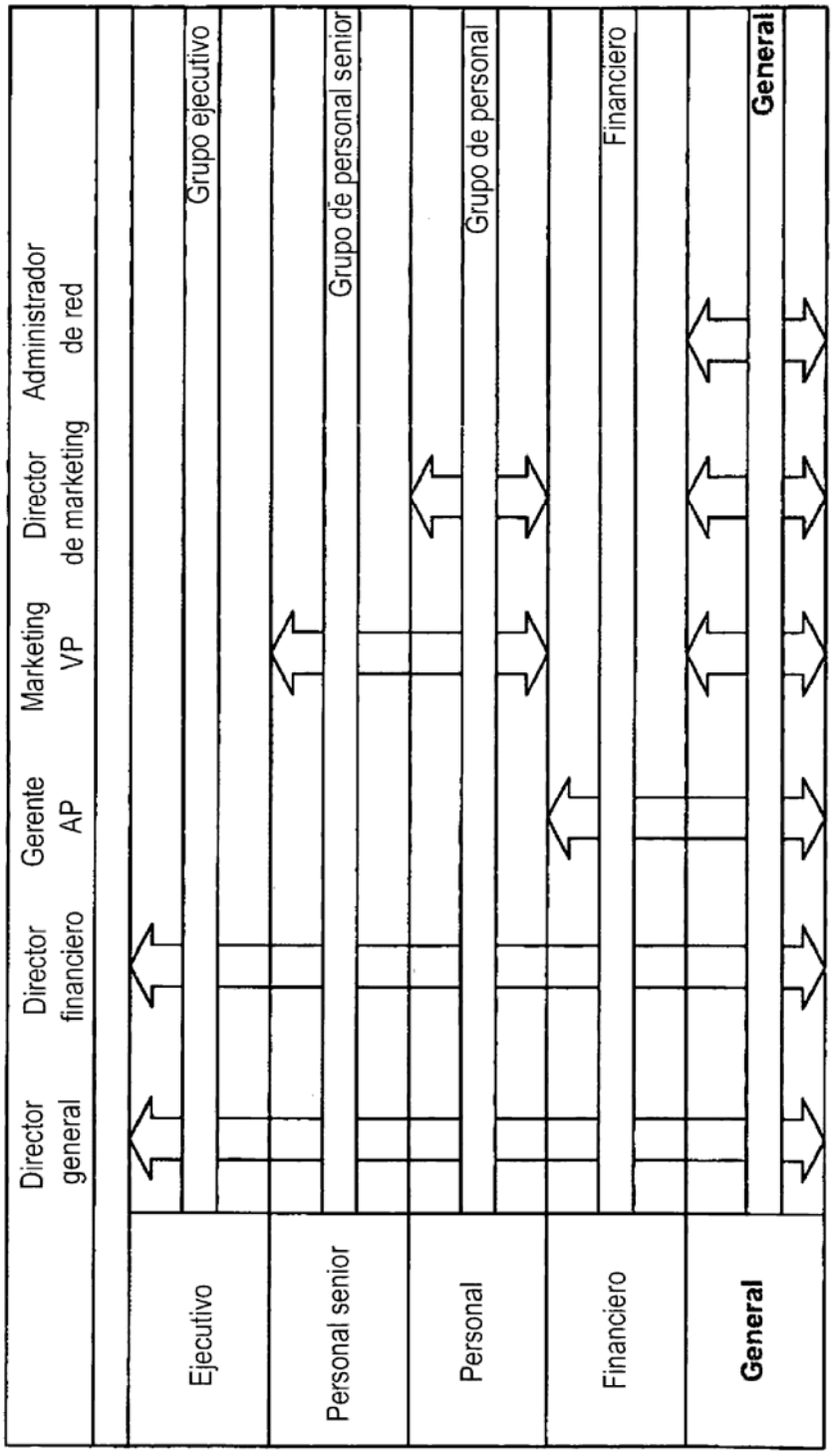

Director general
Director financiero
Gerente AP
Marketing VP
Director de marketing
Administrador de red
Ejecutivo
Grupo ejecutivo
Personal senior
Grupo de personal senior
Personal
Grupo de personal
Financiero
Financiero
General
General

FIG. 25

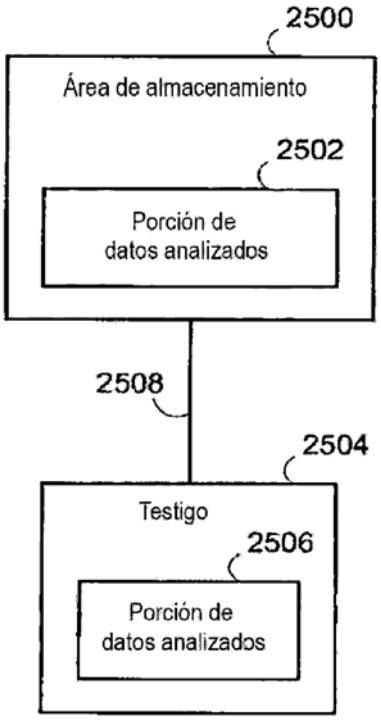

2500
Área de almacenamiento
2502
Porción de datos analizados
2508
2504
Testigo
2506
Porción de datos analizados

FIG. 26

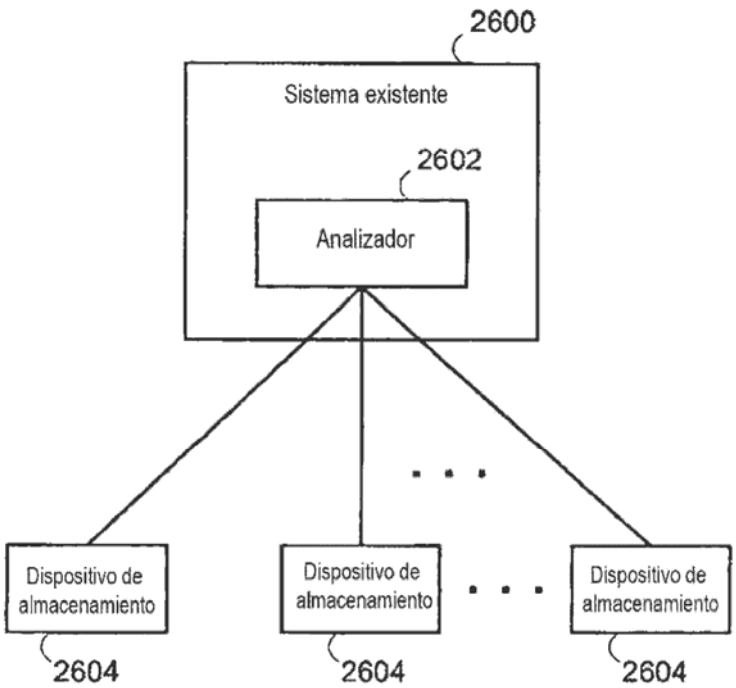

2600
Sistema existente
2602
Analizador
Dispositivo de almacenamiento
2604
Dispositivo de almacenamiento
2604
Dispositivo de almacenamiento
2604

FIG. 27

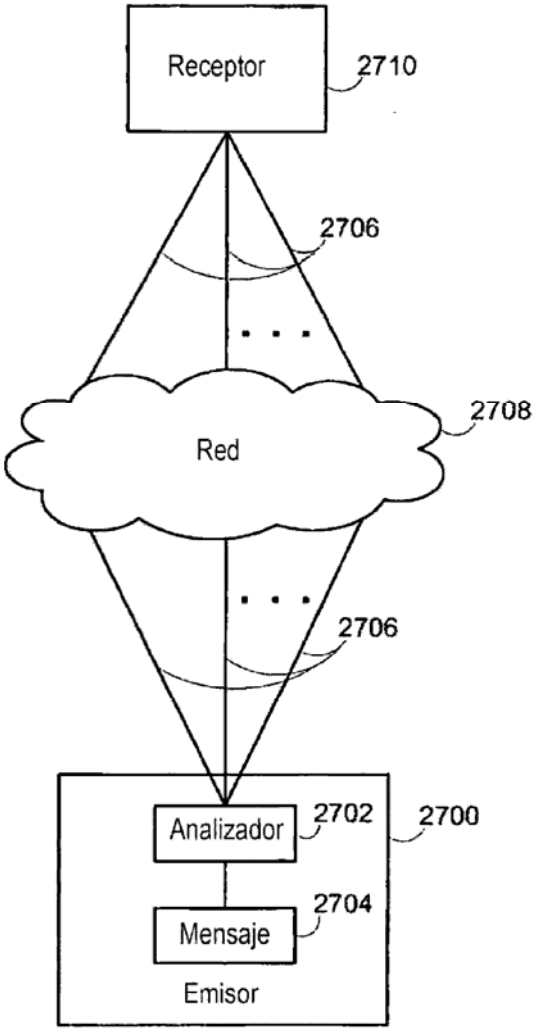

Receptor
2710
2706
2708
Red
2706
Analizador
2702
2700
2704
Mensaje
Emisor

FIG. 28

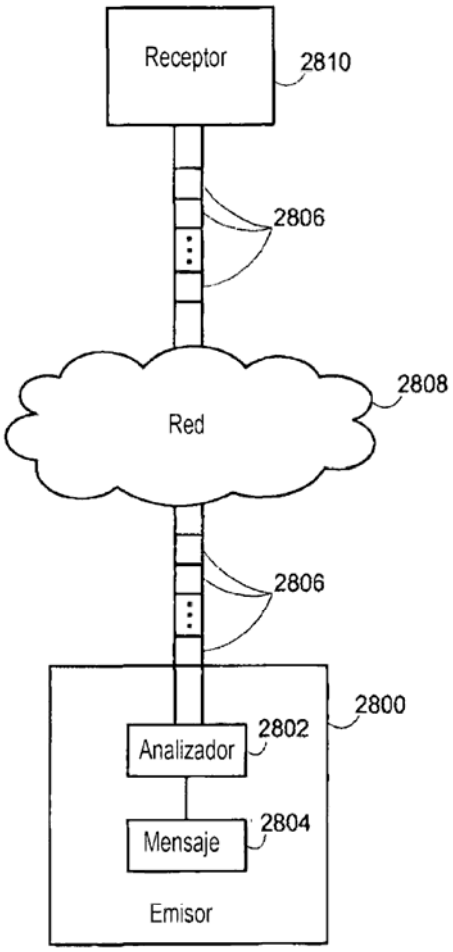

Receptor
2810
2806
2808
Red
2806
2800
2802
Analizador
2804
Mensaje
Emisor

FIG. 29

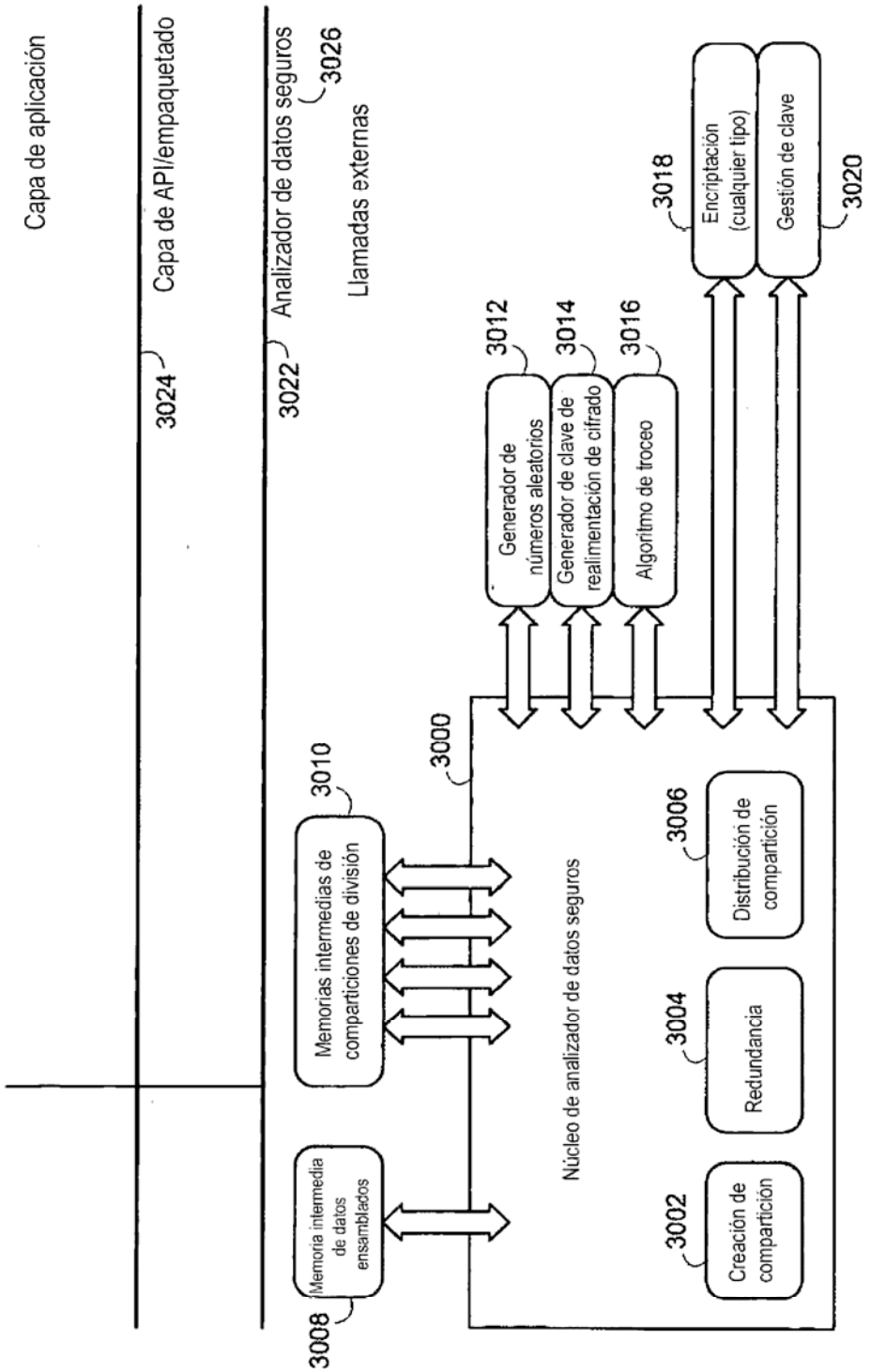

Capa de aplicación
Capa de API/empaquetado
3024
Analizador de datos seguros
3026
3022
Llamadas externas
3012
Generador de números aleatorios
3014
Generador de clave de realimentación de cifrado
3016
Algoritmo de troceo
3018
Encriptación (cualquier tipo)
Gestión de clave
3020
3000
3010
Memorias intermedias de compartimentos de división
Memoria intermedia de datos ensamblados
3008
Núcleo de analizador de datos seguros
3006
Distribución de compartición
3004
Redundancia
3002
Creación de compartición

FIG. 30

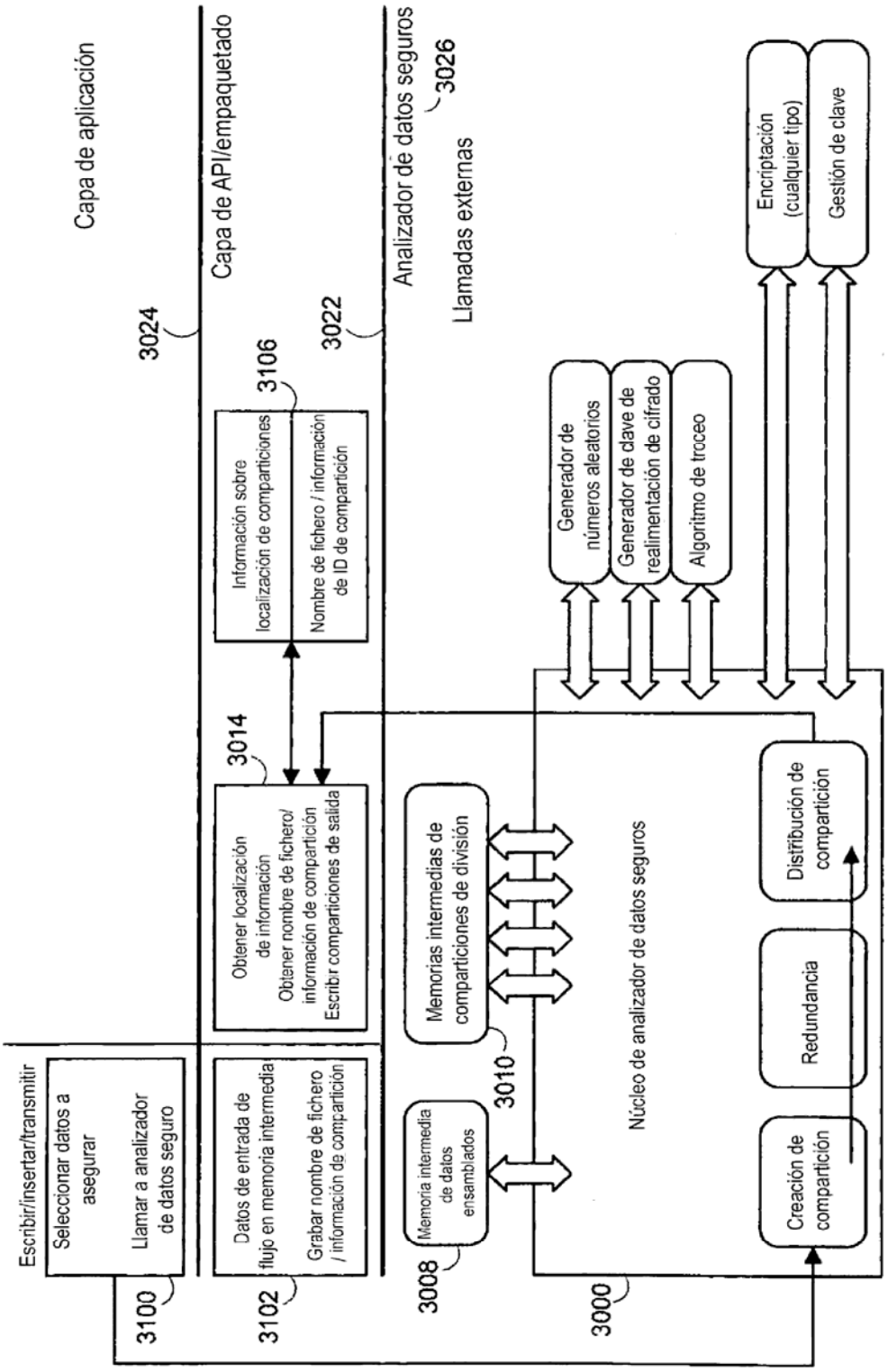

Capa de aplicación
Capa de API/empaquetado
Analizador de datos seguros
3026
Llamadas externas
3024
3022
3106
3014
Escribir/insertar/transmitir
Seleccionar datos a asegurar
Llamar a analizador de datos seguro
3100
Datos de entrada de flujo en memoria intermedia
Grabar nombre de fichero / información de compartición
3102
Obtener localización de información
Obtener nombre de fichero/ información de compartición
Escribir compartíciones de salida
Información sobre localización de compartíciones
Nombre de fichero / información de ID de compartición
Memorias intermedias de compartíciones de división
3010
Memoria intermedia de datos ensamblados
3008
Núcleo de analizador de datos seguros
3000
Generador de números aleatorios
Generador de clave de realimentación de cifrado
Algoritmo de troceo
Encriptación (cualquier tipo)
Gestión de clave
Distribución de compartición
Redundancia
Creación de compartición

FIG. 31

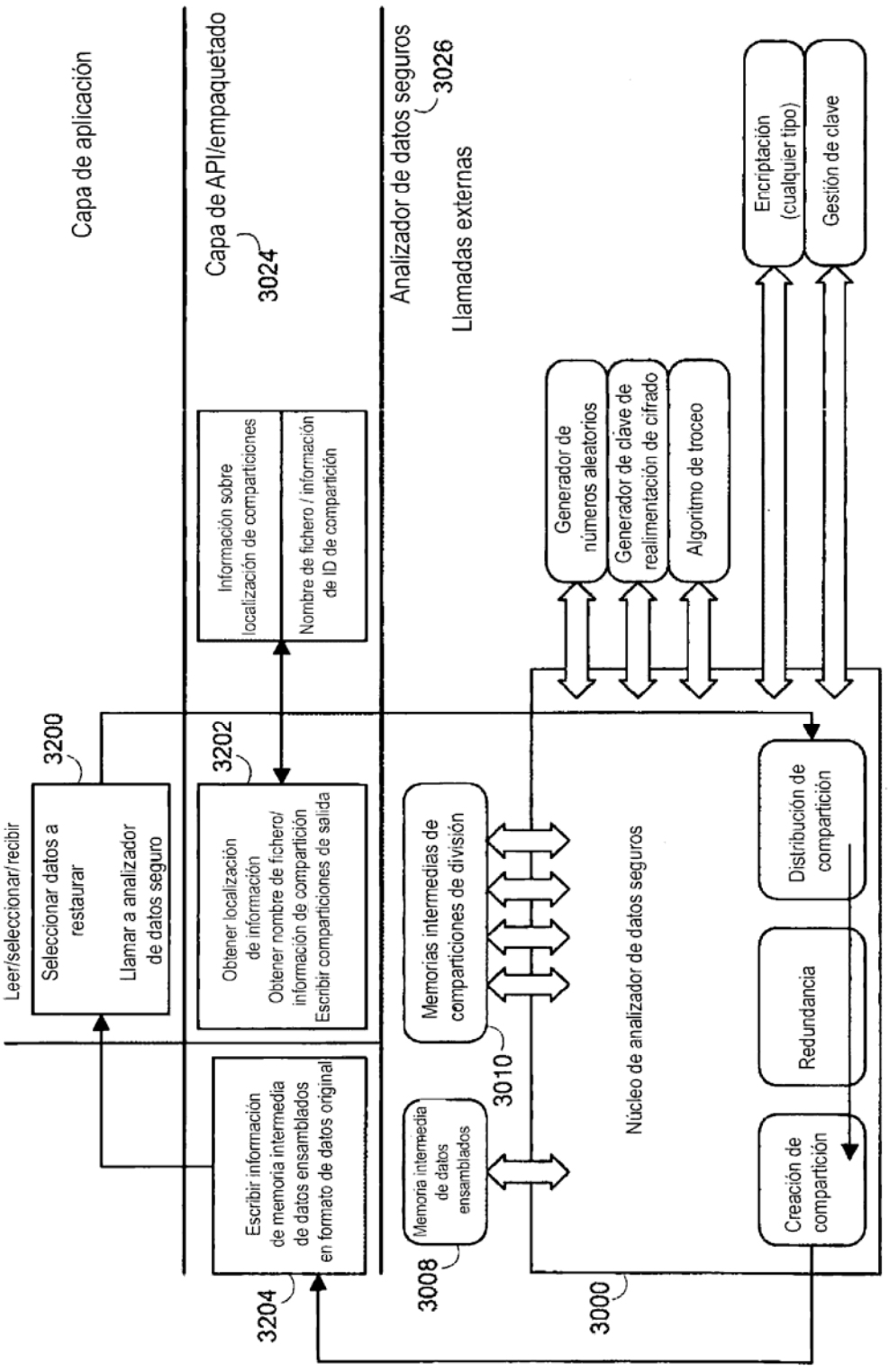

Capa de aplicación
Capa de API/empaquetado
3024
Analizador de datos seguros
3026
Llamadas externas
Leer/seleccionar/recibir
3200
Seleccionar datos a restaurar
Llamar a analizador de datos seguro
3202
Obtener localización de información
Obtener nombre de fichero/ información de compartición
Escribir compartición de salida
Información sobre localización de compartición
Nombre de fichero / información de ID de compartición
Escribir información de memoria intermedia de datos ensamblados en formato de datos original
3204
Memoria intermedia de datos ensamblados
3008
Memorias intermedias de compartición de división
3010
Núcleo de analizador de datos seguros
3000
Generador de números aleatorios
Generador de clave de realimentación de cifrado
Algoritmo de troceo
Encriptación (cualquier tipo)
Gestión de clave
Distribución de compartición
Redundancia
Creación de compartición

FIG. 32

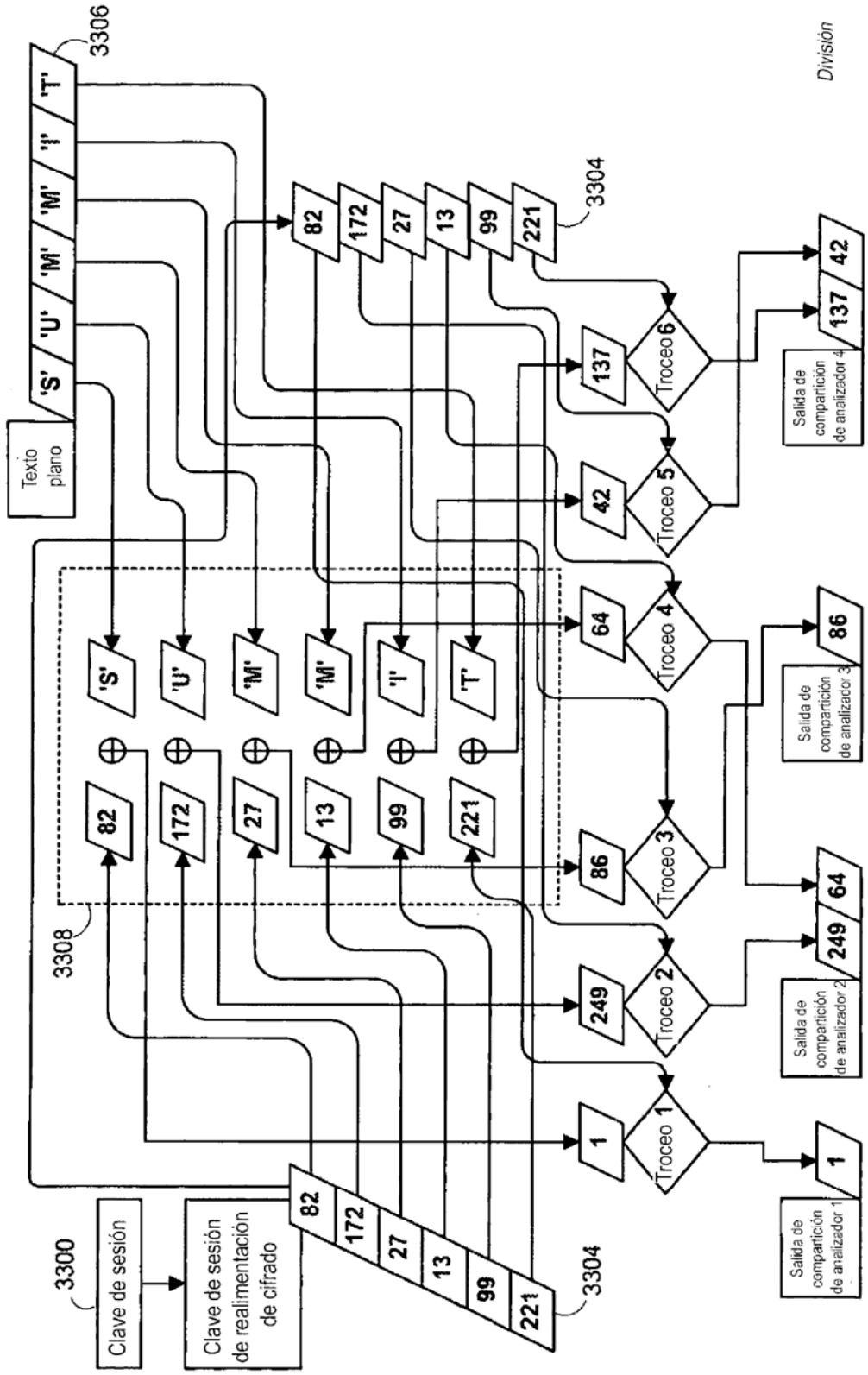

3306
'S' 'U' 'M' 'M' 'I' 'T'
Texto plano
3308
3300
Clave de sesión
Clave de sesión de realimentación de cifrado
3304
82 172 27 13 99 221
División
Troceo 1
Troceo 2
Troceo 3
Troceo 4
Troceo 5
Troceo 6
Salida de compartición de analizador 1
Salida de compartición de analizador 2
Salida de compartición de analizador 3
Salida de compartición de analizador 4

FIG. 33

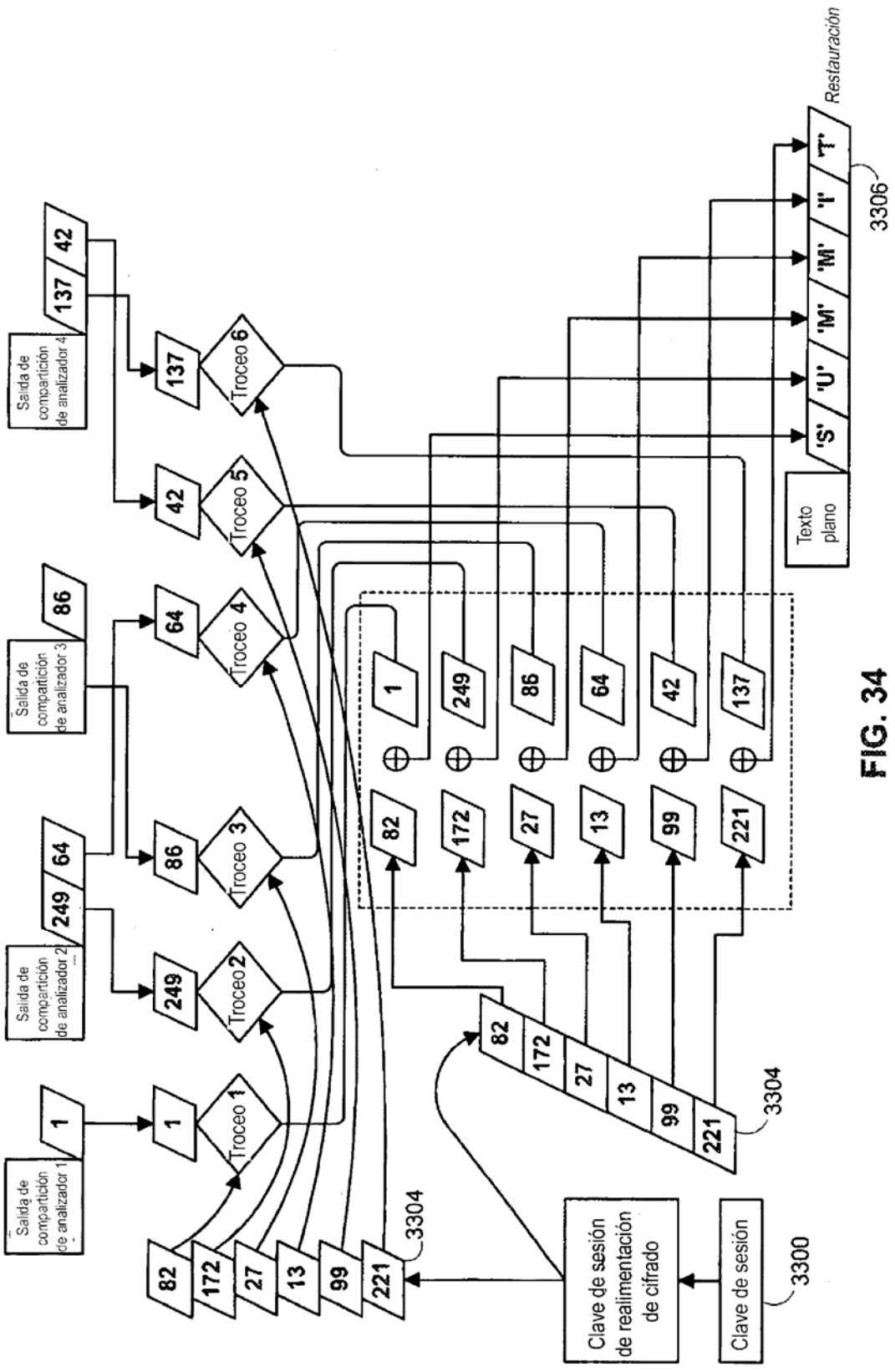

Salida de compartición de analizador 1
Salida de compartición de analizador 2
Salida de compartición de analizador 3
Salida de compartición de analizador 4
Troceo 1
Troceo 2
Troceo 3
Troceo 4
Troceo 5
Troceo 6
Clave de sesión de realimentación de cifrado
Clave de sesión
Texto plano
Restauración
3300
3304
3306

FIG. 34

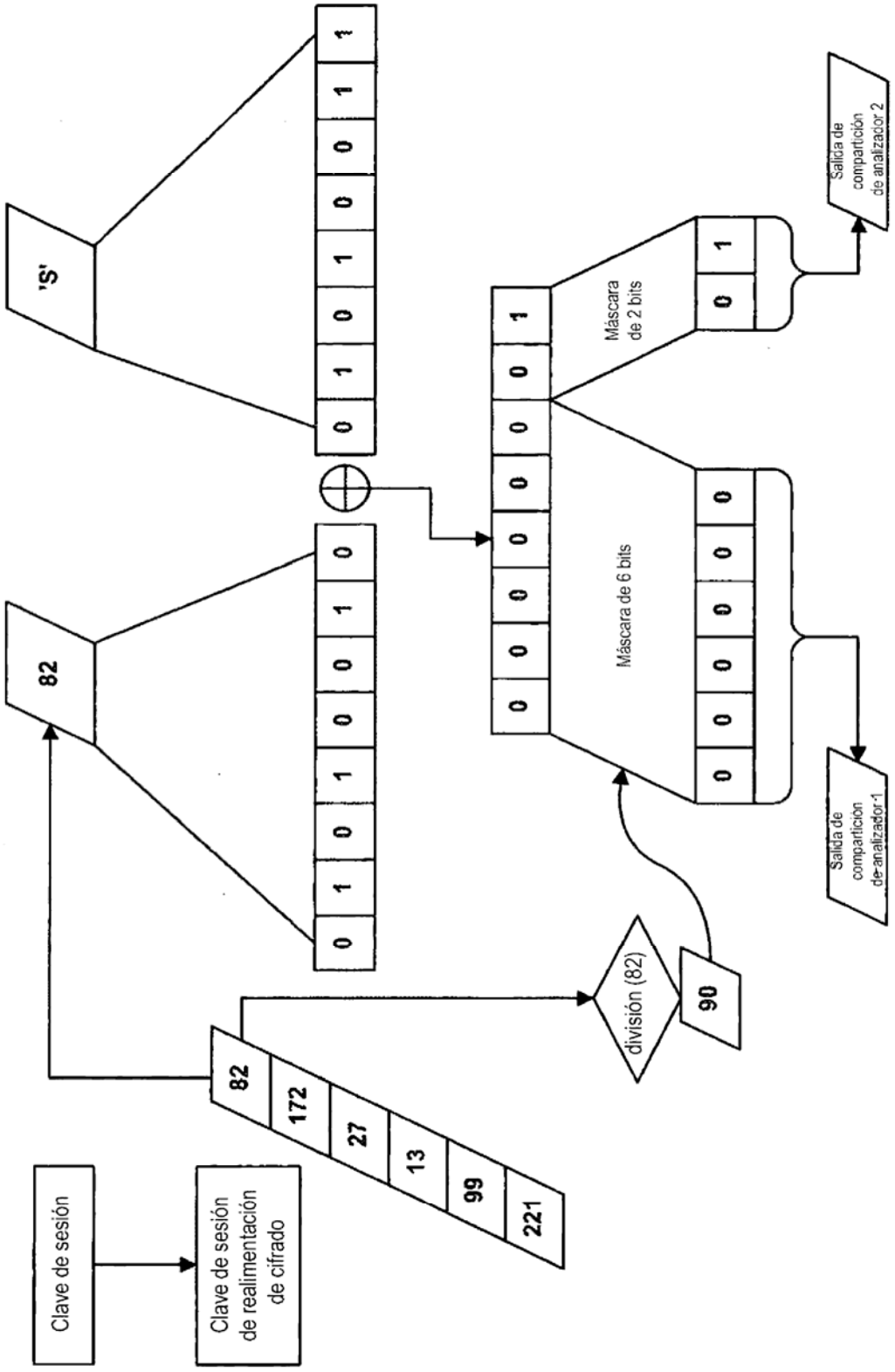

Clave de sesión
Clave de sesión de realimentación de cifrado
82
172
27
13
99
221
division (82)
90
82
'S'
Máscara de 6 bits
Máscara de 2 bits
Salida de compartición de analizador 1
Salida de compartición de analizador 2

FIG. 35

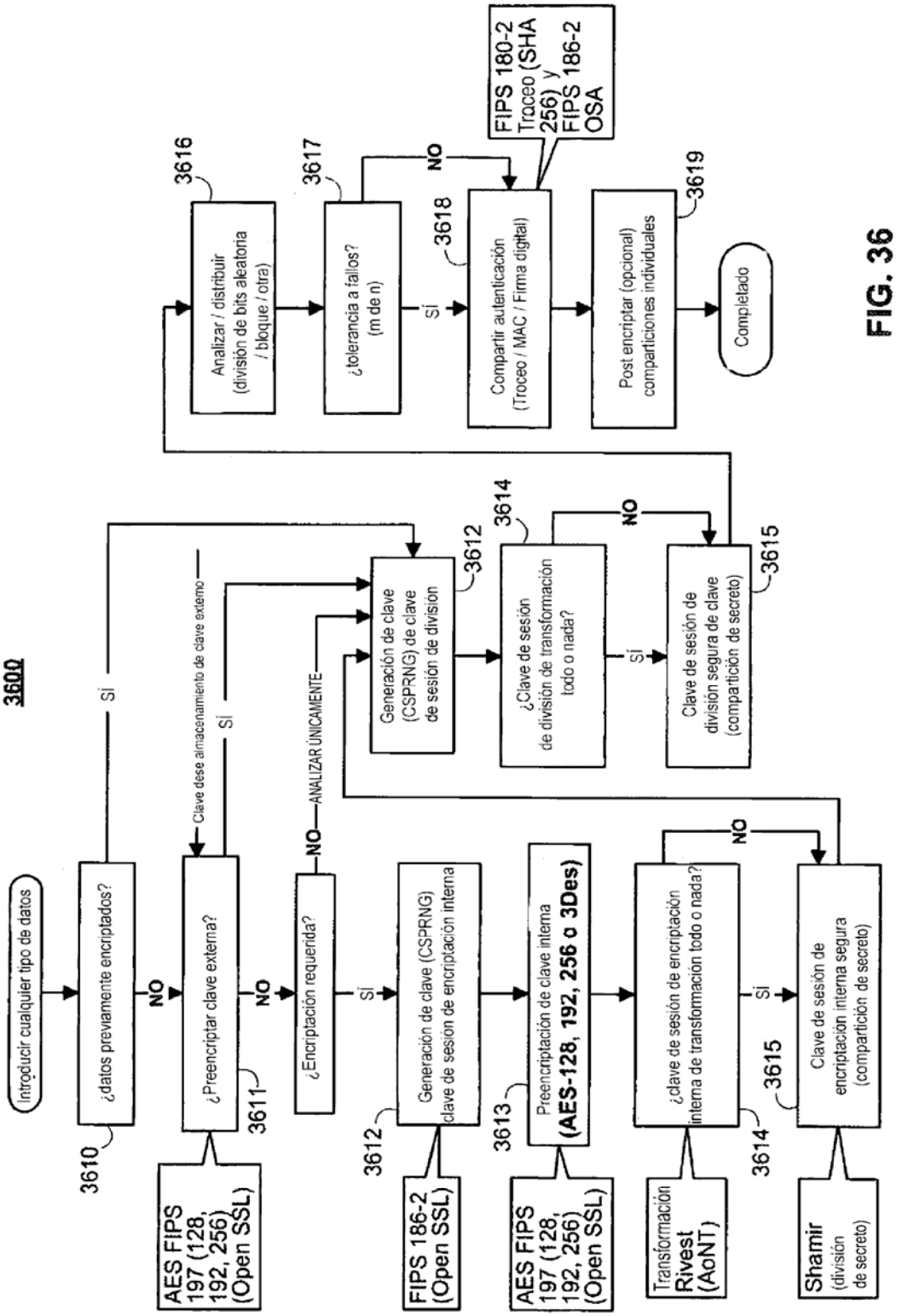

3600
Introducir cualquier tipo de datos
¿datos previamente encriptados?
3610
Sí
NO
¿Preencriptar clave externa?
3611
Clave dese almacenamiento de clave externo
Sí
NO
AES FIPS 197 (128, 192, 256) (Open SSL)
¿Encriptación requerida?
NO
ANALIZAR ÚNICAMENTE
Sí
Generación de clave (CSPRNG) clave de sesion de encriptación interna
3612
FIPS 186-2 (Open SSL)
Preencriptación de clave interna (AES-128, 192, 256 o 3Des)
3613
AES FIPS 197 (128, 192, 256) (Open SSL)
¿clave de sesión de encriptación interna de transformación todo o nada?
3614
NO
Sí
Transformación Rivest (AoNT)
Clave de sesión de encriptación interna segura (compartición de secreto)
3615
Shamir (división de secreto)
Generación de clave (CSPRNG) de clave de sesión de división
3612
¿Clave de sesión de división de transformación todo o nada?
3614
NO
Sí
Clave de sesión de división segura de clave (compartición de secreto)
3615
Analizar / distribuir (división de bits aleatoria / bloque / otra)
3616
¿tolerancia a fallos? (m de n)
3617
NO
Sí
3618
FIPS 180-2 Troceo (SHA 256) y FIPS 186-2 OSA
Compartir autenticación (Troceo / MAC / Firma digital)
Post encriptar (opcional) compartición individuales
3619
Completado

FIG. 36

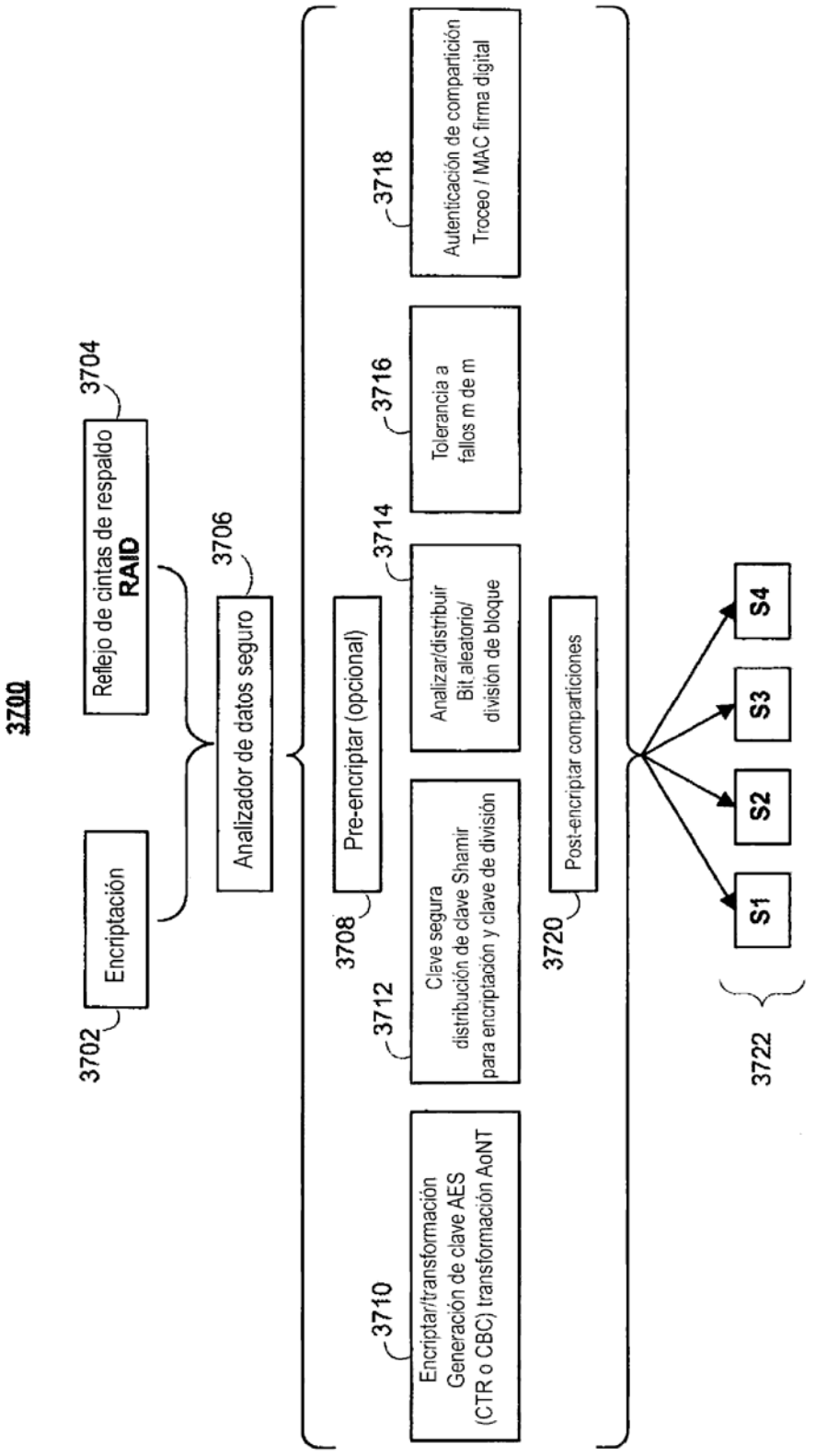

3700
Reflejo de cintas de respaldo RAID
3704
Encriptación
3702
Analizador de datos seguro
3706
Pre-encriptar (opcional)
3708
Post-encriptar compartimentos
3720
Encriptar/transformación Generación de clave AES (CTR o CBC) transformación AoNT
3710
Clave segura distribución de clave Shamir para encriptación y clave de división
3712
Analizar/distribuir Bit aleatorio/ división de bloque
3714
Tolerancia a fallos m de m
3716
Autenticación de compartición Troceo / MAC firma digital
3718
S1
S2
S3
S4
3722

FIG. 37

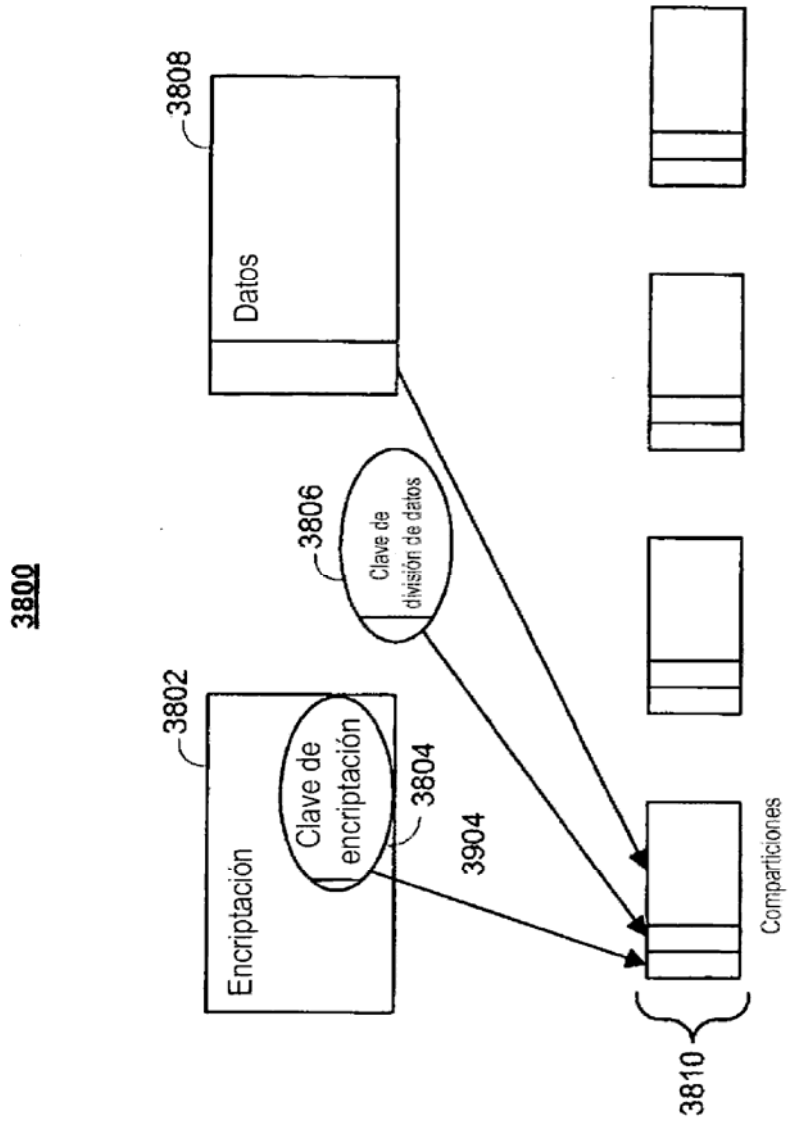

3800
3808
Datos
3806
Clave de división de datos
3802
Encriptación
Clave de encriptación
3804
3904
Compartimiones
3810

FIG. 38

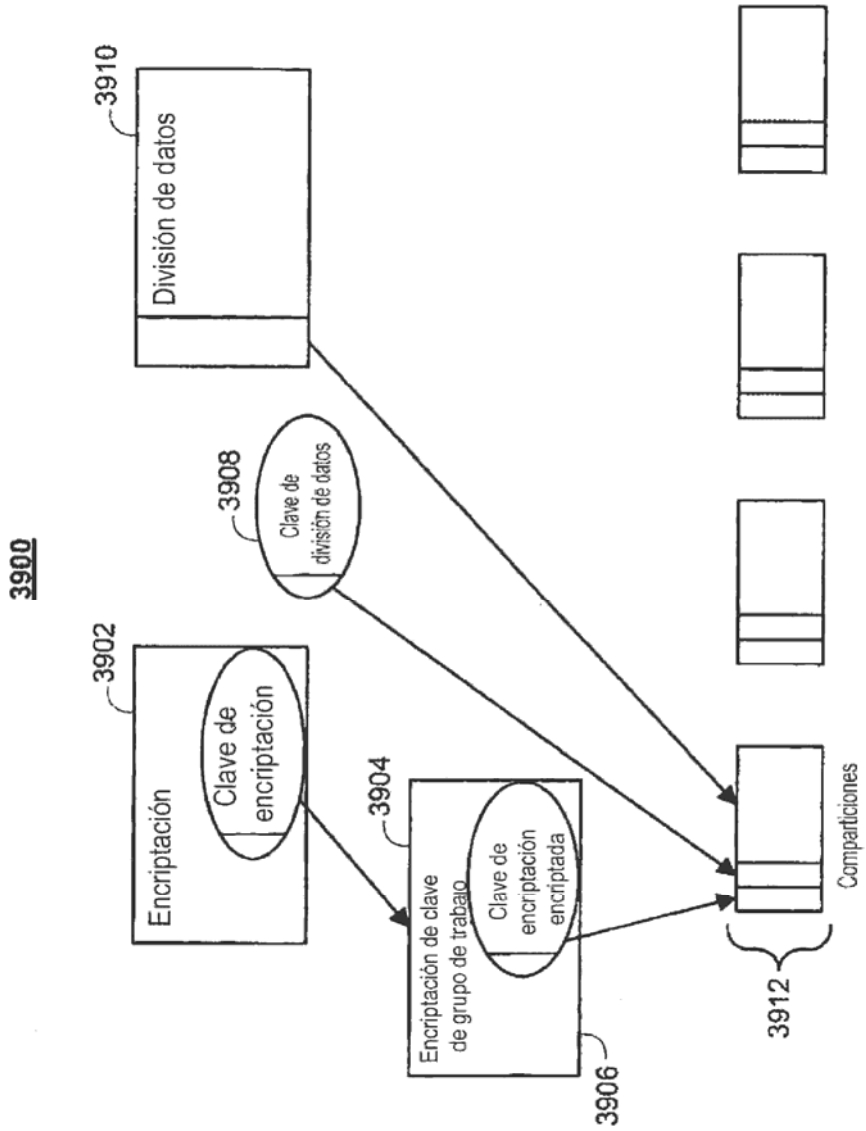

3900
3902
Encriptación
Clave de encriptación
3904
Encriptación de clave de grupo de trabajo
Clave de encriptación encriptada
3906
3908
Clave de división de datos
3910
División de datos
3912
Compartimentos

FIG. 39

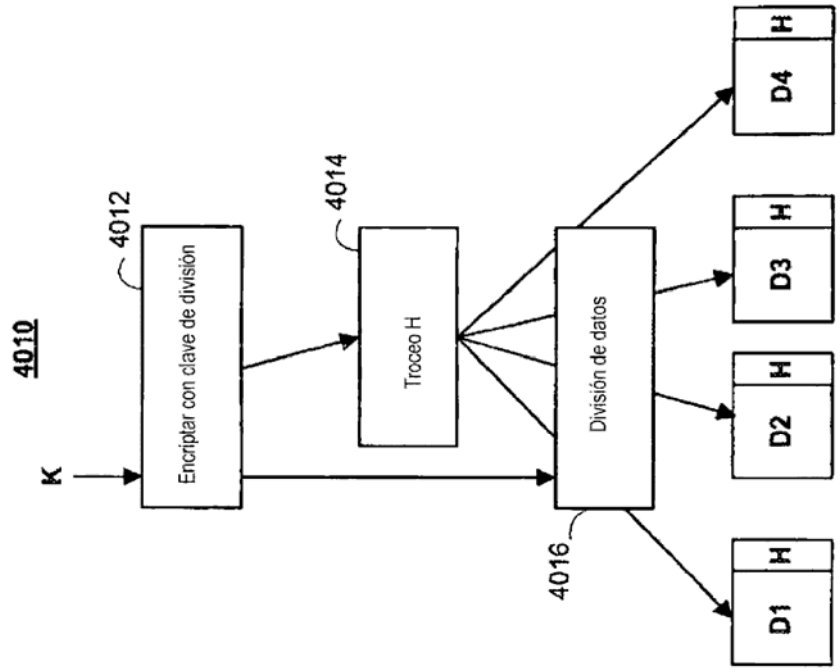


FIG. 40B

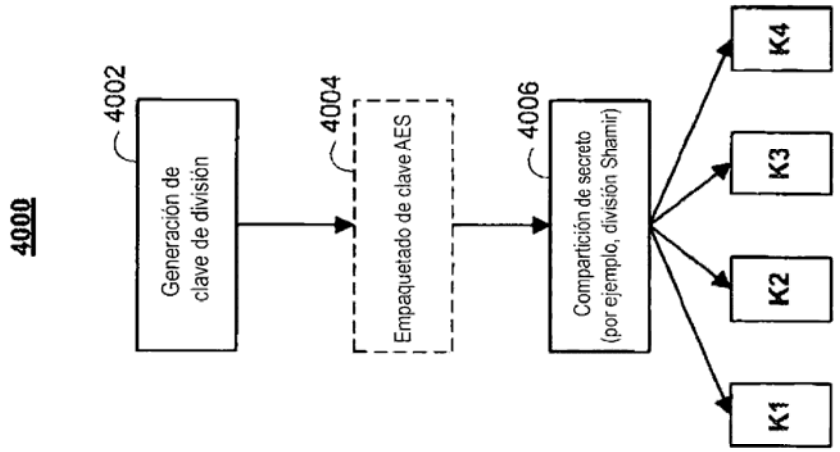


FIG. 40A

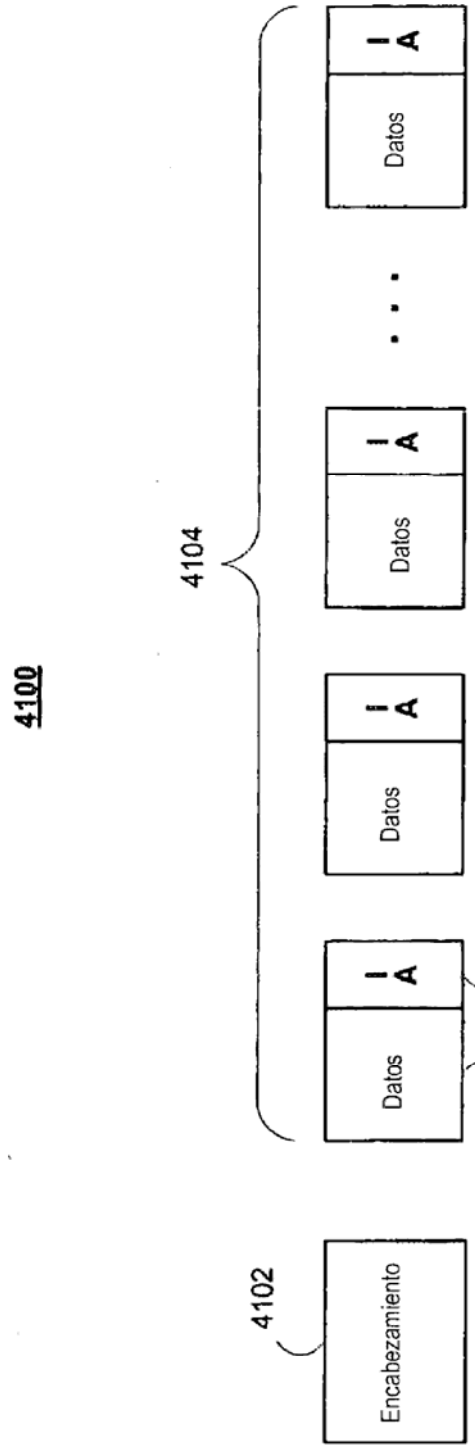


FIG. 41

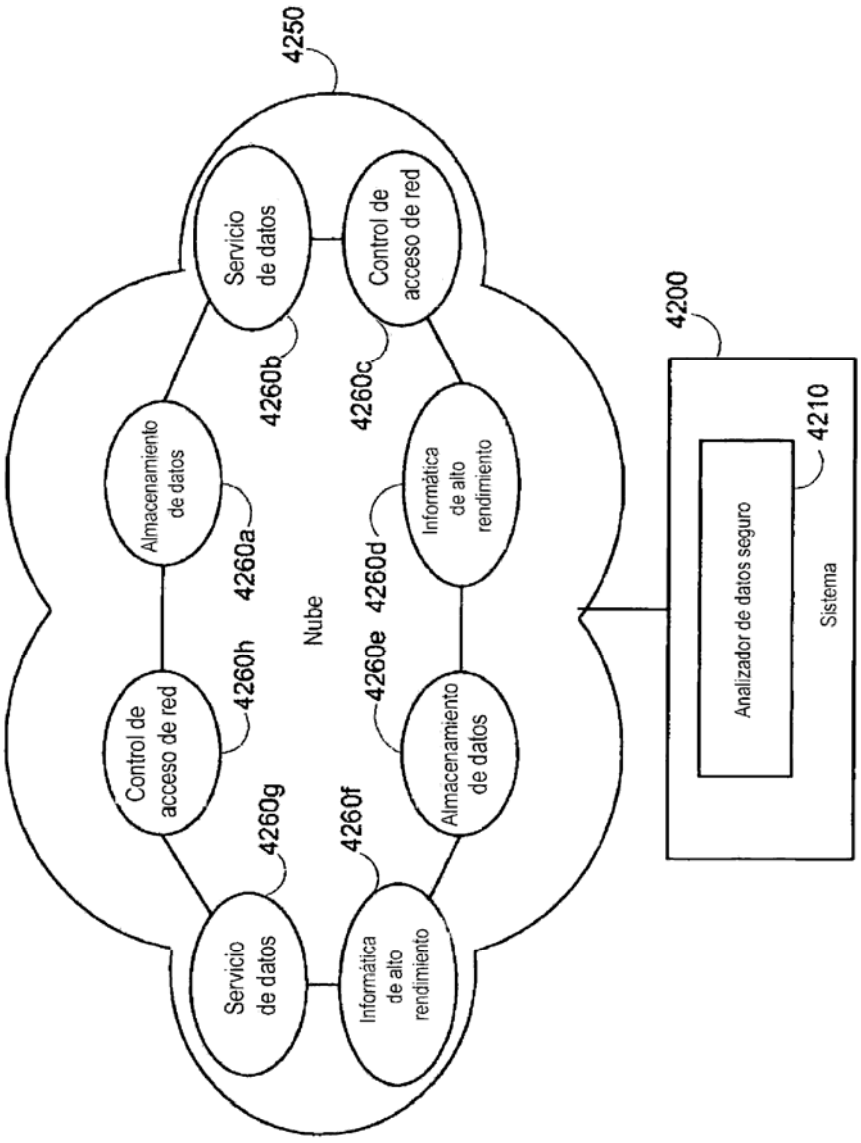

4250
Servicio de datos
Control de acceso de red
4260b
4260c
Almacenamiento de datos
Informática de alto rendimiento
4260a
4260d
Nube
4260h
4260e
Control de acceso de red
Almacenamiento de datos
4260g
4260f
Servicio de datos
Informática de alto rendimiento
4200
Analizador de datos seguro
4210
Sistema

FIG. 42

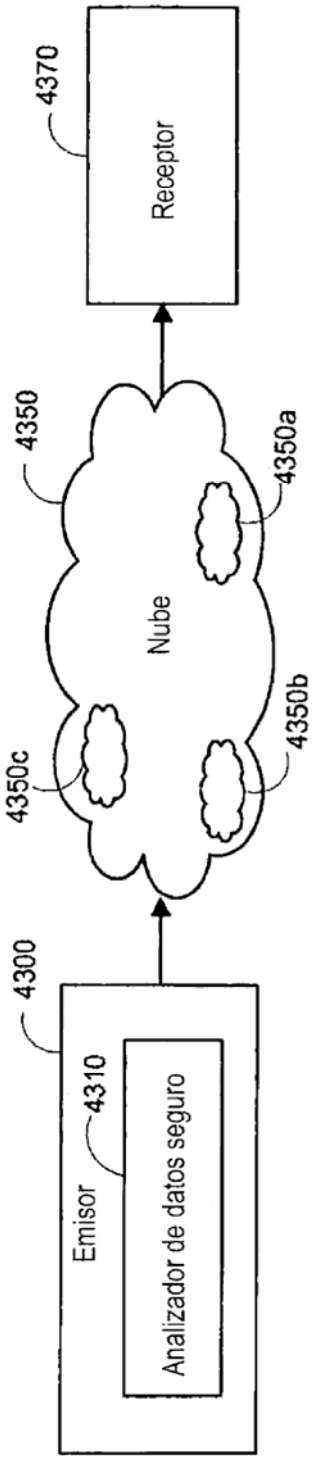

4370
Receptor
4350
4350a
Nube
4350b
4350c
4300
4310
Emisor
Analizador de datos seguro

FIG. 43

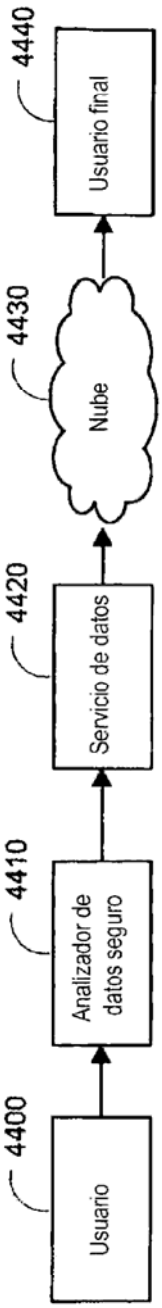

4400
Usuario
4410
Analizador de datos seguro
4420
Servicio de datos
4430
Nube
4440
Usuario final

FIG. 44

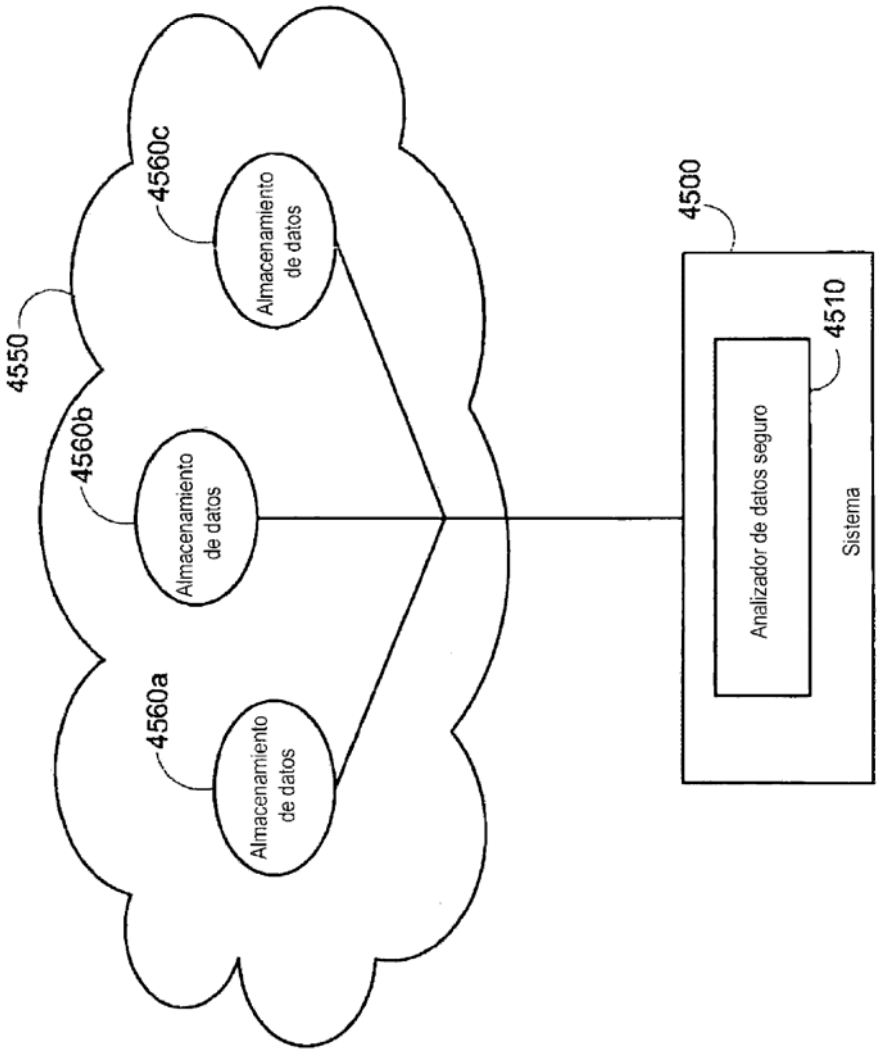

4550
4560c
Almacenamiento de datos
4560b
Almacenamiento de datos
4560a
Almacenamiento de datos
4500
4510
Analizador de datos seguro
Sistema

FIG. 45

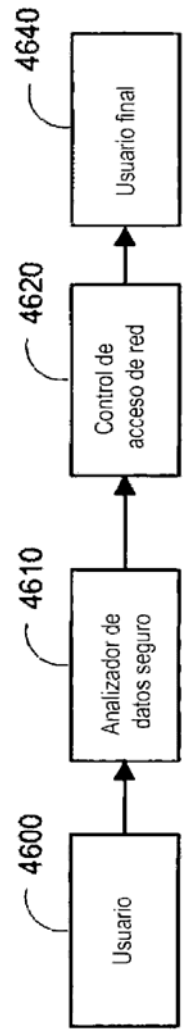

4600
Usuario
4610
Analizador de datos seguro
4620
Control de acceso de red
4640
Usuario final

FIG. 46

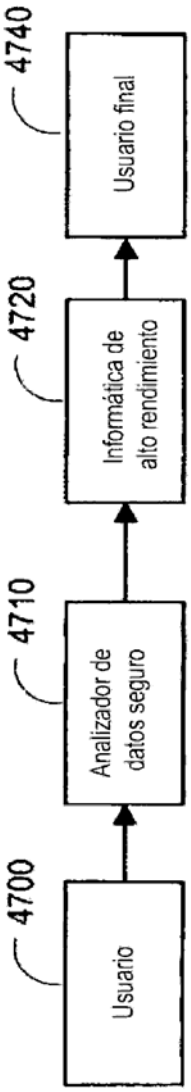

4700
Usuario
4710
Analizador de datos seguro
4720
Informática de alto rendimiento
4740
Usuario final

FIG. 47

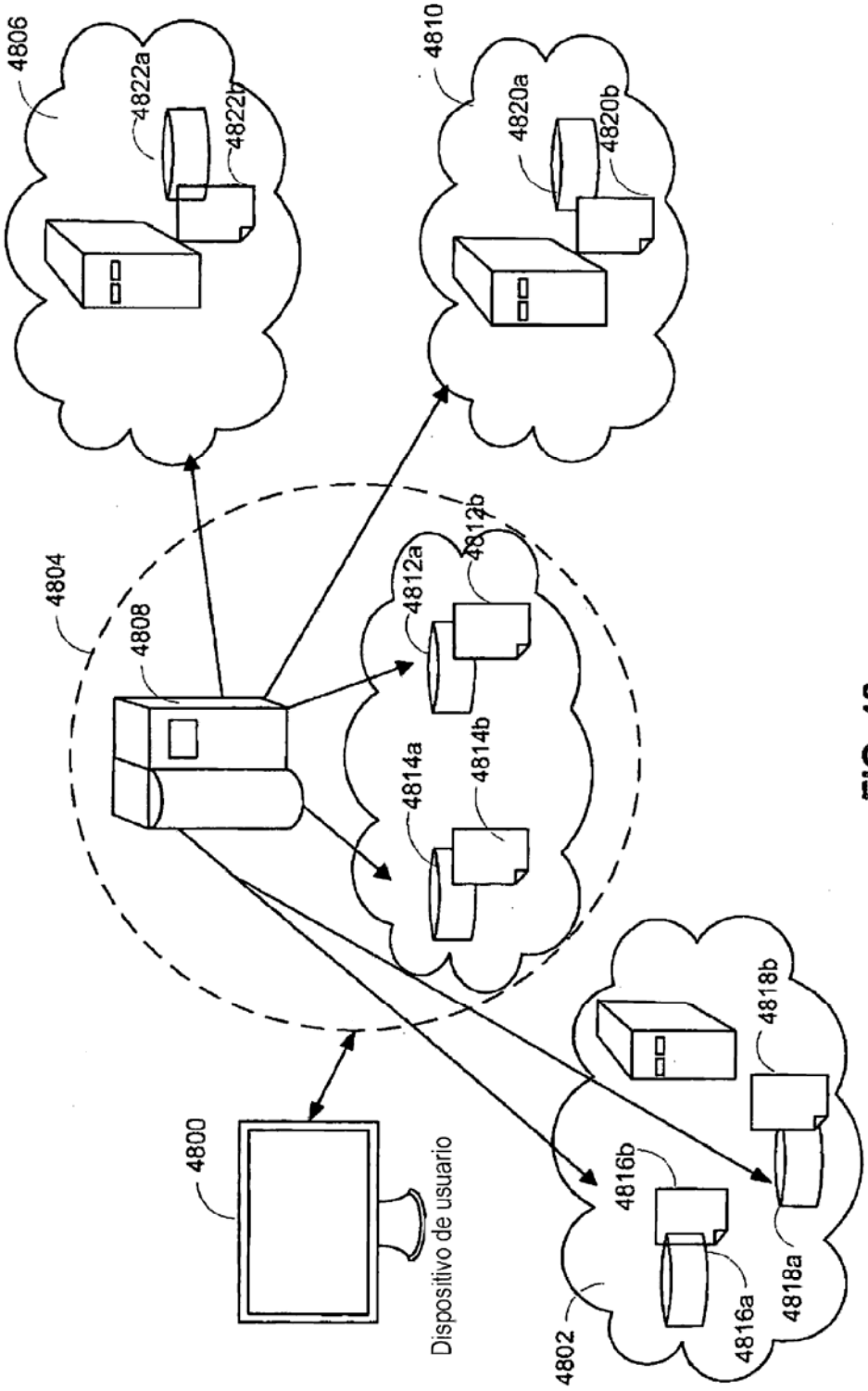

4806
4822a
4822b
4810
4820a
4820b
4804
4808
4812a
4812b
4814a
4814b
4800
Dispositivo de usuario
4802
4816b
4816a
4818a
4818b

FIG. 48

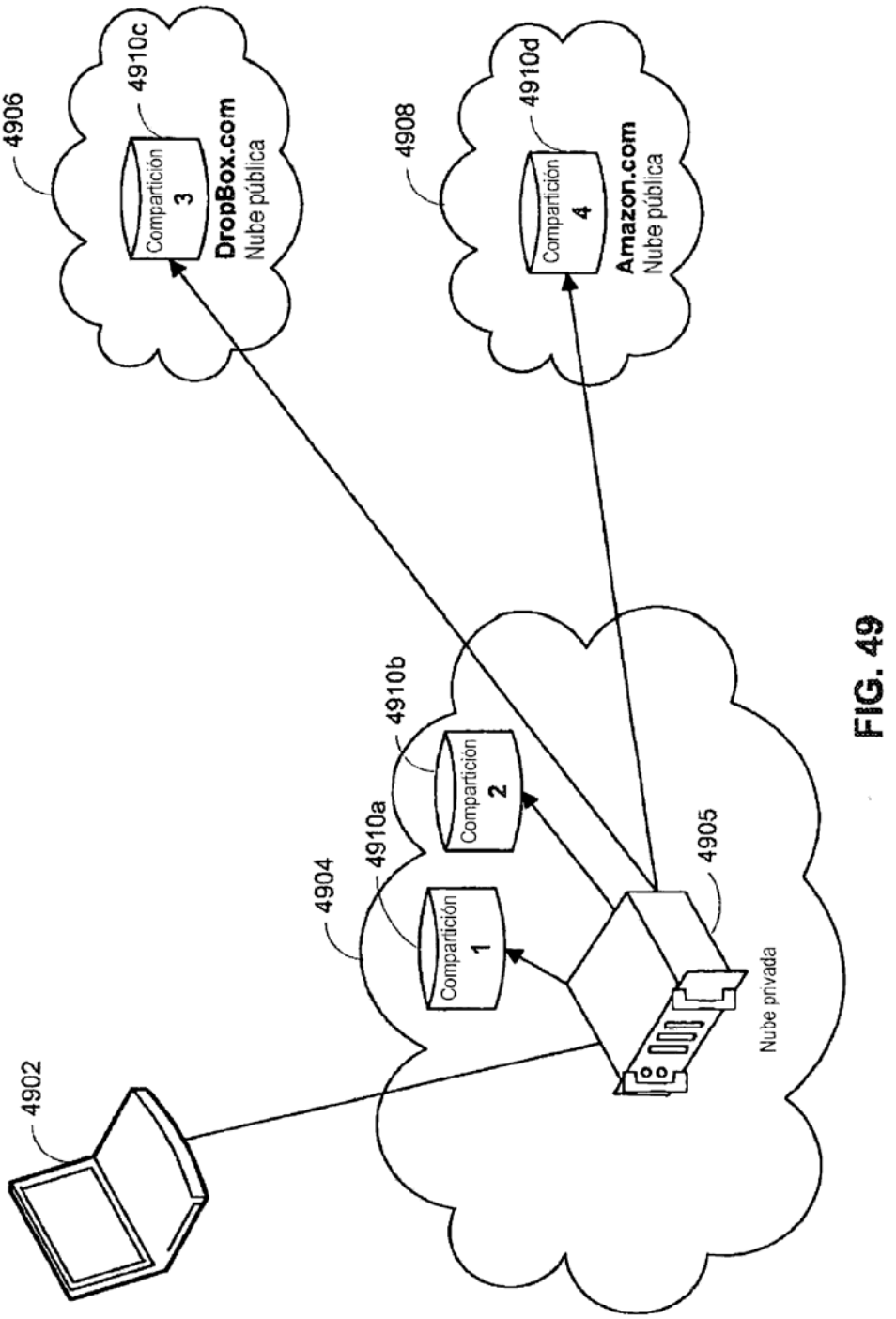

4906
4910c
Compartición 3
DropBox.com
Nube pública
4908
4910d
Compartición 4
Amazon.com
Nube pública
4910b
Compartición 2
4910a
Compartición 1
4904
4905
Nube privada
4902

FIG. 49

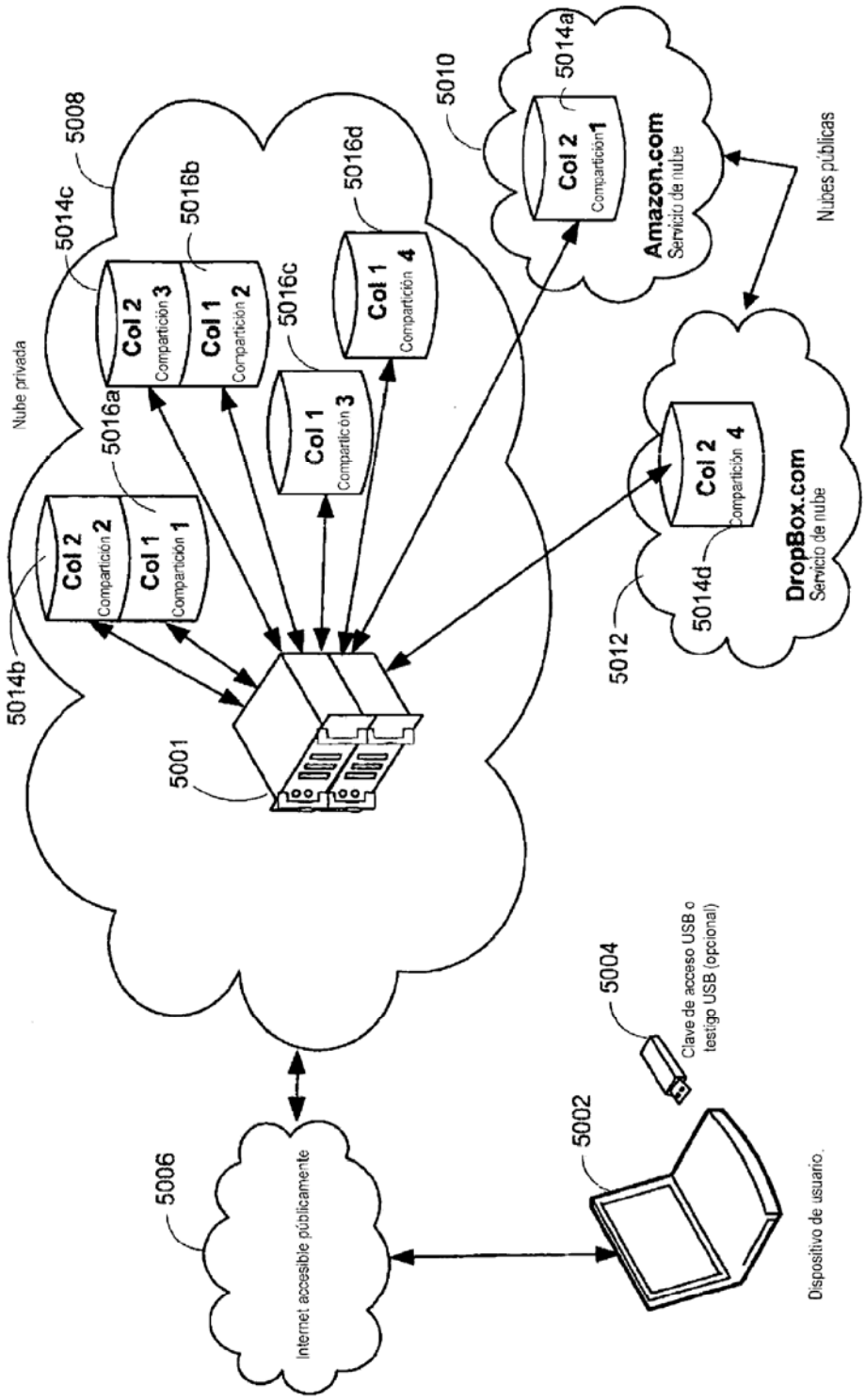

5008
Nube privada
5014c
5016b
5016d
5010
5014a
Col 2
Compartición 3
Col 1
Compartición 2
Col 1
Compartición 4
Col 2
Compartición1
Amazon.com
Servicio de nube
5016a
5016c
Col 2
Compartición 2
Col 1
Compartición 1
Col 1
Compartición 3
Nubes públicas
5014b
5001
5012
Col 2
Compartición 4
5014d
DropBox.com
Servicio de nube
5004
Clave de acceso USB o testigo USB (opcional)
5006
Internet accesible públicamente
5002
Dispositivo de usuario.

FIG. 50

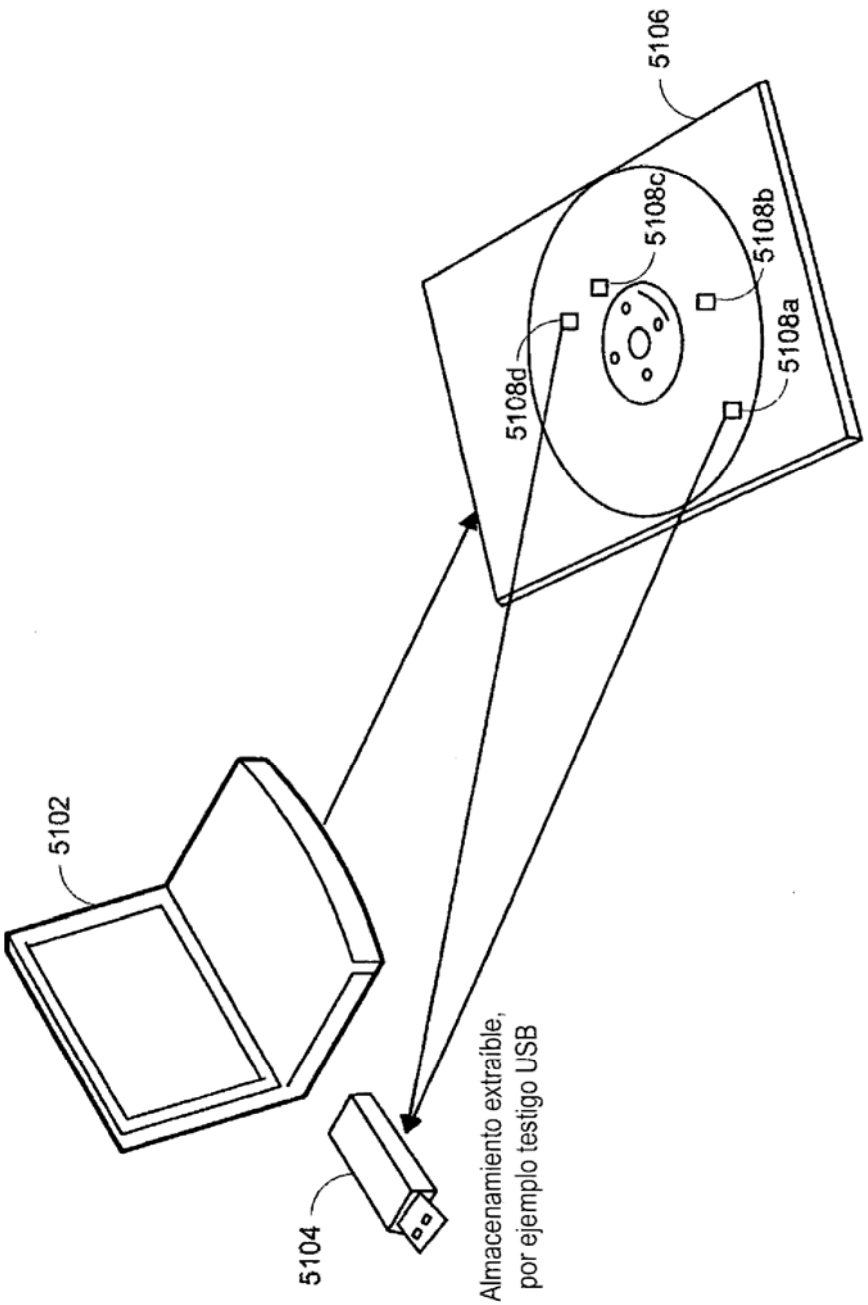

5106
5108c
5108b
5108a
5108d
5102
5104
Almacenamiento extraible,
por ejemplo testigo USB

FIG. 51

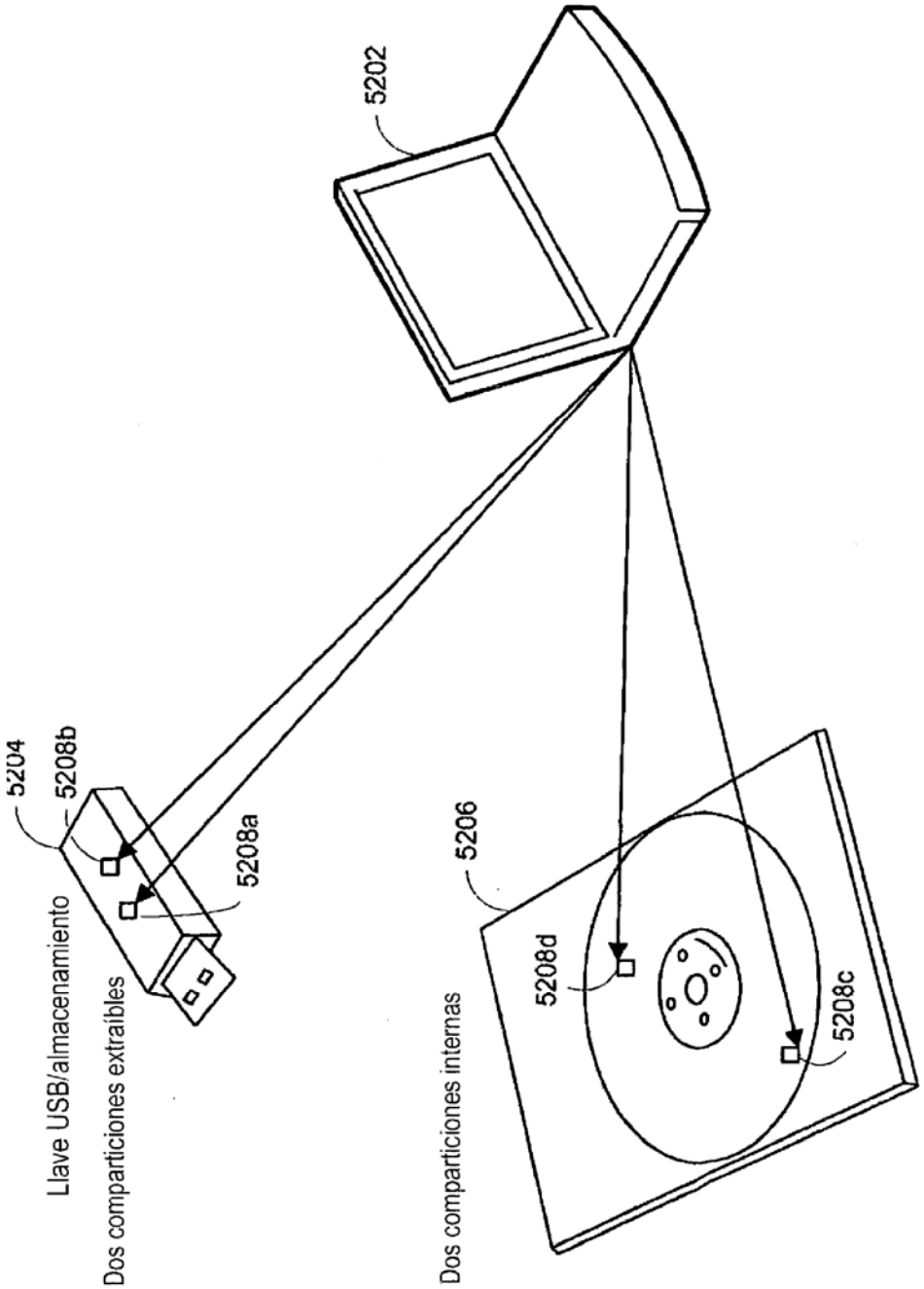

5202
5204
5208b
5208a
Llave USB/almacenamiento
Dos compartimentos extraíbles
5206
5208d
5208c
Dos compartimentos internos

FIG. 52

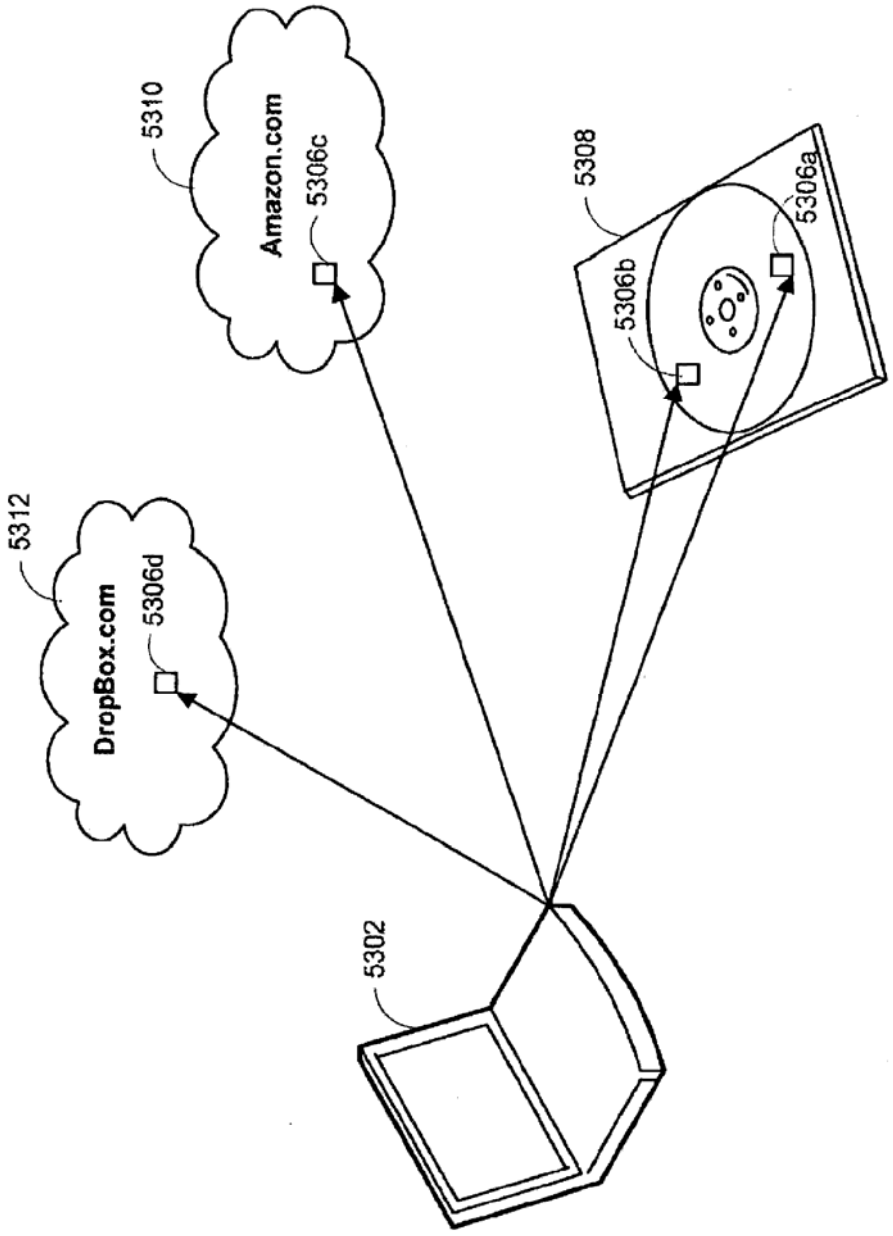

5310
Amazon.com
5306c
5308
5306a
5306b
5312
DropBox.com
5306d
5302

FIG. 53

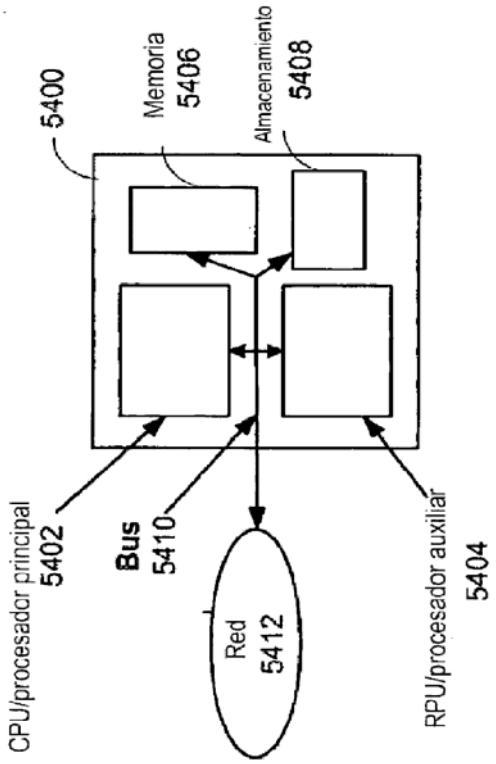

5400
Memoria
5406
Almacenamiento
5408
CPU/procesador principal
5402
Bus
5410
Red
5412
RPU/procesador auxiliar
5404

FIG. 54

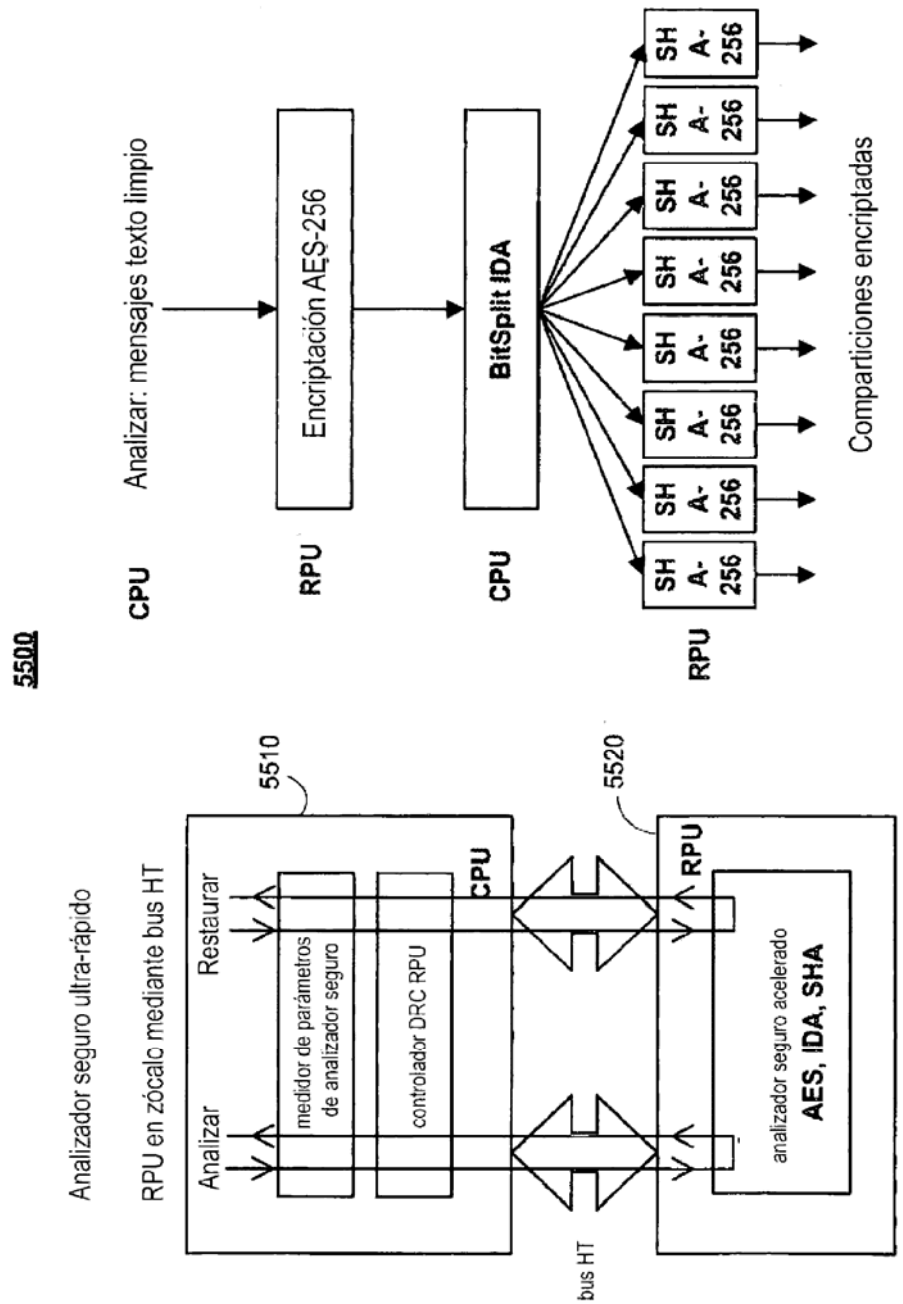

5500
Analizador seguro ultra-rápido
RPU en zócalo mediante bus HT
Analizar
Restaurar
5510
medidor de parámetros de analizador seguro
controlador DRC RPU
CPU
bus HT
5520
RPU
analizador seguro acelerado
AES, IDA, SHA
CPU
Analizar: mensajes texto limpio
Encriptación AES-256
RPU
CPU
BitSplit IDA
RPU
SHA-256
Compartimentos encriptadas

FIG. 55

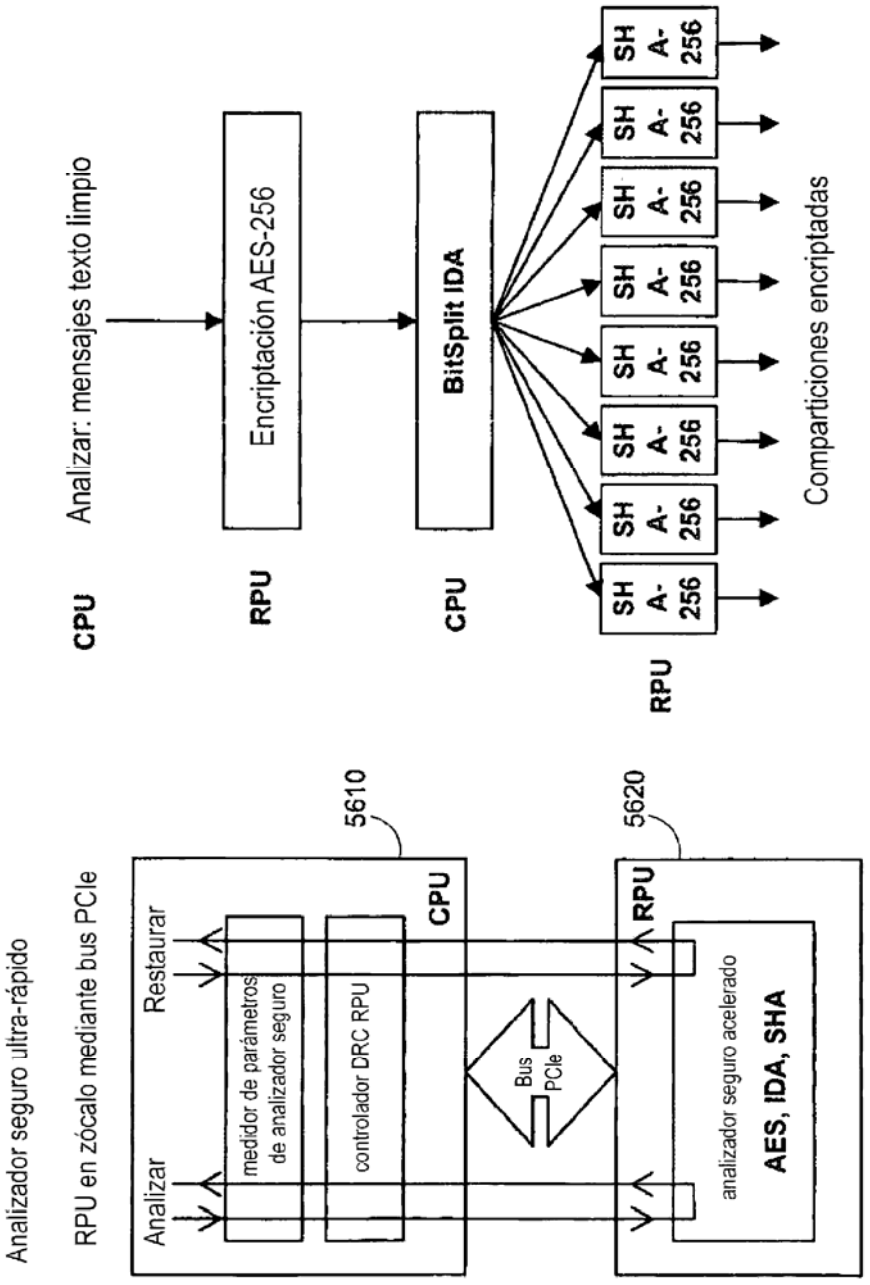

5600
CPU
Analizar: mensajes texto limpio
RPU
Encriptación AES-256
CPU
BitSplit IDA
RPU
SH A-256
Comparticiones encriptadas
Analizador seguro ultra-rápido
RPU en zócalo mediante bus PCIe
5610
CPU
Analizar
Restaurar
medidor de parámetros de analizador seguro
controlador DRC RPU
Bus PCIe
5620
RPU
analizador seguro acelerado
AES, IDA, SHA

FIG. 56

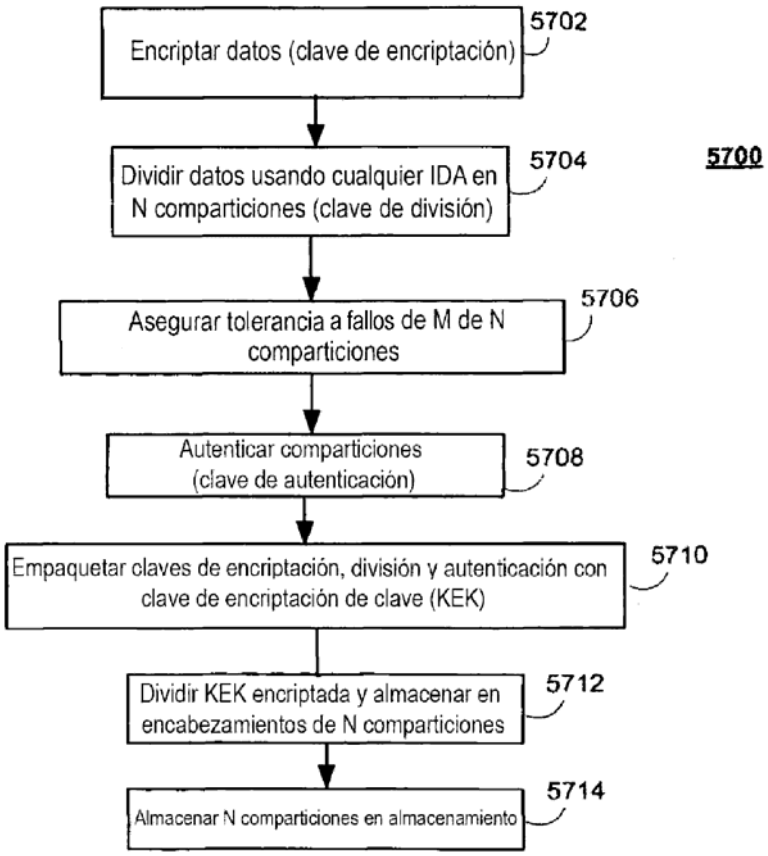

Encriptar datos (clave de encriptación)
5702
Dividir datos usando cualquier IDA en N comparticiones (clave de división)
5704
5700
Asegurar tolerancia a fallos de M de N comparticiones
5706
Autenticar comparticiones (clave de autenticación)
5708
Empaquetar claves de encriptación, división y autenticación con clave de encriptación de clave (KEK)
5710
Dividir KEK encriptada y almacenar en encabezamientos de N comparticiones
5712
Almacenar N comparticiones en almacenamiento
5714

FIG. 57

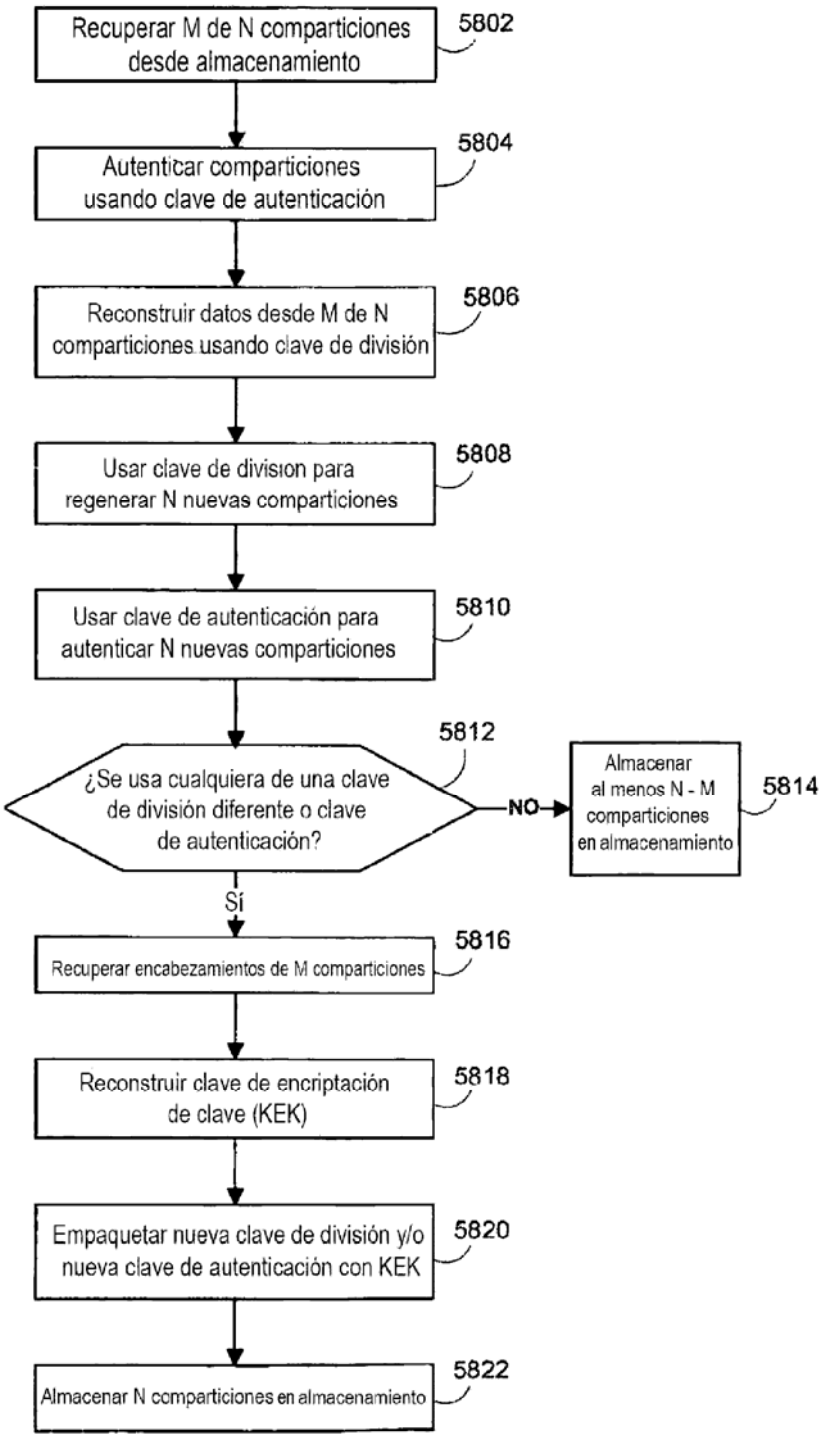

Recuperar M de N comparticiones desde almacenamiento
5802
Autenticar comparticiones usando clave de autenticación
5804
Reconstruir datos desde M de N comparticiones usando clave de división
5806
Usar clave de divisıon para regenerar N nuevas comparticiones
5808
Usar clave de autenticación para autenticar N nuevas comparticiones
5810
¿Se usa cualquiera de una clave de división diferente o clave de autenticación?
5812
NO
Almacenar al menos N - M comparticiones en almacenamiento
5814
Sí
Recuperar encabezamientos de M comparticiones
5816
Reconstruir clave de encriptación de clave (KEK)
5818
Empaquetar nueva clave de división y/o nueva clave de autenticación con KEK
5820
Almacenar N comparticiones en almacenamiento
5822

FIG. 58

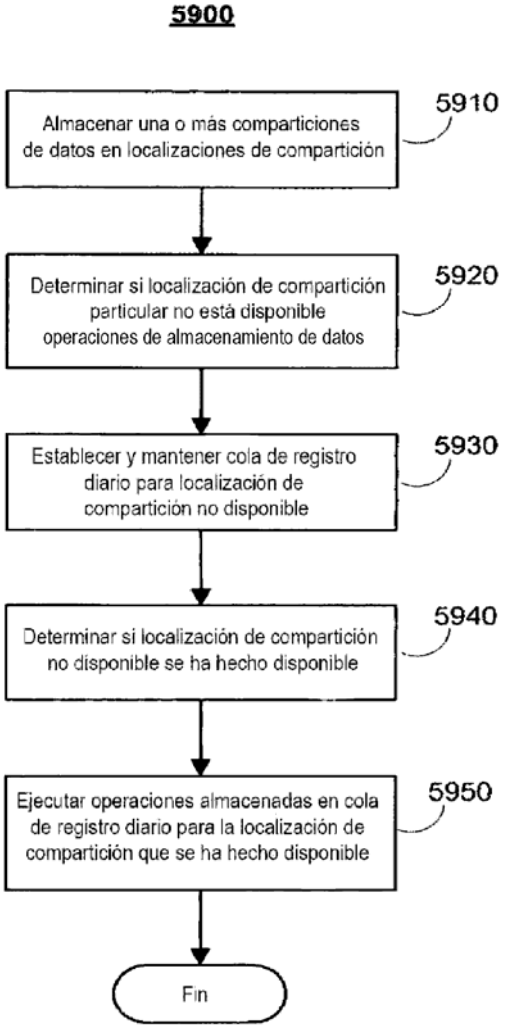

5900
Almacenar una o más compartimentos de datos en localizaciones de compartición
5910
Determinar si localización de compartición particular no está disponible operaciones de almacenamiento de datos
5920
Establecer y mantener cola de registro diario para localización de compartición no disponible
5930
Determinar si localización de compartición no disponible se ha hecho disponible
5940
Ejecutar operaciones almacenadas en cola de registro diario para la localización de compartición que se ha hecho disponible
5950
Fin

FIG. 59

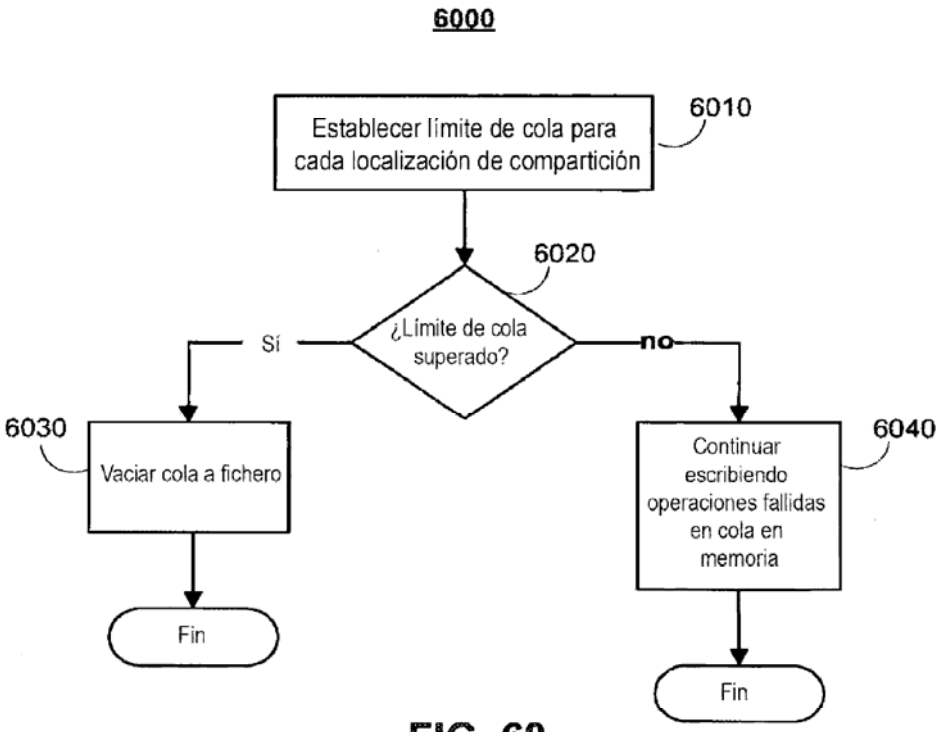

6000
Establecer límite de cola para cada localización de compartición
6010
6020
¿Límite de cola superado?
Sí
no
6030
Vaciar cola a fichero
Fin
6040
Continuar escribiendo operaciones fallidas en cola en memoria
Fin

FIG. 60

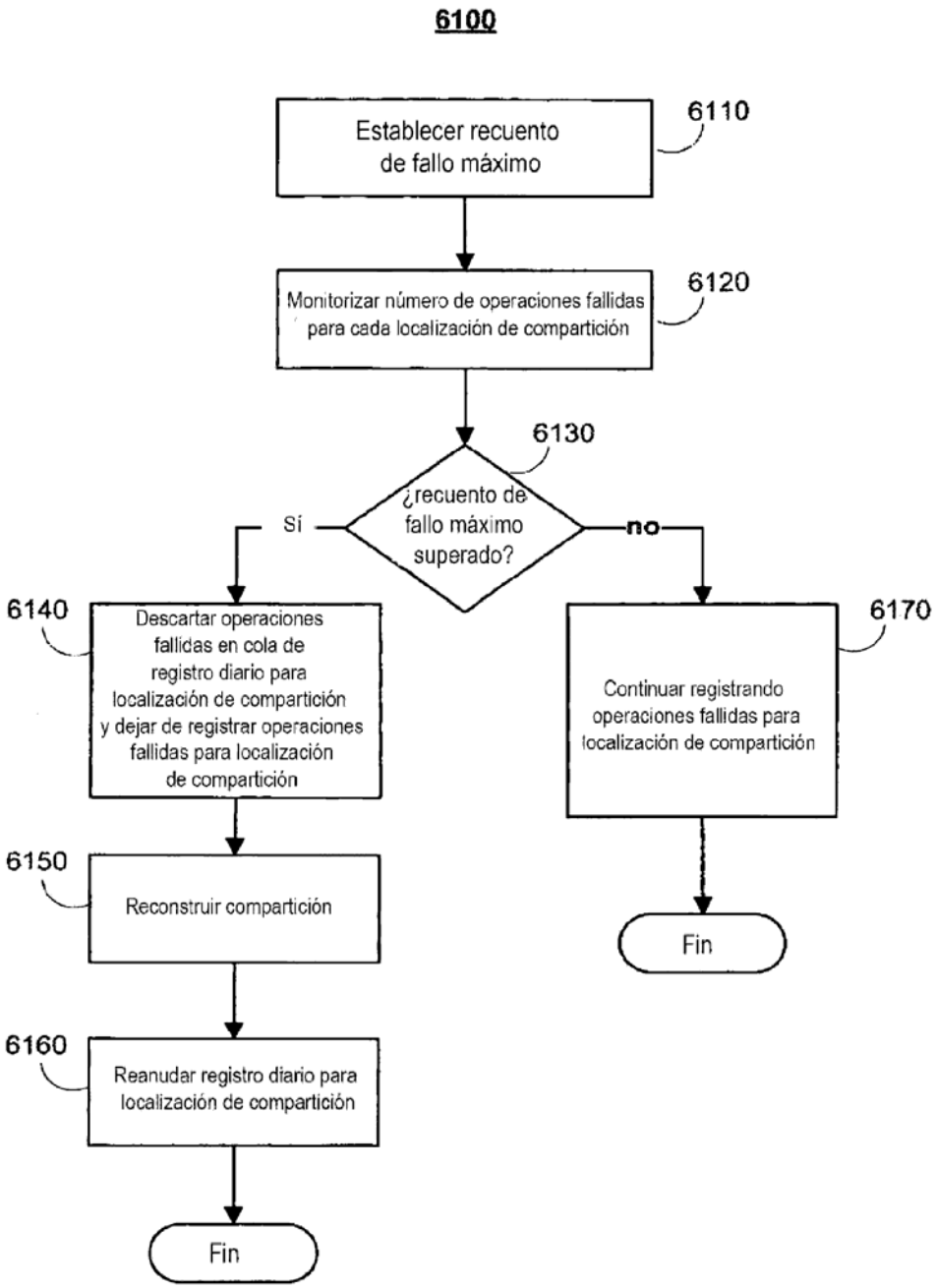

6100
Establecer recuento de fallo máximo
6110
Monitorizar número de operaciones fallidas para cada localización de compartición
6120
6130
¿recuento de fallo máximo superado?
Sí
no
6140
Descartar operaciones fallidas en cola de registro diario para localización de compartición y dejar de registrar operaciones fallidas para localización de compartición
6150
Reconstruir compartición
6160
Reanudar registro diario para localización de compartición
Fin
6170
Continuar registrando operaciones fallidas para localización de compartición
Fin

FIG. 61

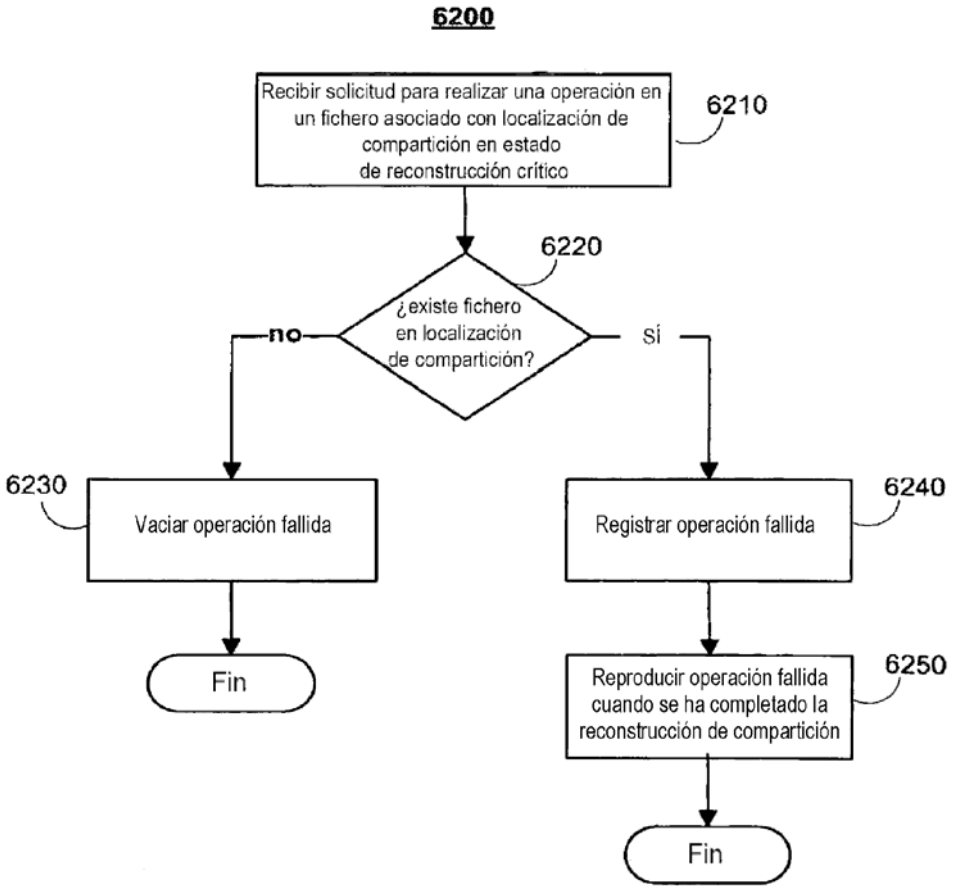

6200
Recibir solicitud para realizar una operación en un fichero asociado con localización de compartición en estado de reconstrucción crítico
6210
6220
¿existe fichero en localización de compartición?
no
sí
6230
Vaciar operación fallida
Fin
6240
Registrar operación fallida
6250
Reproducir operación fallida cuando se ha completado la reconstrucción de compartición
Fin

FIG. 62