(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 658 097**

(51) Int. CI.:

H04L 9/08 (2006.01)
H04L 9/32 (2006.01)
H04L 29/06 (2006.01)
G06F 21/62 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **20.11.2006 PCT/US2006/045066**

(87) Fecha y número de publicación internacional: **08.05.2008 WO08054406**

(96) Fecha de presentación y número de la solicitud europea: **20.11.2006 E 06851765 (5)**

(97) Fecha y número de publicación de la concesión europea: **27.12.2017 EP 1952575**

(54) Título: **Método y sistema de análisis de datos seguro**

(30) Prioridad:

18.11.2005 US 738231 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
08.03.2018

(73) Titular/es:

SECURITY FIRST CORPORATION
22362 GILBERTO, SUITE 130
RANCHO SANTA MARGARITA, CA 926, US

(72) Inventor/es:

O'HARE MARK S.;
ORISINI, RICK L.;
DAVENPORT, ROGER y
WINICK, STEVEN

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Método y sistema de análisis de datos seguro

Campo de la invención

La presente invención se refiere en general a un sistema para asegurar datos del acceso o uso no autorizado.

Antecedentes de la invención

En la sociedad de hoy en día, los individuos y negocios realizan una cantidad cada vez mayor de actividades en y a través de sistemas informáticos. Estos sistemas informáticos, incluyendo redes informáticas propietarias y no propietarias, a menudo almacenan, archivan y transmiten todos los tipos de información sensible. Por lo tanto, existe una necesidad cada vez mayor de asegurar datos almacenados y transmitidos a través de estos sistemas que no puedan leerse o verse comprometidos de otra manera.

Una solución común para asegurar sistemas informáticos es proporcionar funcionalidad de inicio de sesión y contraseña. Sin embargo, la gestión de contraseña ha probado ser bastante costosa con un alto porcentaje de llamadas al soporte técnico relacionadas con problemas de contraseña. Además, las contraseñas proporcionan poca seguridad en que, en general, se almacenan en un fichero susceptible de acceso inapropiado, a través de, por ejemplo, ataques por fuerza bruta.

Otra solución para asegurar sistemas informáticos es proporcionar infraestructuras criptográficas. La criptografía, en general, se refiere a proteger datos transformándolos o encriptándolos en un formato ilegible. Únicamente aquellos que poseen la clave o claves para la encriptación pueden desencriptar los datos en un formato usable. La criptografía se usa para identificar usuarios, por ejemplo, autenticación, para permitir privilegios de acceso, por ejemplo, autorización, para crear certificados y firmas digitales, y similares. Un sistema de criptografía conocido es un sistema de clave pública que usa dos claves, una clave pública conocida por todos y una clave privada conocida únicamente para el individuo o propietario del negocio del mismo. En general, los datos encriptados con una clave se desencriptan con la otra y ninguna calve es recreable a partir de la otra.

Desafortunadamente, incluso los sistemas criptográficos de clave pública típicos anteriores aún dependen en gran medida del usuario para la seguridad. Por ejemplo, los sistemas criptográficos emiten la clave privada al usuario, por ejemplo, a través del explorador del usuario. Los usuarios no sofisticados a continuación almacenan en general la clave privada en un disco duro accesible a otros a través de un sistema informático abierto, tal como, por ejemplo, Internet. Por otra parte, los usuarios pueden elegir nombres pobres para ficheros que contienen su clave privada, tal como, por ejemplo, "clave". El resultado de lo anterior y otros actos es permitir que la clave o claves sean susceptibles de compromiso.

Además de los anteriores compromisos, un usuario puede grabar su clave privada en un sistema informático configurado con un sistema de archivo o de respaldo, dando como resultado potencialmente copias de la clave privada que viajan a través de múltiples dispositivos de almacenamiento informático u otros sistemas. Esta brecha de seguridad a menudo se denomina como “migración de clave”. Similar a la migración de clave, muchas aplicaciones proporcionan acceso a la clave privada del usuario a través de, como máximo, acceso de inicio de sesión y contraseña sencillos. Como se ha mencionado en lo anterior, el acceso de inicio de sesión y contraseña a menudo no proporciona seguridad adecuada.

Una solución para aumentar la seguridad de los sistemas criptográficos anteriores es incluir biometría como parte de la autenticación o autorización. Las biometrías en general incluyen características físicas medibles, tales como, por ejemplo, huellas digitales o voz que pueden comprobarse por un sistema automatizado, tal como, coincidencia de patrón o reconocimiento de patrones de huellas digitales o patrones de voz. En tales sistemas, una biométrica del usuario y/o las claves pueden almacenarse en dispositivos informáticos móviles, tales como, por ejemplo, una tarjeta inteligente, portátil, asistente digital personal, o teléfono móvil, permitiendo de esta manera que la biometría o las claves sean usables en un entorno móvil.

El sistema criptográfico biométrico móvil anterior aún sufre de una diversidad de desventajas. Por ejemplo, el usuario móvil puede perder o romper la tarjeta inteligente o el dispositivo informático portátil, con lo que su acceso a datos potencialmente importantes quedará completamente interrumpido. Como alternativa, una persona maliciosa puede robar la tarjeta inteligente del usuario móvil o dispositivo informático portátil y usarla para robar de manera eficaz los credenciales digitales del usuario móvil. Por otra parte, el dispositivo informático portátil puede conectarse a un sistema abierto, tal como internet, y, como las contraseñas, el fichero donde se almacena la biometría puede ser susceptible de compromiso a través de la falta de atención de la seguridad del usuario a intrusos de seguridad o maliciosos.

El documento US 2004/0049687 se refiere a un método que comprende generar una clave maestra de sesión y encriptar datos, separar los datos encriptados en cuatro comparticiones de acuerdo con el patrón de la clave maestra de sesión, separar la clave maestra de sesión y anexar los datos de clave a los datos analizados encriptados, y encriptar cada compartición y almacenar las claves de encriptación en diferentes localizaciones de las comparticiones de datos encriptados.

El documento "Secured storage using SecureParsertm" por Schnitzer et al., proceedings of the 2005 ACM Workshop on storage security y survivability, Nueva York, 1 de enero de 2005, ISBN: 978-1-5993-233-4 se refiere a un enfoque de división de datos criptográficos, en el que los datos de entrada se dividen aleatoriamente a nivel de bit en múltiples comparticiones que pueden almacenarse a continuación en localizaciones separadas o transmitirse a través de diferentes canales de comunicación. La tecnología en sí misma es una forma de encriptación no codificada y usa un algoritmo de encriptación como su componente de seguridad principal, en el que el concepto de usar comparticiones forma la “clave”.

Sumario de la invención

Basándose en lo anterior, existe una necesidad de proporcionar un sistema criptográfico cuya seguridad es independiente del usuario mientras aún soporta usuarios móviles. Los objetos anteriores se consiguen mediante las características reivindicadas. La invención se define en las reivindicaciones.

Por consiguiente, un aspecto de la presente invención es proporcionar un método para asegurar virtualmente cualquier tipo de datos de acceso o uso no autorizado. El método comprende una o más etapas de analizar, dividir y/o separar los datos a asegurarse en dos o más partes o porciones. El método también comprende encriptar los datos a asegurarse.

La encriptación de los datos puede realizarse antes o después del primer análisis, división y/o separación de los datos. Además, la etapa de encriptación puede repetirse para una o más porciones de los datos. De manera similar, las etapas de análisis, división y/o separación pueden repetirse para una o más porciones de los datos. El método también comprende opcionalmente almacenar los datos analizados, divididos y/o separados que se han encriptado en una localización o en múltiples localizaciones.

Este método también comprende opcionalmente reconstituir o volver a ensamblar los datos asegurados en su forma original para acceso o uso autorizado. Este método puede incorporarse en las operaciones de cualquier ordenador, servidor, motor o similar, que pueda ejecutar las etapas deseadas del método.

Otro aspecto de la presente invención proporciona un sistema para asegurar virtualmente cualquier tipo de datos de acceso o uso no autorizado. Este sistema comprende un módulo de división de datos, un módulo de manejo criptográfico, y, opcionalmente, un módulo de ensamblaje de datos. El sistema puede comprender adicionalmente, en una realización, una o más instalaciones de almacenamiento de datos donde pueden almacenarse datos seguros.

Por consiguiente, un aspecto de la invención es proporcionar un servidor seguro, o motor de confianza, que tiene claves de servidor céntrico, o en otras palabras, almacenar claves criptográficas y datos de autenticación de usuario en un servidor. De acuerdo con esta realización, un usuario accede al motor de confianza para realizar funciones de autenticación y criptográficas, tales como, pero sin limitación, por ejemplo, autenticación, autorización, firma y generación digital, almacenamiento y recuperación de certificados, encriptación, acciones de tipo notario y de tipo poder legal y similares.

Otro aspecto de la invención es proporcionar un proceso de autenticación confiable o fiable. Además, después de una autenticación positiva de manera fiable, puede tomarse un amplio número de diferentes acciones, de proporcionar tecnología criptográfica, a autorización y acceso de sistema o dispositivo, para permitir uso o control de uno o un amplio número de dispositivos electrónicos.

Otro aspecto de la invención es proporcionar claves criptográficas y datos de autenticación en un entorno donde no se pierdan, roben o comprometan, evitando ventajosamente una necesidad de volver a emitir y gestionar nuevas claves y datos de autenticación. De acuerdo con otro aspecto de la invención, el motor de confianza permite que un usuario use un par de claves para múltiples actividades, distribuidores y/o solicitudes de autenticación. De acuerdo con otro aspecto más de la invención, el motor de confianza realiza al menos una etapa de procesamiento criptográfico, tal como, pero sin limitación, encriptar, autenticar o firmar en el lado del servidor, permitiendo de esta manera que los clientes o usuarios posean únicamente recursos informáticos mínimos.

De acuerdo con otro aspecto más de la invención, el motor de confianza incluye uno o múltiples depositarios para almacenar porciones de cada clave criptográfica y datos de autenticación. Las porciones se crean a través de un proceso de división de datos que prohíbe la reconstrucción sin una porción predeterminada de más de una localización en un depositario o desde múltiples depositarios. De acuerdo con otra realización, los múltiples depositarios pueden estar geográficamente remotos de manera que un empleado deshonesto o un sistema

comprometido de otra manera en un depositario no proporcionarán acceso a una clave del usuario o a datos de autenticación.

De acuerdo con otra realización más, el proceso de autenticación permite ventajosamente que el motor de confianza procese múltiples actividades de autenticación en paralelo. De acuerdo con otra realización más, el motor de confianza puede rastrear ventajosamente intentos de acceso fallidos y de esta manera limitar el número de veces que los intrusos maliciosos pueden intentar sabotear el sistema.

De acuerdo con otra realización más, el motor de confianza puede incluir múltiples instancias donde cada motor de confianza puede predecir y compartir las cargas de procesamiento con los otros. De acuerdo con otra realización más, el motor de confianza puede incluir un módulo de redundancia para interrogar una pluralidad de resultados de autenticación para asegurar que más de un sistema autentica al usuario.

Por lo tanto, un aspecto de la invención incluye un sistema criptográfico seguro, que puede ser remotamente accesible, para almacenar datos de cualquier tipo, incluyendo, pero sin limitación, una pluralidad de claves criptográficas privadas para asociarse con una pluralidad de usuarios. El sistema criptográfico asocia cada uno de la pluralidad de usuarios con una o más diferentes claves de la pluralidad de claves criptográficas privadas y realiza funciones criptográficas para cada usuario usando la una o más diferentes claves asociadas sin liberar la pluralidad de claves criptográficas privadas a los usuarios. El sistema criptográfico comprende un sistema de depositario que tiene al menos un servidor que almacena los datos a asegurarse, tal como una pluralidad de claves criptográficas privadas y una pluralidad de datos de autenticación de inscripción. Cada uno de los datos de autenticación de inscripción identifica uno de múltiples usuarios y cada uno de los múltiples usuarios está asociado con una o más diferentes claves de la pluralidad de claves criptográficas privadas. El sistema criptográfico puede comprender también un motor de autenticación que compara datos de autenticación recibidos por uno de los múltiples usuarios a datos de autenticación de inscripción que corresponden al uno de múltiples usuarios y recibidos desde el sistema de depositario, reduciendo de esta manera un resultado de autenticación. El sistema criptográfico también puede comprender un motor criptográfico que, cuando el resultado de autenticación indica identificación apropiada del uno de los múltiples usuarios, realiza funciones criptográficas en nombre del uno de los múltiples usuarios usando la una o más diferentes claves asociadas recibidas desde el sistema de depositario. El sistema criptográfico puede comprender también un motor de transacción conectado para encaminar datos desde los múltiples usuarios al sistema de servidor de depositario, el motor de autenticación y el motor criptográfico.

Otro aspecto de la invención incluye un sistema criptográfico seguro que es opcionalmente accesible de manera remota. El sistema criptográfico comprende un sistema de depositario que tiene al menos un servidor que almacena al menos una clave privada y cualquier otro dato, tal como, pero sin limitación, una pluralidad de datos de autenticación de inscripción, en el que cada uno de los datos de autenticación de inscripción identifica uno de posibles múltiples usuarios. El sistema criptográfico puede comprender también opcionalmente un motor de autenticación que compara datos de autenticación recibidos por los usuarios a datos de autenticación de inscripción que corresponden al usuario y recibidos desde el sistema de depositario, produciendo de esta manera un resultado de autenticación. El sistema criptográfico también comprende un motor criptográfico que, cuando el resultado de autenticación indica identificación apropiada del usuario, realiza funciones criptográficas en nombre del usuario usando al menos dicha clave privada, que puede recibirse desde el sistema de depositario. El sistema criptográfico puede comprender también opcionalmente un motor de transacción conectado para encaminar datos desde los usuarios a otros motores o sistemas tales como, pero sin limitación, el sistema de servidor de depositario, el motor de autenticación y el motor criptográfico.

Otro aspecto de la invención incluye un método de facilitar funciones criptográficas. El método comprende asociar un usuario de múltiples usuarios con una o más claves desde una pluralidad de claves criptográficas privadas almacenadas en una localización segura, tal como un servidor seguro. El método también comprende recibir datos de autenticación desde el usuario, y comparar los datos de autenticación a datos de autenticación que corresponden al usuario, verificando de esta manera la identidad del usuario. El método también comprende utilizar la una o más claves para realizar funciones criptográficas sin liberar la una o más claves al usuario.

Otro aspecto de la invención incluye un sistema de autenticación para identificar de manera inequívoca un usuario a través del almacenamiento seguro de los datos de autenticación de inscripción del usuario. El sistema de autenticación comprende una o más instalaciones de almacenamiento de datos, en el que cada instalación de almacenamiento de datos incluye un segundo medio de almacenamiento accesible por ordenador que almacena al menos una de porciones de datos de autenticación de inscripción. El sistema de autenticación también comprende un motor de autenticación que comunica con la instalación o instalaciones de almacenamiento de datos. El motor de autenticación comprende un módulo de división de datos que opera en los datos de autenticación de inscripción para crear porciones, un módulo de ensamblaje de datos que procesa las porciones de al menos una de las instalaciones de almacenamiento de datos para ensamblar los datos de autenticación de inscripción, y un módulo comparador de datos que recibe datos de autenticación actuales de un usuario y compara los datos de autenticación actuales con los datos de autenticación de inscripción ensamblados para determinar si el usuario se ha identificado de manera inequívoca.

Otro aspecto de la invención incluye un sistema criptográfico. El sistema criptográfico comprende una o más instalaciones de almacenamiento de datos, en el que cada instalación de almacenamiento de datos incluye un segundo medio de almacenamiento accesible por ordenador que almacena al menos una porción de una o más claves criptográficas. El sistema criptográfico también comprende un motor criptográfico que comunica con las instalaciones de almacenamiento de datos. El motor criptográfico también comprende un módulo de división de datos que opera en las claves criptográficas para crear porciones, un módulo de ensamblaje de datos que procesa las porciones desde al menos una de las instalaciones de almacenamiento de datos para ensamblar las claves criptográficas, y un módulo de manejo criptográfico que recibe las claves criptográficas ensambladas y realiza funciones criptográficas con las mismas.

Otro aspecto de la invención incluye un método de almacenamiento de cualquier tipo de datos, incluyendo, pero sin limitación, datos de autenticación en instalaciones de almacenamiento de datos seguras geográficamente remotas protegiendo de esta manera los datos contra composición de cualquier instalación de almacenamiento de datos individual. El método comprende recibir datos en un motor de confianza, combinar en el motor de confianza los datos con un primer valor sustancialmente aleatorio para formar un primer valor combinado, y combinar los datos con un segundo valor sustancialmente aleatorio para formar un segundo valor combinado. El método comprende crear un primer emparejamiento del primer valor sustancialmente aleatorio con el segundo valor combinado, crear un segundo emparejamiento del primer valor sustancialmente aleatorio con el segundo valor sustancialmente aleatorio, y almacenar el primer emparejamiento en una primera instalación de almacenamiento de datos segura. El método comprende almacenar el segundo emparejamiento en una segunda instalación de almacenamiento de datos segura remota de la primera instalación de almacenamiento de datos segura.

Otro aspecto de la invención incluye un método de almacenamiento de cualquier tipo de datos, incluyendo, pero sin limitación, datos de autenticación que comprende recibir datos, combinar los datos con un primer conjunto de bits para formar un segundo conjunto de bits, y combinar los datos con un tercer conjunto de bits para formar un cuarto conjunto de bits. El método también comprende crear un primer emparejamiento del primer conjunto de bits con el tercer conjunto de bits. El método también comprende crear un segundo emparejamiento del primer conjunto de bits con el cuarto conjunto de bits, y almacenar uno del primer y segundo emparejamientos en un primer medio de almacenamiento accesible por ordenador. El método también comprende almacenar el otro del primer y segundo emparejamientos en un segundo medio de almacenamiento accesible por ordenador.

Otro aspecto de la invención incluye un método de almacenamiento de datos criptográficos en instalaciones de almacenamiento de datos seguras geográficamente remotas protegiendo de esta manera los datos criptográficos contra compromiso de cualquier instalación de almacenamiento de datos individual. El método comprende recibir datos criptográficos en un motor de confianza, combinar en el motor de confianza los datos criptográficos con un primer valor sustancialmente aleatorio para formar un primer valor combinado, y combinar los datos criptográficos con un segundo valor sustancialmente aleatorio para formar un segundo valor combinado. El método también comprende crear un primer emparejamiento del primer valor sustancialmente aleatorio con el segundo valor combinado, crear un segundo emparejamiento del primer valor sustancialmente aleatorio con el segundo valor sustancialmente aleatorio, y almacenar el primer emparejamiento en una primera instalación de almacenamiento de datos segura. El método también comprende almacenar el segundo emparejamiento en una segunda instalación de almacenamiento de datos segura remota de la primera instalación de almacenamiento de datos segura.

Otro aspecto de la invención incluye un método de almacenamiento de datos criptográficos que comprende recibir datos de autenticación y combinar los datos criptográficos con un primer conjunto de bits para formar un segundo conjunto de bits. El método comprende también combinar los datos criptográficos con un tercer conjunto de bits para formar un cuarto conjunto de bits, crear un primer emparejamiento del primer conjunto de bits con el tercer conjunto de bits, y crear un segundo emparejamiento del primer conjunto de bits con el cuarto conjunto de bits. El método también comprende almacenar uno del primer y segundo emparejamientos en un primer medio de almacenamiento accesible por ordenador, y almacenar el otro del primer y segundo emparejamientos en un segundo medio de almacenamiento accesible por ordenador.

Otro aspecto de la invención incluye un método de manejo de datos sensibles de cualquier tipo o forma en un sistema criptográfico, en el que los datos sensibles existen en una forma usable únicamente durante acciones por usuarios autorizados, empleando los datos sensibles. El método también comprende recibir en un módulo de software, datos sensibles sustancialmente aleatorizados o encriptados desde un primer medio de almacenamiento accesible por ordenador, y recibir en el módulo de software, datos sustancialmente aleatorizados o encriptados que pueden o pueden no ser datos sensibles, desde uno o más otro segundo medio de almacenamiento accesible por ordenador. El método también comprende procesar los datos sensibles sustancialmente aleatorizados pre-encriptados que pueden o no ser datos sensibles, en el módulo de software para ensamblar los datos sensibles y emplear los datos sensibles en un motor de software para realizar una acción. La acción incluye, pero sin limitación, una de autenticar un usuario y realizar una función criptográfica.

Otro aspecto de la invención incluye un sistema de autenticación segura. El sistema de autenticación segura comprende una pluralidad de motores de autenticación. Cada motor de autenticación recibe datos de autenticación de inscripción diseñados para identificar de manera inequívoca un usuario hasta un grado de certidumbre. Cada

motor de autenticación recibe datos de autenticación actuales para comparar los datos de autenticación de inscripción, y cada motor de autenticación determina un resultado de autenticación. El sistema de autenticación segura también comprende un sistema de redundancia que recibe el resultado de autenticación de al menos dos de los motores de autenticación y determina si el usuario se ha identificado de manera inequívoca.

Otro aspecto de la invención incluye un sistema de datos en movimiento seguro mediante el cual los datos pueden transmitirse en diferentes porciones que se aseguran de acuerdo con la presente invención de manera que una porción cualquiera que se comprometiera no deberá proporcionar suficientes datos para restaurar los datos originales. Esto puede aplicarse a cualquier transmisión de datos, ya sea alámbrica, inalámbrica o física.

Otro aspecto de la invención incluye la integración del analizador de datos seguro de la presente invención en cualquier sistema adecuado donde los datos se almacenan o comunican. Por ejemplo, sistema de correo electrónico, sistemas RAID, sistemas de difusión de vídeo, sistemas de base de datos o cualquier otro sistema adecuado que pueda tener el analizador de datos seguro integrado a cualquier nivel adecuado.

Otro aspecto de la invención incluye usar cualquier algoritmo de análisis y división adecuado para generar comparticiones de datos. Ya sea aleatorio, pseudo-aleatorio, determinístico o cualquier combinación de los mismos que pueda emplearse para analizar y dividir datos.

Breve descripción de los dibujos

La presente invención se describe en más detalle a continuación junto con los dibujos adjuntos, que se pretenden para ilustrar y no para limitar la invención, y en los que:

La Figura 1 ilustra un diagrama de bloques de un sistema criptográfico, de acuerdo con aspectos de una realización de la invención;
La Figura 2 ilustra un diagrama de bloques del motor de confianza de la Figura 1, de acuerdo con aspectos de una realización de la invención;
La Figura 3 ilustra un diagrama de bloques del motor de transacción de la Figura 2, de acuerdo con aspectos de una realización de la invención;
La Figura 4 ilustra un diagrama de bloques del depositario de la Figura 2, de acuerdo con aspectos de una realización de la invención;
La Figura 5 ilustra un diagrama de bloques del motor de autenticación de la Figura 2, de acuerdo con aspectos de una realización de la invención;
La Figura 6 ilustra un diagrama de bloques del motor criptográfico de la Figura 2, de acuerdo con aspectos de una realización de la invención;
La Figura 7 ilustra un diagrama de bloques de un sistema depositario, de acuerdo con aspectos de otra realización de la invención;
La Figura 8 ilustra un diagrama de flujo de un proceso de división de datos de acuerdo con aspectos de una realización de la invención;
La Figura 9, Panel A ilustra un flujo de datos de un proceso de inscripción de acuerdo con aspectos de una realización de la invención;
La Figura 9, Panel B ilustra un diagrama de flujo de un proceso de interoperabilidad de acuerdo con aspectos de una realización de la invención;
La Figura 10 ilustra un flujo de datos de un proceso de autenticación de acuerdo con aspectos de una realización de la invención;
La Figura 11 ilustra un flujo de datos de un proceso de firma de acuerdo con aspectos de una realización de la invención;
La Figura 12 ilustra un flujo de datos y un proceso de encriptación/desencriptación de acuerdo con aspectos y otra realización más de la invención;
La Figura 13 ilustra un diagrama de bloques simplificado de un sistema de motor de confianza de acuerdo con aspectos de otra realización de la invención;
La Figura 14 ilustra un diagrama de bloques simplificado de un sistema de motor de confianza de acuerdo con aspectos de otra realización de la invención;
La Figura 15 ilustra un diagrama de bloques del módulo de redundancia de la Figura 14, de acuerdo con aspectos de una realización de la invención;
La Figura 16 ilustra un proceso para evaluar autenticaciones de acuerdo con un aspecto de la invención;
La Figura 17 ilustra un proceso para asignar un valor a una autenticación de acuerdo con un aspecto como se muestra en la Figura 16 de la invención;
La Figura 18 ilustra un proceso para realizar arbitraje de confianza en un aspecto de la invención como se muestra en la Figura 17; y
La Figura 19 ilustra una transacción de muestra entre un usuario y un distribuidor de acuerdo con aspectos de una realización de la invención 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 intermedia 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 intermedia 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 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 realización de la presente invención.
La Figura 28 es un diagrama de bloques de un sistema de datos en movimiento ilustrativo de acuerdo con una realización de la presente invención.
La Figura 29 es un diagrama de bloques de otro sistema de datos en movimiento ilustrativo de acuerdo con una realización de la presente invención.
Las Figuras 30-32 son diagramas de bloques de un sistema ilustrativo que tiene el analizador de datos seguro integrado de acuerdo con una realización de la presente invención.
La Figura 33 es un diagrama de flujo de proceso de un proceso ilustrativo para analizar y dividir datos de acuerdo con una realización de la presente invención.
La Figura 34 es un diagrama de flujo de proceso de un proceso ilustrativo para restaurar porciones de datos en datos originales de acuerdo con una realización de la presente invención.
La Figura 35 es un diagrama de flujo de proceso de un proceso ilustrativo para dividir datos al nivel de bits de acuerdo con una realización de la presente invención.
La Figura 36 es un diagrama de flujo de proceso de etapas y características ilustrativas, que pueden usarse en cualquier combinación adecuada, con cualquier adición, borrado o modificación adecuada de acuerdo con una realización de la presente invención.
La Figura 37 es un diagrama de flujo de proceso de etapas y características ilustrativas que pueden usarse en cualquier combinación adecuada, con cualquier adición, borrado o modificación adecuada de acuerdo con una 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 puede usarse en cualquier combinación adecuada, con cualquier adición, borrado o modificación adecuada de acuerdo con una 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 puede usarse en cualquier combinación adecuada, con cualquier adición, borrado o modificación adecuada de acuerdo con una 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 pueden usarse en cualquier combinación adecuada, con cualquier adición, borrado o modificación adecuada de acuerdo con una realización de la presente invención.
La Figura 41 es un diagrama de bloques simplificado de un formato de compartición ilustrativo, que puede usarse en cualquier combinación adecuada, con cualquier adición, borrado o modificación adecuada de acuerdo con una realización de la presente invención.

Descripción detallada de la invención

Un aspecto de la presente invención es proporcionar un sistema criptográfico donde uno o más servidores seguros, o un motor de confianza, almacenan claves criptográficas y datos de autenticación de usuario. Los usuarios acceden a la funcionalidad de los sistemas criptográficos convencionales a través del acceso de red al motor de confianza, sin embargo, 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.

Puesto que los usuarios pueden estar seguros de, o confiar en, el sistema criptográfico para realizar autenticación de usuarios y documentos y otras funciones criptográficas, puede incorporarse 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 digitalmente el acuerdo en nombre de o para los participantes, y almacenar un registro del acuerdo firmado digitalmente 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 aspectos de una realización de la invención. Como se muestra en la Figura 1, el sistema criptográfico 100 incluye un sistema de usuario 105, un motor de confianza 110, una autoridad de certificación 115, y un sistema distribuidor 120, que comunica a través de un enlace de comunicación 125.

De acuerdo con una realización de la invención, el sistema de usuario 105 comprende un ordenador de 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. Como se muestra en la Figura 1, el sistema de usuario 105 puede incluir un dispositivo biométrico 107. El dispositivo biométrico 107 puede capturar ventajosamente una biométrica del usuario y transferir la biométrica capturada al motor de confianza 110. De acuerdo con una realización de la invención, el dispositivo biométrico puede comprender ventajosamente un dispositivo que tiene atributos y características similares a aquellas desveladas en la Solicitud de Patente de Estados Unidos N.º 08/926.277, presentada el 5 de septiembre de 1997, titulada “RELIEF OBJECT IMAGE GENERATOR”, Solicitud de Patente de Estados Unidos N.º 09/558.634, presentada el 26 de abril de 2000, titulada “IMAGINE DEVICE FOR A RELIEF OBJECT AND SYSTEM AND METHOD OF USING THE IMAGE DEVICE”, Solicitud de Patente de Estados Unidos N.º 09/435.011, presentada el 5 de noviembre de 1999, titulada “RELIEF OBJECT SENSOR ADAPTOR”, y Solicitud de Patente de Estados Unidos N.º 09/477.943, presentada el 5 de enero de 2000, titulada “PLANAR OPTICAL IMAGE SENSOR AND SYSTEM FOR GENERATING AN ELECTRONIC IMAGE OF A RELIEF OBJECT FOR FINGERPRINT READING”, todas las cuales son de propiedad del cesionario actual.

Además, el sistema de usuario 105 puede conectarse al enlace de comunicación 125 a través de un proveedor de servicio convencional, tal como, por ejemplo, una marcación, línea de abonado digital (DSL), cable módem, conexión de fibra o similares. De acuerdo con otra realización, el sistema de usuario 105 se conecta al 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 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.

Aunque el sistema de usuario 105 se desvela con referencia a las realizaciones anteriores, la invención no pretende 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 realizaciones 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, teléfono móvil, 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. Sin embargo, de acuerdo con una realización, los sistemas operativos continúan proporcionando ventajosamente los protocolos de comunicación apropiados necesarios para establecer comunicación con el enlace de comunicación 125.

La Figura 1 ilustra el motor de confianza 110. De acuerdo con una realización, el motor de confianza 110 comprende uno o más servidores seguros para acceder 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 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 asociados con una transacción actual, a los datos de autenticación proporcionados en un tiempo anterior, tal como, por ejemplo, durante la inscripción. El motor de confianza 110 puede requerir ventajosamente que el usuario produzca los datos de autenticación en el momento de cada transacción, o, el motor de confianza 110 puede permitir ventajosamente al usuario producir periódicamente 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 realización 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 ventajosamente 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 apropiadamente puede emplear ventajosamente 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. Sin embargo, las claves criptográficas privadas usadas 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 realización, el motor de confianza 110 genera y almacena claves criptográficas. De acuerdo con otra realización, al menos una clave criptográfica está asociada con cada usuario. Además, cuando las claves criptográficas incluyen tecnología de clave pública, cada clave privada 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 ventajosamente 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 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 realización, el motor de confianza 110 en primer lugar autentica el usuario, y después de que el usuario ha producido apropiadamente 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 ventajosamente 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 pueden implementarse 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 realización, la autoridad de certificación 115 puede comprender ventajosamente una organización o compañía de terceros confiable que expide certificados digitales, tales como, por ejemplo, VeriSign, Baltimore, Entrust, o similares. El motor de confianza 110 puede transmitir ventajosamente solicitudes de certificados digitales, a través de uno o más protocolos de 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 realización de la invención, el motor de confianza 110 solicita certificados digitales desde varias o todas las autoridades de certificados 115 importantes de manera que el motor de confianza 110 tenga acceso a un certificado digital que corresponde a la norma de certificado de cualquier parte solicitante.

De acuerdo con otra realización, el motor de confianza 110 realiza internamente expediciones de certificados. En esta realización, el motor de confianza 110 puede acceder a un sistema de certificados para generar certificados y/o puede generar internamente 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 desvelará en mayor detalle a continuación.

La Figura 1 ilustra también el sistema distribuidor 120. De acuerdo con una realización, el sistema distribuidor 120 comprende ventajosamente un servidor web. Los servidores web típicos 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) o el Lenguaje de Marcas Extensible (XML). El servidor web acepta solicitudes desde exploradores como Netscape e Internet Explorer y a continuación devuelve los documentos electrónicos apropiados. Puede usarse 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 guiones de Interfaz Común de Pasarela (CGI), seguridad de Capa de Conexiones Seguras (SSL), y Páginas de Servidor Activas (ASP). El sistema distribuidor 120 puede proporcionar ventajosamente contenido electrónico relacionado con transacciones comerciales, personales, educacionales u otras.

Aunque el sistema distribuidor 120 se desvela con referencia a las realizaciones anteriores, la invención no pretende 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 distribuidor 120 puede comprender ventajosamente cualquiera de los dispositivos descritos 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 distribuidor 120. De acuerdo con una realización, el enlace de comunicación 125 comprende preferentemente internet. Internet, 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 desde la parte troncal. Estas ramificaciones, a su vez, tienen redes que se ramifican desde ellas, 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 realización ventajosa, los concentradores de encaminamiento de internet comprenden servidores de sistema de nombre de dominio (DNS) que usan el Protocolo de Control de Transmisión/Protocolo de Internet (TCP/IP) 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 típicamente “sitios web”. Un sitio web se define mediante una dirección de Internet que tiene una página electrónica asociada. La página electrónica puede identificarse mediante un Localizador de Recurso Uniforme (URL). En general, una página electrónica es un documento que organiza la presentación de texto, imágenes gráficas, audio, vídeo, y así sucesivamente.

Aunque el enlace de comunicación 125 se desvela en términos de su 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 aspectos de una realización de la invención. Como se muestra en la Figura 2, el motor de confianza 110 incluye un motor de transacción 205, un depositario 210, un motor de autenticación 215, y un motor criptográfico 220. De acuerdo con una realización de la invención, el motor de confianza 110 incluye también el almacenamiento masivo 225. Como se muestra adicionalmente en la Figura 2, el motor de transacción 205 comunica con el depositario 210, el motor de autenticación 215, y el motor criptográfico 220, junto con el almacenamiento masivo 225. Además, el depositario 210 comunica con el motor de autenticación 215, el motor criptográfico 220, y el almacenamiento masivo 225. Además, el motor de autenticación 215 comunica con el motor criptográfico 220. De acuerdo con una realización de la invención, algunas o todas las comunicaciones anteriores pueden comprender ventajosamente la transmisión de documentos XML a direcciones de IP que corresponden al dispositivo de recepción. Como se ha mencionado en lo anterior, los documentos XML permiten ventajosamente 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 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 ventajosamente datos entrantes desde el enlace de comunicación 125. De acuerdo con una 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 ventajosamente 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 depositario 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 ventajosamente al sistema de usuario 105, a la autoridad de certificación 115, o al sistema distribuidor 120.

De acuerdo con una realización, los datos se encaminan usando técnicas de encaminamiento de HTTP convencionales, tales como, por ejemplo, emplear URL o Indicadores de Recursos Uniformes (URL). Los URI son similares a los URL, sin embargo, los URI indican típicamente la fuente de ficheros o acciones, tal como, por ejemplo, ejecutables, guiones, y similares. Por lo tanto, de acuerdo con una realización, el sistema de usuario 105, la autoridad de certificación 115, el sistema distribuidor 120, y los componentes del motor de confianza 210, incluyen

ventajosamente suficientes datos en los URL o URI de comunicación para que el motor de transacción 205 encamine apropiadamente datos lo largo de todo el sistema criptográfico.

Aunque el encaminamiento de datos se desvela con referencia a su 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 ventajosamente desempaquetarse y reconocerse por su formato, contenido, o similares, de manera que el motor de transacción 205 pueda encaminar apropiadamente datos a través del motor de confianza 110. Además, un experto en la materia reconocerá que el encaminamiento de datos puede adaptarse ventajosamente 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 realización más de la invención, el motor de transacción 205 incluye tecnologías de encriptación de SSL convencionales, de manera que los sistemas anteriores pueden autenticarse a sí mismos, y viceversa, con el motor de transacción 205, durante comunicaciones particulares. Como se usará a lo largo de toda esta divulgación, el término “½ SSL” se refiere a comunicaciones donde un servidor pero no necesariamente el cliente, está autenticado por SSL, y el término “SSL TOTAL” se refiere a comunicaciones donde el cliente y el servidor están autenticados por SSL. Cuando la divulgación actual usa el término “SSL”, la comunicación puede comprender SSL ½ 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 ventajosamente crear un recorrido de auditoría. De acuerdo con una 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 pueden almacenarse ventajosamente en el almacenamiento masivo 225.

La Figura 2 ilustra también el depositario 210. De acuerdo con una realización, el depositario 210 comprende una o más instalaciones de almacenamiento, tales como, por ejemplo, un servidor de directorio, un servidor de base de datos o similares. Como se muestra en la Figura 2, el depositario 210 almacena claves criptográficas y datos de autenticación de inscripción. Las claves criptográficas pueden corresponder ventajosamente al motor de confianza 110 o a los usuarios del sistema criptográfico 100, tales como el usuario o distribuidor. Los datos de autenticación de inscripción pueden incluir ventajosamente 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 pueden obtenerse ventajosamente 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 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, como se ha mencionado en lo anterior, los datos de las comunicaciones a y desde el depositario 210 pueden transferirse usando URL, URI, HTTP o documentos XML, con cualquiera de los anteriores teniendo ventajosamente solicitudes de datos y formatos embebidos en los mismos.

Como se ha mencionado anteriormente, el depositario 210 puede comprender ventajosamente una pluralidad de instalaciones de almacenamiento de datos seguras. En una realización de este tipo, las instalaciones de almacenamiento de datos seguras pueden configurarse de manera que un compromiso de la seguridad en una instalación de almacenamiento de datos individual no comprometerá las claves criptográficas o los datos de autenticación almacenados en la misma. Por ejemplo, de acuerdo con esta realización, las claves criptográficas y los datos de autenticación se operan matemáticamente para aleatorizar estadísticamente y sustancialmente los datos almacenados en cada instalación de almacenamiento de datos. De acuerdo con una realización, la aleatorización de los datos de una instalación de almacenamiento de datos individual 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 realización, el motor de autenticación 215 comprende un comparador configurado para comparar datos desde el motor de transacción 205 con datos desde el depositario 210. Por ejemplo, durante la autenticación, un usuario suministra datos de autenticación actuales al motor de confianza 110 de manera que el motor de transacción 205 recibe los datos de autenticación actuales. Como se ha mencionado en lo anterior, el motor de transacción 205 reconoce las solicitudes de datos, preferentemente en el URL o URI, y encamina los datos de autenticación al motor de autenticación 215. Además, tras la solicitud, el depositario 210 reenvía los datos de autenticación de inscripción que corresponden al 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 comparación.

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

Como se muestra en la Figura 2, el motor de confianza 110 incluye también el motor criptográfico 220. De acuerdo con una realización, el motor criptográfico comprende un módulo de manejo criptográfico, configurado para proporcionar ventajosamente funciones criptográficas convencionales, tales como, por ejemplo, funcionalidad de infraestructura de clave pública (PKI). Por ejemplo, el motor criptográfico 220 puede expedir ventajosamente 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 depositario 210 de manera que al menos las claves criptográficas privadas no estén disponibles fuera del motor de confianza 110. De acuerdo con otra realización, el motor criptográfico 220 aleatoriza y divide al menos los datos de 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 realización, las funciones del motor criptográfico pueden combinarse con y realizarse mediante el motor de autenticación 215.

De acuerdo con una realización, las comunicaciones a y desde el motor criptográfico incluyen comunicaciones seguras, tal como tecnología de SSL. Además, pueden emplearse ventajosamente 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. Como se ha mencionado en lo anterior, el motor de transacción 205 mantiene los datos que corresponden a un recorrido de auditoría y almacena tales datos en el almacenamiento masivo 225. De manera similar, de acuerdo con una realización de la invención, el depositario 210 mantiene datos que corresponden a un recorrido de auditoría y almacena tales datos en el dispositivo de almacenamiento masivo 225. Los datos de recorrido de auditoría del depositario 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 depositario 210 y la respuesta de las mismas. Además, el almacenamiento masivo 225 puede usarse para almacenar certificados digitales que tienen la clave pública de un usuario contenida en el mismo.

Aunque el motor de confianza 110 se desvela con referencia a sus realizaciones preferida y alternativa, la invención no pretende 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 ventajosamente únicamente autenticación, o como alternativa, únicamente algunas o todas las funciones criptográficas, tales como encriptación y desencriptación de datos. De acuerdo con tales realizaciones, uno del motor de autenticación 215 y el motor criptográfico 220 puede eliminarse ventajosamente, creando de esta manera un diseño más sencillo para el motor de confianza 110. Además, el motor criptográfico 220 puede comunicar también con una autoridad de certificación de manera que la autoridad de certificación esté incorporada en el motor de confianza 110. De acuerdo con otra realización más, el motor de confianza 110 puede realizar ventajosamente 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 aspectos de una realización de la invención. De acuerdo con esta realización, el motor de transacción 205 comprende un sistema operativo 305 que tiene un hilo de manejo y un hilo de escucha. El sistema operativo 305 puede ventajosamente ser similar a aquellos 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 depositario 210, el motor de autenticación 215, el motor criptográfico 220, o el almacenamiento masivo 225. Como se muestra en la Figura 3, los datos entrantes y salientes pueden asegurarse ventajosamente a través de, por ejemplo, tecnología de SSL.

La Figura 4 ilustra un diagrama de bloques del depositario 210 de la Figura 2 de acuerdo con aspectos de una realización de la invención. De acuerdo con esta realización, el depositario 210 comprende uno o más servidores de protocolo ligero de acceso al directorio (LDAP). 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 preferentemente datos 405 que corresponden a las claves criptográficas y datos 410 que corresponden a los datos de autenticación de inscripción. De acuerdo con una realización, el depositario 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 preferentemente mecanismos para

asegurar un alto grado de confiabilidad, o seguridad, en los datos almacenados en la misma. Por ejemplo, la localización física del depositario 210 puede incluir ventajosamente 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 ventajosamente soluciones de software para proteger los datos almacenados. Por ejemplo, el depositario 210 puede crear y almacenar ventajosamente datos 415 que corresponden a un recorrido de auditoría de acciones tomadas. Además, las comunicaciones entrantes y salientes pueden ventajosamente encriptarse con la encriptación de clave pública acoplada con tecnologías de SSL convencionales.

De acuerdo con otra realización, el depositario 210 puede comprender instalaciones de almacenamiento de datos distintas y físicamente separadas, como se desvela 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 aspectos de una 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. Como se muestra en la Figura 5, el motor de autenticación 215 incluye acceso a al menos una clave privada 510. La clave privada 510 puede usarse ventajosamente por ejemplo, para desencriptar datos desde el motor de transacción 205 o el depositario 210, que se encriptaron con una correspondiente clave pública 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 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 hardware, software, o soluciones combinadas para comparaciones de patrones, tales como, por ejemplo, aquellos que representan patrones de huellas digitales o patrones de voz. Además, de acuerdo con una realización, el comparador 515 del motor de autenticación 215 puede comparar ventajosamente troceos convencionales de documentos para presentar un resultado de comparación. De acuerdo con una realización de la invención, el comparador 515 incluye la aplicación de heurística 530 a la comparación. La heurística 530 puede tratar ventajosamente 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 a partir de 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 puede determinarse 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 donde es aceptable autenticarse a un nivel de confianza inferior. Esto podría incluir una transacción que tenga un valor bajo de dólares asociado con ella (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 remotamente en un ordenador gubernamental).

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

De acuerdo con otra realización de la invención, el comparador 515 puede rastrear ventajosamente 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 ventajosamente 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 realización, el limitador de intentos 535 comprende un módulo de software 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 ventajosamente intentos de autenticación adicionales. Tal denegación puede implementarse ventajosamente a través de, por ejemplo, devolviendo el comparador 515 un resultado negativo independientemente de los datos de autenticación actuales que se están transmitiendo. Por otra parte, el motor de transacción 205 puede bloquear ventajosamente 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 ventajosamente un módulo de software, hardware, 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 realización, los datos originales no son recreables desde una porción individual. El módulo de ensamblaje de datos 525 comprende ventajosamente un módulo de software, hardware, o combinación configurado para operar matemáticamente en las anteriores porciones sustancialmente aleatorizadas, de manera que la combinación de las mismas proporciona los datos descifrados originales. De acuerdo con una realización, el motor de autenticación 215 emplea el módulo de división de datos 520 para aleatorizar y dividir 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 usables.

La Figura 6 ilustra un diagrama de bloques del motor criptográfico 220 del motor de confianza 200 de la Figura 2 de acuerdo con aspectos de una realización de la invención. Similar al motor de 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. 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 similar a aquellos de la Figura 5. Sin embargo, de acuerdo con una realización, el módulo de división de datos 610 y el módulo de ensamblaje de datos 620 procesan datos de clave criptográfica, a diferencia de los anteriores datos de autenticación de inscripción. Aunque, 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 pueden combinarse con aquellos 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 realización, el módulo de manejo criptográfico 625 puede comprender módulos de software o programas, hardware, o ambos. De acuerdo con otra 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 ventajosamente una infraestructura de clave pública, tal como Privacidad Bastante Buena (PGP), 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, hardware, 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 depositario 700 de acuerdo con aspectos de una realización de la invención. Como se muestra en la Figura 7, el sistema depositario 700 comprende ventajosamente múltiples instalaciones de almacenamiento de datos, por ejemplo, las instalaciones de almacenamiento de datos D1, D2, D3, y D4. Sin embargo, se entiende fácilmente por los expertos en la materia que el sistema depositario puede tener únicamente una instalación de almacenamiento de datos. De acuerdo con una realización de la invención, cada una de las instalaciones de almacenamiento de datos D1 a D4 puede comprender ventajosamente algunos o todos los elementos desvelados con referencia al depositario 210 de la Figura 4. Similar al depositario 210, las instalaciones de almacenamiento de datos D1 a D4 comunican con el motor de transacción 205, el motor de autenticación 215, y el motor criptográfico 220, preferentemente a través de SSL convencional. Enlaces de comunicación que transfieren, por ejemplo, documentos XML. Las comunicaciones desde el motor de transacción 205 pueden incluir ventajosamente solicitudes para datos, en el que la solicitud se difunde ventajosamente 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 solicitudes para datos desde el motor de transacción 205, el sistema depositario 700 reenvía ventajosamente 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 usables. 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 realización, el motor de autenticación 215 y el motor criptográfico 220 pueden emplear ventajosamente 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 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 realización de la invención, el sistema depositario 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 ventajosamente separadas geográficamente, el sistema depositario 700 proporciona redundancia junto con medidas de seguridad adicionales. Por ejemplo, de acuerdo con una 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, puesto que, de acuerdo con una realización, los datos almacenados en cada instalación de almacenamiento de datos están aleatorizados e indescifrables, el compromiso de cualquier instalación de almacenamiento de datos individual no compromete necesariamente los datos sensibles. Además, en la 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.

Aunque el sistema depositario 700 se desvela con referencia a sus realizaciones preferida y alternativa, la invención no pretende 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 depositario 700. Por ejemplo, el sistema depositario 700 puede comprender una, dos o más instalaciones de almacenamiento de datos. Además, los datos sensibles pueden operarse matemáticamente de manera que las porciones desde dos o más instalaciones de almacenamiento de datos son necesarias para reensamblar y descifrar los datos sensibles.

Como se ha mencionado en lo anterior, el motor de autenticación 215 y el motor criptográfico 220 incluyen cada uno un módulo de división de datos 520 y 610, respectivamente, para dividir cualquier tipo o forma de datos sensibles, 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 aspectos de una realización de la invención. Como se muestra en la Figura 8, el proceso de división de datos 800 comienza en la etapa 805 cuando se reciben los datos sensibles “S” mediante el módulo de división de datos del motor de autenticación 215 o el motor criptográfico 220. Preferentemente, en la etapa 810, el módulo de división de datos a continuación genera un número, valor o cadena o conjunto de bits sustancialmente aleatorio, “A.” Por ejemplo, el número aleatorio A puede generarse en un amplio número de diversas técnicas convencionales disponibles para un experto en la materia, para producir números aleatorios de alta calidad adecuados para uso en aplicaciones criptográficas. Además, de acuerdo con una realización, el número aleatorio A comprende una longitud de bits que puede ser cualquier longitud adecuada, tal como más corta, más larga o igual 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 realización preferida, la generación de los números estadísticamente aleatorios A y C puede hacerse ventajosamente en paralelo. El módulo de división de datos a continuación combina los números A y C con los datos sensibles S de manera 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 preferentemente tienen lugar en las etapas 825 y 830, respectivamente, y, de acuerdo con una realización, las combinaciones anteriores también tienen lugar en paralelo. El proceso de división de datos 800 a continuación continúa a la etapa 835 donde los números aleatorios A y C y los números B y D se emparejan de manera que ninguno de los emparejamientos contenga datos suficientes, por sí mismos, para reorganizar y descifrar los datos sensibles originales S. Por ejemplo, los números pueden emparejarse como sigue: AC, AD, BC, y BD. De acuerdo con una realización, cada uno de los emparejamientos anteriores se distribuye a uno de los depositarios D1 a D4 de la Figura 7. De acuerdo con otra realización, cada uno de los emparejamientos anteriores se distribuye aleatoriamente a uno de los depositarios D1 a D4. Por ejemplo, durante un primer proceso de división de datos 800, el emparejamiento AC puede enviarse al depositario 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 puede enviarse al depositario D4, a través de, por ejemplo, una selección aleatoria de la dirección de IP de D4.

Además, los emparejamientos pueden almacenarse todos en un depositario, y pueden almacenarse en localizaciones separadas en dicho depositario.

Basándose en lo anterior, el proceso de división de datos 800 coloca ventajosamente porciones de los datos sensibles en cada una de las cuatro instalaciones de almacenamiento de datos D1 a D4, de manera que ninguna instalación de almacenamiento de datos D1 a D4 única incluya suficientes datos encriptados para recrear los datos sensibles originales S. Como se ha mencionado en lo anterior, tal aleatorización de los datos en porciones encriptadas no usables individualmente 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.

Aunque el proceso de división de datos 800 se desvela con referencia a su realización preferida, la invención no pretende 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 ventajosamente los datos en dos números, por ejemplo, el número aleatorio A y el número B y, distribuir aleatoriamente A y B a través de dos instalaciones de almacenamiento de datos. Además, el proceso de división de datos 800 puede dividir ventajosamente los datos entre un amplio número de instalaciones de almacenamiento de datos a través de la generación de números aleatorios adicionales. Los datos pueden dividirse en cualquier unidad deseada, seleccionada, predeterminada o de tamaño asignado aleatoriamente 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 usable, aumentando de esta manera la seguridad de los datos sensibles. Es fácilmente 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 pueden seleccionarse o predeterminarse para que sean todos del mismo tamaño, un conjunto fijo de diferentes tamaños, una combinación de tamaños o tamaños generados aleatoriamente. De manera similar, las unidades de datos pueden distribuirse en una o más compartimentaciones de acuerdo con un tamaño de unidad de datos fijo o predeterminado, un patrón o combinación de tamaños de unidad de datos, o un tamaño o tamaños de unidad de datos generados aleatoriamente por compartición.

Como se ha mencionado en lo anterior, para recrear los datos sensibles S, las porciones de datos necesitan desaleatorizarse y reorganizarse. Este procedimiento puede tener lugar ventajosamente en los módulos de ensamblaje de datos, 525 y 620, del motor de autenticación 215 y del motor criptográfico 220, respectivamente. El módulo de ensamblaje de datos, por ejemplo, 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 usable. Por ejemplo, de acuerdo con una realización 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 manera 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 ventajosamente 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 usable 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 usables están disponibles únicamente en el motor de autenticación 215. Análogamente, cuando los datos sensibles S incluyen datos de clave criptográfica privada, los datos de clave criptográfica privada no aleatorizados usables están disponibles únicamente en el motor criptográfico 220.

Aunque los procesos de división y ensamblaje de datos se desvelan con referencia a sus realizaciones preferidas, la invención no pretende 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, puede usarse encriptación de clave pública para asegurar adicionalmente los datos en las instalaciones de almacenamiento de datos D1 a D4. Además, es fácilmente evidente para los expertos en la materia que el módulo de división de datos descrito en el presente documento es también una realización separada y distinta de la presente invención que puede incorporarse en, combinarse con o hacerse parte de otra manera de cualquier sistema informático preexistente, paquetes de software, bases de datos o combinaciones de los mismos, u otras realizaciones de la presente invención, tal como el motor de confianza, el motor de autenticación, y el motor de transacción desvelados y descritos en el presente documento.

La Figura 9A ilustra un flujo de datos de un proceso de inscripción 900 de acuerdo con aspectos de una realización de la invención. Como se muestra en la Figura 9A, el proceso de inscripción 900 comienza en la etapa 905 cuando un usuario desea inscribirse con el motor de confianza 110 del sistema criptográfico 100. De acuerdo con esta

realización, el sistema de usuario 105 incluye ventajosamente una miniaplicación del lado 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 realización, los datos de autenticación de inscripción incluyen ID de usuario, contraseña o contraseñas, biométrica o biométricas o similares. De acuerdo con una realización, durante el proceso de consulta, la miniaplicación del lado de cliente comunica preferentemente 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 ventajosamente 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 realización, la transmisión se codifica con la clave pública del motor de autenticación 215.

De acuerdo con una 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 Joe User. Cuando Joe User desea inscribirse como Joe User, Director General de Mega Corp., entonces de acuerdo con esta realización, Joe User 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 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 ventajosamente las dos identidades de Joe User. 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, Joe User el cabeza de familia, Joe User el miembro de Charitable Foundations, y similares. Incluso aunque el usuario pueda tener múltiples identidades, de acuerdo con esta realización, el motor de confianza 110 almacena preferentemente únicamente un conjunto de datos de inscripción. Además, los usuarios pueden ventajosamente añadir, editar/actualizar, o borrar identidades a medida que lo necesiten.

Aunque el proceso de inscripción 900 se desvela con referencia a su realización preferida, la invención no pretende 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) 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 puede inscribirse 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 confiable, tal como un notario digital. Por ejemplo, y el usuario puede aparecer en persona en el tercero confiable, producir credenciales tales como certificado de nacimiento, permiso de conducción, ID de militar o similares, y la parte tercera confiable puede incluir ventajosamente, por ejemplo, su firma digital en la emisión de la inscripción. La parte tercera confiable 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. Como se ha mencionado en lo anterior, 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. Como se ha mencionado en lo anterior, el motor de autenticación 215 puede aleatorizar ventajosamente qué porciones se transfieren a qué depositarios.

A menudo durante el proceso de inscripción 900, el usuario deseará también tener un certificado digital expedido de manera que él o ella pueda recibir documentos encriptados desde otros usuarios fuera del sistema criptográfico 100. Como se ha mencionado en lo anterior, 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 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 realización, el módulo de manejo criptográfico 625 genera un par de claves, 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 realización, una copia de la clave pública. En la etapa 945, el motor criptográfico 220 transmite una solicitud para un certificado digital al motor de transacción 205. De acuerdo con una realización, la solicitud incluye ventajosamente una solicitud normalizada, tal como PKCS10, embebida en, por ejemplo, un documento XML. La solicitud para un certificado digital puede corresponder ventajosamente a 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 ventajosamente 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 manera 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 para el certificado digital típicamente se envía a la autoridad de certificación 115. Sin embargo, 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 ventajosamente el proceso de división de datos 800 anteriormente descrito de manera 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 ventajosamente 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.

Como se desvela en las etapas 935 a 960, una realización de la invención incluye la solicitud para un certificado que se almacena eventualmente en el motor de confianza 110. Puesto que, de acuerdo con una realización, el módulo de manejo criptográfico 625 expide las claves usadas por el motor de confianza 110, cada certificado corresponde a la clave privada. Por lo tanto, el motor de confianza 110 puede proporcionar ventajosamente interoperabilidad a través de la monitorización de los certificados propiedad de, o asociados con un usuario. Por ejemplo, cuando el motor criptográfico 220 recibe una solicitud para 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 asociadas con el mismo, para realizar la función solicitada. Cuando un certificado de este tipo no existe, el módulo de manejo criptográfico 625 puede ventajosamente y de manera 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 aspectos de una realización de la invención, desvela las etapas anteriores para asegurar que el módulo de manejo criptográfico 625 realiza funciones criptográficas usando claves apropiadas.

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

De acuerdo con una 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 pueden implementarse como se desvela 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 puede almacenarse en el depositario 210 o sistema depositario 700. El módulo de manejo criptográfico 625 puede solicitar ventajosamente que se reensamble la clave privada coincidente desde, por ejemplo, el depositario 210, y a continuación en la etapa 976, usar la clave privada coincidente para realizar acciones o funciones criptográficas. Por ejemplo, como se ha mencionado en lo anterior, el módulo de manejo criptográfico 625 puede realizar ventajosamente 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 donde el módulo de manejo criptográfico 625 determina si el usuario posee un certificado de certificación cruzada. De acuerdo con una realización, la certificación cruzada entre autoridades de certificación tiene lugar cuando una primera autoridad de certificación determina confiar 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, pueden “certificarse” 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 ventajosamente qué niveles y qué certificados desde la segunda autoridad de certificación pueden sustituirse para qué niveles y qué certificados desde la primera. Cuando se hace oficialmente 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 realización de la invención, el módulo de manejo criptográfico 625 puede desarrollar ventajosamente certificaciones cruzadas fuera de aquellas 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) 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 aquellos 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, 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 anterior, 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 realización, los requisitos de autenticación anteriores pueden proporcionarse ventajosamente 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, donde el módulo de manejo criptográfico 825 obtiene el certificado desde la autoridad de certificación elegida. De acuerdo con una 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 ventajosamente 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 realización, el módulo de manejo criptográfico 625 puede generar ventajosamente uno o más nuevos pares de claves, y usar las claves públicas que corresponden a los mismos, para solicitar el certificado desde la autoridad de certificación.

De acuerdo con otra realización, el motor de confianza 110 puede incluir ventajosamente uno o más módulos de expedición de certificados que pueden expedir uno o más tipos de certificado. De acuerdo con esta 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 corresponden al 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 desde el usuario. Por ejemplo, el motor de confianza 110 puede solicitar nuevos datos de autenticación de inscripción que comprenden, por ejemplo, datos biométricos. También, 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, tarjeta de seguridad social, tarjeta bancaria, certificado de nacimiento, 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 anterior proceso de interoperabilidad 970, el módulo de manejo criptográfico 625 proporciona ventajosamente 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 anterior 986 del proceso de interoperabilidad 970 puede incluir ventajosamente aspectos de arbitraje confiable, analizados en mayor detalle a continuación, 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), protocolos de estado de certificados en línea (OCSP), o similares.

La Figura 10 ilustra un flujo de datos de un proceso de autenticación 1000 de acuerdo con aspectos de una realización de la invención. De acuerdo con una realización, el proceso de autenticación 1000 incluye recoger datos de autenticación actuales desde un usuario y compararlos a los de los datos de autenticación de inscripción del usuario. Por ejemplo, el proceso de autenticación 1000 comienza en la etapa 1005 donde un usuario desea realizar una transacción con, por ejemplo, un distribuidor. Tales transacciones pueden incluir, por ejemplo, seleccionar una opción de compra, solicitar acceso a un área o dispositivo restringidos del sistema 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 ventajosamente 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 manera que las transacciones imitadas puedan rechazarse por el motor de confianza 110.

La solicitud de autenticación puede incluir ventajosamente qué nivel de autenticación es necesario para una transacción particular. Por ejemplo, el distribuidor puede especificar un nivel particular de confianza que se requiere para la transacción en la expedición. Si la autenticación no puede realizarse en este nivel de confianza, 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 realización, la ID de transacción y la solicitud de autenticación pueden generarse ventajosamente mediante una miniaplicación del lado del distribuidor u otro programa de software. 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, desde el 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 preferentemente documentos XML encriptados con al menos tecnología de ½ SSL convencional. En la etapa 1020, el motor de transacción 205 recibe la transmisión, reconoce preferentemente 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 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, aunque la identificación de distribuidor puede comunicarse también a través de una porción no aleatoria de la ID de transacción. En la 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 depositario 700 transfiere las porciones de los datos de autenticación de inscripción que corresponden al usuario al motor de autenticación 215. En la etapa 1045, el motor de autenticación 215 desencripta la transmisión usando su clave privada y compara los datos de autenticación de inscripción a los datos de autenticación actuales proporcionados por el usuario.

La comparación de la etapa 1045 puede aplicar ventajosamente autenticación sensible a contexto heurística, como se ha hecho referencia en lo anterior, 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 realizaciones 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 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 realización, se pasa un mensaje de confirmación al usuario.

Basándose en lo anterior, el proceso de autenticación 1000 mantiene ventajosamente 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 o ella produjeron datos de autenticación válidos.

Aunque el proceso de autenticación 1000 se desvela con referencia a sus realizaciones preferida y alternativa, la invención no pretende 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 puede sustituirse ventajosamente por casi cualquier aplicación solicitante, incluso aquellas 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) o una API criptográfica (CAPI) 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 todos hacer las solicitudes de autenticación que pueden rellenarse mediante el proceso de autenticación 1000. De hecho, después de proporcionar el proceso de autenticación confiable anterior 1000, 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. Como se ha mencionado en lo anterior, 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 puede emplearse ventajosamente para desarrollar soluciones de inicio de sesión únicas elegantes, tales como, desbloquear una bóveda de datos sensibles. Por ejemplo, la autenticación satisfactoria o positiva puede proporcionar al usuario autenticado la capacidad para acceder automáticamente a cualquier número de contraseñas para un número casi ilimitado de sistemas y aplicaciones. Por ejemplo, la autenticación de un usuario puede proporcionar al usuario acceder a contraseña, inicio de sesión, credenciales financieras, o similares, 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 una bóveda de datos sensibles, los usuarios pueden elegir contraseñas verdaderamente grandes y aleatorias puesto 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 asociado con un dato memorable, nombre, etc.

De acuerdo con una realización, una bóveda de datos sensibles asociada con un usuario dado puede almacenarse ventajosamente en las instalaciones de almacenamiento de datos del depositario 210, o dividirse y almacenarse en el sistema depositario 700. De acuerdo con esta 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 realización, el motor de confianza 110 puede incluir un sistema separado para almacenar la bóveda de datos sensibles. Por ejemplo, el motor de confianza 110 puede incluir un motor de

software independiente que implementa la funcionalidad de la bóveda 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 realización, el motor de software sirve los datos sensibles solicitados después de que el motor de software recibe una señal que indica autenticación de usuario positiva desde el motor de confianza 110.

En otra realización más, la bóveda de datos puede implementarse por un sistema de terceros. Similar a la realización del motor de software, el sistema de terceros puede servir ventajosamente 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 realización más, la bóveda de datos puede implementarse en el sistema de usuario 105. Un motor de software del lado del usuario puede servir ventajosamente los datos anteriores después de recibir una señal que indica autenticación de usuario positiva desde el motor de confianza 110.

Aunque las bóvedas de datos anteriores se desvelan con referencia a realizaciones 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, una bóveda de datos particular puede incluir aspectos de algunas o todas las realizaciones anteriores. Además, cualquiera de las bóvedas de datos anteriores puede emplear una o más solicitudes de autenticación a tiempos variables. Por ejemplo, cualquiera de las bóvedas de datos puede requerir autenticación de cada una o más transacciones, periódicamente, 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 aspectos de una realización de la invención. Como se muestra en la Figura 11, el proceso de firma 1100 incluye etapas similares a aquellas del proceso de autenticación 1000 descrito en lo anterior con referencia a la Figura 10. De acuerdo con una realización de la invención, el proceso de firma 1100 autentica en primer lugar al usuario y a continuación realiza una o más de varias funciones de firma digital como se analizará en mayor detalle a continuación. De acuerdo con otra realización, el proceso de firma 1100 puede almacenar ventajosamente datos relacionados con el mismo, tales como troceos de mensajes o documentos, o similares. Estos datos pueden usarse ventajosamente en una auditoria o cualquier otro evento, tal como por ejemplo, cuando una parte participante intenta rechazar una transacción.

Como se muestra en la Figura 11, durante las etapas de autenticación, el usuario y distribuidor pueden ventajosamente ponerse de acuerdo en un mensaje, tal como, por ejemplo, un contrato. Durante la firma, el proceso de firma 1100 asegura ventajosamente que el contrato firmado por el usuario es idéntico al contrato suministrado por el distribuidor. Por lo tanto, de acuerdo con una 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 ventajosamente una cantidad significativamente reducida de datos, proporcionando un sistema criptográfico más eficaz y rentable. Además, el troceo almacenado puede compararse ventajosamente a 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 puede usarse 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 a 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 al troceo del mensaje suministrado por el usuario. Por tanto, el motor de autenticación 215 asegura ventajosamente 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 realización de la invención, la solicitud incluye un troceo del mensaje o contrato. Sin embargo, un experto en la materia reconocerá a partir de la 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 preferentemente un documento XML 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 manera que cada una de las instalaciones de almacenamiento de datos D1 a D4 transmite su respectiva porción de la clave o claves criptográficas que corresponden a una parte firmante. De acuerdo con otra realización, el motor criptográfico 220 emplea alguna o todas las etapas del proceso de interoperabilidad 970 analizado en lo anterior, de manera que el motor criptográfico 220 determina en primer lugar la clave o claves apropiadas a solicitar desde el depositario 210 o el sistema depositario 700 para la parte firmante, y toma acciones para proporcionar claves coincidentes apropiadas. De acuerdo con otra realización más, el motor de autenticación 215 o el motor criptográfico 220 pueden solicitar ventajosamente una o más de las claves asociadas con la parte firmante y almacenadas en el depositario 210 o el sistema depositario 700.

De acuerdo con una realización, la parte firmante incluye uno o ambos del usuario y el distribuidor. En tal caso, el motor de autenticación 215 solicita ventajosamente las claves criptográficas que corresponden al usuario y/o al distribuidor. De acuerdo con otra realización, la parte firmante incluye el motor de confianza 110. En esta realización, el motor de confianza 110 está certificando que el proceso de autenticación 1000 autenticó apropiadamente al usuario, distribuidor o 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 realización, el motor de confianza 110 realiza una función similar a un notario digital. En esta 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 apropiadamente. En esta realización, el motor de autenticación 215 puede solicitar ventajosamente ensamblaje de las claves criptográficas que corresponden al usuario, el distribuidor, o ambos. De acuerdo con otra realización, el motor de autenticación 215 puede solicitar ventajosamente ensamblaje de las claves criptográficas que corresponden al motor de confianza 110.

De acuerdo con otra realización, el motor de confianza 110 realiza funciones similares a un poder legal. Por ejemplo, el motor de confianza 110 puede firmar digitalmente el mensaje en nombre de un tercero. En tal caso, el motor de autenticación 215 solicita las claves criptográficas asociadas con el tercero. De acuerdo con esta realización, el proceso de firma 1100 puede incluir ventajosamente 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 puede usarse una firma de terceros particular.

Basándose en lo anterior, en la etapa 1110, el motor de autenticación solicita las claves criptográficas desde las instalaciones de almacenamiento de datos D1 a D4 que corresponden a la parte firmante. En la etapa 1115, las instalaciones de almacenamiento de datos D1 a D4 transmiten sus respectivas porciones de la clave criptográfica que corresponden a la parte firmante al motor criptográfico 220. De acuerdo con una realización, las transmisiones anteriores incluyen tecnologías de SSL. De acuerdo con otra realización, las transmisiones anteriores pueden súper-encriptarse ventajosamente 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 realización, la transmisión anterior puede incluir ventajosamente 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 realización, el motor de transacción 205 transmite también un mensaje de confirmación al usuario. Aunque el proceso de firma 1100 se desvela con referencia a sus realizaciones preferida y alternativa, la invención no pretende 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 puede sustituirse con una aplicación de usuario, tal como una aplicación de correo electrónico. Por ejemplo, el usuario puede desear firmar digitalmente un correo electrónico particular con su firma digital. En una realización de este tipo, la transmisión a lo largo de todo el proceso de firma 1100 puede incluir ventajosamente 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 sistemas restringidos 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 ventajosamente 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 aspectos de una realización de la invención. 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 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. Sin embargo, en sistemas criptográficos de clave simétrica, o sistemas donde el emisor y 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 anterior, 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 ventajosamente que se ha encriptado una clave síncrona con la clave pública del usuario. Por tanto, como se ha mencionado en lo anterior, 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 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 distribuidor solicitante. A continuación, de acuerdo con una realización, la aplicación o distribuidor solicitante usa la clave de sesión para desencriptar el mensaje encriptado.

Aunque el proceso de desencriptación 1200 se desvela con referencia a sus realizaciones 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 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 ventajosamente 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 distribuidor solicitante puede transmitir ventajosamente al motor de transacción 205 del motor de confianza 110, una solicitud para la clave pública del usuario. La aplicación o distribuidor solicitante realiza esta solicitud puesto que la aplicación o 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. 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 corresponde al usuario, al motor de transacción 205. En la etapa 1250, el motor de transacción 205 transmite el certificado digital a la aplicación o distribuidor solicitante. De acuerdo con una 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 ventajosamente 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 confiable 1300 de acuerdo con aspectos de otra realización más de la invención. 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, respectivamente. Para facilitar un entendimiento más completo de la invención, la Figura 13 ilustra cada motor de confianza, 1305, 1310, 1315, y 1320 como que tiene un motor de transacción, un depositario, y un motor de autenticación. Sin embargo, un experto en la materia reconocerá que cada motor de transacción puede comprender ventajosamente alguno, una combinación, o todos los elementos y canales de comunicación desvelados con

referencia a las Figuras 1-8. Por ejemplo, una realización puede incluir ventajosamente motores de confianza que tienen uno o más motores de transacciones, depositarios y servidores criptográficos o cualquier combinación de los mismos.

De acuerdo con una realización de la invención, cada uno de los motores de confianza 1305, 1310, 1315 y 1320 están geográficamente separados, de manera 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 ventajosamente el tiempo de respuesta del sistema mientras 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. 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 a los datos de autenticación de inscripción del usuario. Por lo tanto, de acuerdo con un ejemplo, el usuario proporciona ventajosamente 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 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 depositarios de, por ejemplo, cada uno de los motores de confianza, 1305 a 1320. De acuerdo con esta realización, cada depositario 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 depositarios para responder, y ensambla los datos de autenticación de inscripción en forma descifrada. El motor de autenticación 1322 compara los datos de autenticación de inscripción con los datos de autenticación actuales y devuelve un resultado de autenticación al motor de transacción 1321 del motor de confianza 1305.

Basándose en lo anterior, el sistema de motor de confianza 1300 emplea el más cercano de una pluralidad de motores de confianza geográficamente separados, 1305 a 1320, para realizar el proceso de autenticación. De acuerdo con una realización de la invención, el encaminamiento de la información al motor de transacción más cercano puede realizarse ventajosamente en miniaplicaciones del lado de cliente que se ejecutan en uno o más del sistema de usuario 105, sistema distribuidor 120, o autoridad de certificación 115. De acuerdo con una realización alternativa, puede emplearse un proceso de decisión más sofisticado para seleccionar desde los motores de confianza 1305 a 1320. Por ejemplo, la decisión puede basarse 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 mientras mantiene las ventajas de seguridad asociadas con las instalaciones de almacenamiento de datos geográficamente remotas, tales como aquellas analizadas con referencia a la Figura 7 donde cada instalación de almacenamiento de datos almacena porciones aleatorizadas de datos sensibles. Por ejemplo, un compromiso de seguridad en, por ejemplo, el depositario 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 depositario 1325 contiene únicamente datos aleatorizados no descifrables que, sin más, son completamente inútiles.

De acuerdo con otra realización, el sistema de motor de confianza 1300 puede incluir ventajosamente múltiples motores criptográficos dispuestos similares a los motores de autenticación. Los motores criptográficos pueden realizar ventajosamente funciones criptográficas tales como aquellas desveladas con referencia a las Figuras 1-8. De acuerdo con otra realización más, el sistema de motor de confianza 1300 puede sustituir ventajosamente los múltiples motores de autenticación con múltiples motores criptográficos, realizando de esta manera funciones criptográficas tales como las desveladas con referencia a las Figuras 1-8. De acuerdo con otra 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, como se ha desvelado en lo anterior.

Aunque el sistema de motor de confianza 1300 se desvela con referencia a sus realizaciones 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 depositarios, uno o más motores de autenticación, o uno o más motores criptográficos o combinaciones de los mismos.

La Figura 14 ilustra un diagrama de bloques simplificado de un sistema de motor de confianza 1400 de acuerdo con aspectos de otra realización más de la invención. Como se muestra en la Figura 14, el sistema de motor de confianza 1400 incluye múltiples motores de confianza 1405, 1410, 1415 y 1420. De acuerdo con una realización, cada uno de los motores de confianza 1405, 1410, 1415 y 1420, comprende alguno o todos los elementos del motor de confianza 110 desvelado con referencia a las Figuras 1-8. De acuerdo con esta realización, cuando las miniaplicaciones del lado del cliente del sistema de usuario 105, del sistema 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 desvelado 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 depositarios 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 depositarios a continuación comunica 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 depositarios de cada uno de los motores de confianza 1405 a 1420. De acuerdo con esta 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 desde el 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 análogamente el resultado de los motores de autenticación desde 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 desde tres motores de autenticación y transmitir ese resultado al motor de transacción del cuarto motor de confianza. El comparador compara el resultado de autenticación desde 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 corresponde al motor de confianza no asociado con los tres motores de autenticación.

Basándose en lo anterior, el módulo de redundancia determina un resultado de autenticación desde los datos recibidos desde los motores de autenticación que están preferentemente geográficamente remotos del motor de confianza de el 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 puede aplicarse también al motor criptográfico de cada uno de los motores de confianza 1405 a 1420. Sin embargo, 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 uso en la presente invención.

De acuerdo con otra realización más de la invención, el sistema de motor de confianza 1400 puede emplear ventajosamente 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 puede implementarse ventajosamente durante una comparación de troceo de documentos proporcionados mediante una o más partes durante una transacción particular.

Aunque la invención anterior se ha descrito en términos de ciertas realizaciones preferidas y alternativas, serán evidentes otras realizaciones 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, 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 puede establecerse para expirar después de una cantidad de tiempo predeterminada Por tanto, el motor de confianza 110 puede liberar una clave privada a un usuario donde la clave privada fuera válida durante, por ejemplo, 24 horas. De acuerdo con una realización de este tipo, el motor de confianza 110 puede expedir ventajosamente 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 realización, tal reconocimiento puede

provenir de datos suministrados en la solicitud para un servicio particular, tal como, una solicitud para autenticación que conduce a acceso o uso, una solicitud para funcionalidad criptográfica, o similares. De acuerdo con una 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 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 anteriormente descrito, puede proporcionarse autenticación sensible al contexto usando técnicas como se describirán a continuación. La autenticación sensible al contexto, por ejemplo 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 motor de confianza 110, como se describirá a continuación.

Como se ha analizado anteriormente, la autenticación son los procesos de probar que un usuario es quien él dice ser. 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 debe autenticarse a sí mismo. El usuario debe demostrar al motor de confianza 110 que él 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.

Como se usa en el presente documento, “autenticación” hará referencia ampliamente 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 una pieza particular de conocimiento, testigo físico o lectura biométrica. “Datos de autenticación” se refieren a 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 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 depositario 210 y comparar los datos de autenticación proporcionados por el mismo usuario. Una 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 depositario 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 asociados con cada instancia de autenticación individual en la etapa 1605. Esto es necesario de 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 deberían compararse 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 podrá autenticarse 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; sin embargo, en ciertas circunstancias puede usarse 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 captura 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, como se conoce por los expertos en la materia, que puede determinarse 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 puede determinarse 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 hardware 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.

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 pueden agruparse como factores relacionados con la fiabilidad 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 asociados con esa instancia de autenticación. Cada uno de estos factores puede variar independientemente 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 puesto 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 puesto que el conocimiento puede transferirse 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, puesto que no hay garantía de que la persona correcta esté en posesión del testigo apropiado.

Sin embargo, las técnicas biométricas son intrínsecamente más fiables puesto que es en general más difícil de proporcionar a otra persona con la capacidad de usar tus huellas digitales de una manera conveniente, incluso intencionadamente. Puesto 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. Sin embargo, incluso las técnicas biométricas pueden tener algunas ocasiones en las que se genera una falsa aceptación o un falso rechazo. Estas ocurrencias pueden reflejarse 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 puesto 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 puede expresarse de diferentes maneras. La fiabilidad se expresa de manera deseable en alguna métrica que pueda usarse 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, puede asignarse a las huellas digitales una fiabilidad intrínseca del 97 %, mientras que puede asignarse a las contraseñas únicamente una fiabilidad intrínseca del 50 %. Los expertos en la materia reconocerán que estos valores particulares son meramente ejemplares y pueden variar entre implementaciones específicas.

El segundo factor para el que debe evaluarse la fiabilidad es la fiabilidad de la inscripción. Esto es parte del proceso de “inscripción gradual” anteriormente mencionado. 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 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 confiable para el operador del motor de confianza 110; inscripción anónima o pseudónima 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 puede considerarse extremadamente fiable para fines en la compañía, pero puede confiarse 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 confiables proporcionados durante una inscripción anterior con el mismo motor de confianza 110 pueden considerarse tan fiables como eran los datos de inscripción original, incluso aunque 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 asociado con los datos de inscripción originales. De esta manera por ejemplo, una inscripción anónima o seudónima puede a continuación elevarse a una inscripción completa demostrando alguna inscripción oficial de la identidad del individuo que coincide con los datos inscritos.

Los factores de fiabilidad anteriormente analizados son generalmente valores que pueden determinarse con antelación de cualquier instancia de autenticación particular. Esto es puesto que están basados en la inscripción y en la técnica, en lugar de en la autenticación real. En una 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 realización ventajosa de la presente invención, tales fiabilidades pueden incluirse con los propios datos de inscripción. De esta manera, estos factores se entregan automáticamente al motor de autenticación 215 junto con los datos de inscripción enviados desde el depositario 210.

Aunque estos factores pueden determinarse 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. Adicionalmente, aunque 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 asociados con unos únicos datos de instancia específica pueden variar en cada ocasión. Estos factores, como se analizarán a continuación, deben evaluarse 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 satisfactoriamente, y la autenticación falla. La manera en la que esto se evalúa puede cambiar dependiendo de la técnica de autenticación usada. La comparación de tales datos se realiza mediante la función del comparador 515 del motor de autenticación 215 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 típicamente 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.

Sin embargo, ciertos tipos de datos de autenticación, tales como cuestionarios y biométricas, generalmente no son autenticadores binarios. Por ejemplo, una huella digital puede coincidir con una huella digital de referencia a grados variables. Hasta cierto punto, esto puede deberse a variaciones en la calidad de los datos capturados 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 puesto 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). Finalmente, en situaciones 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 puede asignarse de manera deseable un valor de coincidencia parcial mediante el comparador 515. De esta manera, la huella digital puede decirse que es un 85 % de coincidencia, la huella vocal un 65 % de coincidencia y el cuestionario 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. Sin embargo, como se ha analizado anteriormente, esto es únicamente uno de los factores que pueden usarse al determinar la fiabilidad de una instancia de autenticación dada. Obsérvese también que incluso aunque pueda determinarse 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 (100 %) o fallidas (0 %), basándose en si el grado de coincidencia pasa o no un nivel de coincidencia umbral particular. Un proceso de este tipo puede usarse para proporcionar un nivel de paso/fallo sencillo de coincidencia para sistemas que podría producir de otra manera coincidencias parciales.

Otro factor a 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. Como se ha analizado anteriormente, las circunstancias se refieren a los metadatos asociados con una instancia de autenticación particular. Esto puede incluir sin limitación información tal como: la dirección de red del autenticador, hasta el punto de que puede determinarse; 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 pueden usarse para producir un perfil del tipo de autenticación que se solicita normalmente por el usuario. A continuación, esta información puede usarse 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 desde una dirección de red durante su 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 puesto 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 pueden usarse 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 pueda ponerse en el sistema que se está usando por un usuario cuando interactúa con un sistema 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 puede leerse mediante un explorador web u otro software en el sistema de usuario. Si estos datos se permite que residan en el sistema de usuario entre sesiones (una “cookie persistente”), pueden enviarse 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, particularmente 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 como se ha descrito anteriormente en las etapas 1610 y 1615 respectivamente, se usan para producir una fiabilidad global para la instancia de autenticación proporcionada en la etapa 1620. Un medio para hacer esto es simplemente expresar cada fiabilidad como un porcentaje y 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 (100 %), y la técnica que se está usando es identificación por huella digital (97 %), y los datos de huella digital iniciales se registraron a través del empleador del usuario con el motor de confianza 110 (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 (99 %). La fiabilidad global de esta instancia de autenticación podría calcularse 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 puede calcularse también usando técnicas que tratan los diferentes factores de fiabilidad de manera diferente, por ejemplo usando fórmulas donde se asignan diferentes pesos a cada factor de fiabilidad. Adicionalmente, los expertos en la materia reconocerán que los valores reales usados pueden representar valores distintos de porcentajes y pueden usar sistemas no aritméticos. Una realización puede incluir un módulo usado mediante un solicitante de la autenticación para establecer los pesos para cada factor y los algoritmos usados al establecer la fiabilidad global de la instancia de autenticación.

El motor de autenticación 215 puede usar las técnicas anteriores y variaciones de las mismas para determinar la fiabilidad de una única instancia de autenticación, indicada como la etapa 1620. Sin embargo, 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 como se muestra en la etapa 1630 y se evaluará como se ha descrito anteriormente en las etapas 1610, 1615 y 1620.

Obsérvese que muchos de los factores de fiabilidad analizados pueden variar de una de estas instancias a otra. Por ejemplo, la fiabilidad 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. Adicionalmente, 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. Finalmente, incluso aunque 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 pueden asignarse 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. Sin embargo, 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 puede modelarse 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 anteriormente descritas (huella digital, tarjeta inteligente, contraseña) producirán fiabilidades de 86 %, 75 %, y 72 % que corresponderían a no fiabilidades de (100-86) %, (100-75) % y (100-72) %, o 14 %, 25 %, y 28 %, respectivamente. Multiplicando estas no fiabilidades, obtenemos una no fiabilidad acumulada de 14 % * 25 % * 28 % - .98 % no fiabilidad, que corresponde a una fiabilidad del 99,02 %.

En un modo adicional de operación, pueden aplicarse 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.

Sin embargo, 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).

Adicionalmente, 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 usados 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 asociada con las circunstancias que rodean los eventos de autenticación. Esta disposición podría usarse para facilitar la carga sobre los usuarios durante horas de operación normal, no requiriendo más del usuario que él inicie sesión en la máquina correcta durante las horas laborales. Sin embargo, 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 pueden definirse 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 podrían establecerse 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 anteriormente descrito es meramente ejemplar, 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 puede desearse una diversidad de combinación de etapas. Adicionalmente, ciertas etapas, tales como la evaluación de la fiabilidad de cada instancia de autenticación proporcionada, pueden llevarse 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 anteriormente descrito falla al cumplir 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 como se ha descrito anteriormente con referencia a las Figuras 10 y 11. Como se muestra en ellas, 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 desde el 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.

Sin embargo, es posible también que el distribuidor pueda solicitar un nivel particular de confianza para completar una transacción particular. Este nivel requerido puede incluirse con la solicitud de autenticación (por ejemplo autenticar este usuario al 98 % de confianza) o puede determinarse mediante el motor de confianza 110 basándose en otros factores 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, puede requerirse un grado más alto de confianza. De manera similar, para transacciones con grados altos de riesgo puede requerirse un alto grado de confianza. A la inversa, para transacciones que son de bajo riesgo o de bajo valor, pueden requerirse 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 como se muestra en la Figura 17. En circunstancias 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 como se ha analizado anteriormente con referencia a la Figura 10, etiquetando cualquier diferencia como una autenticación negativa.

Como se muestra en la Figura 17, la primera etapa después de recibir los datos en la etapa 1050 es para que el motor de transacción 205 determine el nivel de confianza que se requiere para una autenticación positiva para esta transacción particular en la etapa 1710. Esta etapa puede realizarse mediante uno de varios modos diferentes. El nivel de confianza requerido puede especificarse 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 depositario 210 u otro almacenamiento que es accesible mediante el motor de transacción 205. Esta preferencia puede leerse a continuación y usarse cada vez que se realiza una solicitud de autenticación mediante este solicitante de la autenticación. La preferencia puede asociarse también con un usuario particular y una medida de seguridad de manera que se requiera siempre un nivel de confianza particular para autenticar a ese usuario, almacenándose la preferencia de usuario en el depositario 210 u otro medio de almacenamiento accesible mediante el motor de transacción 205. El nivel requerido puede obtenerse 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 software 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 puede usarse 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 apropiadamente el nivel requerido de confianza para transacciones indiciadas con el servidor web del distribuidor.

De esta manera, las solicitudes de transacción desde los usuarios pueden asignarse a un nivel de confianza requerido de acuerdo con las políticas del distribuidor y tal información puede reenviarse 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 que el individuo que se está autenticando es de hecho quien él se identifica como él mismo. Por ejemplo, si la transacción es una donde el distribuidor desea bastante grado de certeza puesto que se están cambiando bienes de manos, el distribuidor puede requerir un nivel de confianza del 85 %. Para la situación 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. Sin embargo, 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 debe autenticarse 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.

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 al nivel de confianza de autenticación que el motor de autenticación 215 calculó para la autenticación actual (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 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 como se muestra en la etapa 1055 (véase la Figura 10).

Sin embargo, 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 como se describe a continuación tiene lugar en el motor de transacción 205 del motor de confianza 110. Puesto 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 puede realizarse fuera del motor de autenticación 215. Sin embargo, 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 podría estructurarse como alternativa para tener lugar parcial o completamente en el propio motor de autenticación 215.

Como se ha mencionado anteriormente, el arbitraje de confianza es un proceso 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. 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 puede determinarse basándose en las circunstancias de la autenticación, por ejemplo si esta autenticación ya ha sido a través de múltiples ciclos de arbitraje, así como sobre las preferencias de cualquiera del distribuidor o usuario, como se analizará adicionalmente a continuación.

En tales circunstancias donde el arbitraje no es posible, el proceso continúa a la etapa 1810 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 puede usarse ventajosamente para evitar que las autenticaciones estén pendientes indefinidamente 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 distribuidor. Pueden ponerse también limitaciones tras el número de intentos que pueden realizarse al proporcionar una autenticación satisfactoria. Tales limitaciones pueden manejarse mediante un limitador de intentos 535 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 como se muestra en la etapa 1820. En la forma más sencilla, esto puede indicar simplemente que la autenticación fue insuficiente. Puede enviarse 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 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 confiable) y el usuario, por ejemplo, mediante llamada de teléfono. Esta llamada de teléfono u otra autenticación no informática puede usarse 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 aunque no se puedan proporcionar datos de autenticación adicionales, el contexto adicional 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 uso en consideración de la solicitud de autenticación.

Adicionalmente, 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 más confiable. 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 puede aún autenticarse satisfactoriamente a un muy alto nivel como puede requerirse mediante el distribuidor, incluso aunque él 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 él dice que es.

Sin embargo, puesto que el motor de confianza 110 está potenciando artificialmente el nivel de confianza proporcionado por el usuario, hay un riesgo superior para el operador del motor de confianza 110, puesto 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 eficazmente las autenticaciones del usuario). El usuario paga al operador del motor

de confianza 110 para tomar el riesgo de autenticar a un nivel superior de confianza que el que realmente se ha proporcionado.

Puesto que un sistema de cobertura de este tipo permite a alguien comprar efectivamente 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 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 debe permitirse. 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 donde el nivel de confianza de autenticación sin la cobertura sea superior a un cierto límite. Esto puede usarse 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 pueden evaluarse 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 actualmente 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 puesto 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 generalmente 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.

Sin embargo, 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, puesto que la llamada de teléfono proporciona efectivamente 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; sin embargo, 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, puede generarse una autenticación positiva en el motor de transacción 205 en la etapa 1740 (véase la Figura 17). Si no, puede intentarse arbitraje adicional como se ha analizado anteriormente 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 descrito anteriormente para la cobertura del lado del usuario. En este punto, sin embargo, en lugar del coste que corresponde al riesgo que se está tomando por el motor de confianza 110 al autenticar por encima del nivel de confianza de autenticación real producido, el coste de la cobertura corresponde al riesgo que se está tomando 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 así mismo del riesgo adicional asociado con un nivel inferior de confianza en la autenticación del usuario. Como se ha descrito anteriormente, puede ser ventajoso para el distribuidor considerar únicamente comprar tal cobertura para cubrir el hueco de confianza en condiciones 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 eficazmente su requisito de nivel de confianza alto: puesto 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 como se ha descrito anteriormente.

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 pueden manejarse 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, puede cobrarse 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 efectivamente 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, pueden enviarse nuevos mensajes al usuario y distribuidor, y el proceso puede repetirse 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 debe satisfacerse para generar una autenticación positiva. Sin embargo, 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 anteriormente descrito y mostrado en las Figuras 16-18 puede llevarse a cabo usando diversos modos de comunicación como se ha descrito anteriormente 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 distribuidor que facilitan tales transacciones de arbitraje y cobertura. En otro modo de operación alternativo, pueden usarse operaciones de correo electrónico seguras para mediar el arbitraje anteriormente descrito, permitiendo de esta manera evaluaciones diferidas y procesamiento en lotes de las autenticaciones. Los expertos en la materia reconocerán que pueden usarse 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 como se ha descrito anteriormente. Este ejemplo ilustra el proceso global entre un usuario y un distribuidor según median mediante el motor de confianza 110. Aunque las diversas etapas y componentes como se han descrito en detalle anteriormente pueden usarse para llevar a cabo la siguiente transacción, el proceso ilustrado se centra en la interacción entre el motor de confianza 110, el usuario y el 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 para una firma al motor de confianza 110 en la etapa 1905. El usuario proporcionará también datos de autenticación que se usarán como se ha descrito anteriormente 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 como se ha analizado anteriormente, 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 para 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 digitalmente el contrato por ambas partes, el distribuidor incluye también datos de autenticación por sí mismo de modo que la firma del distribuidor en el contrato pueda verificarse más tarde si fuera necesario.

Como se ha analizado anteriormente, 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 desde el 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. Puede realizarse el arbitraje de confianza en este punto si fuera necesario, como se ha descrito anteriormente, para que el distribuidor se autentique satisfactoriamente 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 como se describe a continuación. Como se ha analizado anteriormente con referencia a las Figuras 17 y 18, puede realizarse 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) 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 anteriormente descrito. 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) 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 típico, está disponible un número de API para los programadores. Cada API proporciona un conjunto de llamadas de función que pueden realizarse 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) 2010 proporcionada por Microsoft con sus sistemas operativos Windows, y la Arquitectura Común de Seguridad de Datos (CDSA), patrocinada por IBM, Intel y otros miembros del Grupo Abierto. CAPI se usará como una API de seguridad ejemplar en el análisis que sigue. Sin embargo, el SPM criptográfico descrito podría usarse con CDSA u otra API de seguridad como se conoce en la técnica.

Esta API se usa mediante un sistema de usuario 105 o sistema distribuidor 120 cuando se realiza una llamada para una función criptográfica. Incluidas entre estas funciones pueden estar solicitudes 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 como se describen en el presente documento o se conocen por los expertos en la materia.

Tales funciones criptográficas se realizan normalmente localmente 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 software 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) 2015, 2020 como se ha hecho referencia anteriormente que proporcionan recursos con los que se llevan a cabo las funciones criptográficas. Tales SPM pueden incluir las bibliotecas de software 2015 para realizar operaciones de encriptación o desencriptación, o controladores y aplicaciones 2020 que pueden acceder a hardware especializado 2025, tal como dispositivos de exploración biométricos. Así como CAPI 2010 proporciona funciones que pueden usarse mediante una aplicación

2000 del sistema 105, los SPM 2015, 2020 proporcionan CAPI con acceso a las funciones y recursos de nivel inferior 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 realizaciones 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 como se describe en el presente documento podría enviar solicitudes de operaciones criptográficas a una red localizada remotamente accesible 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 ella 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. Sin embargo, estas funciones se ponen a disposición de manera eficaz para un sistema de usuario 105 a través de CAPI 2010 de manera que parecen estar localmente disponibles en el propio sistema de usuario 105. Sin embargo, 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 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 como serán evidentes para los expertos en la materia.

En una 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 realización comprende un módulo de división de datos que comprende la funcionalidad mostrada en la Figura 8 y descrita en este punto. En una 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 software analizador que comprende funcionalidad de división de datos, encriptación y desencriptación, reconstitución o reensamblaje. Esta 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 software 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 puede diseñarse, en una realización, de una manera en niveles modulares, y cualquier proceso de encriptación es adecuado para 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 criptográficamente, almacenada dispersada y de manera segura en múltiples localizaciones; 3) encriptar, dividir criptográficamente, encriptar cada compartición, a continuación almacenada dispersada y de manera segura en múltiples localizaciones; y 4) encriptar, dividir criptográficamente, 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 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 usada 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 realización, preferentemente 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 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 como se describe en esta 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 realización puede incluirse en el conjunto de software, o en otra realización puede integrase en una infraestructura existente o cualquier otra localización deseada.

Una división criptográfica (criptodivisión) particiona los datos en N número de comparticiones. El particionamiento 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 aleatoriamente. Las unidades pueden estar también con diferente tamaño, basándose en cualquiera de un conjunto de valores aleatorios o predeterminados. Esto significa que los datos pueden observarse 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 aleatoriamente. Las unidades a continuación se distribuyen (aleatoriamente o mediante un conjunto de valores predeterminado) en las N comparticiones. Esta distribución podría implicar también un mezclado del orden de las unidades en las comparticiones. Es fácilmente evidente para los expertos en la materia que la distribución de las unidades de datos en las comparticiones puede realizarse 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 aleatoriamente.

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 comparticiones seleccionado para que sea 4. Cada byte se distribuiría en una de las 4 comparticiones. 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 corresponde a las cuatro comparticiones. 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 corresponden a una de las cuatro comparticiones. La distribución de los bytes de datos en las cuatro comparticiones 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 byte de orden 23 de datos en la compartición r23. Es fácilmente evidente para los expertos en la materia que puede usarse 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, podría realizarse la operación inversa.

En otra realización del proceso de criptodivisión de la presente invención, una opción para el proceso de criptodivisión es proporcionar suficiente redundancia en las comparticiones de manera que únicamente sea necesario un subconjunto de las comparticiones para reensamblar o restaurar los datos a su forma original o usable. Como un ejemplo no limitante, la criptodivisión puede hacerse como una criptodivisión “3 de 4” de manera que únicamente tres de las cuatro comparticiones sean necesarias para reensamblar o restaurar los datos a su forma original o usable. Esto se denomina también como una “criptodivisión M de N” en el que N es el número total de comparticiones, y M es al menos uno menor que N. Es fácilmente 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 realización del proceso de la criptodivisión de la presente invención, cada unidad de los datos se almacena en dos comparticiones, la primera compartición y la compartición de reserva. Usando el proceso de criptodivisión de “3 de 4” anteriormente descrito, una compartición cualquiera puede perderse, y esto es suficiente para reensamblar o restaurar los datos originales sin unidades de datos perdidos puesto que únicamente se requieren tres de las cuatro comparticiones totales. Como se describe en el presente documento, se genera un número aleatorio que corresponde a una de las comparticiones. 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 realización, para generar el número aleatorio de compartición principal y de reserva. 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, puede generarse 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 realización anteriormente descrita 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 comparticiones diferentes. Es fácilmente evidente para los expertos en la materia que puede haber muchas maneras de realizar

criptodivisión redundante y criptodivisión no redundante además de las realizaciones desveladas en el presente documento. Por ejemplo, las unidades de datos en cada compartición podrían mezclarse utilizando un algoritmo diferente. Este mezclado de unidad de datos puede realizarse 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 descritos en el presente documento, y todas las otras realizaciones de la criptodivisión y métodos de mezclado de datos de la presente invención pueden realizarse 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 realización de código fuente que podría realizar el proceso de criptodivisión descrito en el presente documento es:

DATA [1:24] - serie de bytes con los datos 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 realización de código fuente que realizaría el proceso de RAID de criptodivisión descrito 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[compartiónprincipal[1]] y compartición[(copmartiónprincipal[1]+compartición_de_reserva[1]) mod 4, con el mismo proceso como en la criptodivisión anteriormente descrita. Este método será escalable a cualquier tamaño de N, donde únicamente son necesarias N-1 comparticiones para restaurar los datos.

La recuperación, recombinación, reensamblaje o 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 pueden integrarse 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 usadas para encriptar los datos y presentarlos no usables sin la clave. Los datos, sin embargo, permanecen enteros e intactos y son objeto de ataque. El analizador de datos seguro de la presente invención, en una realización, trata este problema realizando un análisis criptográfico y dividiendo el fichero encriptado en dos o más porciones o comparticiones, y en otra

realización, preferentemente 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 realización del analizador de datos seguro de la presente invención y un ejemplo de cómo puede utilizarse se muestra en la Figura 21 y se describe a continuación. Sin embargo, es fácilmente evidente para los expertos en la materia que el analizador de datos seguro de la presente invención puede utilizarse en una amplia diversidad de maneras además del ejemplo no limitante a continuación. Como una opción de despliegue, y en una realización, el analizador de datos seguro puede implementarse con gestión de clave de sesión externa o almacenamiento interno seguro de claves de sesión. Tras la implementación, se generará una Clave Maestra de Analizador que se usará para asegurar la aplicación y para fines de encriptación. Debería observarse 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.

Como se muestra en la Figura 21, esta 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 realización del método, la clave maestra de sesión se almacenará junto con las comparticiones de datos aseguradas en un depositario 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 fácilmente evidente para los expertos en la materia que ciertas etapas de los métodos descritos en el presente documento pueden realizarse en diferente orden, o repetirse múltiples veces, según sea necesario. Es también fácilmente evidente para los expertos en la materia que las porciones de los datos pueden manejarse de manera diferente de unas a otras. Por ejemplo, pueden realizarse múltiples etapas de análisis en únicamente una porción de los datos analizados. Cada porción de datos analizados puede asegurarse de manera única en cualquier manera deseable con la condición únicamente de que los datos puedan reensamblarse, reconstituirse, reformarse, desencriptarse o restaurarse a su forma original u otra usable.

Como se muestra en la Figura 22 y se describe en el presente documento, otra 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 realización del método de la presente invención, la clave maestra de sesión se almacenará en una tabla de gestión de claves separada en un depositario 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 fácilmente evidente para los expertos en la materia que ciertas etapas del método descrito en el presente documento pueden realizarse en diferente orden, o repetirse múltiples veces, según sea necesario. Es también fácilmente evidente para los expertos en la materia que las porciones de los datos pueden manejarse de manera diferente de unas a otras. Por ejemplo, pueden realizarse múltiples etapas de separación o análisis en únicamente una porción de los datos analizados. Cada porción de datos analizados puede asegurarse de manera única en cualquier manera deseable con la condición únicamente de que los datos puedan reensamblarse, reconstituirse, reformarse, desencriptarse o restaurarse a su forma original u otra usable.

Como se muestra en la Figura 23, esta 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 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 realización del método, la clave maestra de sesión se almacenará junto con las comparticiones de datos aseguradas en un depositario 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 fácilmente evidente para los expertos en la materia que ciertas etapas de los métodos descritos en el presente documento pueden realizarse en diferente orden, o repetirse múltiples veces, según sea necesario. Es también fácilmente evidente para los expertos en la materia que las porciones de los datos pueden manejarse de manera diferente de unas a otras. Por ejemplo, pueden realizarse múltiples etapas de análisis en únicamente una porción de los datos analizados. Cada porción de datos analizados puede asegurarse de manera única en cualquier manera deseable con la condición únicamente de que los datos puedan reensamblarse, reconstituirse, reformarse, desencriptarse o restaurarse a su forma original u otra usable.

Como se muestra en la Figura 24 y se describe en el presente documento, otra 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 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 realización del método de la presente invención, la clave maestra de sesión se almacenará en una tabla de gestión de claves separada en un depositario 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 fácilmente evidente para los expertos en la materia que ciertas etapas del método descrito en el presente documento pueden realizarse en diferente orden, o repetirse múltiples veces, según sea necesario. Es también fácilmente evidente para los expertos en la materia que las porciones de los datos pueden manejarse de manera diferente de unas a otras. Por ejemplo, pueden realizarse múltiples etapas de separación o análisis en únicamente una porción de los datos analizados. Cada porción de datos analizados puede asegurarse de manera única en cualquier manera deseable con la condición únicamente de que los datos puedan reensamblarse, reconstituirse, reformarse, desencriptarse o restaurarse a su forma original u otra usable.

Es adecuada una amplia diversidad de metodologías para uso en los métodos de la presente invención, como es fácilmente evidente para los expertos en la materia. El algoritmo Relleno de un Solo Uso, se considera en ocasiones uno de los métodos de encriptación más seguros, y es adecuado para uso en el método de la presente invención. Usar el algoritmo Relleno de un Solo Uso requiere que se genere una clave que es tan larga como los datos a asegurarse. El uso de este método puede ser menos deseable en ciertas circunstancias tales como aquellas que dan como resultado la generación y gestión de claves muy largas debido al tamaño del conjunto de datos a asegurar. En el algoritmo Relleno de un Solo Uso (OTP), 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 depositarios 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 a asegurar se pasan a través de la primera operación de encriptación, datos seguros = datos XOR clave secreta 5:

S = D XOR K5

Para 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 pueden realizarse 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 realización, puede no desearse tener un depositario 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 depositario de datos diferente:

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

Adicionalmente, 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 descrito 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):

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

En el ejemplo de clave de sesión incorporada descrito 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):

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

A menos que se recuperen todas las cuatro comparticiones, los datos no pueden reensamblarse de acuerdo con este ejemplo. Incluso si todas las cuatro comparticiones se capturaran, 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 realización del método de la presente invención, y describe también, en otra realización, el algoritmo usado para colocar particiones en depositarios de modo que las comparticiones desde todos los depositarios pueden combinarse para formar el material de autenticación secreto. Los cálculos necesarios son muy sencillos y rápidos. Sin embargo, con el algoritmo Relleno de un Solo Uso (OTP) puede haber circunstancias que producen que sea menos deseable, tales como un gran conjunto de datos a asegurar, puesto que el tamaño de clave es el mismo tamaño que los datos a almacenarse. 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 descrita en el presente documento. En lugar de un valor aleatorio de n bytes, se genera un valor aleatorio n’ = min(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 puede usarse para generar las claves usadas en la función XOR. El algoritmo de Cifrado de Flujo RS1 es interoperable con otros algoritmos de cifrado de flujo disponibles comercialmente, tales como el RC4™ algoritmo de cifrado de flujo de RSA Security, Inc y es adecuado para 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 XOR E(K1)

SD2 = S2 XOR E(K2)

SD3 = S3 XOR E(K3)

SDn = Sn XOR E(Kn)

donde E(K1) a E(Kn) son los primeros n' bytes de salida del algoritmo de Cifrado de Flujo RS1 con clave por K1 a Kn. Las comparticiones se colocan ahora en depositarios de datos 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 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 puesto que es sencillamente más corto. Es fácilmente evidente para los expertos en la materia que son adecuados una amplia diversidad de métodos o algoritmos de encriptación para 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 comparticiones en movimiento de los datos a diferentes localizaciones en uno o más depositarios de datos o dispositivos de almacenamiento, que pueden estar en diferentes localizaciones lógicas, físicas o geográficas. Cuando las comparticiones 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 comprensible para mantener la seguridad de los datos sensibles. Los datos se encriptan con una clave segura y se dividen en una o más comparticiones, y en una realización, cuatro comparticiones, de acuerdo con la clave segura. La clave segura se almacena de manera segura con un puntero de referencia que se asegura en cuatro comparticiones de acuerdo con una clave segura. Las comparticiones de datos se encriptan a continuación individualmente y las claves se almacenan de manera segura con diferentes comparticiones encriptadas. Cuando se combina, el proceso completo para asegurar datos de acuerdo con los métodos desvelados en el presente documento se hace un paquete comprensivo para seguridad de datos.

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

1. Todas las comparticiones o porciones del conjunto de datos.
2. Conocimiento de y capacidad para reproducir el flujo de proceso del método usado 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 puede aplicarse mediante el uso de la Clave Maestra del Analizador. Puede requerirse una toma de contacto de autenticación mutua entre el analizador de datos seguro y la aplicación en esta realización de la presente invención antes de cualquier acción tomada.

La seguridad del sistema dicta que no hay método de "puerta trasera" para la recreación de los datos originales. Para instalaciones donde pueden surgir problemas de recuperación de datos, el analizador de datos seguro puede potenciarse para proporcionar un espejo de las cuatro comparticiones y el depositario de la clave maestra de sesión. Las opciones de hardware tales como RAID (sistemas redundantes de discos de bajo costo, usados para dispersar la información a través de varios discos) y opciones de software tales como replicación pueden ayudar también en la planificación de recuperación de datos.

Gestión de clave

En una 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 pueden usarse, incluyen, pero sin limitación:

La clave maestra del analizador

Esta clave es una clave individual asociada con la instalación del analizador de datos seguro. Si se instala en el servidor en el que se ha desplegado 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 hardware

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 puede generarse 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. Puede incorporarse 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 puede asegurarse 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, puede generarse una Clave de Encriptación de Compartición individual para encriptar adicionalmente las comparticiones. Las claves de encriptación de compartición pueden almacenarse en diferentes comparticiones a la compartición que se encriptó.

Es fácilmente 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 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 puede asegurarse 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 puede restringirse ventajosamente 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 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 pueden usarse, incluyen, pero sin limitación:

1. La clave maestra del analizador

Esta clave es una clave individual asociada con la instalación del analizador de datos seguro. Si se instala en el servidor en el que se ha desplegado 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 hardware 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 puede generarse 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 puede asegurarse 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

Puede generarse 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. Puede incorporarse 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, puede generarse una Clave de Encriptación de Compartición individual para encriptar adicionalmente las comparticiones. Las claves de encriptación de compartición pueden almacenarse en diferentes comparticiones a la compartición que se encriptó.

Es fácilmente 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 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 puede asegurarse usando los métodos y sistema como se describe en el presente documento. Por ejemplo, el acceso a una base de datos particular en una compañía u organización puede restringirse ventajosamente 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.

Grupo de trabajo, proyecto, pc/portátil individual o seguridad de datos 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. Adicionalmente, todas las formas de datos que pueden asegurarse 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 hardware que el usuario tiene a su disposición.

En una realización de la presente invención, los métodos de aseguración de datos se utilizan como se describe a continuación en un entorno de grupo de trabajo. En una realización, 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 desplegó la Clave Maestra del Analizador.

En una realización, pueden proporcionarse 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 realización, la gestión de clave puede establecerse 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., como se definen mediante una organización, y el acceso a datos asegurados puede limitarse a solamente aquellos 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 realización permite la compartición de datos asegurados entre diferentes grupos en una compañía u organización mientras 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 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, donde se requiera alguna compartición, pero no pueda permitirse 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 como sigue. Se usa una clave Maestra de Analizador como una generación de series 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 descritos en el presente documento se usan para compartir ficheros en grupos de usuarios.

En el ejemplo mostrado en la Figura 25 y descrito 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 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 puede hacerse automáticamente 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 los credenciales compartidos, 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 a usarse 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 puede usarse con cualquier otro sistema informático o plataforma de software, cualquiera que puede ser, por ejemplo, integrarse en programas de aplicación existentes o usada independiente para seguridad de ficheros.

Es fácilmente evidente para los expertos en la materia que una combinación cualquiera o combinación de algoritmos de encriptación son adecuadas para uso en los métodos y sistemas de la presente invención. Por ejemplo, las etapas de encriptación pueden repetirse, en una realización, para producir un esquema de encriptación de múltiples capas. Además, puede usarse un algoritmo de encriptación diferente, o combinación de algoritmos de encriptación, en etapas de encriptación repetidas de manera que se aplican diferentes algoritmos de encriptación a las diferentes capas del esquema de encriptación en múltiples capas. Como tal, el propio esquema de encriptación puede hacerse 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 pseudo-aleatorio) se compara al valor o valores anexados y puede tomarse 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 podría realizarse 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 puede implementarse 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 pueda usarse 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), cualquier otra información adecuada, o cualquier combinación de las mismas.

El analizador de datos seguro de la presente invención puede usarse en cualquier aplicación adecuada. En concreto, el analizador de datos seguro descrito 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 descritos son meramente realizaciones ilustrativas que pueden modificarse de cualquier manera adecuada para satisfacer deseos adecuados. Por ejemplo, el análisis y división puede basarse 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 puede usarse para implementar testigos físicos seguros, en los que los datos almacenados en un testigo físico pueden requerirse para acceder a datos adicionales almacenados en otro área de almacenamiento. En un enfoque adecuado, un testigo físico, tal como una unidad flash USB compacta, un disco flexible, un disco óptico, una tarjeta inteligente, o cualquier otro testigo físico adecuado, puede usarse para almacenar una de al menos dos porciones de datos analizados de acuerdo con la presente invención. Para acceder a los datos originales, necesitaría accederse a la unidad flash USB. Por tanto, un ordenador personal que mantiene una porción de datos analizados necesitaría tener la unidad flash USB, que tiene la otra porción de datos analizados, conectada antes de que pueda accederse a los datos originales. La Figura 26 ilustra esta aplicación. El área de almacenamiento 2500 incluye una porción de datos analizados 2502. El testigo físico 2504, que tiene una porción de datos analizados 2506 necesitaría acoplarse 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 a los datos originales. Esto es útil en una situación 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 puede usarse cualquier otro enfoque para usar testigos físicos.

El analizador de datos seguro de la presente invención puede usarse 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 pueden analizarse 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 USB, etc.), o cualquier otro dispositivo adecuado. Una o más otras porciones de los datos de inscripción del usuario analizados pueden almacenarse 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 deben obtenerse también mediante la porción de datos analizada y dividida apropiada).

El analizador de datos seguro de la presente invención puede integrarse 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 software, hardware, o ambos para implementar cualquier aplicación adecuada. El sistema 2600 puede ser un sistema existente en el que el analizador de datos seguro 2602 puede reacondicionarse como un componente integrado. Como alternativa, el analizador de datos seguro 2602 puede integrarse en cualquier sistema 2600 adecuado desde, por ejemplo, su etapa de diseño más temprana. El analizador de datos seguro 2600 puede integrarse en cualquier nivel adecuado del sistema 2600. Por ejemplo, el analizador de datos seguro 2602 puede integrarse en el sistema 2600 a un nivel suficientemente de fondo de manera 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 puede usarse 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 puede integrarse en un núcleo de sistema operativo (por ejemplo, Linux, Unix, o cualquier otro sistema operativo comercial o propietario adecuado). Esta integración puede usarse 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 software 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 puede integrarse 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 software 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 puede integrarse en un controlador de RAID (como hardware o software). Esto permite el almacenamiento seguro de datos a múltiples unidades mientras se mantiene tolerancia a fallos en caso de fallo de unidad.

El analizador de datos seguro de la presente invención puede integrarse en una base de datos para proteger, por ejemplo, información de tabla sensible. Por ejemplo, en un enfoque adecuado, los datos asociados con celdas particulares de una tabla de base de datos (por ejemplo, celdas individuales, una o más columnas particulares, una o más filas particulares, cualquier combinación de las mismas, o una tabla de base de datos entera) pueden analizarse 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 puede concederse mediante métodos de autenticación tradicionales (por ejemplo, consulta de nombre de usuario y contraseña).

El analizador seguro de la presente invención puede integrarse 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 puede usarse 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 puesto 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 pueden combinarse a lo largo de una trayectoria secuencialmente de 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 pueden combinarse 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 emisor 2700, que puede incluir cualquier hardware adecuado, tal como un terminal informático, un ordenador personal, dispositivo portátil (por ejemplo, PDA, Blackberry), teléfono celular, red informática, cualquier otro hardware adecuado o cualquier combinación de los mismos. El sistema emisor 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 pueden comunicarse 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 pueden comunicarse 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 hardware adecuado como se ha descrito anteriormente con respecto al sistema emisor 2700. Las porciones de datos separadas llevadas a lo largo de las trayectorias de comunicación 2706 se recombinan en el sistema recepción 2710 para generar el mensaje original o los datos de acuerdo con la presente invención.

La Figura 29 muestra un sistema emisor 2800, que puede incluir cualquier hardware adecuado, tal como un terminal informático, ordenador personal, dispositivo portátil (por ejemplo, PDA), teléfono celular, red informática, cualquier otro hardware adecuado o cualquier combinación de los mismos. El sistema emisor 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 pueden comunicarse 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 pueden comunicarse en serie a través de la trayectoria de comunicación 2806 con respecto entre sí. El sistema de recepción 2810 puede ser cualquier hardware adecuado como se ha descrito anteriormente con respecto al sistema emisor 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 puede usarse. Por ejemplo, en otro enfoque adecuado, las características de los sistemas de las Figuras 28 y 29 pueden combinarse 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 puede integrarse 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 puede integrarse 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 puede implementarse en un componente de fondo tal como el servidor de intercambio, caso en el que los mensajes pueden analizarse, dividirse y comunicarse automáticamente 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 pueden analizarse y separarse en múltiples flujos conteniendo cada uno una porción de los datos analizados. Los múltiples flujos pueden transmitirse 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 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 puede integrarse para protección de y 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) 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) adecuado tal como Blackberries y teléfonos inteligentes puede asegurarse 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, impresora, escáner, teclado, enrutador de red, dispositivo de autenticación biométrico (por ejemplo, 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 pueden aplicarse 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 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 usado 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, donde n <= m. Por ejemplo, si cada una de las cuatro porciones se almacena en una localización física diferente con relación a 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 pueden aún recuperarse desde las porciones en las otras dos localizaciones. Puede usarse cualquier valor adecuado para n o m.

Además, la característica n de m de la presente invención puede usarse 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 puede usarse para proporcionar a un grupo de entidades con una clave a nivel de grupo que permite a los miembros del grupo acceder a información particular autorizada a accederse por 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 puede requerirse 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. Puede aplicarse 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 multi-nacionales 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 usados actualmente). Esta capacidad es aplicable también para compañías u otras organizaciones en las que la información que necesita conocerse por uno o más individuos específicos (en o sin la organización) puede comunicarse 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 multi-nivel 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, pueden usarse más redes (por ejemplo, una red separada para alto secreto), pero la presente invención permite sustancialmente menos que en la disposición actual en la que se usa una red separada para cada nivel de clasificación.

Se entenderá que puede usarse cualquier combinación de las aplicaciones anteriormente descritas del analizador seguro de la presente invención. Por ejemplo, la aplicación de clave de grupo puede usarse junto con la aplicación de seguridad de datos en movimiento (es decir, en la que los datos que se comunican a través de una red pueden accederse únicamente por un miembro del respectivo grupo, y 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 puede integrarse 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 un término 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, puede usarse para permitir programas escritos para que una base de datos particular comunique con otras bases de datos sin codificación personalizada.

El analizador de datos seguro de la presente invención puede implementarse teniendo cualquier combinación de cualquier capacidad adecuada, tales como aquellas analizadas en el presente documento. En algunas realizaciones de la presente invención, por ejemplo, el analizador de datos seguro puede implementarse teniendo únicamente ciertas capacidades mientras que otras capacidades pueden obtenerse a través del uso de software, hardware externo 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 puede implementarse con muy pocas capacidades integradas. 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 anteriormente descrita (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 puede integrarse en el analizador de datos seguro 3000.

La memoria intermedia de datos ensamblada 3008 puede ser cualquier memoria adecuada usada para almacenar los datos originales (aunque 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 puede usarse 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 pueden usarse 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 puede integrarse y cualquiera de las características ilustradas puede eliminarse, hacerse más robusta, hacerse menos robusta, o puede modificarse de otra manera de cualquiera manera adecuada. Las memorias intermedias 3008 y 3010 son de manera análoga meramente ilustrativas y pueden modificarse, eliminarse o añadirse de cualquier manera adecuada.

Cualquier módulo adecuado implementado en software, hardware o ambos puede llamar por o puede llamar al analizador de datos seguro 3000. Si se desea, incluso pueden sustituirse capacidades que están integradas en el analizador de datos seguro 3000 mediante uno o más módulos externos. 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. Puede usarse cualquier otro módulo adecuado además de o en lugar de aquellos ilustrados.

El generador de clave de realimentación de cifrado 3014 puede generar, externamente 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 a analizar y dividir. Puede usarse 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.

Para 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.), puede usarse una capa de empaquetado que puede hacer uso de, por ejemplo, llamadas de función de API. Puede usarse 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 puede usarse 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 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 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, puede almacenarse 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) apropiadamente (por ejemplo, escritas en uno o más dispositivos de almacenamiento, comunicadas a una red, etc.).

La Figura 32 muestra de manera ilustrativa cómo puede usarse 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 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 pueden usarse 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. Puede usarse cualquier otro proceso, componente o ambos adecuados además de o en lugar de aquellos 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 realización de la presente invención. 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 puede analizarse 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 puede generarse la clave de sesión de realimentación de cifrado 3304.

En un enfoque adecuado, los datos originales 3306 pueden encriptarse antes del análisis, división o ambos. Por ejemplo, como ilustra la Figura 33, a los datos originales 3306 puede realizarse 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 puede usarse cualquier otra técnica de encriptación adecuada en lugar de o además de la técnica de XOR ilustrada. Se entenderá adicionalmente que aunque 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 puede realizarse 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 necesita usarse troceo. En su lugar, puede emplearse cualquier otra técnica adecuada para dividir datos.

La Figura 34 es un diagrama de bloques de un flujo de proceso ilustrativo para restaurar datos originales 3306 desde dos o más porciones de datos originales 3306 analizadas y divididas de acuerdo con una 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 puede a continuación usarse 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 puede implementarse la división de bits en el ejemplo de las Figuras 33 y 34. Un troceo puede usarse (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. Puede usarse cualquier otra técnica adecuada.

Se entenderá que cualquier referencia a funcionalidad de troceo realizada en el presente documento puede realizarse con respecto a cualquier algoritmo de troceo adecuado. Estos incluyen por ejemplo, MD5 y SHA-1.

Pueden usarse diferentes algoritmos de troceo en diferentes momentos y por diferentes componentes de la presente invención.

Después de que se ha determinado un punto de división de acuerdo con el procedimiento ilustrativo anterior o a través de cualquier otro procedimiento o algoritmo, puede realizarse una determinación con respecto a qué porciones de datos anexar a cada uno de los segmentos izquierdo y derecho. Puede usarse cualquier algoritmo adecuado para realizar esta determinación. Por ejemplo, en un enfoque adecuado, puede crearse 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 puede determinarse 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 pseudo-aleatorio adecuado, que puede generarse y ampliarse al tamaño de los datos originales. Por ejemplo, puede realizarse una función de troceo de un byte correspondiente en el valor aleatorio o pseudo-aleatorio. 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.

Puede anexarse 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 pueden anexarse en consecuencia para cada compartición en, por ejemplo, una manera en orden cíclico (por ejemplo, donde el tamaño de los datos originales es 4 MB, entonces la compartición 1 obtiene sus propias comparticiones así como aquellas de las comparticiones 2 y 3; la compartición 2 obtiene su propia

compartición así como aquellas de las comparticiones 3 y 4; la compartición 3 obtiene su propia compartición así como aquellas de las comparticiones 4 y 1; y la compartición 4 obtiene sus propias comparticiones así como aquellas de las comparticiones 1 y 2). Puede usarse cualquier redundancia adecuada de acuerdo con la presente invención.

Se entenderá que puede usarse 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 puede procesarse aleatoria o pseudo-aleatoriamente en una base bit a bit. Puede usarse un valor aleatorio o pseudo-aleatorio (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 pseudo-aleatorio puede indicar a qué compartición anexar el bit respectivo. En un enfoque adecuado el valor aleatorio o pseudo-aleatorio puede generarse como, o ampliarse a, 8 veces el tamaño de los datos originales de modo que la función de troceo puede realizarse en un byte correspondiente del valor aleatorio o pseudo-aleatorio 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 puede usarse de acuerdo con la presente invención. Se apreciará adicionalmente que los datos de redundancia pueden anexarse a las comparticiones de datos tal como, por ejemplo, en la manera inmediatamente descrita anteriormente de acuerdo con la presente invención.

En un enfoque adecuado, el análisis y división no necesita ser aleatorio o pseudo-aleatorio. En su lugar, puede usarse cualquier algoritmo determinístico adecuado para analizar y dividir datos. Por ejemplo, puede emplearse 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 secuencialmente de una manera en orden cíclico. Se apreciará adicionalmente que los datos de redundancia pueden anexarse a las comparticiones de datos tal como, por ejemplo, de la manera anteriormente descrita de acuerdo con la presente invención.

En una 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, donde son necesarias menos de todas las porciones para restaurar los datos originales), entonces incluso aunque 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 pueden requerirse 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. Puede requerirse que se proporcionen y desencripten las porciones encriptadas para restaurar los datos originales. Las diferentes porciones encriptadas pueden encriptarse con diferentes claves de encriptación. Por ejemplo, esta característica puede usarse 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 a 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, puede usarse una clave pública para encriptar una o más porciones de datos que pueden ser una compartición obligatoria requerida para restaurar los datos originales. Puede usarse a continuación una clave privada para desencriptar la compartición para usarse para restaurar los datos originales.

Puede usarse cualquier paradigma adecuado de este tipo que haga uso de comparticiones obligatorias donde sean necesarias menos de todas las comparticiones para restaurar los datos originales.

En una realización adecuada de la presente invención, la distribución de datos en un número finito de comparticiones de datos puede procesarse aleatoria o pseudo-aleatoriamente de manera 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 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 con relación a 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 %. Debería deducirse, 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 %. Puede usarse cualquier probabilidad adecuada de acuerdo con la presente invención.

Se entenderá que el analizador de datos seguro puede programarse también para distribuir datos a comparticiones de acuerdo con un porcentaje exacto (o casi exacto). Por ejemplo, el analizador de datos seguro puede programarse 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 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 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. Puede usarse 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.

Como se ha analizado anteriormente, 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. También, como se ha analizado anteriormente, las claves de división pueden asegurarse en comparticiones de datos generadas mediante el analizador de datos seguro. Puede usarse cualquier algoritmo adecuado para asegurar las claves de división para asegurarlas entre las comparticiones de datos. Por ejemplo, puede usarse el algoritmo Shamir para asegurar las claves de división con las que la información que puede usarse para reconstruir una clave de división se genera y anexa a las comparticiones de datos. Puede usarse cualquier otro algoritmo adecuado de este tipo de acuerdo con la presente invención.

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

De acuerdo con una realización de la presente invención, una Transformación Todo o Nada (AoNT), tal como una Transformación de Paquete Completo, puede usarse 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 usada para encriptar un conjunto de datos antes de análisis y división de acuerdo con la presente invención puede transformarse mediante un algoritmo AoNT. La clave de encriptación transformada puede a continuación distribuirse entre las comparticiones de datos de acuerdo con, por ejemplo, el algoritmo Shamir o cualquier otro algoritmo adecuado. Para reconstruir la clave de encriptación, el conjunto de datos encriptados debe restaurarse (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, puede usarse 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 pueden usarse junto con la característica AoNT. En concreto, los datos de redundancia pueden incluirse en las porciones de datos de manera que son necesarias menos de todas las porciones de datos para restaurar el conjunto de datos encriptados.

Se entenderá que AoNT puede aplicarse a las claves de encriptación usadas 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 corresponde al conjunto de datos antes del análisis y división. Análogamente, AoNT puede aplicarse a las claves de división.

En una realización de la presente invención, las claves de encriptación, claves de división, o ambas usadas de acuerdo con la presente invención pueden encriptarse 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 realización de la presente invención, puede proporcionarse 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, pueden usarse otros algoritmos de división de clave (por ejemplo, compartición secreta) tales como Blakely en lugar de Shamir, o la encriptación AES podría sustituirse 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 uso en una realización de la invención. Debería entenderse que cualquier algoritmo adecuado o combinación de algoritmos puede usarse 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 pueden dividirse eventualmente en un número predefinido de comparticiones. Si el algoritmo de división requiere una clave, puede generarse una clave de encriptación de división en la etapa 3612 usando un generador de números pseudo-aleatorios criptográficamente seguro. La clave de encriptación de división puede transformarse opcionalmente usando una Transformación Todo o Nada (AoNT) 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 pueden a continuación dividirse en el número predefinido de comparticiones en la etapa 3616. Puede usarse 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, puede embeberse información de autenticación/integridad en las comparticiones en la etapa 3618. Cada compartición puede opcionalmente post-encriptarse en la etapa 3619.

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

En algunas realizaciones, los datos de entrada pueden encriptarse 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 puede proporcionarse desde un almacenamiento de clave externo. Si el algoritmo de división requiere una clave, la clave de encriptación de división puede generarse usando un generador de números pseudo-aleatorios criptográficamente seguro en la etapa 3612. La clave de división puede transformarse 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. Puede usarse 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, puede embeberse información de autenticación/integridad en las comparticiones en la etapa 3618. Cada compartición puede opcionalmente post-encriptarse en la etapa 3619.

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

En algunas realizaciones, puede generarse una clave de encriptación usando un generador de números pseudo-aleatorios 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 puede transformarse 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 pueden a continuación dividirse 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 pseudo-aleatorios criptográficamente seguro puede tener lugar en la etapa 3612. La clave de división puede transformarse 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 pueden a continuación dividirse en un número predefinido de comparticiones en la etapa 3616. Puede usarse 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 puede a continuación opcionalmente post-encriptarse en la etapa 3619.

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

En algunas realizaciones, los datos pueden dividirse 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 pseudo-aleatorios criptográficamente seguro puede tener lugar en la etapa 3612. La clave de división puede transformarse 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 pueden a continuación dividirse en la etapa 3616. Puede usarse 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, puede embeberse información de autenticación/integridad en las comparticiones en la etapa 3618. Cada compartición puede opcionalmente post-encriptarse en la etapa 3619.

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

El analizador de datos seguro puede ofrecer protección de datos flexible facilitando la separación física. Los datos pueden encriptarse 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 pueden perderse o corromperse en la transmisión. Las comparticiones perdidas o corrompidas pueden recrearse desde la tolerancia a fallos o la información de integridad anexada a las comparticiones, como se analiza en más detalle a continuación.

Para 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 pre-encriptación: cuando se selecciona la pre-encriptación de las comparticiones, puede pasarse una clave externa al analizador de datos seguro. Esta clave puede generarse y almacenarse externamente en un almacenamiento de claves (u otra localización) y puede usarse para encriptar opcionalmente datos antes de la división de datos.

Clave de encriptación de división: esta clave puede generarse internamente y usarse mediante el analizador de datos seguro para encriptar los datos antes de la división. Esta clave puede a continuación almacenarse 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, puede usarse para aplicar claves los algoritmos de particionamiento de datos cuando se selecciona división aleatoria. Cuando se usa una división aleatoria, puede generarse una clave de sesión de división internamente y usarse mediante el analizador de datos seguro para particionar los datos en comparticiones. Esta clave puede almacenarse de manera segura en las comparticiones usando un algoritmo de división de clave.

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

En algunas realizaciones, cuando se aseguran los datos usando el analizador de datos seguro de esta manera, la información puede únicamente reensamblarse 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 realizaciones. Como se ha descrito anteriormente, dos funciones bien adecuadas para el analizador de datos seguro 3706 pueden incluir encriptación 3702 y respaldo 3704. Como tal, el analizador de datos seguro 3706 puede integrarse con un sistema RAID o de respaldo o un motor de encriptación de hardware o software en algunas realizaciones.

Los procesos de clave principal asociados con el analizador de datos seguro 3706 pueden incluir uno o más de proceso de pre-encriptación 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 post-encriptación 3720. Estos procesos pueden ejecutarse en varios órdenes o combinaciones adecuados, 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 pre-encriptación, 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. Como se ha descrito anteriormente, los datos pueden distribuirse a cada una de estas comparticiones aleatoriamente (o pseudo-aleatoriamente) en algunas realizaciones. En otras realizaciones, puede usarse un algoritmo determinístico (o alguna combinación de aleatoriedad adecuada, pseudo-aleatoriedad, 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, puede desplegarse una clave de grupo de trabajo a miembros de grupo en algunas realizaciones de la invención. La clave de grupo de trabajo debería protegerse 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 pre-encriptación y post-encriptación, aunque estas etapas pueden incluirse en otras realizaciones.

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 pueden a continuación dividirse y almacenarse en las comparticiones 3810 de acuerdo con la presente invención. Las porciones de división de la clave de encriptación 3806 pueden almacenarse 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.

Para restaurar los datos, la clave de encriptación de división 3806 puede recuperarse y restaurarse de acuerdo con la presente invención. La operación de división puede a continuación invertirse para restaurar el texto de cifrado. La clave de encriptación 3804 puede también recuperarse y restaurarse, y el texto de cifrado puede a continuación desencriptarse usando la clave de encriptación.

Cuando se utiliza una clave de grupo de trabajo, el proceso anterior puede cambiarse para proteger ligeramente la clave de encriptación con la clave de grupo de trabajo. La clave de encriptación puede a continuación encriptarse 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 puede a continuación encriptarse con la clave de grupo de trabajo en la etapa 3904. La clave de encriptación encriptada con la clave de grupo de trabajo puede a continuación dividirse en porciones y almacenarse con las comparticiones 3912. La clave de división 3908 puede también dividirse y almacenarse en las comparticiones 3912. Finalmente, 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 puede recuperarse y restaurarse de acuerdo con la presente invención. La operación de división puede a continuación invertirse 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) puede recuperarse y restaurarse. La clave de encriptación puede a continuación desencriptarse usando la clave de grupo de trabajo. Finalmente, el texto de cifrado puede desencriptarse usando la clave de encriptación.

Hay varios métodos seguros para desplegar 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 comúnmente usadas en algunas realizaciones se proporcionan a continuación:

Almacenamiento de clave basado en hardware

Las soluciones basadas en hardware 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 hardware 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 pueden generarse mediante una autoridad confiable y distribuirse a los usuarios, o generarse en el hardware. Adicionalmente, muchos sistemas de almacenamiento de claves proporcionan autenticación multi-factor, 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 software

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

Para asegurar claves en disco, la gestión de claves basada en software 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 hardware), 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 multi-factor.

El analizador de datos seguro de la presente invención puede usarse ventajosamente 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. Como se ha analizado anteriormente, se entenderá que el analizador de datos seguro puede integrarse también para protección y tolerancia a fallos de cualquier tipo de datos en movimiento a través de cualquier medio de transporte, incluyendo, por ejemplo, medios de transporte cableado, inalámbrico o físico. Como un ejemplo, las aplicaciones de voz sobre el protocolo de internet (VoIP) 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 puede eliminarse 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 pueden dividirse y restaurarse eficazmente “al vuelo” con retardo y almacenamiento en memoria intermedia mínimos, dando como resultado una solución comprensiva 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 para integrarse con una aplicación de VoIP, el analizador de datos seguro puede integrarse 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 realizaciones, el soporte para datos en red en movimiento puede proporcionarse mediante el analizador de datos seguro de la presente invención en dos fases distintas -- una fase de generación de encabezamiento y una fase de particionamiento de datos. El proceso de generación de encabezamiento simplificado 4000 y el proceso de partición de datos simplificado 4010 se muestran en las Figuras 40A y 40B, respectivamente. Uno o ambos de estos procesos pueden realizarse en paquetes de red, bloques de sistema de ficheros, o cualquier otra información adecuada.

En algunas realizaciones, el proceso de generación de encabezamientos 4000 puede realizarse una vez en el inicio de un flujo de paquete de paquetes de red. En la etapa 4002, puede generarse una clave de encriptación de división, K, aleatoria (o pseudo-aleatoria). La clave de encriptación de división, K, puede a continuación encriptarse opcionalmente (por ejemplo, usando la clave de grupo de trabajo anteriormente descrita) en la etapa de empaquetado de clave AES 4004. Aunque puede usarse un empaquetado de clave AES en algunas realizaciones, puede usarse cualquier algoritmo de encriptación de clave o de empaquetado de clave adecuado en otras realizaciones. 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 puede analizarse 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, puede usarse 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 puede a continuación embeberse en una de las comparticiones de salida (por ejemplo, en los encabezamientos de compartición). Finalmente, puede anexarse un bloque de integración de compartición y (opcionalmente) una etiqueta de post-autenticación (por ejemplo, MAC) al bloque de encabezamiento de cada compartición. Cada bloque de encabezamiento puede diseñarse 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 particionamiento 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) puede calcularse en el texto de cifrado resultante desde la etapa 4012. Por ejemplo, puede calcularse un troceo de SHA-256. En la etapa 4106, los paquetes de datos o bloques de datos pueden a continuación particionarse en dos o más comparticiones de datos usando uno de los algoritmos de división de datos anteriormente descritos de acuerdo con la presente invención. En algunas realizaciones, los paquetes de datos o bloques de datos pueden dividirse de 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) puede a continuación anexarse a cada compartición de datos. Puede calcularse también una etiqueta de post-autenticación opcional (por ejemplo, MAC) y anexarse a cada compartición de datos en algunas realizaciones.

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 puede incluirse 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 pueden almacenarse en un formato binario compacto.

Por ejemplo, en algunas realizaciones, 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 post-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) puede incluirse también en el encabezamiento. Cualquier otro valor adecuado o información puede incluirse también en el encabezamiento de compartición.

Como se muestra en el formato de compartición ilustrativo 4100 de la Figura 41, el bloque de encabezamiento 4102 puede asociarse con dos o más bloques de salida 4104. Cada bloque de encabezamiento, tal como el bloque de encabezamiento 4102, puede diseñarse para ajustarse en un único paquete de datos de red. En algunas realizaciones, después de que se transmite el bloque de encabezamiento 4102 desde una primera localización a una segunda localización, los bloques de salida pueden transmitirse a continuación. Como alternativa, el bloque de encabezamiento 4102 y los bloques de salida 4104 pueden transmitirse 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. Como se ha descrito anteriormente, cada compartición de datos puede asegurarse 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 pre-particionados. 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 puede a continuación verificarse frente al troceo de compartición.

Aunque se han descrito anteriormente algunas aplicaciones comunes del analizador de datos seguro, debería entenderse claramente que la presente invención puede integrarse con cualquier aplicación de red para aumentar la seguridad, tolerancia a fallos, anonimidad, cualquier combinación adecuada de lo anterior.

Adicionalmente, otras combinaciones, adiciones, sustituciones y modificaciones serán evidentes para los expertos en la materia en vista de la divulgación del presente documento. Por consiguiente, la presente invención no se ha de considerar limitada por la reacción de las realizaciones preferidas sino que se ha de definir por una referencia a las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un método para asegurar una transmisión de bloques de datos en un flujo de datos, comprendiendo el método:

encriptar cada bloque de datos en el flujo de datos con una clave de encriptación;
distribuir porciones de la clave de encriptación en al menos dos encabezamientos de compartición;
distribuir unidades de datos de los bloques de datos encriptados en al menos dos comparticiones de datos, en el que cada una de las al menos dos comparticiones de datos contiene una distribución sustancialmente aleatoria de un respectivo subconjunto de las unidades de datos; y
transmitir las al menos dos comparticiones de datos y los al menos dos encabezamientos de compartición a una localización remota a través de al menos una ruta de comunicaciones, mediante la cual el flujo de datos puede restaurarse de al menos dos comparticiones de datos de las al menos dos comparticiones de datos y de al menos dos encabezamientos de compartición de los al menos dos encabezamientos de compartición.

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

generar información de integridad para cada bloque de datos encriptados en el flujo de datos; y
transmitir la información de integridad a la localización remota.

3. El método de la reivindicación 2, en el que la información de integridad se transmite con las al menos dos comparticiones de datos.

4. El método de la reivindicación 2, en el que la información de integridad se selecciona a partir del grupo que consiste en un troceo, una firma de MAC y una firma digital.

5. El método de la reivindicación 1, en el que distribuir porciones de la clave de encriptación comprende distribuir porciones de la clave de encriptación usando un algoritmo de compartición secreto.

6. El método de la reivindicación 5, en el que el algoritmo de compartición secreto se selecciona a partir del grupo que consiste en Shamir y Blakely.

7. El método de la reivindicación 1, en el que transmitir las al menos dos comparticiones de datos y los al menos dos encabezamientos de compartición comprende transmitir las al menos dos comparticiones de datos y los al menos dos encabezamientos de compartición en una única ruta de comunicaciones en una transmisión en serie.

8. El método de la reivindicación 1, en el que transmitir las al menos dos comparticiones de datos y los al menos dos encabezamientos de compartición comprende transmitir las al menos dos comparticiones de datos y los al menos dos encabezamientos de compartición a través de múltiples rutas de comunicaciones en paralelo.

9. El método de la reivindicación 1, en el que la transmisión se realiza usando una aplicación de compartición de ficheros.

10. El método de la reivindicación 1, en el que la transmisión se realiza usando una aplicación de voto o encuesta.

11. El método de la reivindicación 1, en el que la transmisión se realiza usando una aplicación de voz sobre IP (VoIP).

12. El método de la reivindicación 1, en el que los bloques de datos se seleccionan a partir del grupo que consiste en paquetes de datos de red, paquetes de voz de red y bloques de datos de sistema de ficheros.

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

anexar información de redundancia a las al menos dos comparticiones de datos; y
transmitir la información de redundancia a la localización remota.

14. El método de la reivindicación 1, que comprende adicionalmente encriptar la clave de encriptación con una clave de grupo de trabajo antes de distribuir la clave de encriptación.

15. El método de la reivindicación 14, en el que encriptar la clave de encriptación con la clave de grupo de trabajo comprende encriptar la clave de encriptación usando una función de compresión de AES.

Figura 1

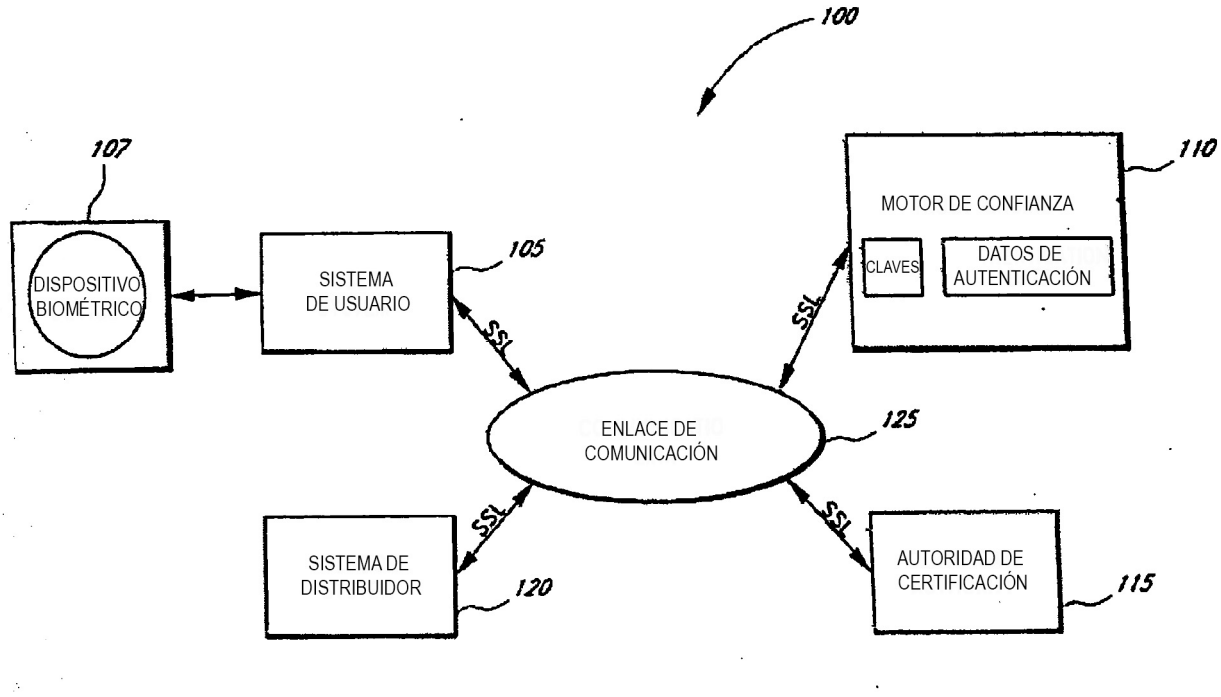

100
107
DISPOSITIVO BIOMÉTRICO
SISTEMA DE USUARIO
105
SSL
MOTOR DE CONFIANZA
110
CLAVES
DATOS DE AUTENTICACIÓN
SSL
ENLACE DE COMUNICACIÓN
125
SSL
SSL
SISTEMA DE DISTRIBUIDOR
120
AUTORIDAD DE CERTIFICACIÓN
115

Figura 2

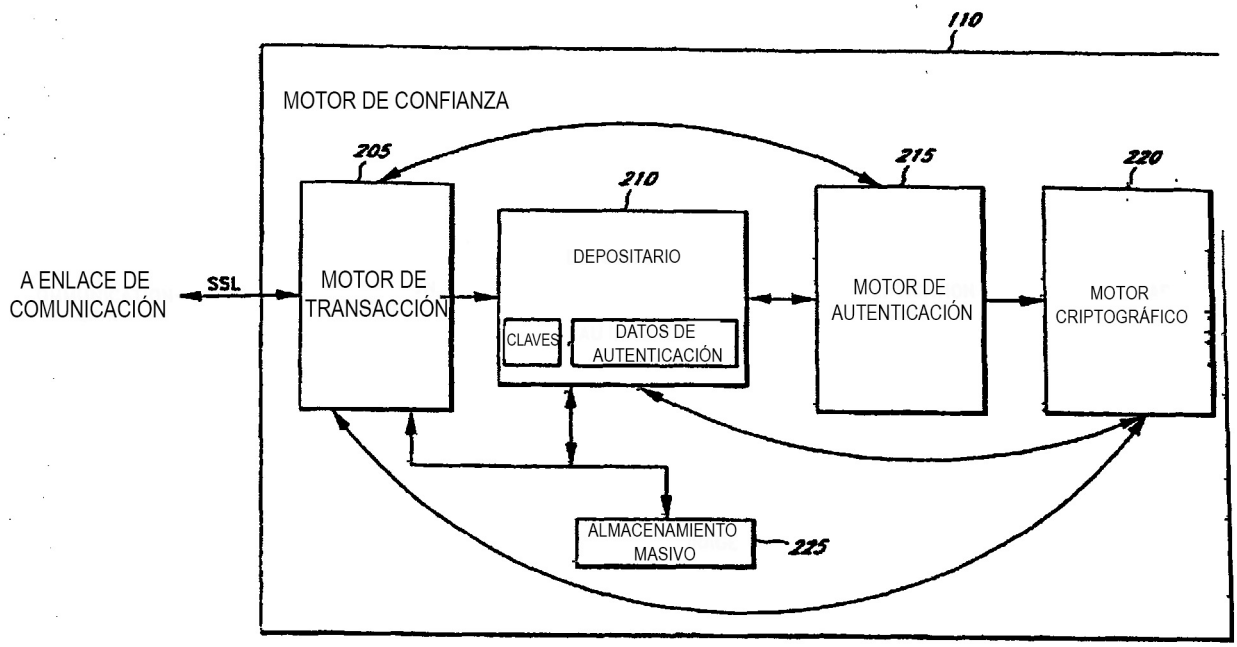

110
MOTOR DE CONFIANZA
205
210
215
220
A ENLACE DE COMUNICACIÓN
SSL
MOTOR DE TRANSACCIÓN
DEPOSITARIO
CLAVES
DATOS DE AUTENTICACIÓN
MOTOR DE AUTENTICACIÓN
MOTOR CRIPTOGRÁFICO
ALMACENAMIENTO MASIVO
225

Figura 3

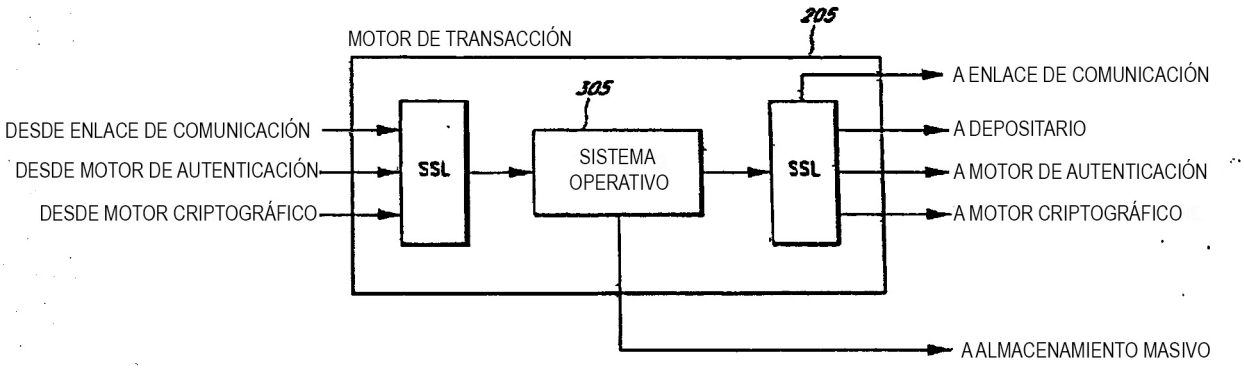

MOTOR DE TRANSACCIÓN
305
305
DESDE ENLACE DE COMUNICACIÓN
DESDE MOTOR DE AUTENTICACIÓN
DESDE MOTOR CRIPTOGRÁFICO
SSL
SISTEMA OPERATIVO
SSL
A ENLACE DE COMUNICACIÓN
A DEPOSITARIO
A MOTOR DE AUTENTICACIÓN
A MOTOR CRIPTOGRÁFICO
A ALMACENAMIENTO MASIVO

Figura 4

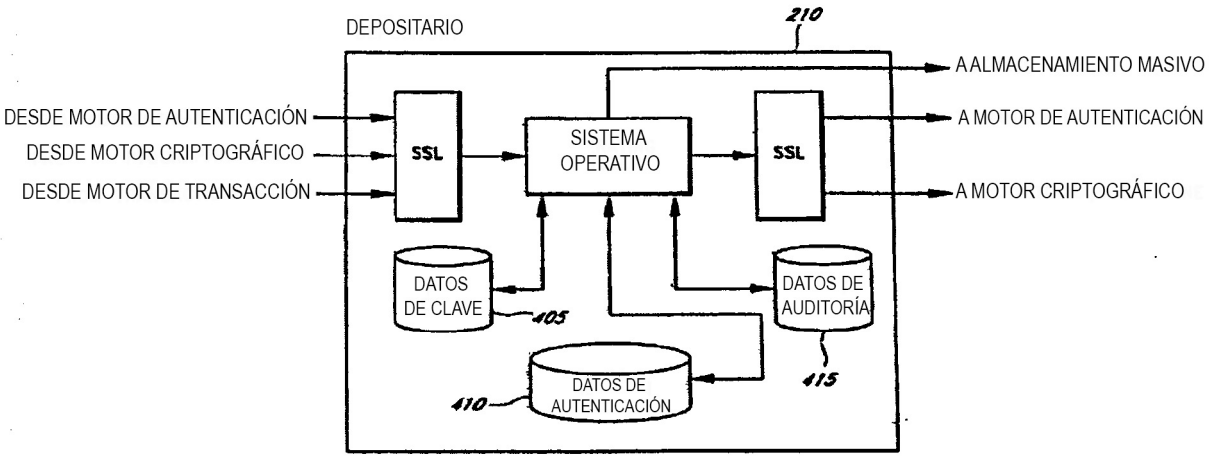

DEPOSITARIO
210
A ALMACENAMIENTO MASIVO
DESDE MOTOR DE AUTENTICACIÓN
DESDE MOTOR CRIPTOGRÁFICO
DESDE MOTOR DE TRANSACCIÓN
SSL
SISTEMA OPERATIVO
SSL
A MOTOR DE AUTENTICACIÓN
A MOTOR CRIPTOGRÁFICO
DATOS DE CLAVE
405
DATOS DE AUDITORÍA
415
DATOS DE AUTENTICACIÓN
410

Figura 5

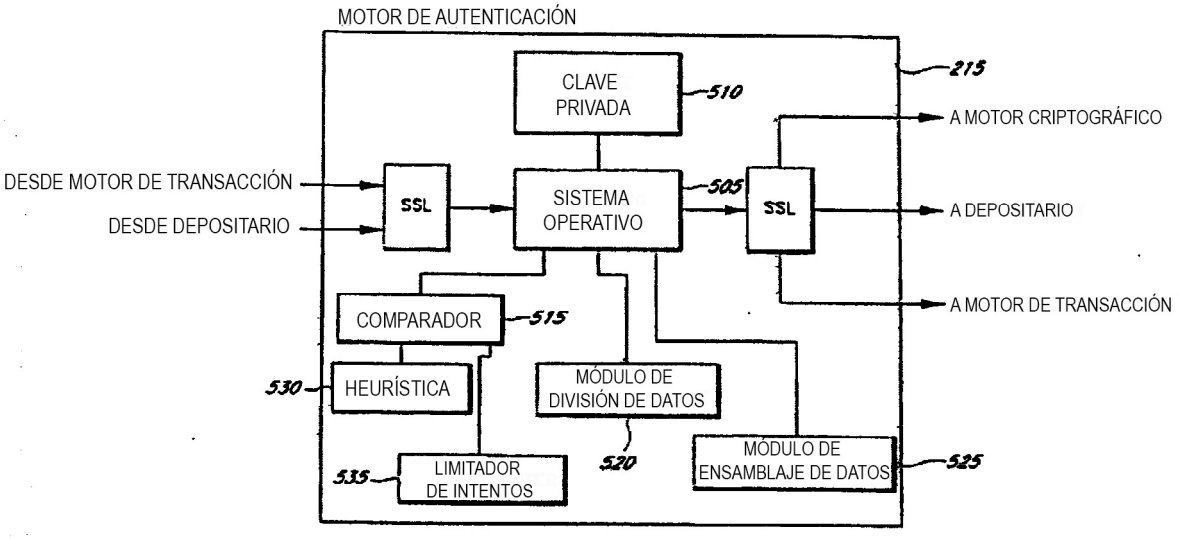

MOTOR DE AUTENTICACIÓN
CLAVE PRIVADA
510
215
A MOTOR CRIPTOGRÁFICO
DESDE MOTOR DE TRANSACCIÓN
DESDE DEPOSITARIO
SSL
SISTEMA OPERATIVO
505
SSL
A DEPOSITARIO
A MOTOR DE TRANSACCIÓN
COMPARADOR
515
530
HEURÍSTICA
MÓDULO DE DIVISIÓN DE DATOS
520
MÓDULO DE ENSAMBLAJE DE DATOS
525
535
LIMITADOR DE INTENTOS

Figura 6

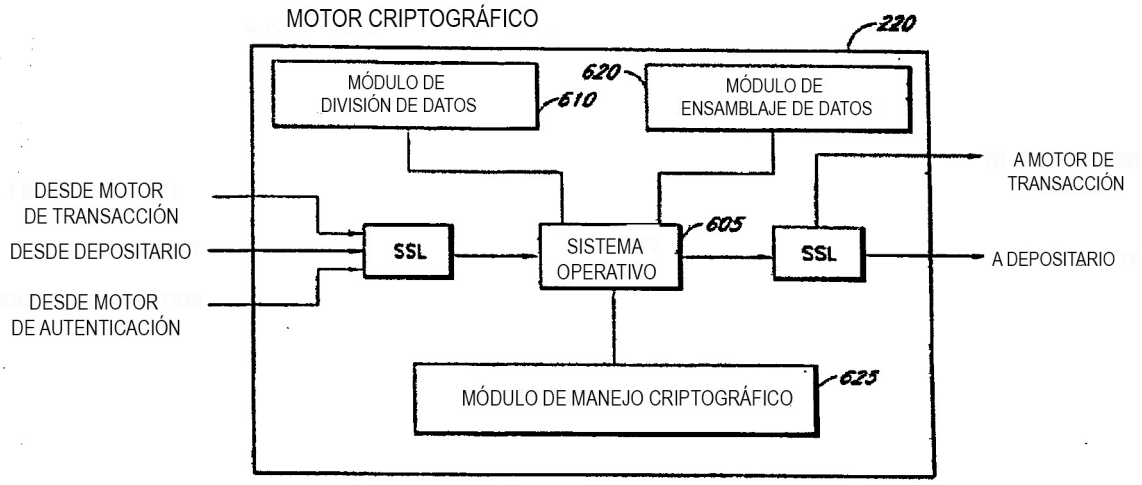

MOTOR CRIPTOGRÁFICO
220
MÓDULO DE DIVISIÓN DE DATOS
610
620
MÓDULO DE ENSAMBLAJE DE DATOS
A MOTOR DE TRANSACCIÓN
DESDE MOTOR DE TRANSACCIÓN
DESDE DEPOSITARIO
DESDE MOTOR DE AUTENTICACIÓN
SSL
SISTEMA OPERATIVO
605
SSL
A DEPOSITARIO
MÓDULO DE MANEJO CRIPTOGRÁFICO
625

Figura 7

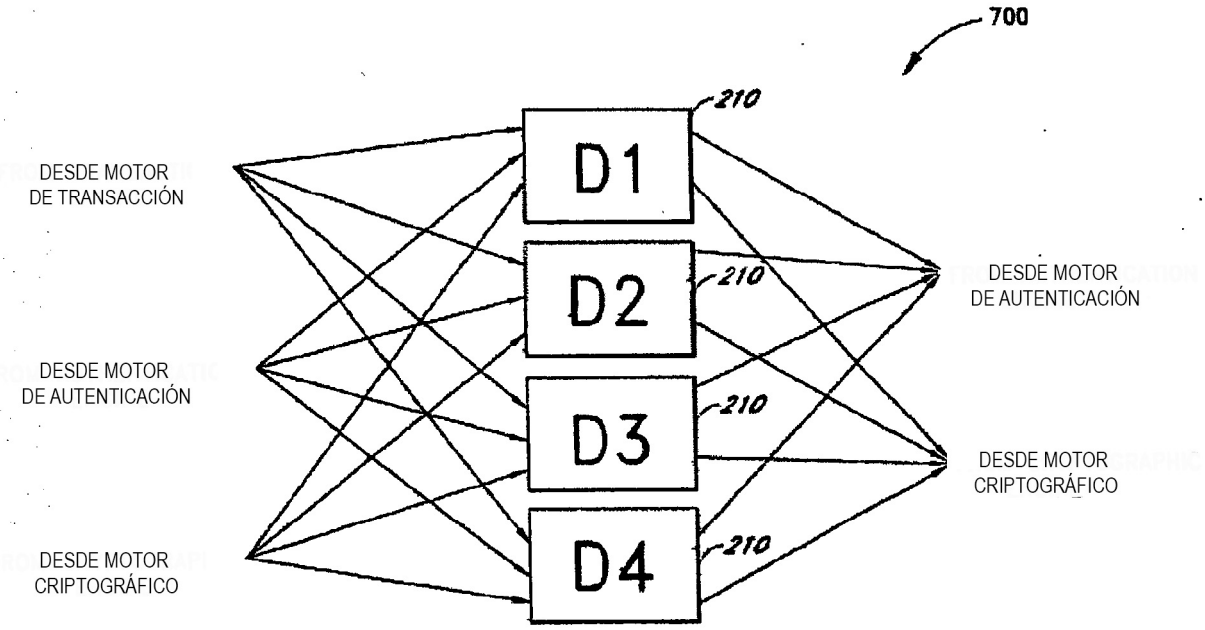

700
210
D1
D2
D3
D4
DESDE MOTOR DE TRANSACCIÓN
DESDE MOTOR DE AUTENTICACIÓN
DESDE MOTOR CRIPTOGRÁFICO
DESDE MOTOR DE AUTENTICACIÓN
DESDE MOTOR CRIPTOGRÁFICO

Figura 8

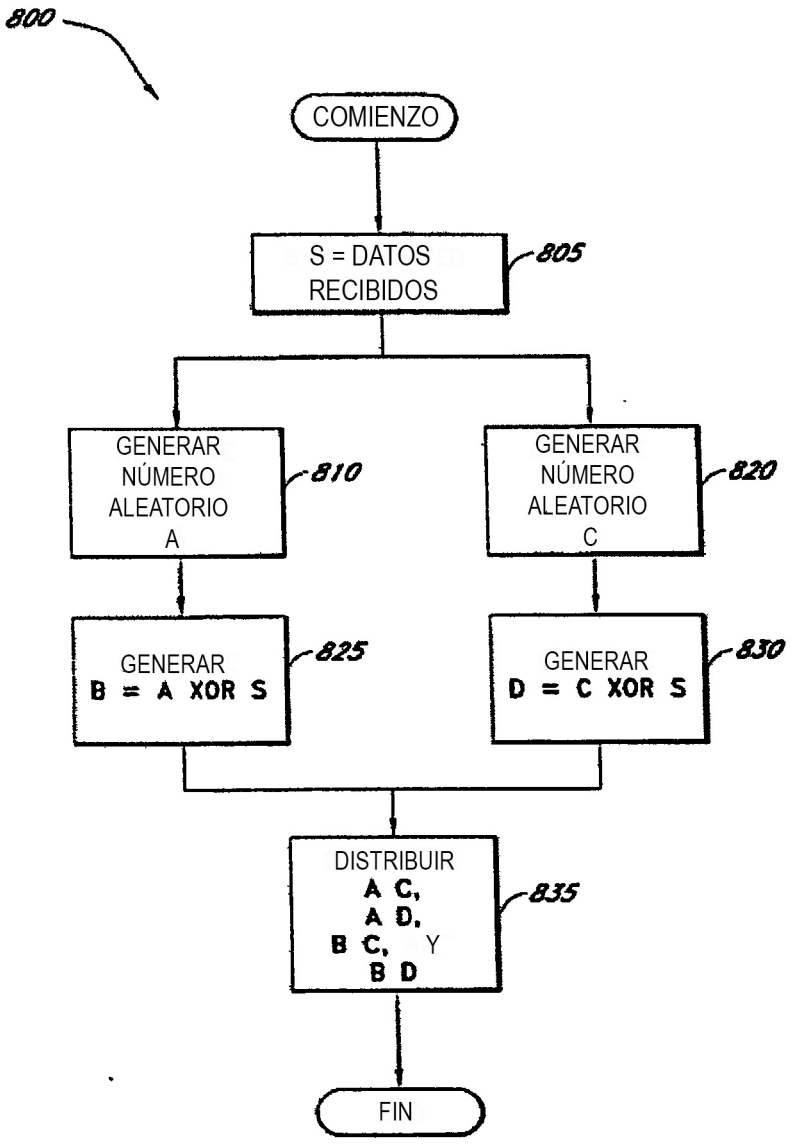
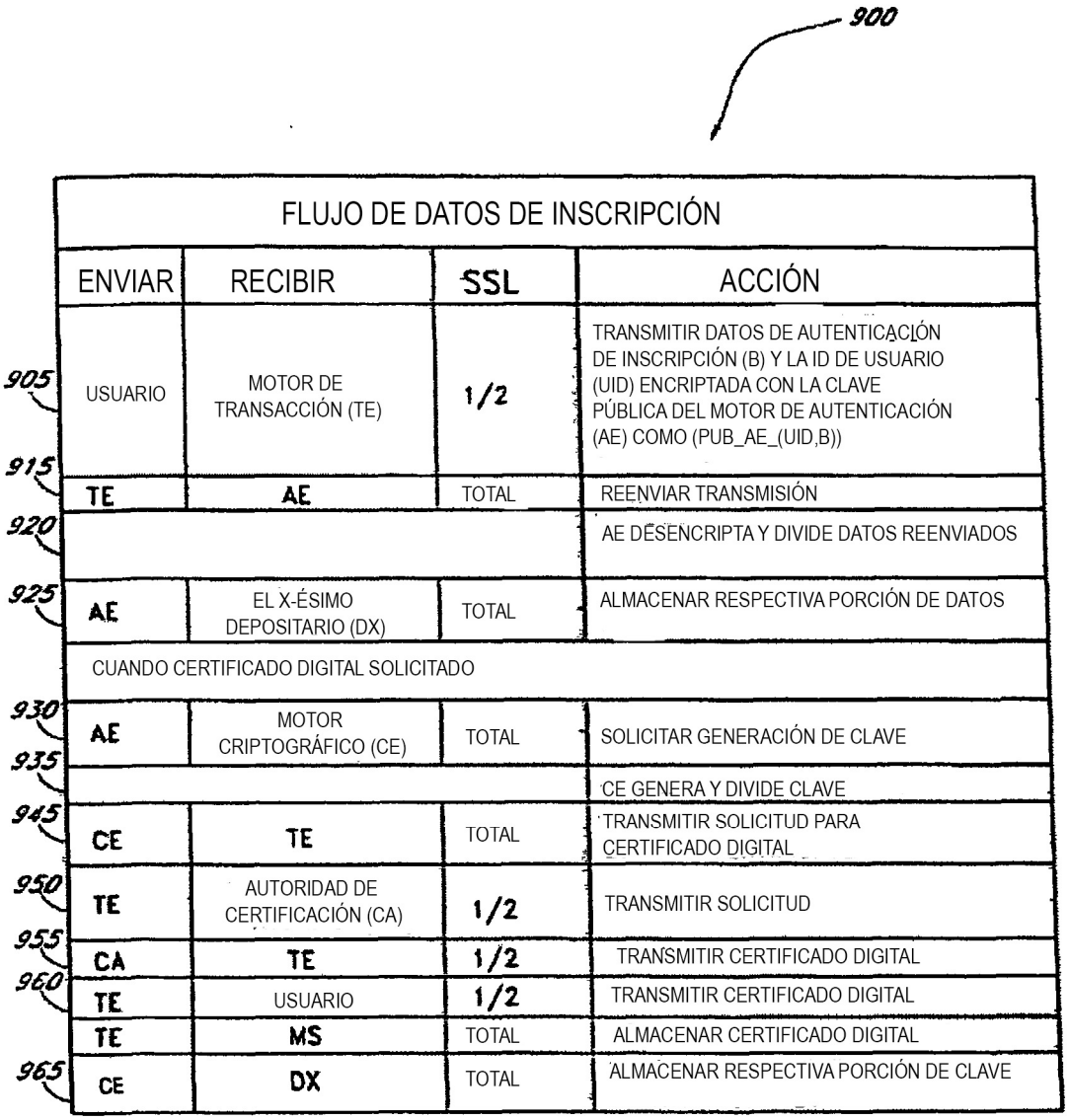

800
COMIENZO
S = DATOS RECIBIDOS
805
GENERAR NÚMERO ALEATORIO A
810
GENERAR NÚMERO ALEATORIO C
820
GENERAR B = A XOR S
825
GENERAR D = C XOR S
830
DISTRIBUIR A C, A D, B C, Y B D
835
FIN

Figura 9, Panel A



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))
TE	AE	TOTAL	REENVIAR TRANSMISIÓN
			AE DESENCRIPTA Y DIVIDE DATOS REENVIADOS
AE	EL X-ÉSIMO DEPOSITARIO (DX)	TOTAL	ALMACENAR RESPECTIVA PORCIÓN DE DATOS
CUANDO CERTIFICADO DIGITAL SOLICITADO			
AE	MOTOR CRIPTOGRÁFICO (CE)	TOTAL	SOLICITAR GENERACIÓN DE CLAVE
			CE GENERA Y DIVIDE CLAVE
CE	TE	TOTAL	TRANSMITIR SOLICITUD PARA CERTIFICADO DIGITAL
TE	AUTORIDAD DE CERTIFICACIÓN (CA)	1/2	TRANSMITIR SOLICITUD
CA	TE	1/2	TRANSMITIR CERTIFICADO DIGITAL
TE	USUARIO	1/2	TRANSMITIR CERTIFICADO DIGITAL
TE	MS	TOTAL	ALMACENAR CERTIFICADO DIGITAL
CE	DX	TOTAL	ALMACENAR RESPECTIVA PORCIÓN DE CLAVE

Figura 9, Panel B

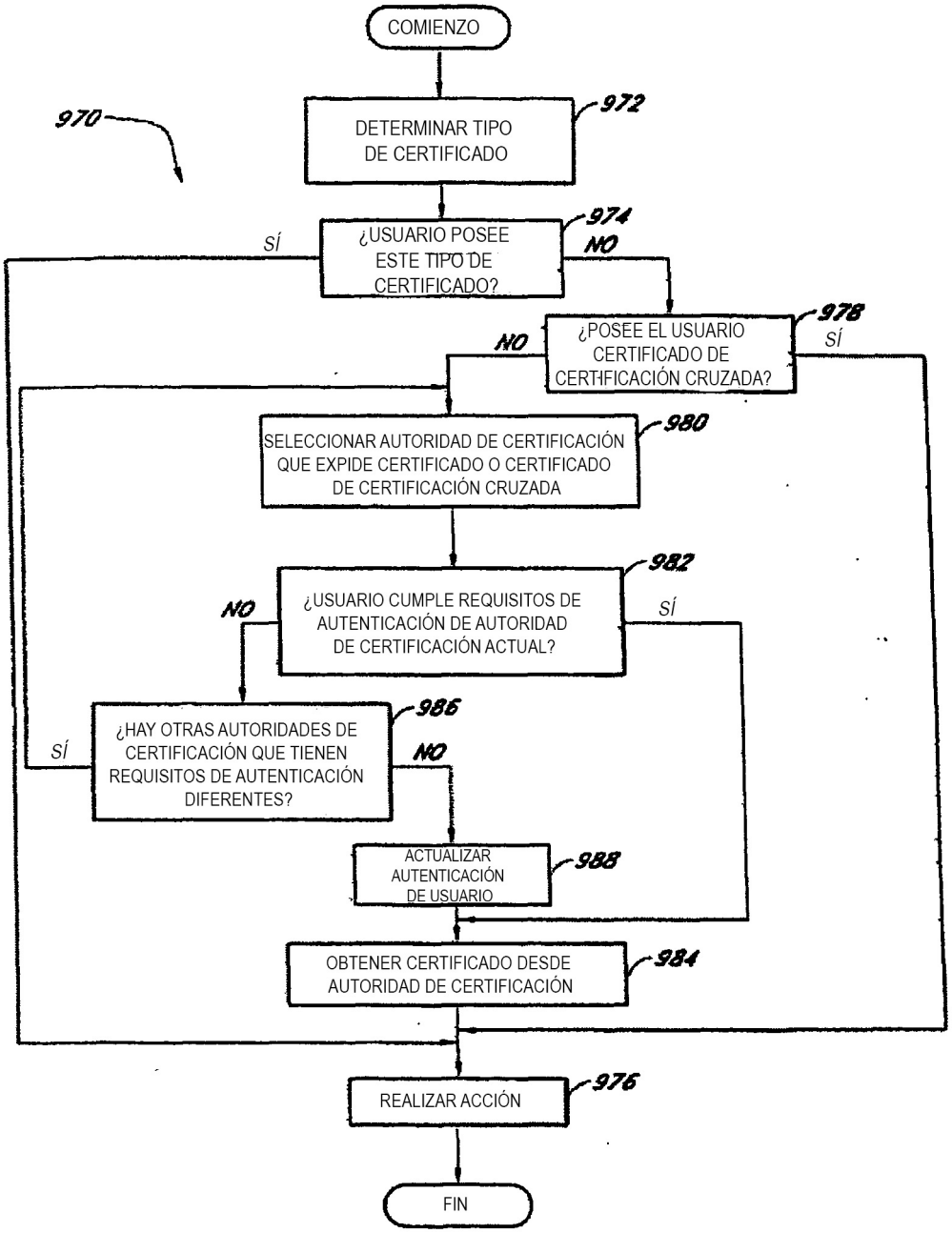
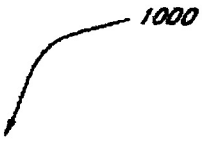


Figura 10



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 AUTENTICACION 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 DEPOSITARIO (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
1050				COMPARA CON B'
	AE	TE	TOTAL	TID, LO RELLENADO EN AR
	TE	DISTRIBUIDOR	TOTAL	TID, SÍ/NO
1055	TE	USUARIO	1/2	TID, MENSAJE DE CONFIRMACION

Figura 11

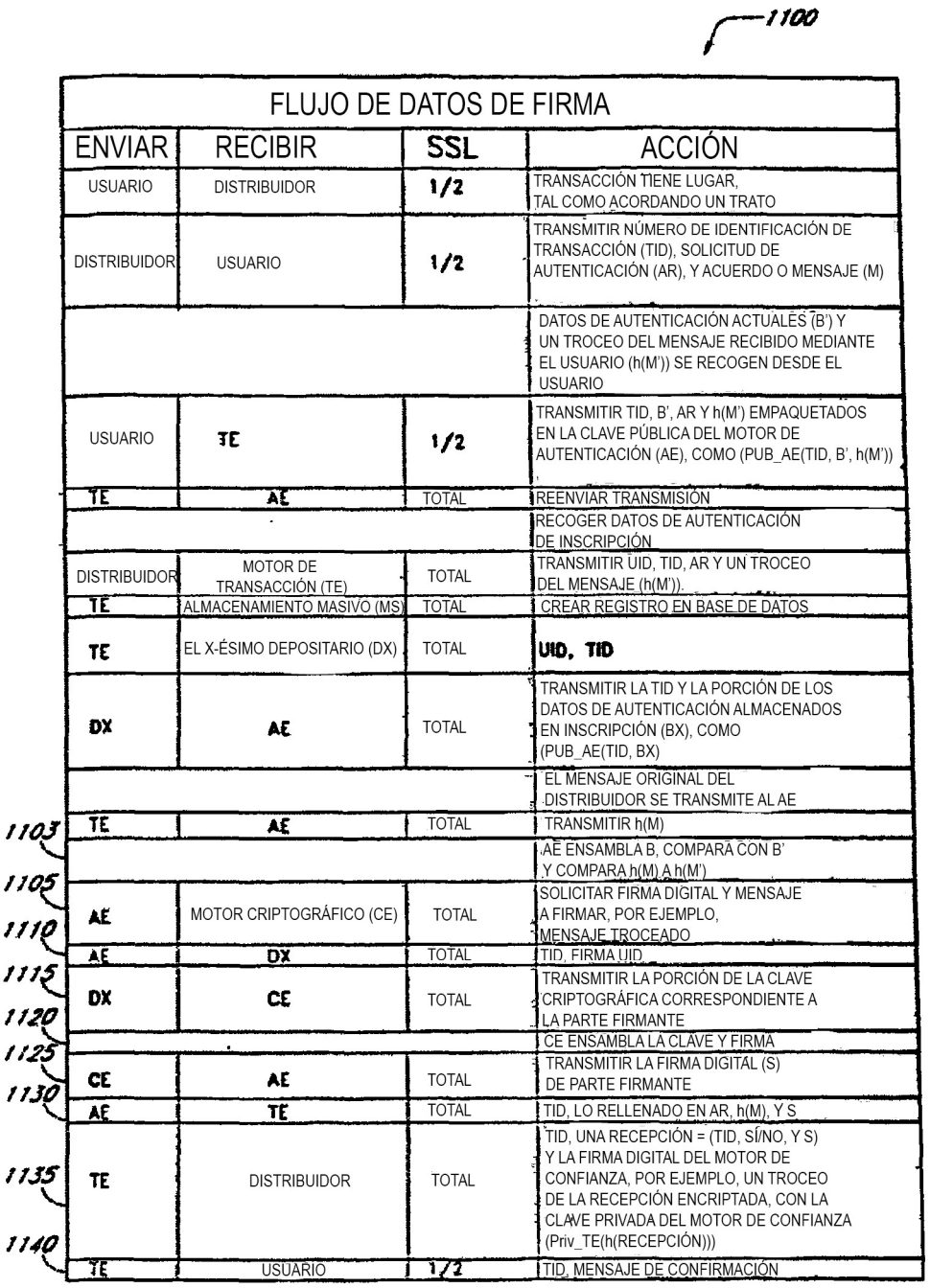

1100
FLUJO DE DATOS DE FIRMA
ENVIAR
RECIBIR
SSL
ACCIÓN
USUARIO
DISTRIBUIDOR
1/2
TRANSACCIÓN TIENE LUGAR, TAL COMO ACORDANDO UN TRATO
DISTRIBUIDOR
USUARIO
1/2
TRANSMITIR NÚMERO DE IDENTIFICACIÓN DE TRANSACCIÓN (TID), SOLICITUD DE AUTENTICACIÓN (AR), Y ACUERDO O MENSAJE (M)
DATOS DE AUTENTICACIÓN ACTUALES (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
ALMACENAMIENTO MASIVO (MS)
TOTAL
CREAR REGISTRO EN BASE DE DATOS
TE
EL X-ÉSIMO DEPOSITARIO (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
1103
TE
AE
TOTAL
TRANSMITIR h(M)
AE ENSAMBLA B, COMPARA CON B' Y COMPARA h(M) A h(M')
1105
1110
AE
MOTOR CRIPTOGRÁFICO (CE)
TOTAL
SOLICITAR FIRMA DIGITAL Y MENSAJE A FIRMAR, POR EJEMPLO, MENSAJE TROCEADO
AE
DX
TOTAL
TID, FIRMA UID
1115
1120
DX
CE
TOTAL
TRANSMITIR LA PORCIÓN DE LA CLAVE CRIPTOGRÁFICA CORRESPONDIENTE A LA PARTE FIRMANTE
1125
CE ENSAMBLA LA CLAVE Y FIRMA
1130
CE
AE
TOTAL
TRANSMITIR LA FIRMA DIGITAL (S) DE PARTE FIRMANTE
AE
TE
TOTAL
TID, LO RELLENADO EN AR, h(M), Y S
1135
1140
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)))
TE
USUARIO
1/2
TID, MENSAJE DE CONFIRMACIÓN

Figura 12

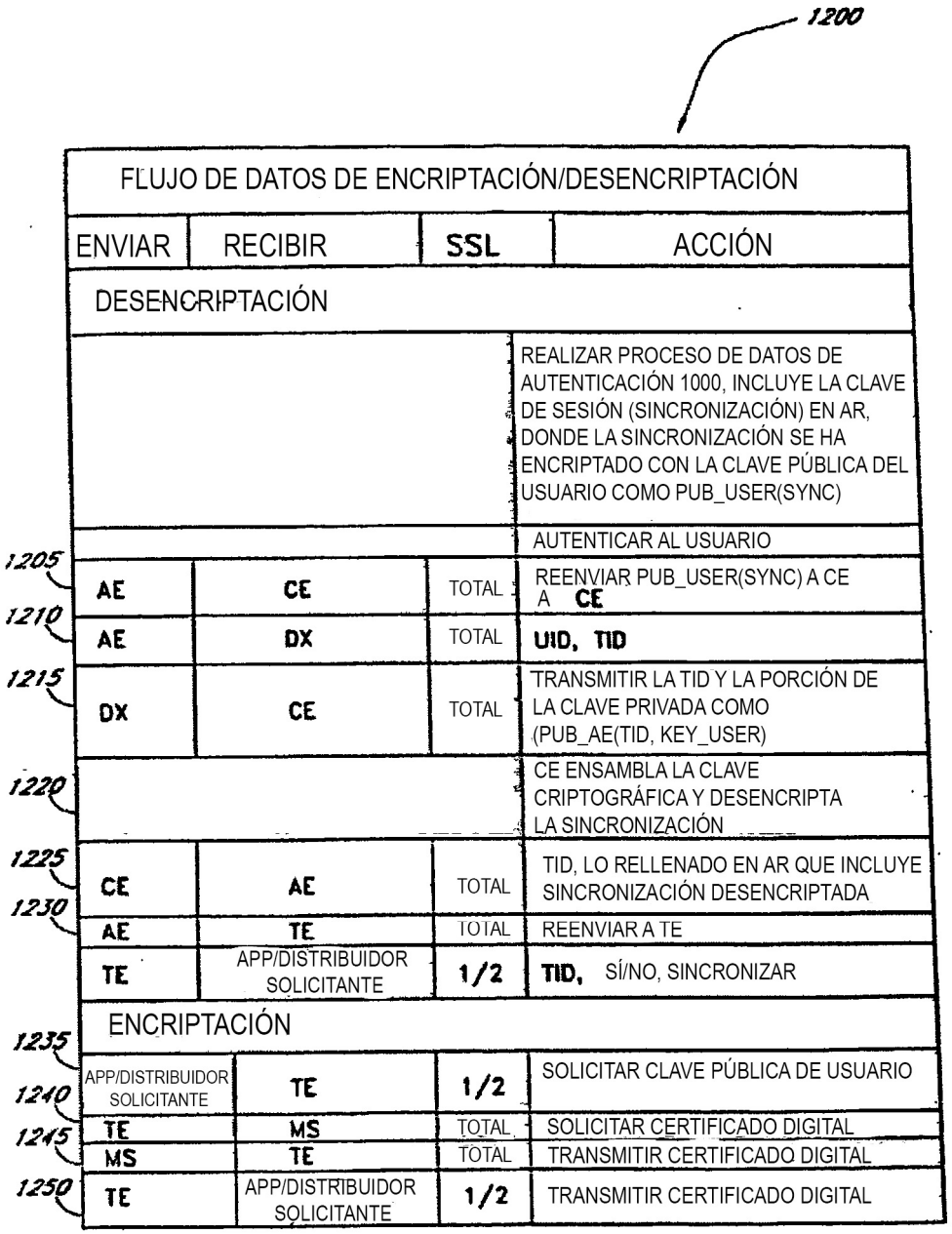

1200
FLUJO DE DATOS DE ENCRIPTACIÓN/DESENCRIPTACIÓN
ENVIAR
RECIBIR
SSL
ACCIÓN
DESENCRIPTACIÓN
REALIZAR PROCESO DE DATOS DE AUTENTICACIÓN 1000, INCLUYE LA CLAVE DE SESIÓN (SINCRONIZACIÓN) EN AR, DONDE LA SINCRONIZACIÓN SE HA ENCRIPTADO CON LA CLAVE PÚBLICA DEL USUARIO COMO PUB_USER(SYNC)
AUTENTICAR AL USUARIO
1205
AE
CE
TOTAL
REENVIAR PUB_USER(SYNC) A CE A CE
1210
AE
DX
TOTAL
UID, TID
1215
DX
CE
TOTAL
TRANSMITIR LA TID Y LA PORCIÓN DE LA CLAVE PRIVADA COMO (PUB_AE(TID, KEY_USER)
1220
CE ENSAMBLA LA CLAVE CRIPTOGRÁFICA Y DESENCRIPTA LA SINCRONIZACIÓN
1225
CE
AE
TOTAL
TID, LO RELLENADO EN AR QUE INCLUYE SINCRONIZACIÓN DESENCRIPTADA
1230
AE
TE
TOTAL
REENVIAR A TE
TE
APP/DISTRIBUIDOR SOLICITANTE
1/2
TID, SÍ/NO, SINCRONIZAR
ENCRIPTACIÓN
1235
APP/DISTRIBUIDOR SOLICITANTE
TE
1/2
SOLICITAR CLAVE PÚBLICA DE USUARIO
1240
TE
MS
TOTAL
SOLICITAR CERTIFICADO DIGITAL
1245
MS
TE
TOTAL
TRANSMITIR CERTIFICADO DIGITAL
1250
TE
APP/DISTRIBUIDOR SOLICITANTE
1/2
TRANSMITIR CERTIFICADO DIGITAL

Figura 13

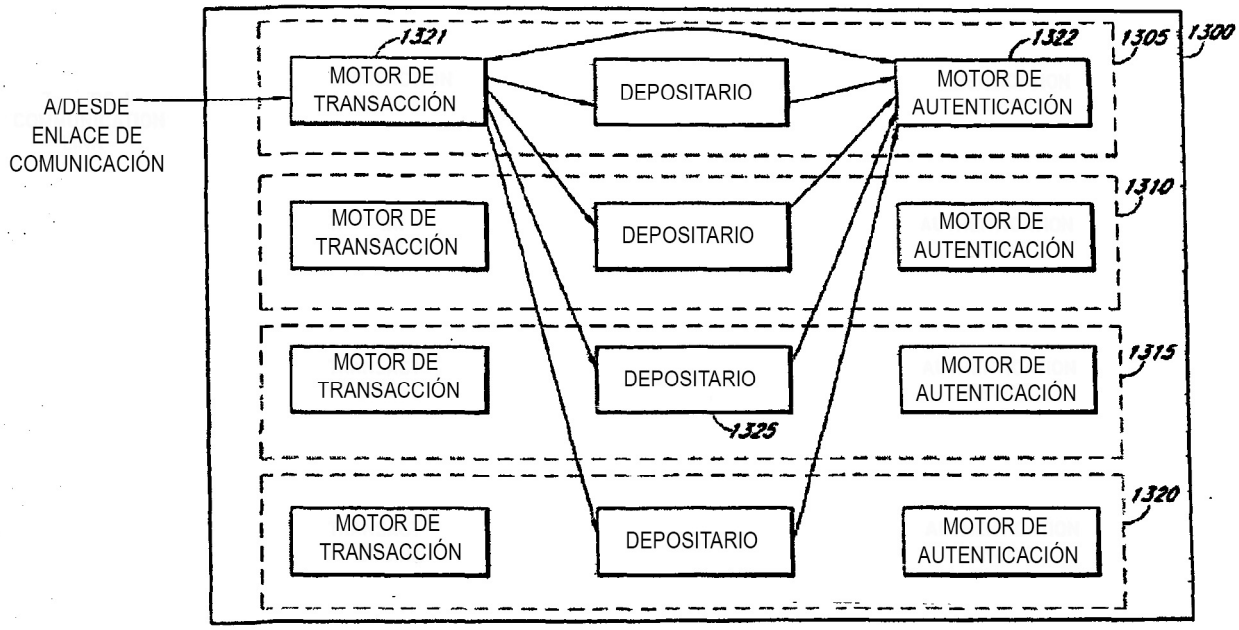

A/DESDE ENLACE DE COMUNICACIÓN
1321
MOTOR DE TRANSACCIÓN
DEPOSITARIO
1322
MOTOR DE AUTENTICACIÓN
1305
1300
MOTOR DE TRANSACCIÓN
DEPOSITARIO
MOTOR DE AUTENTICACIÓN
1310
MOTOR DE TRANSACCIÓN
DEPOSITARIO
MOTOR DE AUTENTICACIÓN
1315
1325
MOTOR DE TRANSACCIÓN
DEPOSITARIO
MOTOR DE AUTENTICACIÓN
1320

Figura 14

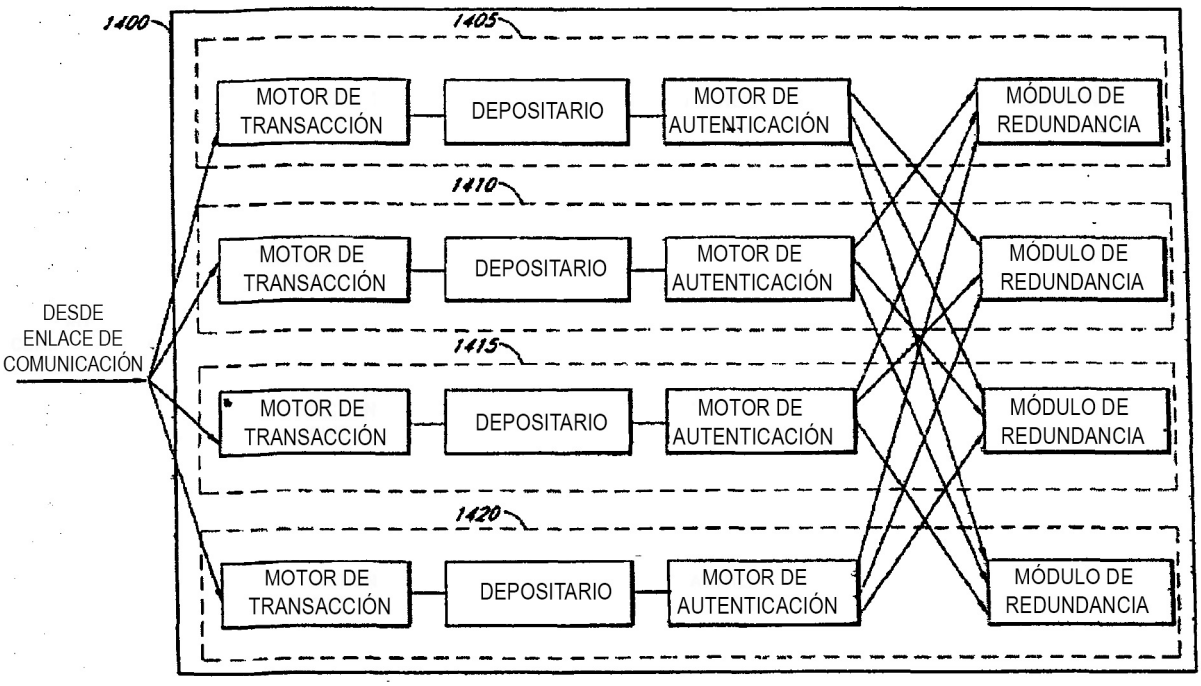

1400
1405
MOTOR DE TRANSACCIÓN
DEPOSITARIO
MOTOR DE AUTENTICACIÓN
MÓDULO DE REDUNDANCIA
1410
MOTOR DE TRANSACCIÓN
DEPOSITARIO
MOTOR DE AUTENTICACIÓN
MÓDULO DE REDUNDANCIA
DESDE ENLACE DE COMUNICACIÓN
1415
MOTOR DE TRANSACCIÓN
DEPOSITARIO
MOTOR DE AUTENTICACIÓN
MÓDULO DE REDUNDANCIA
1420
MOTOR DE TRANSACCIÓN
DEPOSITARIO
MOTOR DE AUTENTICACIÓN
MÓDULO DE REDUNDANCIA

Figura 15

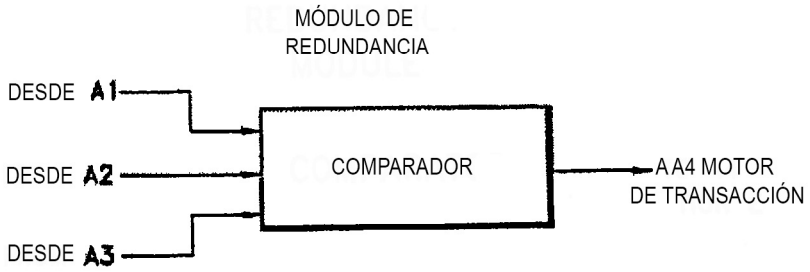

MÓDULO DE
REDUNDANCIA
DESDE A1
DESDE A2
DESDE A3
COMPARADOR
A A4 MOTOR
DE TRANSACCIÓN

Figura 16

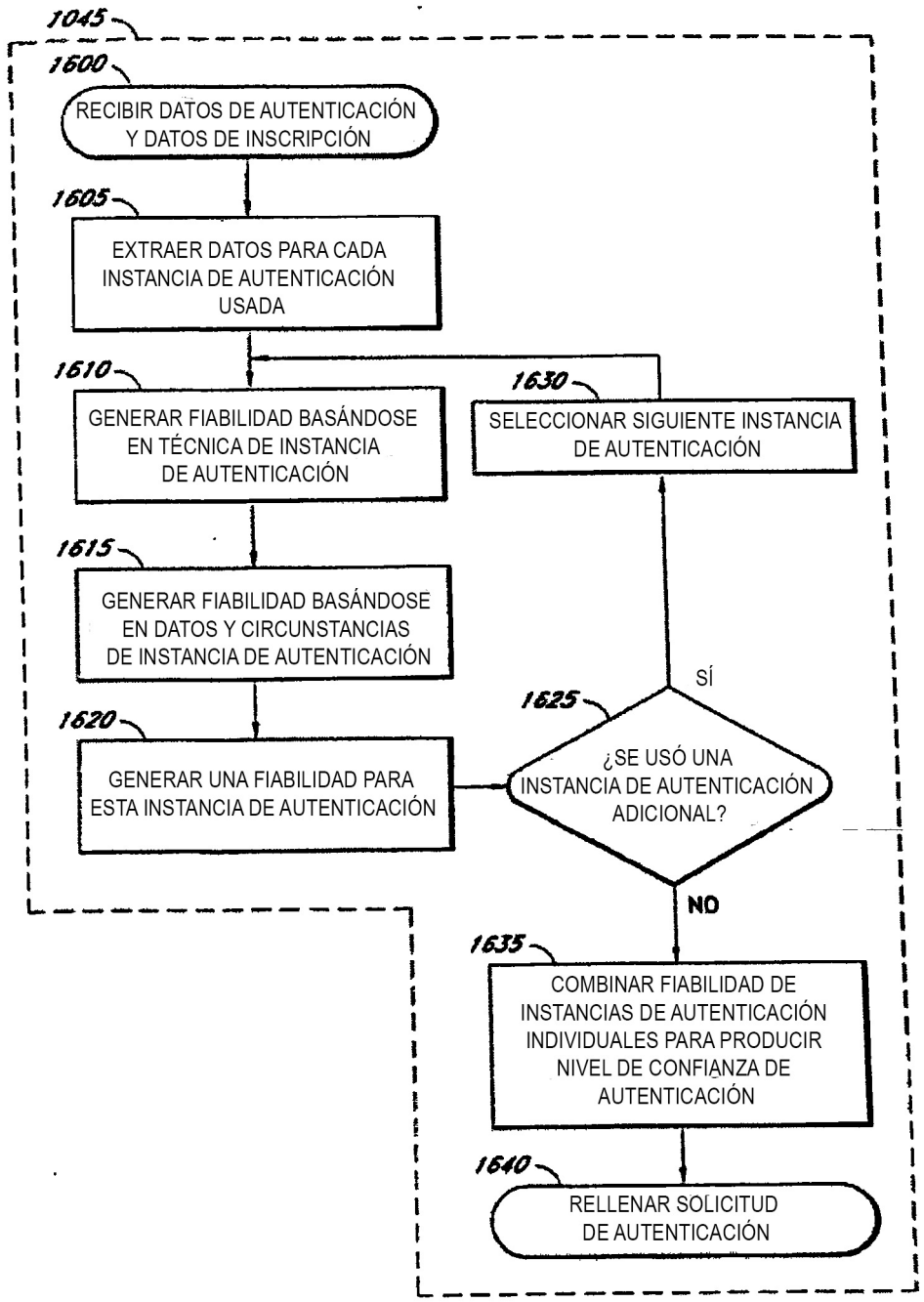

1045
1600
RECIBIR DATOS DE AUTENTICACIÓN Y DATOS DE INSCRIPCIÓN
1605
EXTRAER DATOS PARA CADA INSTANCIA DE AUTENTICACIÓN USADA
1610
GENERAR FIABILIDAD BASÁNDOSE EN TÉCNICA DE INSTANCIA DE AUTENTICACIÓN
1615
GENERAR FIABILIDAD BASÁNDOSE EN DATOS Y CIRCUNSTANCIAS DE INSTANCIA DE AUTENTICACIÓN
1620
GENERAR 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

Figura 17

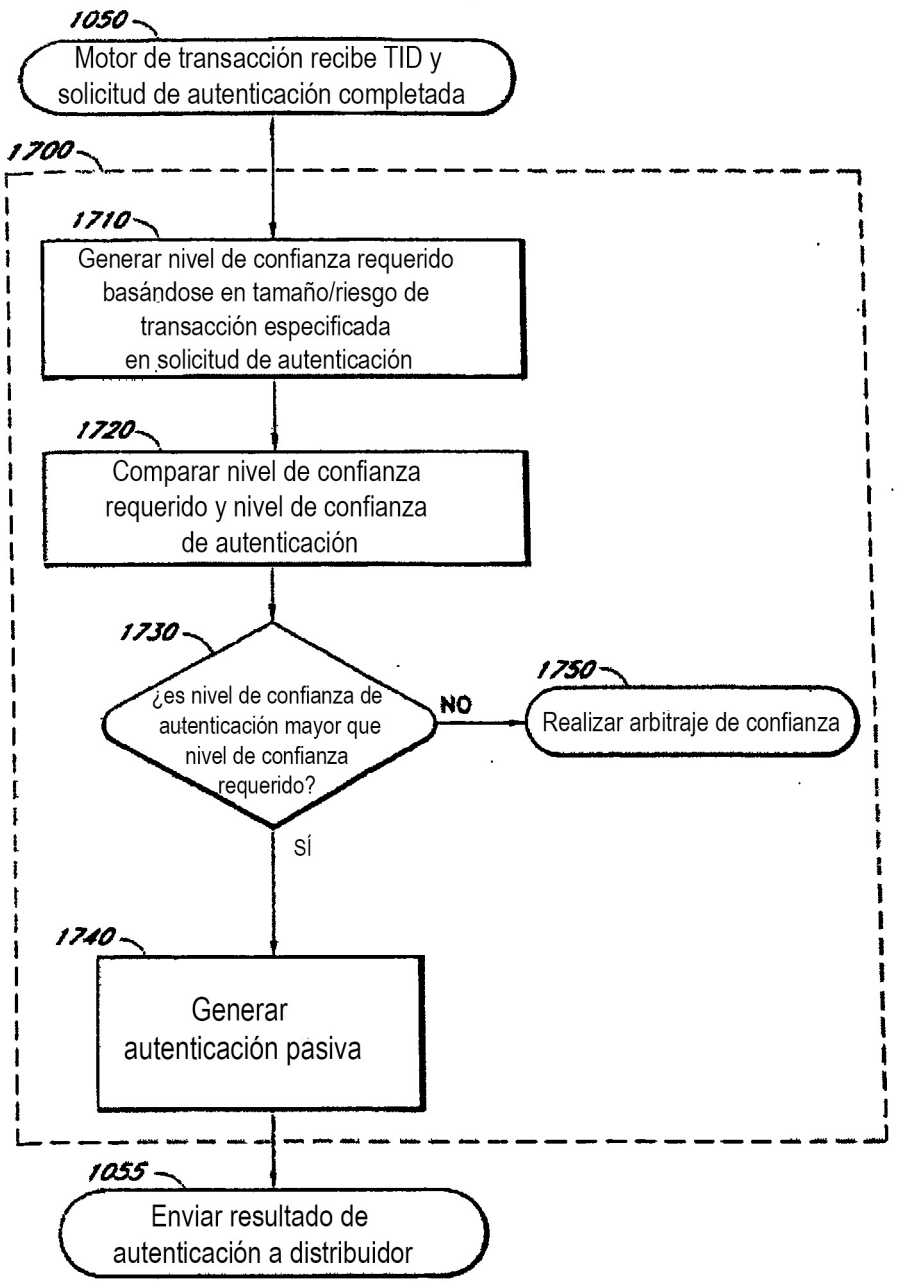

1050
Motor de transacción recibe TID y solicitud de autenticación completada
1700
1710
Generar nivel de confianza requerido basándose en tamaño/riesgo de transacción especificada en solicitud de autenticación
1720
Comparar nivel de confianza requerido y nivel de confianza de autenticación
1730
¿es nivel 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

Figura 18

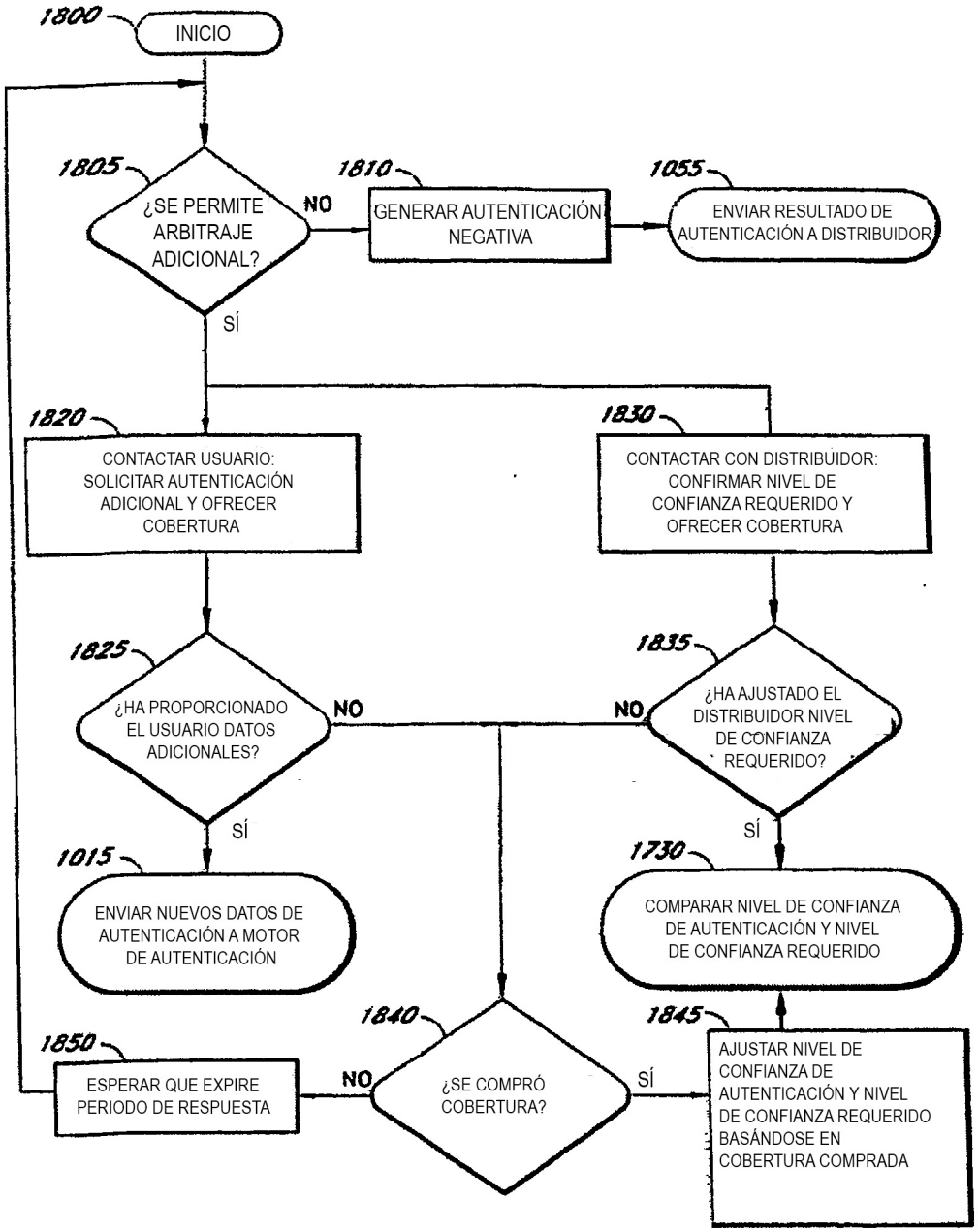

1800
INICIO
1805
¿SE PERMITE ARBITRAJE ADICIONAL?
NO
1810
GENERAR AUTENTICACIÓN NEGATIVA
1055
ENVIAR RESULTADO DE AUTENTICACIÓN A DISTRIBUIDOR
SÍ
1820
CONTACTAR USUARIO: SOLICITAR AUTENTICACIÓN ADICIONAL Y OFRECER COBERTURA
1830
CONTACTAR CON DISTRIBUIDOR: CONFIRMAR NIVEL DE CONFIANZA REQUERIDO Y OFRECER COBERTURA
1825
¿HA PROPORCIONADO EL USUARIO DATOS ADICIONALES?
NO
1835
¿HA AJUSTADO EL DISTRIBUIDOR NIVEL DE CONFIANZA REQUERIDO?
NO
SÍ
SÍ
1015
ENVIAR NUEVOS DATOS DE AUTENTICACIÓN A MOTOR DE AUTENTICACIÓN
1730
COMPARAR NIVEL DE CONFIANZA DE AUTENTICACIÓN Y NIVEL DE CONFIANZA REQUERIDO
1840
¿SE COMPRÓ COBERTURA?
1845
AJUSTAR NIVEL DE CONFIANZA DE AUTENTICACIÓN Y NIVEL DE CONFIANZA REQUERIDO BASÁNDOSE EN COBERTURA COMPRADA
1850
ESPERAR QUE EXPIRE PERIODO DE RESPUESTA
NO
SÍ

Figura 19

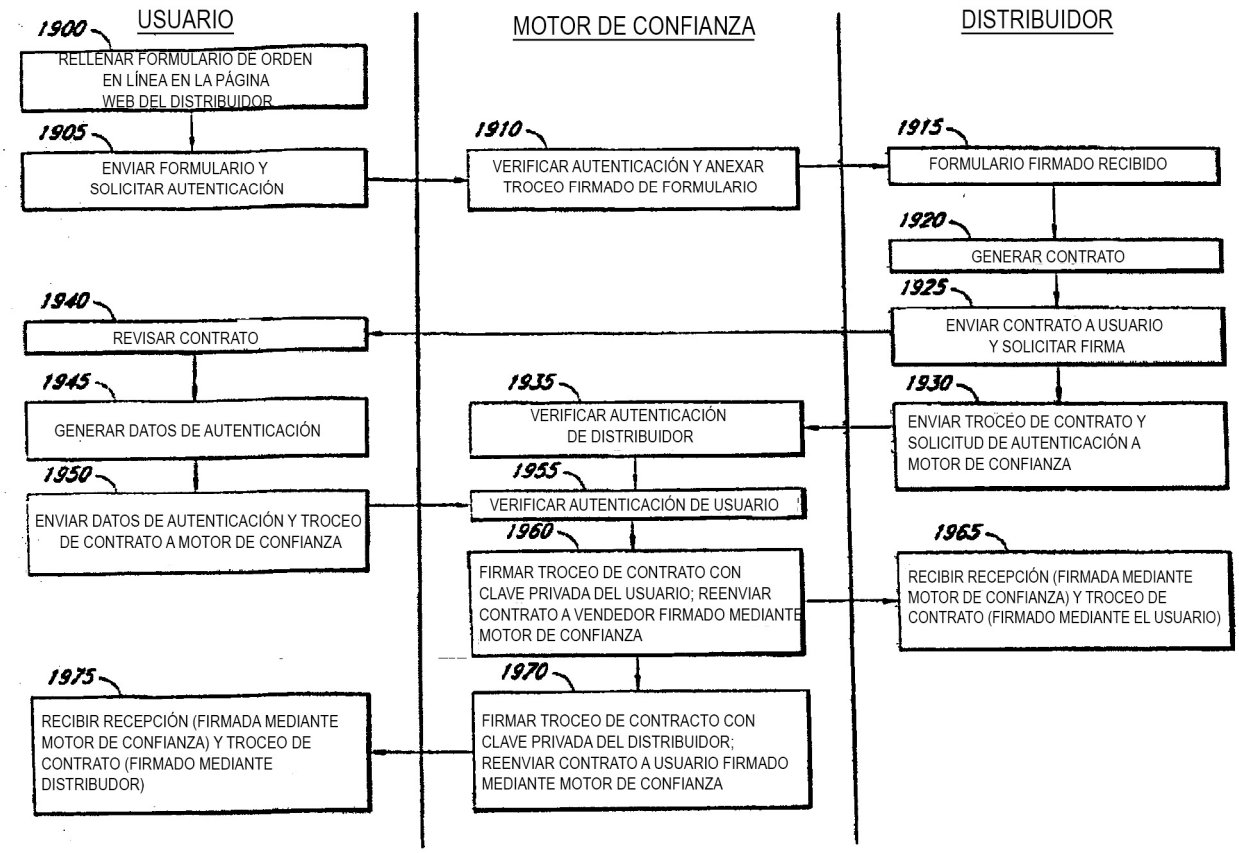

USUARIO
MOTOR DE CONFIANZA
DISTRIBUIDOR
1900
RELLENAR FORMULARIO DE ORDEN EN LÍNEA EN LA PÁGINA WEB DEL DISTRIBUIDOR
1905
ENVIAR FORMULARIO Y SOLICITAR AUTENTICACIÓN
1910
VERIFICAR AUTENTICACIÓN Y ANEXAR TROCEO FIRMADO DE FORMULARIO
1915
FORMULARIO FIRMADO RECIBIDO
1920
GENERAR CONTRATO
1925
ENVIAR CONTRATO 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 MEDIANTE MOTOR DE CONFIANZA
1965
RECIBIR RECEPCIÓN (FIRMADA MEDIANTE MOTOR DE CONFIANZA) Y TROCEO DE CONTRATO (FIRMADO MEDIANTE EL USUARIO)
1970
FIRMAR TROCEO DE CONTRACTO CON CLAVE PRIVADA DEL DISTRIBUIDOR; REENVIAR CONTRATO A USUARIO FIRMADO MEDIANTE MOTOR DE CONFIANZA
1975
RECIBIR RECEPCIÓN (FIRMADA MEDIANTE MOTOR DE CONFIANZA) Y TROCEO DE CONTRATO (FIRMADO MEDIANTE DISTRIBUDOR)

Figura 20

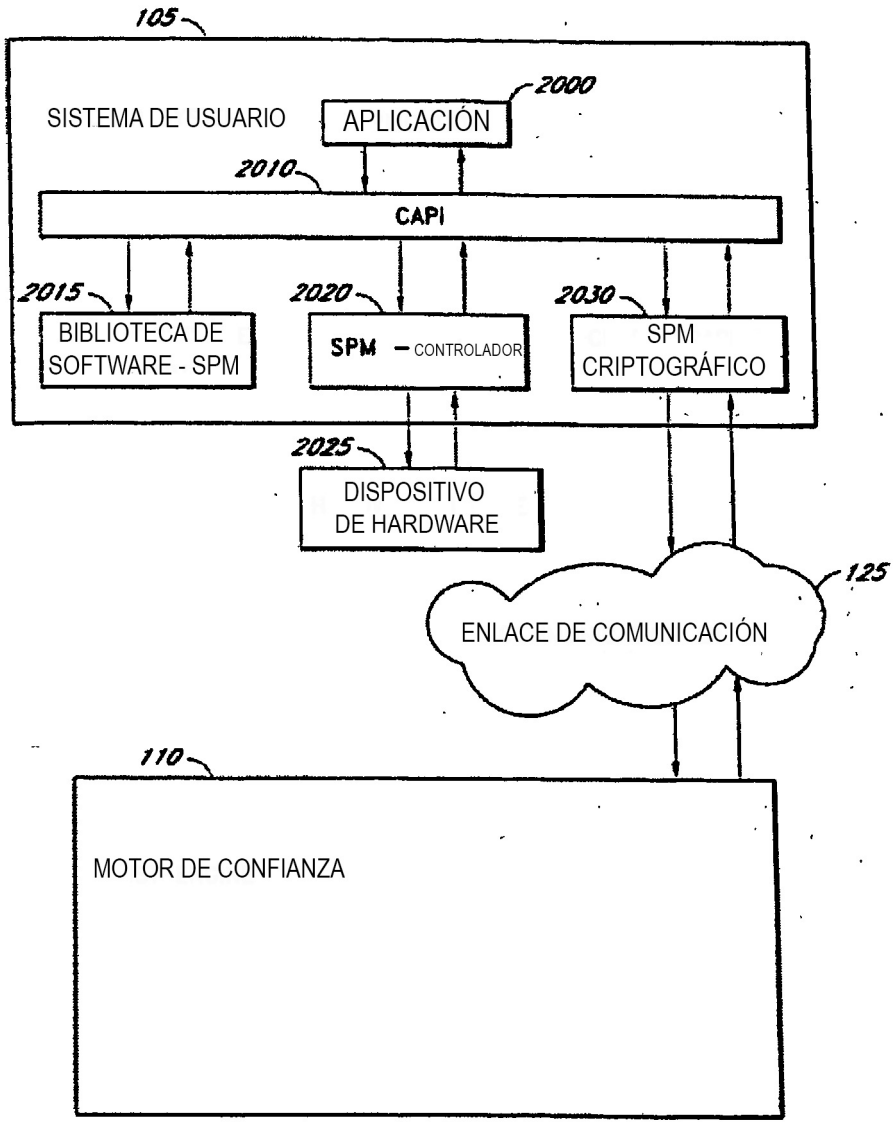

105
SISTEMA DE USUARIO
APLICACIÓN
2000
2010
CAPI
2015
BIBLIOTECA DE SOFTWARE - SPM
2020
SPM – CONTROLADOR
2030
SPM CRIPTOGRÁFICO
2025
DISPOSITIVO DE HARDWARE
125
ENLACE DE COMUNICACIÓN
110
MOTOR DE CONFIANZA

Figura 21

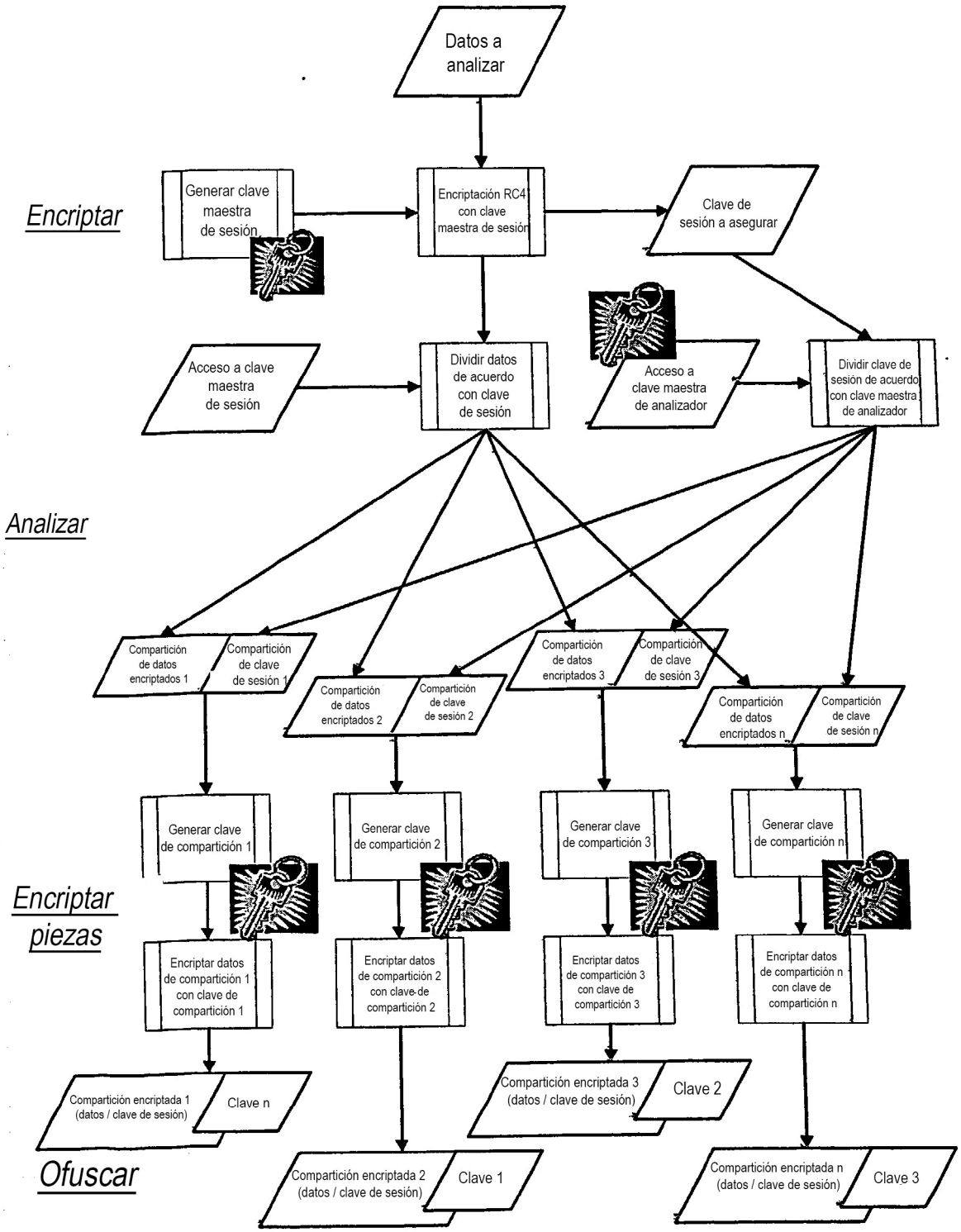

Datos a analizar
Encriptar
Generar clave maestra de sesión
Encriptación RC4 con clave maestra de sesión
Clave de sesión a asegurar
Acceso a clave maestra de sesión
Dividir datos de acuerdo con clave de sesión
Acceso a clave maestra de analizador
Dividir clave de sesión de acuerdo con clave maestra de 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
Encriptar piezas
Generar clave de compartición 1
Generar clave de compartición 2
Generar clave de compartición 3
Generar clave de compartición n
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

Figura 22

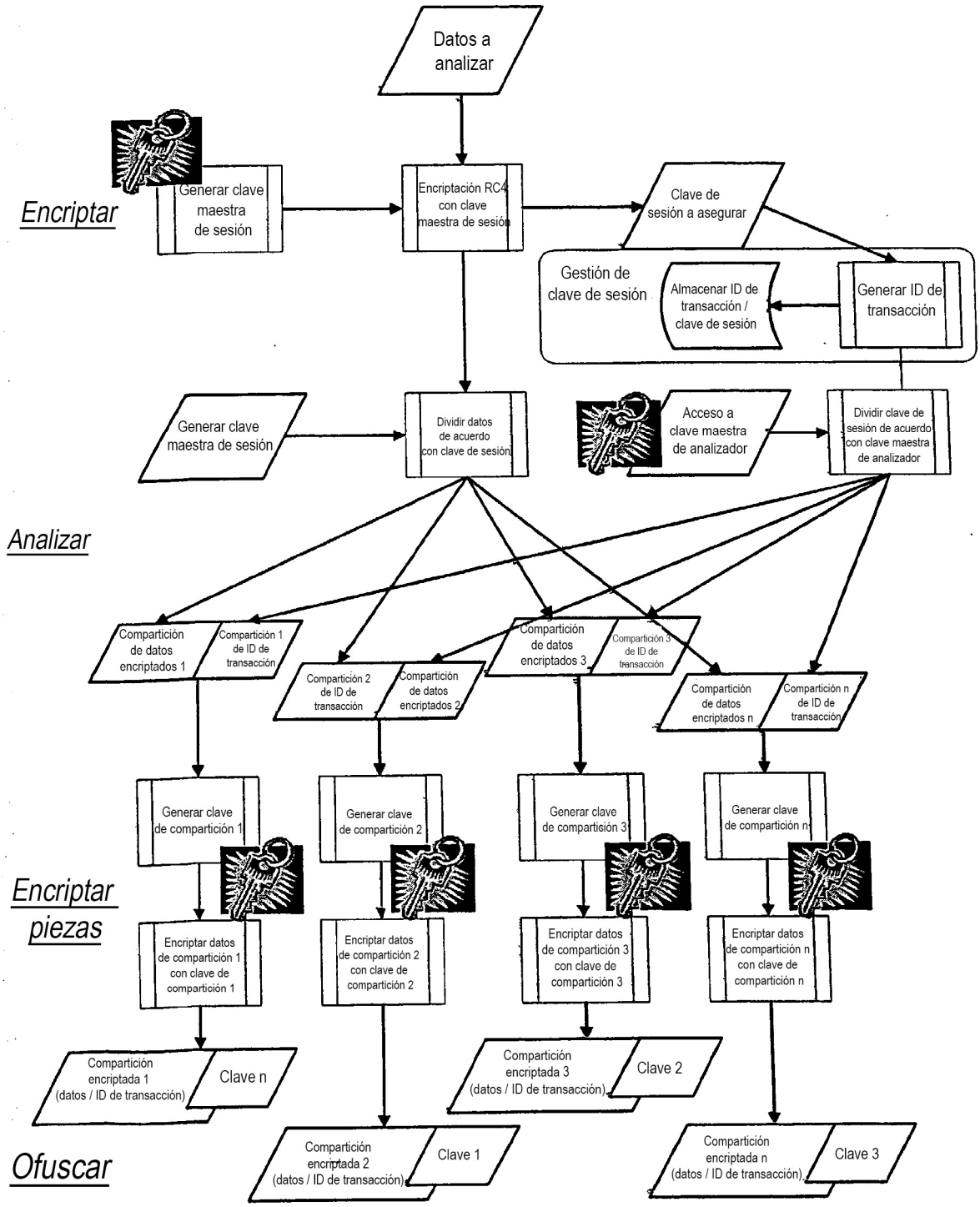

Datos a analizar
Encriptar
Generar clave maestra de sesión
Encriptación RC4 con clave maestra de sesión
Clave de sesión a asegurar
Gestión de clave de sesión
Almacenar ID de transacción / clave de sesión
Generar ID de transacción
Generar clave maestra de sesión
Dividir datos de acuerdo con clave de sesión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

Figura 23

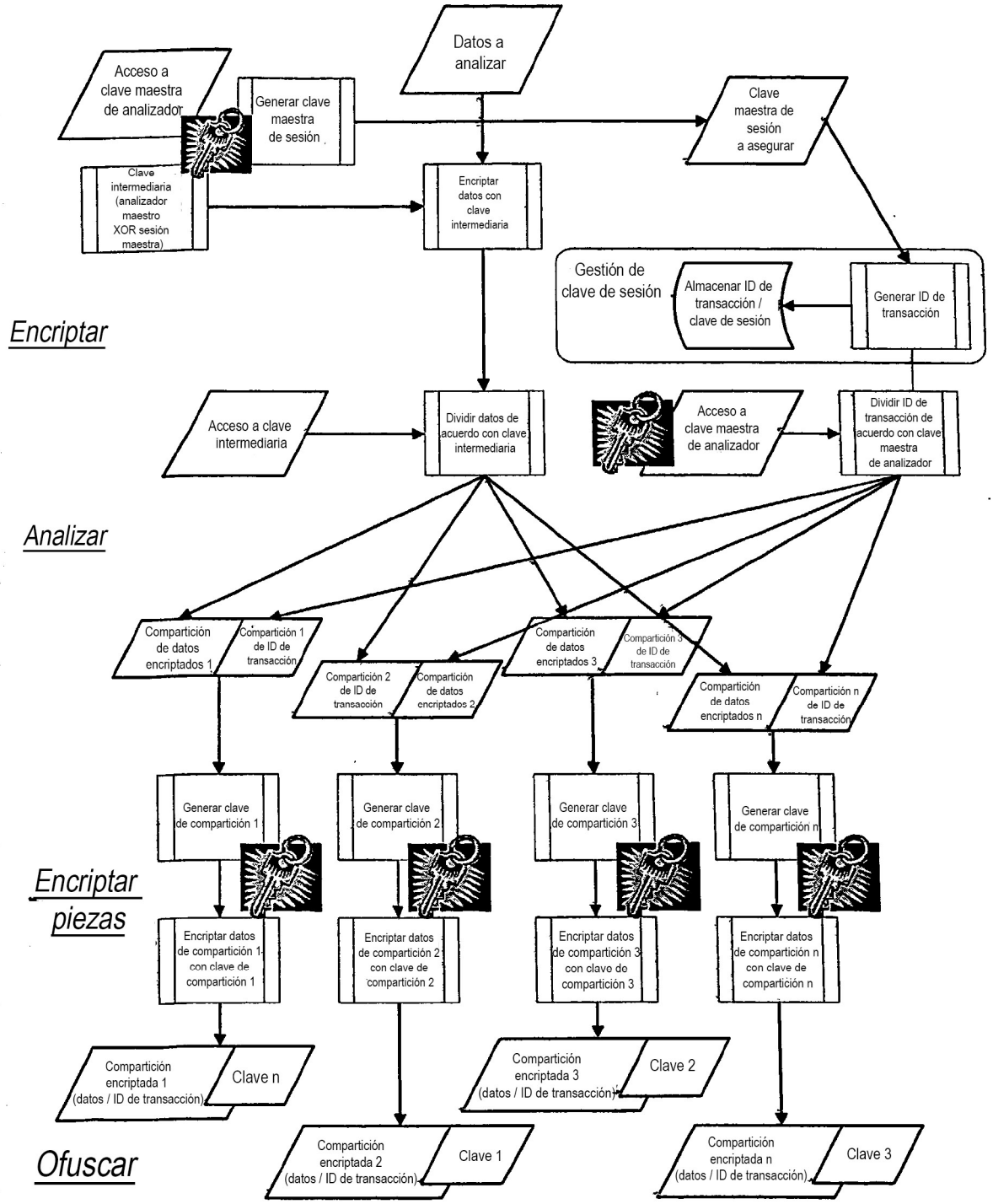

Datos a analizar
Acceso a clave maestra de analizador
Generar clave maestra de sesión
Clave maestra de sesión a asegurar
Clave intermediaria (analizador maestro XOR sesión maestra)
Encriptar datos con clave intermediaria
Gestión de clave de sesión
Almacenar ID de transacción / clave de sesión
Generar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

Figura 24

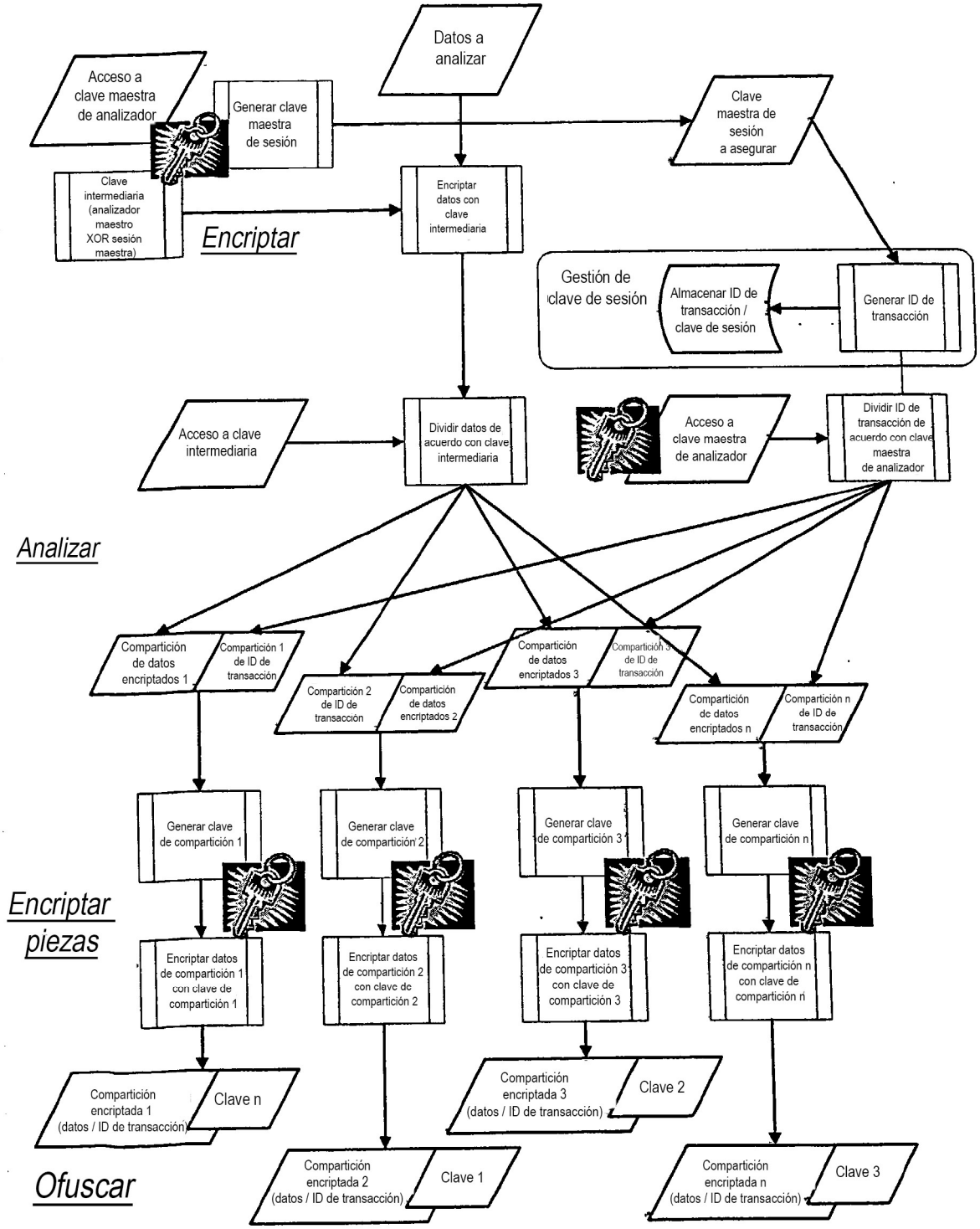
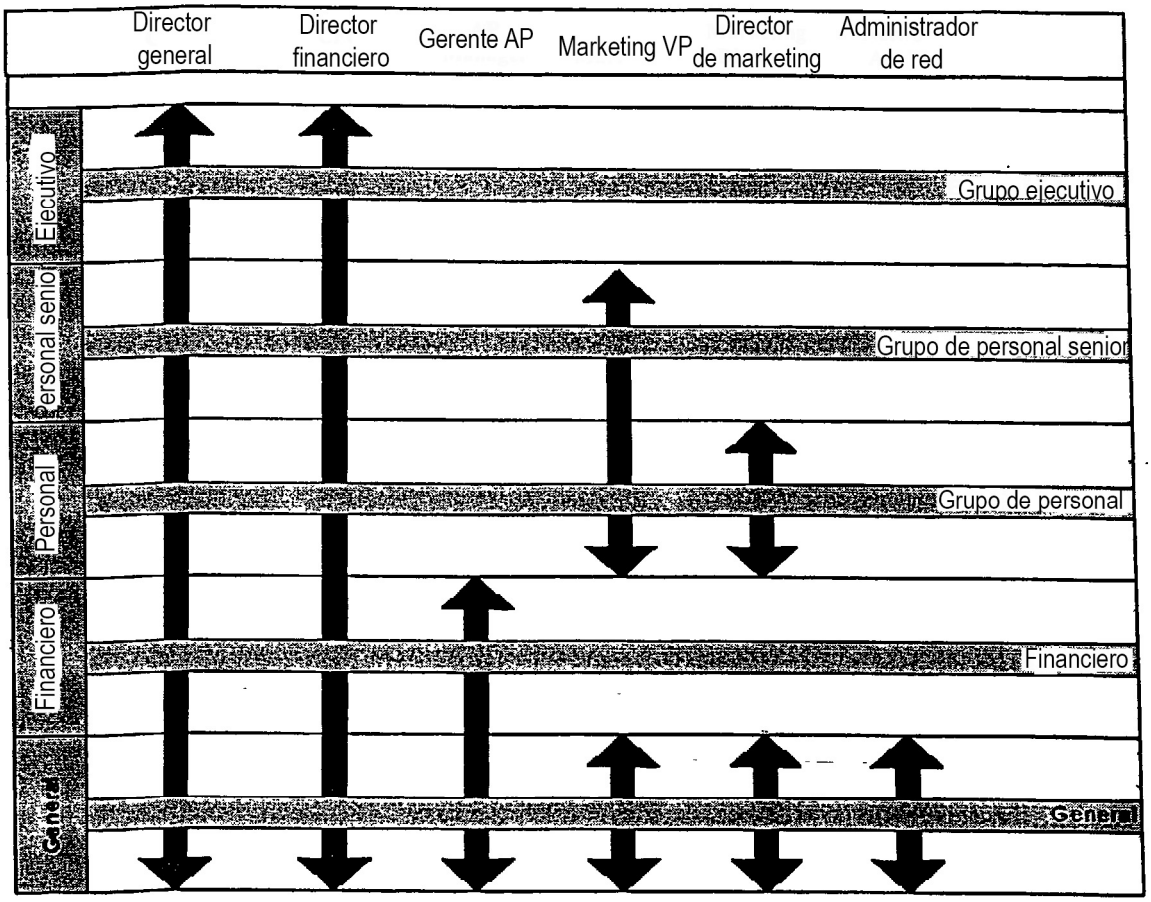

Datos a analizar
Acceso a clave maestra de analizador
Generar clave maestra de sesión
Clave maestra de sesión a asegurar
Clave intermediaria (analizador maestro XOR sesión maestra)
Encriptar datos con clave intermediaria
Encriptar
Gestión de clave de sesión
Almacenar ID de transacción / clave de sesión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

Figura 25


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

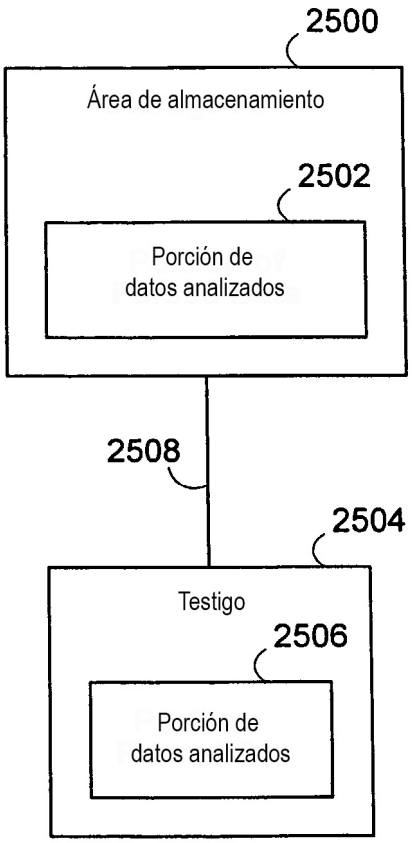

2500
Área de almacenamiento
2502
Porción de datos analizados
2508
2504
Testigo
2506
Porción de datos analizados

Figura 26

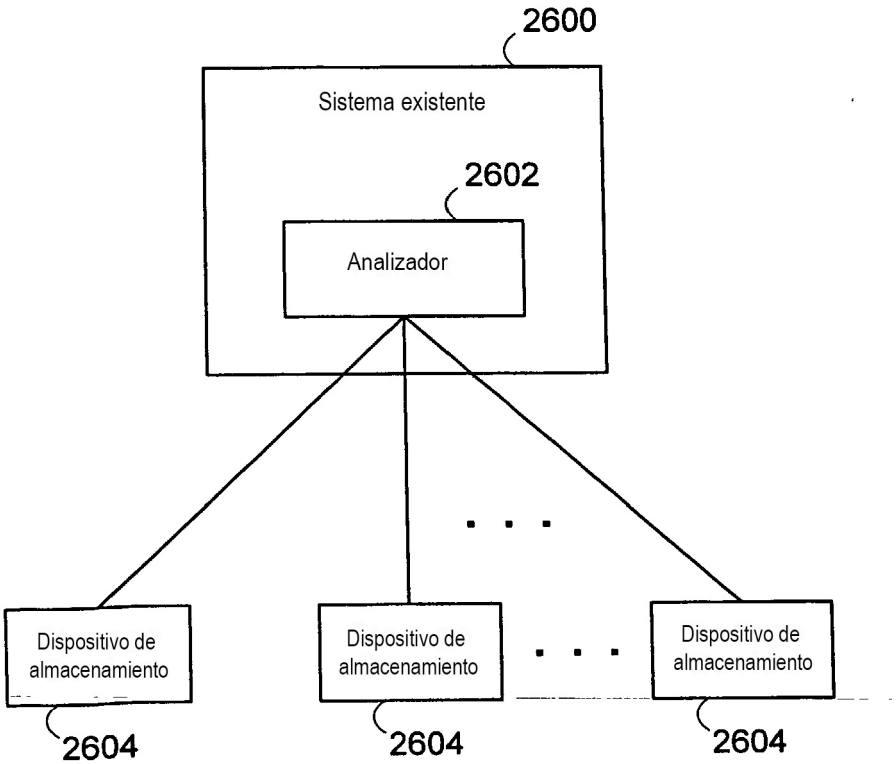

2600
Sistema existente
2602
Analizador
Dispositivo de almacenamiento
2604
Dispositivo de almacenamiento
2604
Dispositivo de almacenamiento
2604

Figura 27

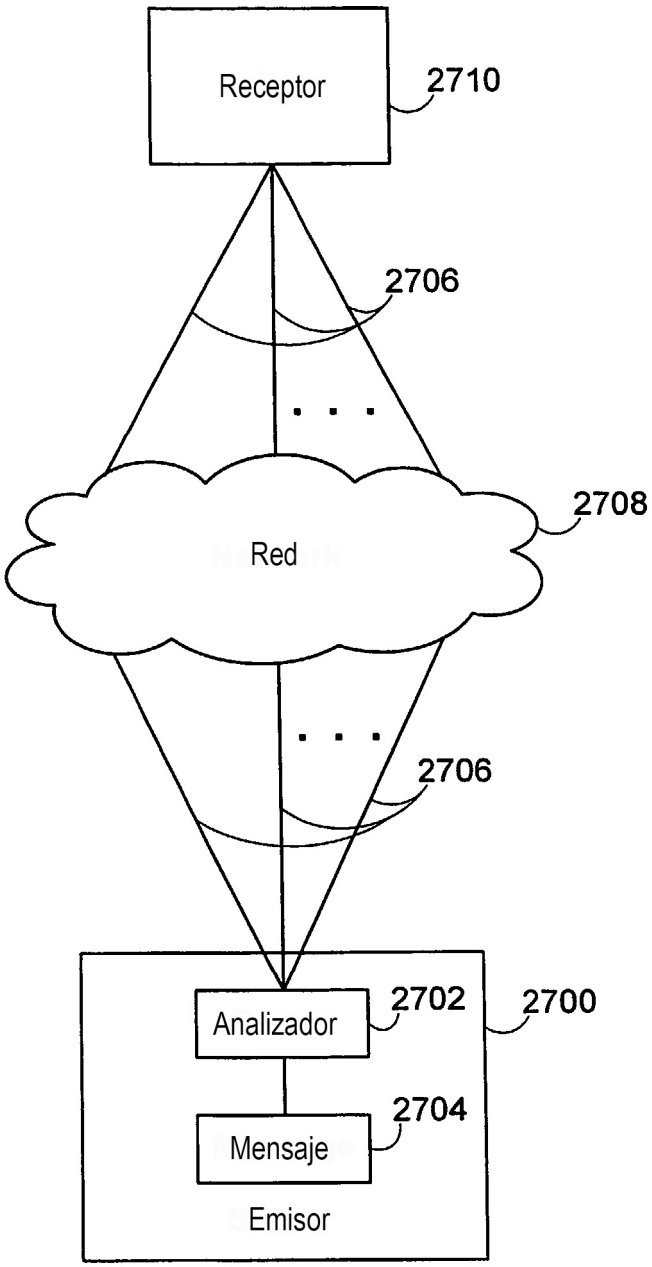

Receptor
2710
2706
2708
Red
2706
2702
2700
Analizador
2704
Mensaje
Emisor

Figura 28

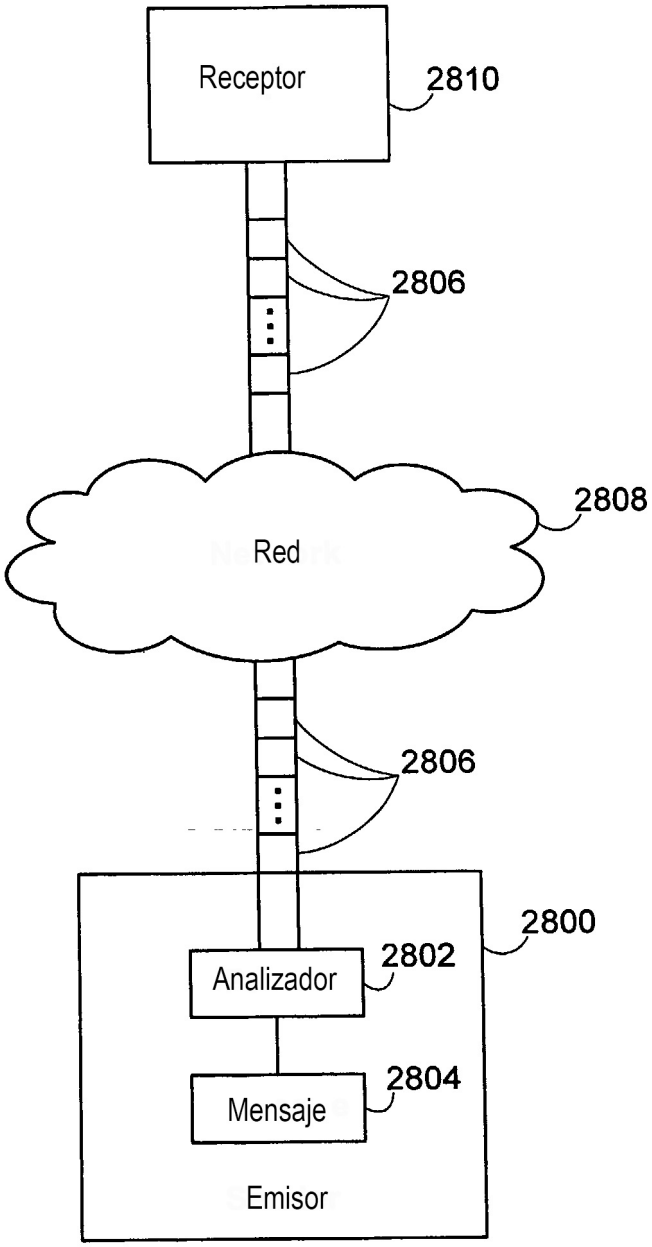

Receptor
2810
2806
2808
Red
2806
2800
Analizador
2802
Mensaje
2804
Emisor

Figura 29

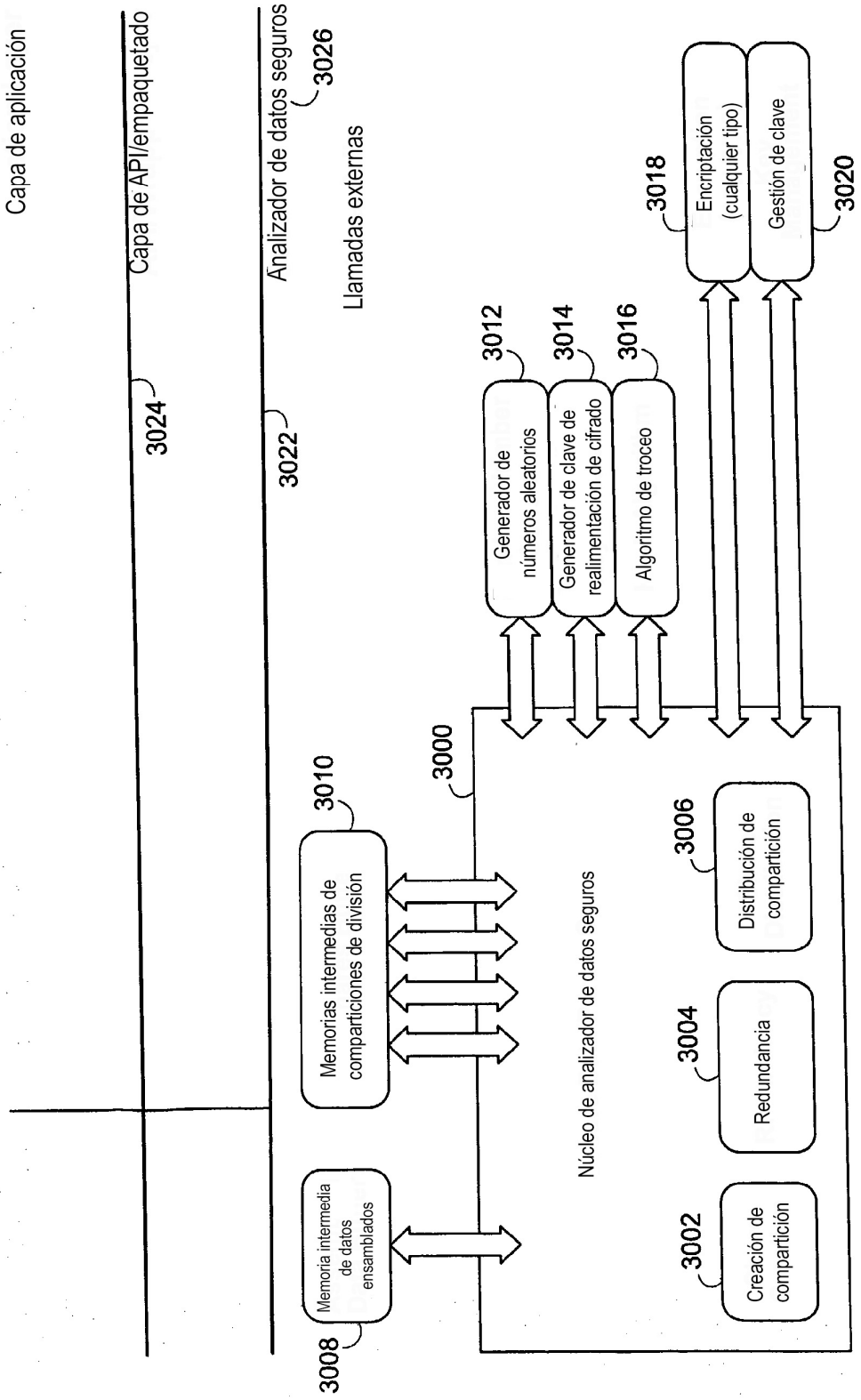

Capa de aplicación
Capa de API/empaquetado
Analizador de datos seguros
Llamadas externas
3024
3022
3026
3000
3008
Memoria intermedia de datos ensamblados
3010
Memorias intermedias de comparticiones de división
Núcleo de analizador de datos seguros
3002
Creación de compartición
3004
Redundancia
3006
Distribución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

Figura 30

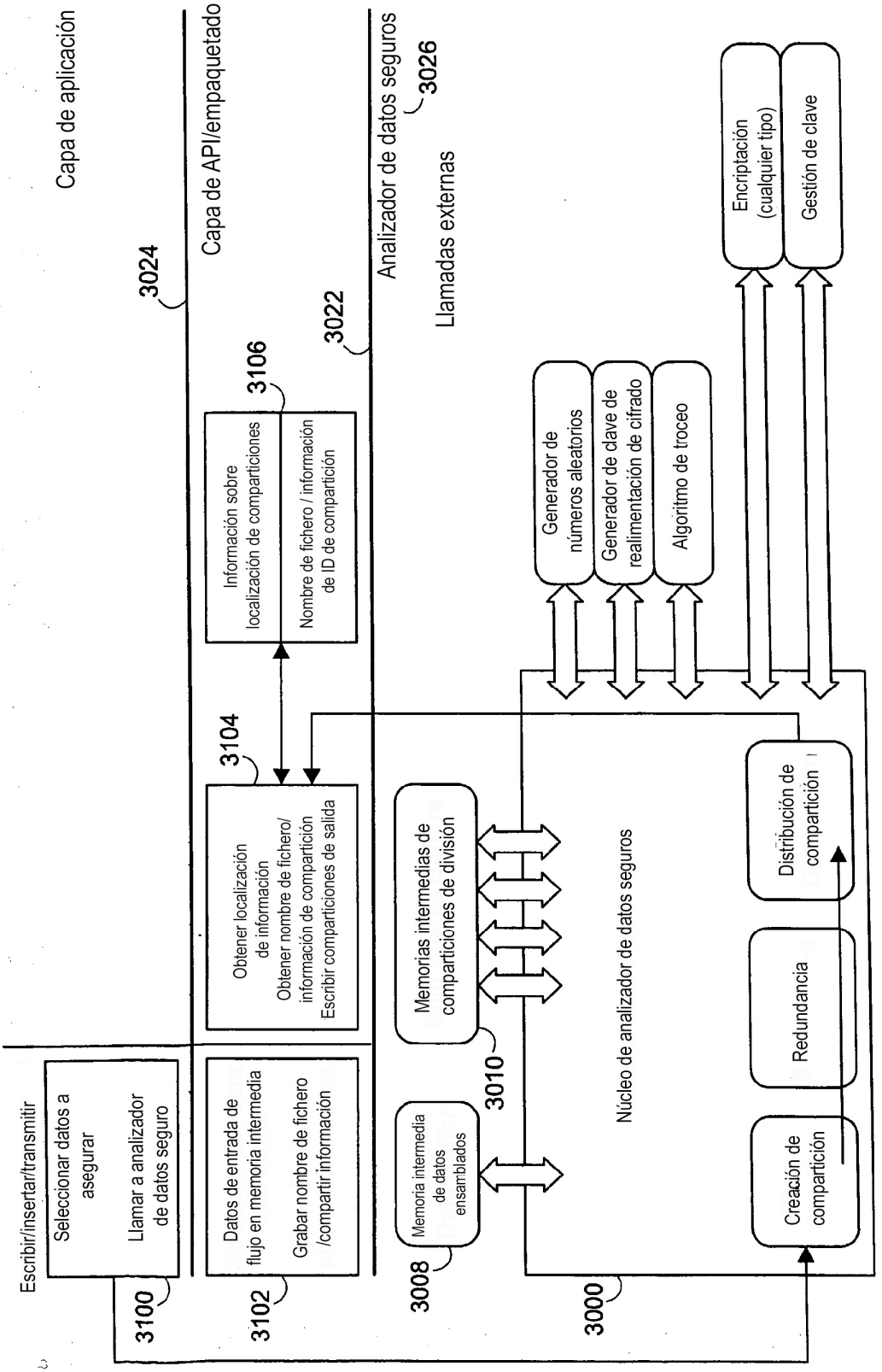

Capa de aplicación
Capa de API/empaquetado
Analizador de datos seguros
3026
Llamadas externas
3024
3022
3106
3104
Escribir/insertar/transmitir
Seleccionar datos a asegurar
Llamar a analizador de datos seguro
3100
Datos de entrada de flujo en memoria intermedia
Grabar nombre de fichero /compartir información
3102
Obtener localización de información
Obtener nombre de fichero/ información de compartición
Escribir comparticiones de salida
Información sobre localización de compartición
Nombre de fichero / información de ID de compartición
Memorias intermedias de compartición 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

Figura 31

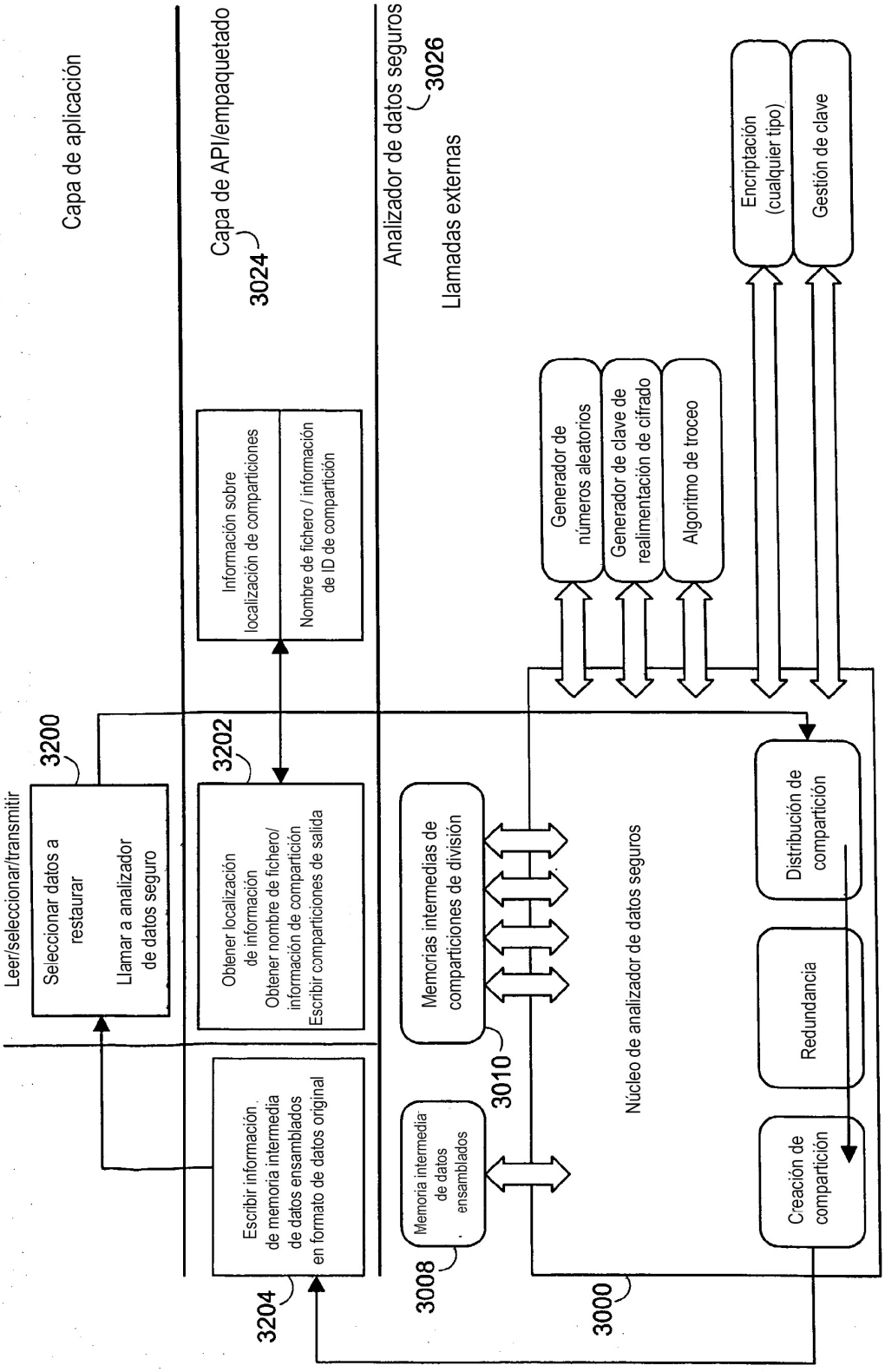

Capa de aplicación
Capa de API/empaquetado
3024
Analizador de datos seguros
3026
Llamadas externas
Leer/seleccionar/transmitir
3200
Seleccionar datos a restaurar
Llamar a analizador de datos seguro
3202
Obtener localización de información
Obtener nombre de fichero/ información de compartición
Escribir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

Figura 32

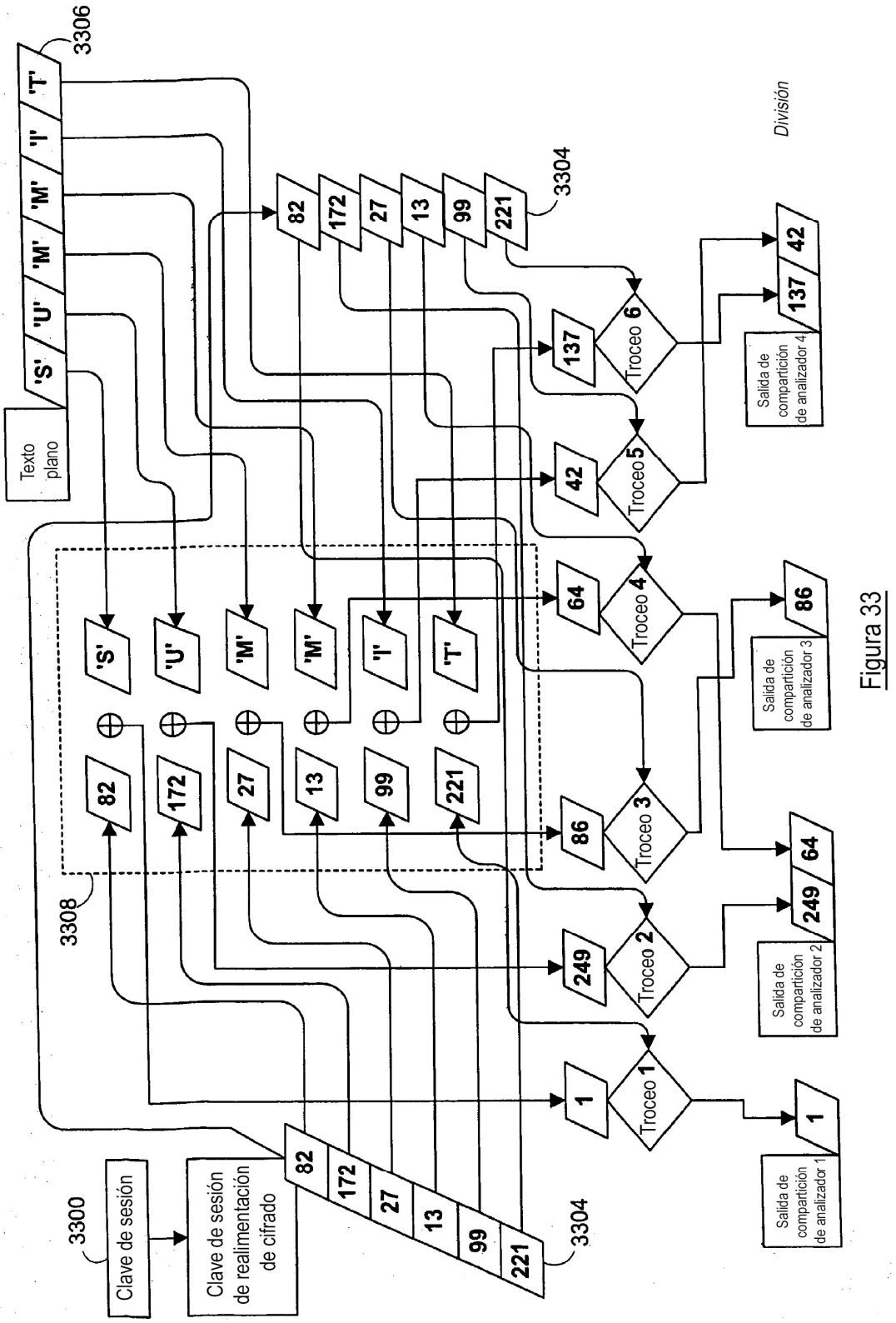

3306
'S' 'U' 'M' 'M' 'I' 'T'
Texto plano
3304
82 172 27 13 99 221
División
Troceo 6
Troceo 5
Troceo 4
Troceo 3
Troceo 2
Troceo 1
137 42
42
64
86
249 64
1
Salida de compartición de analizador 4
Salida de compartición de analizador 3
Salida de compartición de analizador 2
Salida de compartición de analizador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

Figura 33

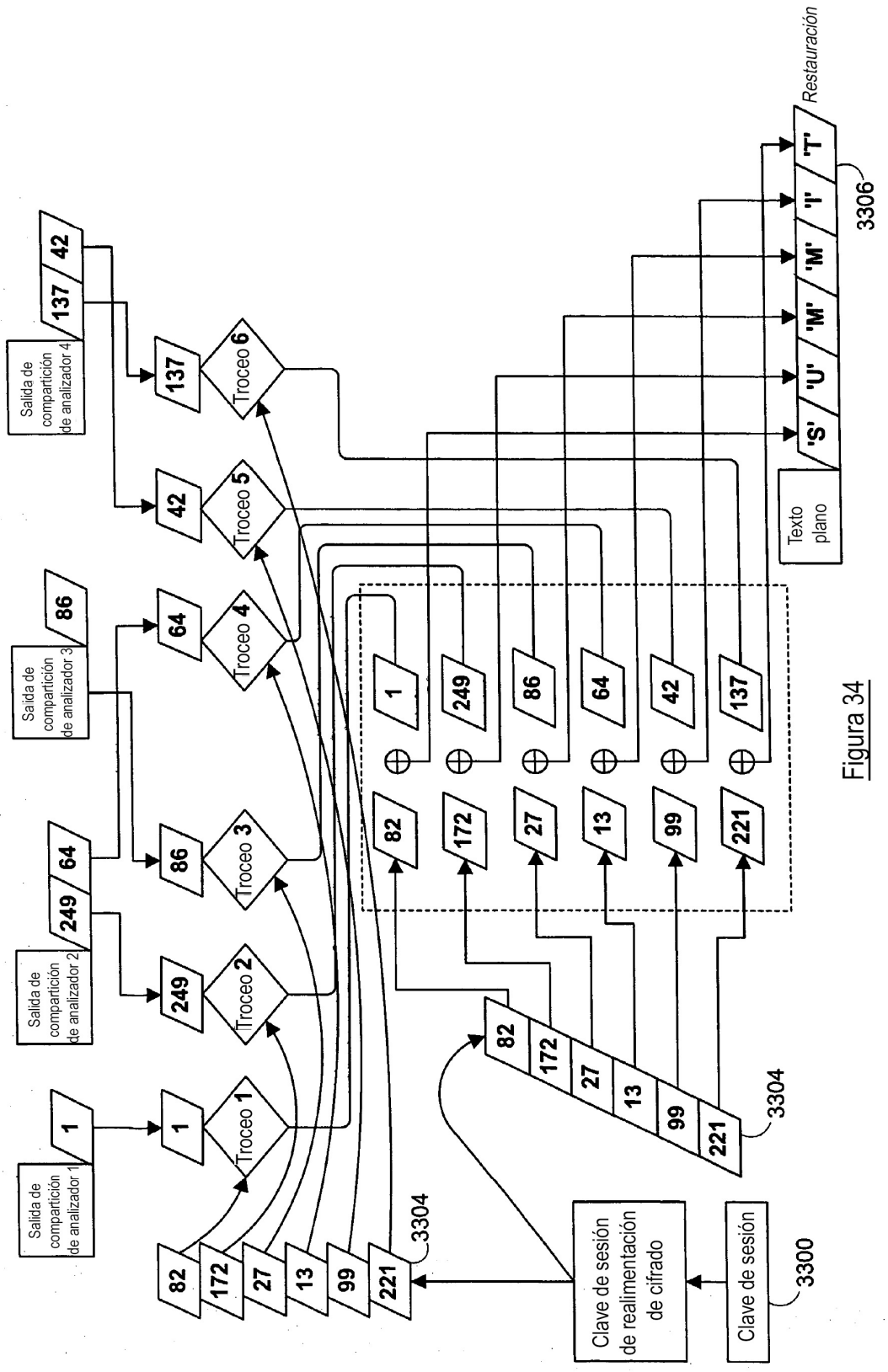

Salida de compartición de analizador 1
Salida de compartición de analizador 2
Salida de compartición de analizador 3
Salida de compartición de analizador 4
Troceo 1
Troceo 2
Troceo 3
Troceo 4
Troceo 5
Troceo 6
Clave de sesión de realimentación de cifrado
Clave de sesión
3300
3304
3306
Texto plano
Restauración
'S' 'U' 'M' 'M' 'I' 'T'

Figura 34

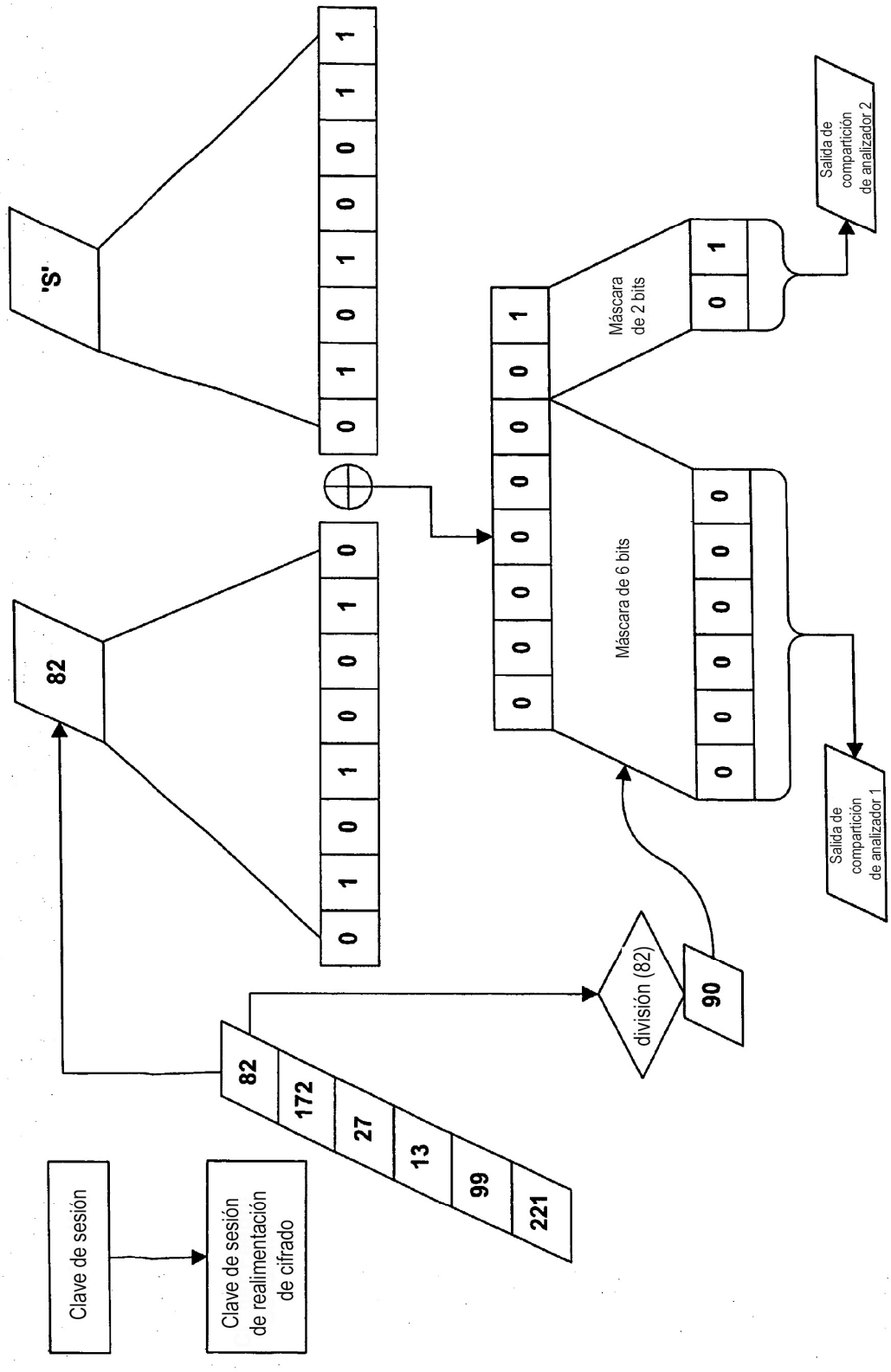

Clave de sesión
Clave de sesión de realimentación de cifrado
82
172
27
13
99
221
división (82)
90
'S'
0 1 0 1 0 1 1 0
82
0 1 0 1 0 0 1 0
Máscara de 6 bits
0 0 0 0 0 0
Máscara de 2 bits
0 1
0 0 0 0 0 0
0 0 0 0 0 0
Salida de compartición de analizador 1
Salida de compartición de analizador 2

Figura 35

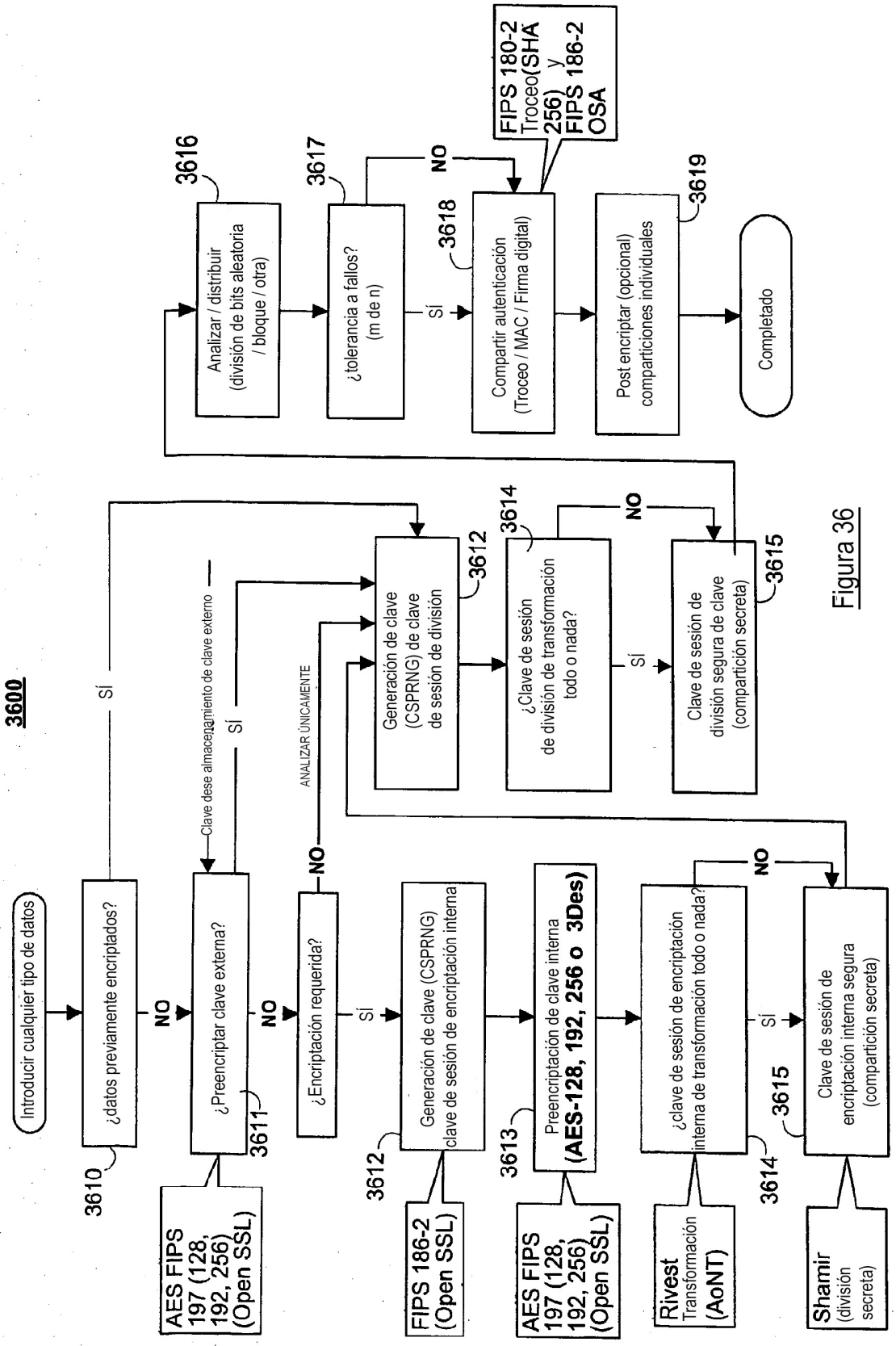

3600
Introducir cualquier tipo de datos
¿datos previamente encriptados?
3610
SÍ
NO
¿Preencriptar clave externa?
3611
SÍ
NO
Clave dese almacenamiento de clave externo
AES FIPS 197 (128, 192, 256) (Open SSL)
¿Encriptación requerida?
SÍ
NO
ANALIZAR ÚNICAMENTE
Generación de clave (CSPRNG) clave de sesión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

Figura 36

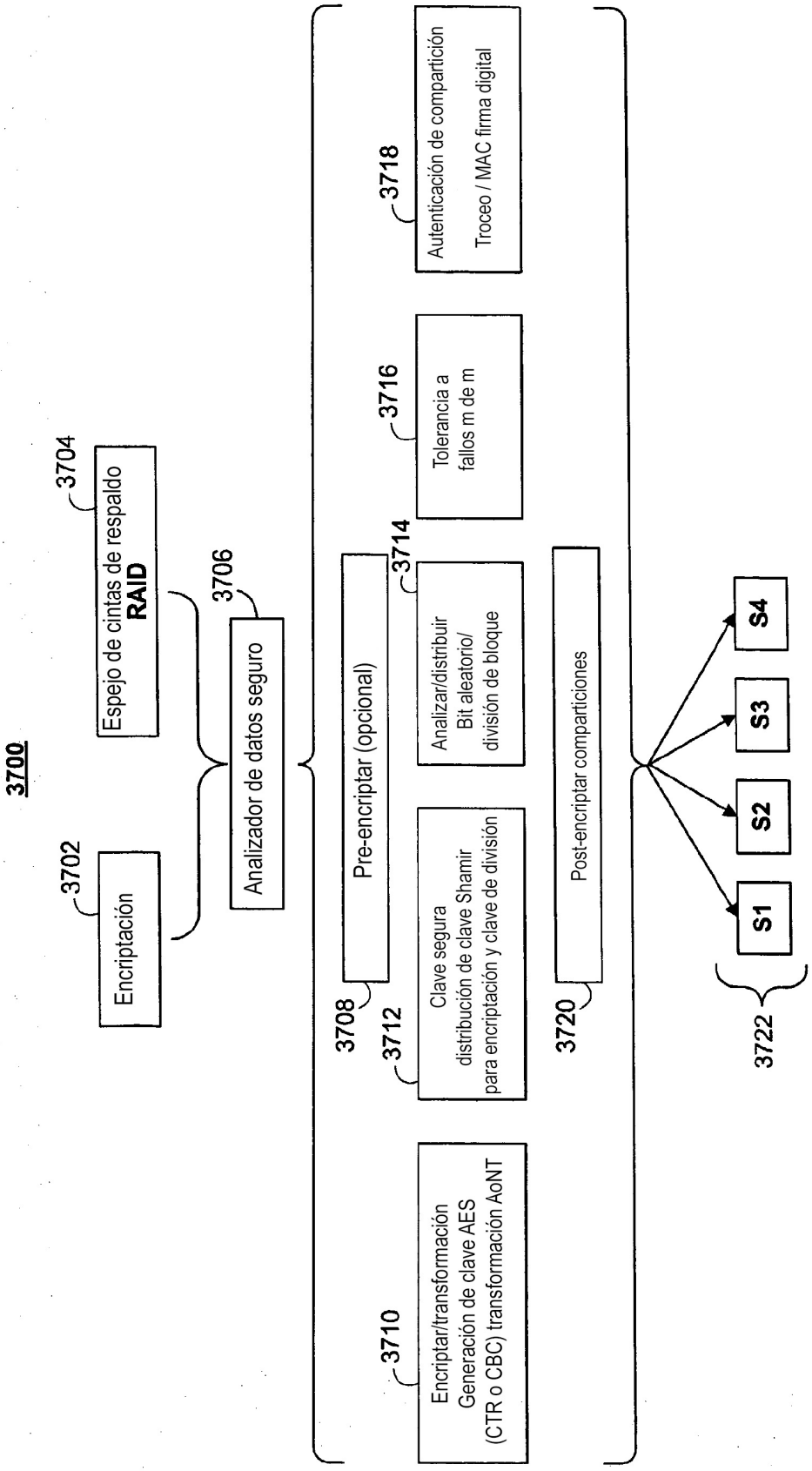

3700
3702
Encriptación
3704
Espejo de cintas de respaldo
RAID
3706
Analizador de datos seguro
3708
Pre-encriptar (opcional)
3710
Encriptar/transformación
Generación de clave AES
(CTR o CBC) transformación AoNT
3712
Clave segura
distribución de clave Shamir
para encriptación y clave de división
3714
Analizar/distribuir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

Figura 37

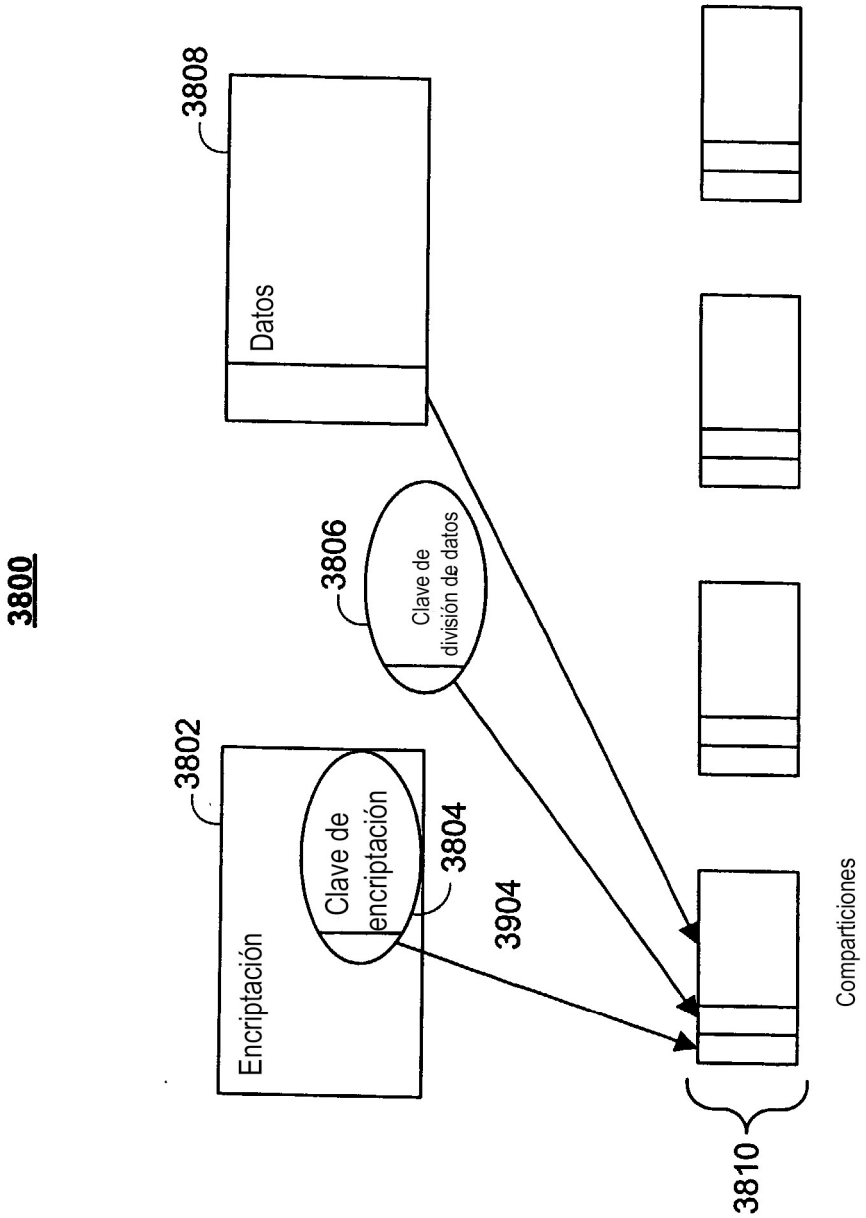

3800
3808
Datos
3806
Clave de división de datos
3802
Encriptación
Clave de encriptación
3804
3904
Compartimentos
3810

Figura 38

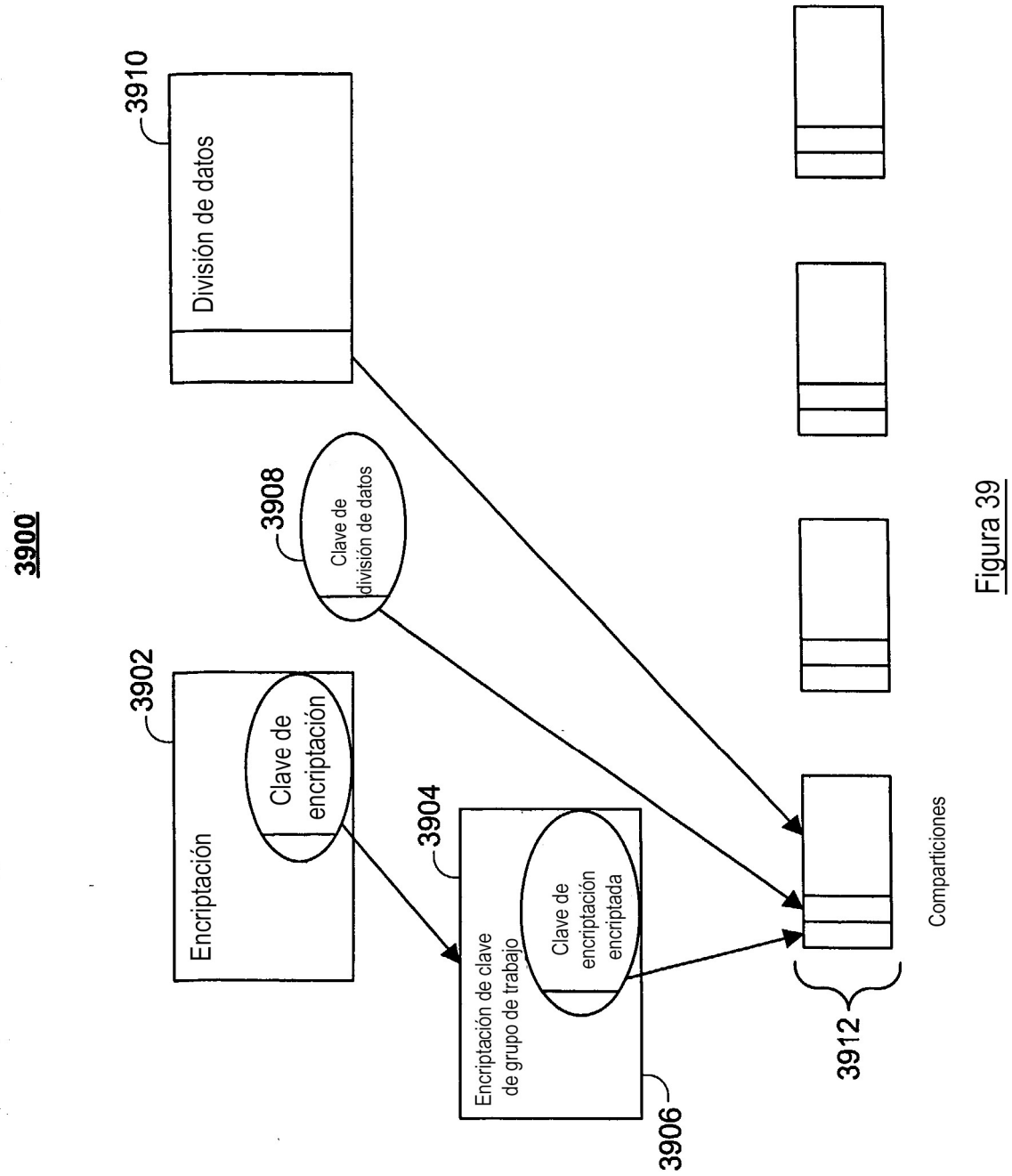

3900
3910
División de datos
3908
Clave de división de datos
3902
Encriptación
Clave de encriptación
3904
Encriptación de clave de grupo de trabajo
Clave de encriptación encriptada
3906
3912
Compartimentos

Figura 39

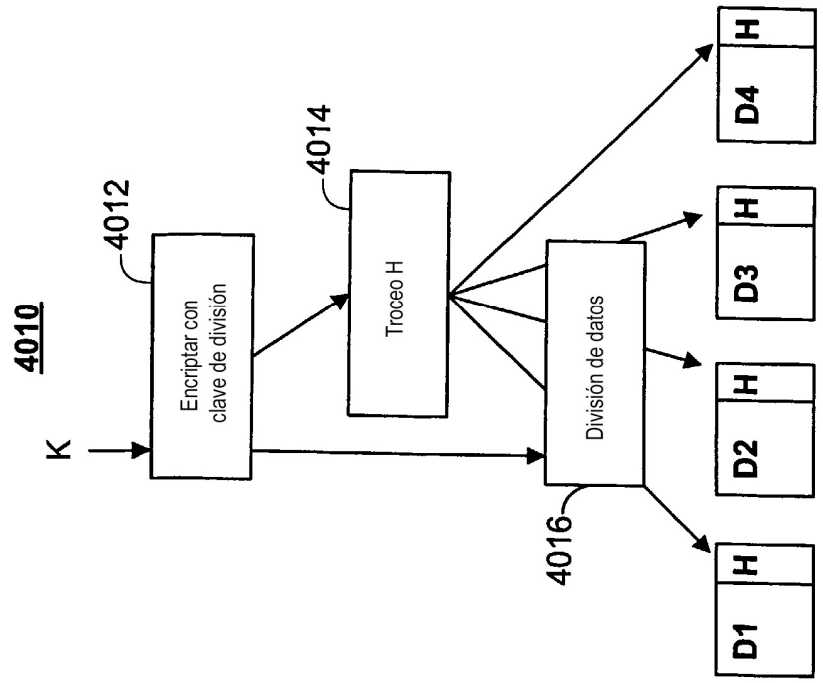


Figura 40B

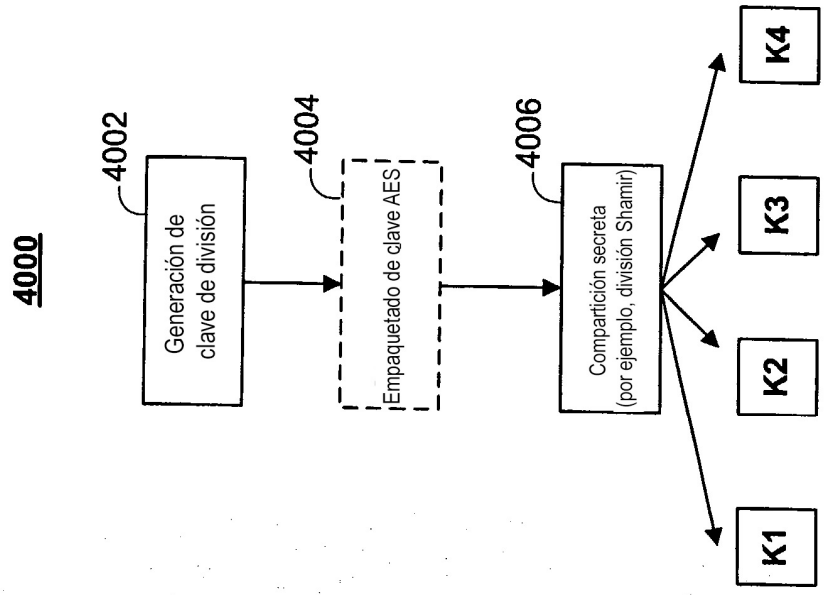


Figura 40A

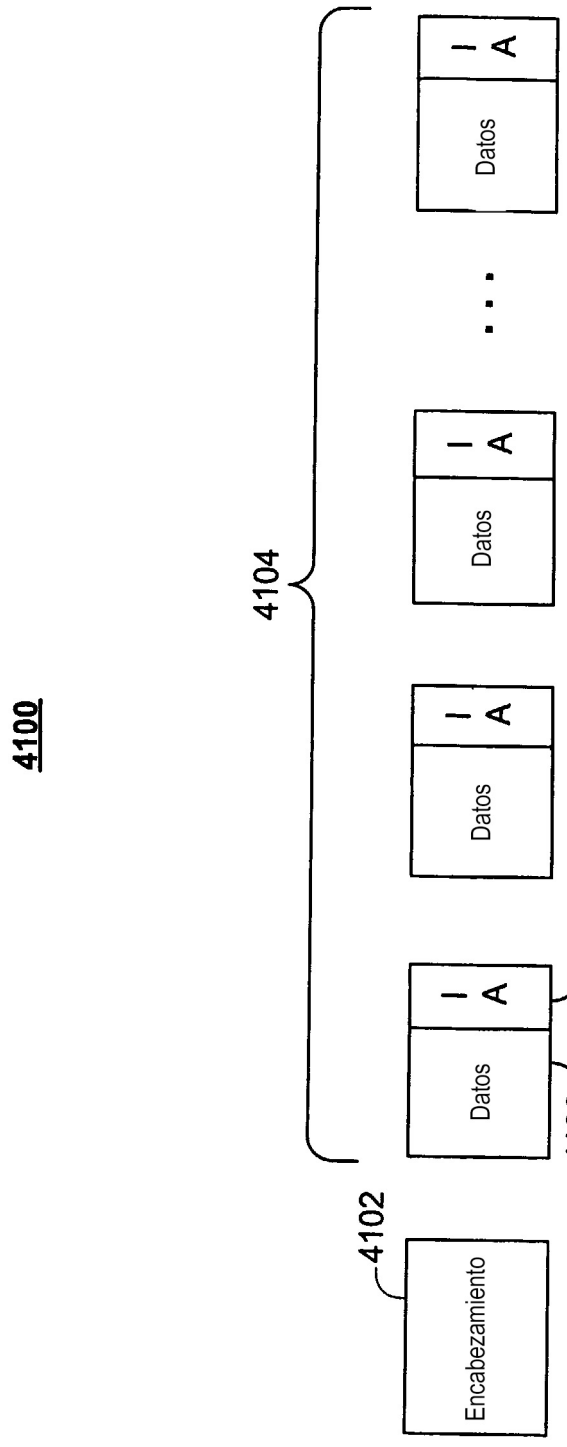

4100
4102
Encabezamiento
4104
Datos
I A
4106
4108
Datos
I A
Datos
I A
Datos
I A
. . .

Figura 41