(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 665 887**

(51) Int. CI.:

G06F 21/34 (2013.01)
G06F 21/62 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **06.04.2010 PCT/EP2010/002159**

(87) Fecha y número de publicación internacional: **14.10.2010 WO10115607**

(96) Fecha de presentación y número de la solicitud europea: **06.04.2010 E 10725375 (9)**

(97) Fecha y número de publicación de la concesión europea: **17.01.2018 EP 2414983**

(54) Título: **Sistema de datos seguro**

(30) Prioridad:

03.04.2009 EP 09157326

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
30.04.2018

(73) Titular/es:

DIGIDENTITY B.V. (100.0%)
Waldorpstraat 17p
2521 CA 's-Gravenhage, NL

(72) Inventor/es:

WENDT, MARCEL ARMAND;
DE BIE, WOUTER PETRUS MARIA y
MACKENBACH, CAREL MAURITS

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Sistema de datos seguro

Campo de la invención

La invención se refiere a un sistema de datos seguro y, en particular, aunque no exclusivamente, a un procedimiento y a un sistema para almacenar y/o acceder a datos de forma segura, un servidor de datos seguro y un producto de programa de ordenador para la ejecución de dicho procedimiento.

Antecedentes de la invención

Hoy en día, Internet se está desarrollando rápidamente hacia un canal generalmente aceptado para realizar transacciones entre el público y partes comerciales y/o gubernamentales. Debido al carácter abierto y anónimo de Internet, al mismo tiempo, cuestiones relacionadas con la protección de la información sensible, por ejemplo, información de transacciones, enviada a través de Internet y accesible a través de Internet, son una preocupación cada vez mayor entre el público. Por lo tanto, deben existir mecanismos para garantizar que solo el propietario legítimo tenga acceso y control sobre la información en cuestión.

Para lograr transacciones electrónicas legalmente válidas para la protección de datos, requisitos son formulados por organizaciones (inter)gubernamentales, por ejemplo, en la forma de legislación y/o recomendaciones de protección de datos como se describe, por ejemplo, en el documento TS 101 456 del ETSI. Deben tomarse medidas técnicas apropiadas contra el procesamiento no autorizado o ilegal de datos sensibles (es decir, datos personales, privados, legales y/o comerciales) que se almacenan centralmente en las instalaciones de un tercero. Además, los datos almacenados centralmente deben protegerse de la divulgación sin el consentimiento del usuario.

Un mecanismo importante para garantizar el acceso a la información sensible es el proceso de autentificación, es decir, el proceso de verificación de la identidad de una parte. Muchas transacciones electrónicas requieren la capacidad de identificar al creador de la información electrónica de la misma manera que los documentos se firman usando una firma manuscrita. Esto se puede lograr actualmente mediante el uso de un certificado electrónico digital emitido por una autoridad de certificación (CA) de confianza. El certificado asocia un par de claves públicas y privadas con la identidad del propietario del certificado. Un remitente puede firmar un mensaje encriptando (parte de) un mensaje usando su clave privada y un destinatario puede verificar la identidad del remitente de un mensaje desencriptando el mensaje firmado usando la clave pública del remitente. Otro mecanismo importante para garantizar el acceso correcto es el proceso de autorización para verificar si, después de la autentificación del solicitante, el solicitante tiene derecho a acceder y/o a modificar la información solicitada. Especialmente en los grandes sistemas de acceso a datos donde la información confidencial se almacena centralmente, se requiere un procedimiento de autorización fuerte.

Un problema relacionado con los sistemas de almacenamiento de datos es la gestión de la información de seguridad. Al realizar transacciones electrónicas, a las partes no les gusta ser molestadas con problemas de seguridad como la distribución, instalación y gestión de certificados digitales. Por lo tanto, aunque el proceso de autentificación y autorización debe ser fuerte, al mismo tiempo debe ser simple y fácil de gestionar para un usuario.

Otro problema se refiere al acceso a datos confidenciales que se almacenan en un sistema central gestionado por un tercero. Normalmente, dicho sistema está configurado para que el administrador del sistema y las partes autorizadas por el administrador puedan acceder al menos a parte de los datos. Por lo tanto, reglas complejas y costosas deben estar implementadas y protegidas para garantizar la privacidad de los datos.

Sin embargo, otro problema se refiere al almacenamiento central de datos sensibles. Los datos almacenados centralmente pueden ser un objetivo atractivo para los piratas informáticos u otras partes no autorizadas que intentan comprometer los datos o acceder a los datos y/o utilizar los datos para fines no autorizados. Por lo tanto, existe una necesidad en la técnica anterior de un sistema de almacenamiento de datos seguro mejorado.

El documento US 2002/178366 A1 divulga un servidor de acceso a datos con áreas específicas del usuario donde los datos se almacenan en forma encriptada. La autentificación de usuario implica desencriptar la clave privada del usuario con una contraseña proporcionada por el usuario y, posteriormente, utilizar la clave privada desencriptada para realizar operaciones en nombre del usuario autentificado.

Sumario de la invención

Es un objeto de la invención reducir o eliminar al menos uno de los inconvenientes conocidos en la técnica anterior y proporcionar, en un primer aspecto de la invención, un procedimiento para gestionar una o más unidades de almacenamiento de datos personales para de forma segura y almacenar centralmente datos privados, en el que cada una de dichas unidades de datos personales puede conectarse a un servidor de datos seguro y en el que cada una de dichas unidades de datos personales puede estar asociada con una clave privada encriptada mediante un código de identificación de suscriptor y una clave de aleatorización personal encriptada por una clave pública. El procedimiento puede comprender al menos una de las etapas de: recibir una solicitud de acceso desde un cliente,

comprendiendo dicha solicitud un código de identidad de suscriptor asociado con una unidad de almacenamiento de datos personales; autentificar a dicho cliente desencriptando la clave privada almacenada en dicha unidad de almacenamiento de datos personales utilizando el código de identidad del suscriptor contenido en dicha solicitud de acceso; almacenar la clave privada en una memoria segura del servidor seguro, encriptándose dicha clave privada con una clave de sesión; y/o, transmitir la clave de sesión a dicho cliente.

El procedimiento permite la gestión central de unidades de almacenamiento de datos personales de una manera segura y eficiente. El acceso es gestionado por el servidor seguro utilizando información de seguridad personal. La información de seguridad personal puede comprender un par de claves privada y pública (obtenidas, por ejemplo, desde un certificado de suscriptor) que se almacena de forma segura en la unidad de almacenamiento de datos personales. Al almacenar y gestionar de forma centralizada la información de seguridad personal, no se requiere un esquema complejo de distribución de certificados. Después de la autentificación del suscriptor, el servidor seguro desbloquea la información de seguridad personal para el acceso a los datos y/o con fines de transacción. Este esquema central es particularmente ventajoso para terminales con capacidades limitadas, por ejemplo, terminales de teléfonos móviles o de tipo de cliente ligero.

En una realización, la autentificación puede comprender además la etapa de comparar un hash desde la clave privada asociada con dicha unidad de datos personal con la comprobación de la clave privada desencriptada con el código de identidad de suscriptor contenida en dicha solicitud de acceso. El procedimiento proporciona así una unidad de almacenamiento de datos personales que solo se puede desbloquear utilizando el código de identidad de suscriptor del suscriptor. Por lo tanto, a diferencia de un sistema de almacenamiento de datos central convencional, el administrador del SDS no tiene acceso a los datos en las unidades de almacenamiento de datos personales. No se requieren reglas de privacidad de datos complejas para garantizar la privacidad de los datos. Cualquier solicitud de acceso (es decir, divulgación de datos) se enruta al suscriptor que puede o no haber autorizado el acceso de la parte solicitante (solo lectura) a los datos solicitados.

En otra realización, la autentificación puede comprender además al menos una de las etapas de: enviar un desafío, preferentemente en un canal fuera de banda, al suscriptor de la unidad de almacenamiento de datos personales; recibir una respuesta del suscriptor; y/o comparar dicha respuesta con una respuesta esperada almacenada en el servidor de datos seguro. Por lo tanto, el procedimiento permite la implementación simple de autentificación de múltiples factores para fines de autentificación fuerte.

En otra realización más, la clave pública y la clave privada pueden estar asociadas con un certificado de suscriptor, teniendo preferentemente dicho certificado una vida útil limitada. En una variante adicional, la duración de un certificado puede determinarse mediante una duración de tiempo predeterminada, un número predeterminado de sesiones y/o unas acciones de revocación de la CA que emitió el certificado.

En una variante, el servidor seguro puede comprender una lista de revocación de uno o más certificados revocados y/o de suscriptor. En otra variante, la autentificación puede comprender la etapa de verificar si el certificado de suscriptor asociado con el código de identidad del suscriptor está listado en la lista de revocación.

En otra variante, el procedimiento puede comprender al menos una de las etapas de: establecer una sesión, preferiblemente una sesión web segura, entre el cliente y el servidor seguro; y/o generar una clave de sesión asociada con dicha sesión, siendo dicha clave de sesión válida para una parte predeterminada de dicha sesión.

En una variante adicional, el procedimiento puede comprender al menos una de las etapas de: recibir una solicitud de datos desde el cliente, comprendiendo dicha solicitud de datos una clave de sesión; desencriptar la clave privada almacenada en la memoria usando la clave de sesión; y/o desencriptar la clave de aleatorización almacenada en la unidad de almacenamiento de datos personales utilizando la clave privada.

En todavía una variante adicional de la unidad de almacenamiento de datos personal puede comprender datos personales aleatorizados por una clave de aleatorización personal y/o la solicitud de datos puede comprender información de acceso de datos para la identificación de los datos a acceder. En una variante, el procedimiento puede comprender la etapa de desaleatorizar al menos parte de los datos identificados en la información de acceso a datos y almacenados en dicha unidad de almacenamiento de datos personales utilizando la clave de aleatorización personal. Por lo tanto, la invención reduce en gran medida el riesgo de divulgación no autorizada de grandes partes de las unidades de almacenamiento de datos personales, que se reducirá en gran medida a medida que los datos de cada unidad se encriptan utilizando una única clave de encriptado personal (simétrica) y el desencriptado de todas las unidades requiere conocimiento de las contraseñas de todos los suscriptores. Si un intruso logra comprometer una unidad de almacenamiento de datos personales mediante el acceso no autorizado a una contraseña, la seguridad de las otras unidades de almacenamiento de datos personales aún se conserva.

En una variante, el procedimiento puede comprender la etapa de transmitir los datos desaleatorizados al cliente. En otra variante, el procedimiento puede comprender la etapa de firmar los datos transmitidos al cliente utilizando la clave privada. La invención permite así la firma de datos utilizando el certificado de suscriptor que se almacena centralmente con la unidad de almacenamiento de datos personales y la transmisión de los datos firmados a una parte fiable que requiere de dichos datos para una transacción electrónica. Este esquema es particularmente

ventajoso, ya que no requiere la instalación de certificados de suscriptor en el terminal del suscriptor, por ejemplo, un teléfono móvil. La firma de los datos en la transacción es manejada centralmente por el servidor seguro.

En aún otra variante, el procedimiento puede comprender al menos una de las etapas de: transmitir datos a un servidor seguro; codificar los datos usando la clave de aleatorización personal; y/o almacenar los datos aleatorizados en dicha unidad de almacenamiento de datos personales.

En un aspecto adicional, la invención puede referirse a un servidor seguro de datos para la gestión de una o más unidades de almacenamiento de datos personales conectadas a dicho servidor seguro, en el que cada unidad de almacenamiento de datos puede estar asociada con una clave privada encriptada por un código de identificación de suscriptor y una clave de aleatorización personal encriptada por una clave pública. El servidor de datos puede comprender: un receptor para recibir una solicitud de inicio de sesión desde un cliente, comprendiendo dicha solicitud un código de identidad de suscriptor asociado con una unidad de almacenamiento de datos personales; un desencriptador de clave privada para desencriptar la clave privada de dicha unidad de almacenamiento de datos personales utilizando el código de identidad del suscriptor en dicha solicitud de acceso; un generador para generar una clave de sesión; un encriptador de clave de sesión para encriptar la clave privada usando una clave de sesión; y/o un transmisor para transmitir la clave de sesión a dicho cliente.

En aún un aspecto adicional, la invención puede referirse a un sistema de almacenamiento seguro de datos, que comprende un servidor de datos seguro como se describe anteriormente. El servidor de datos seguro puede estar conectado a una o más bases de datos, comprendiendo dichas bases de datos una o más unidades de almacenamiento de datos personales, en el que el sistema puede comprender además uno o más clientes para acceder a dichas unidades de almacenamiento de datos personales.

La invención también puede referirse a un producto de programa de ordenador que comprende porciones de código de software configuradas para, cuando se ejecuta en la memoria de un ordenador, preferiblemente un servidor de datos seguro, la ejecución de las etapas del procedimiento según cualquiera de las reivindicaciones de procedimiento como se describe anteriormente.

La invención se ilustrará adicionalmente con referencia a los dibujos adjuntos, que esquemáticamente muestran realizaciones de acuerdo con la invención. Se entenderá que la invención no está de ninguna manera restringida a estas realizaciones específicas. La invención se define mediante las reivindicaciones adjuntas.

Breve descripción de los dibujos

La figura 1 representa un esquema de un sistema de almacenamiento de datos seguro de acuerdo con una realización de la invención.
La figura 2 representa un esquema del registro de un suscriptor con el sistema de almacenamiento de datos seguro.
La figura 3 representa un inicio de sesión para su uso con un servidor de datos seguro de acuerdo con una realización de la invención.
La figura 4 representa un procedimiento de configuración para su uso con un servidor de datos seguro de acuerdo con una realización de la invención.
La figura 5 representa un esquema de una transacción usando un sistema de almacenamiento de datos seguro de acuerdo con una realización de la invención.
La figura 6 representa un esquema de una transacción que usa un sistema de almacenamiento de datos seguro de acuerdo con otra realización de la invención.

Descripción detallada

La figura 1 representa un esquema de un sistema **100** de almacenamiento de datos seguro de ejemplo de acuerdo con una realización de la invención. El sistema comprende un servidor **102** de datos seguro (SDS) conectado a una o más bases **104** de datos (DB). Uno o más terminales **106, 108** de suscriptores pueden conectarse al SDS a través de una o más redes **110** de comunicaciones, tal como Internet, una red local (LAN) y/o una red de área extensa (WAN). Un terminal puede ser un ordenador personal, un PDA, un teléfono inteligente, un proveedor de servicios, etc. El terminal típicamente comprende un Sistema Operativo (OS) que comprende un núcleo que gestiona los recursos del terminal, por ejemplo, una o más Unidades de Procesamiento Central (CPU), una memoria para almacenar instrucciones de programa y datos y dispositivos de Entrada/Salida (E/S). Además, el sistema operativo comprende interfaces de programación de aplicaciones (API) a través de las cuales los programas de aplicación pueden acceder a servicios de Internet (inalámbricos). El OS del terminal puede ejecutar software de cliente que utiliza sesiones web de tipo HTTP y, por ejemplo, el protocolo de capa de conexión segura (SSL) y/o lenguaje de marcado de aserción de seguridad (SAML) para proporcionar una interfaz segura entre el terminal de suscriptor y el SDS.

El SDS puede estar configurado para almacenar y acceder a datos sensibles centralmente de un suscriptor que está registrado en el sistema de almacenamiento de datos. Estos datos pueden comprender, por ejemplo, datos de autentificación, contraseñas, datos financieros, comerciales y/o médicos, datos de identidad, tales como pasaportes y datos biométricos, etc. Estos datos que requieren almacenamiento seguro pueden almacenarse en la base de

datos, que para ese propósito puede dividirse en unidades **112a-112d** de almacenamiento de datos personales (PDSU). Cada PDSU está bajo el control total del suscriptor: un suscriptor puede acceder a la PDSU para leer, escribir y borrar datos almacenados en la PDSU. Además, durante una autorización o transacción, el suscriptor puede autorizar a un tercero para acceder (es decir, divulgar) una parte predeterminada de los datos. Para garantizar la privacidad y la integridad de los datos, los datos en cada PDSU se almacenan en forma encriptada utilizando un esquema de encriptado ventajoso que se describirá a continuación con más detalle.

El acceso a una PDSU puede requerir un esquema de autentificación fuerte, por ejemplo, autentificación de múltiples factores en forma de un esquema de tipo desafío-respuesta usando una tarjeta inteligente y/o mensajería móvil. Para este fin, el SDS puede estar conectado a uno o más servidores **114, 116** de autentificación, por ejemplo, un servidor de SMS, MMS o IVR utilizado en el proceso de autentificación de múltiples factores. Para un manejo eficiente y conveniente del procedimiento de autentificación, se puede usar una identidad digital (ID) como nombre de usuario. Con ese fin, el servidor de datos seguro puede comprender un proveedor **118** de identidad para asociar un suscriptor con una ID digital. Dicha identificación digital puede tener la forma de una URL, por ejemplo, my.trust-id.com/name, como se define, por ejemplo, en el estándar OpenID o en el estándar ENUM. Al ingresar una ID digital en un sitio web habilitado para ID digital de un proveedor **120** de servicios (la parte fiable), un suscriptor será redireccionado al SDS para autentificar al suscriptor. Una vez autenticado, el SDS puede enviar a la parte fiable un mensaje que confirma la autentificación (no) exitosa.

Además, el sistema de almacenamiento de datos seguro puede ser parte de un sistema de confianza jerárquico, tal como una infraestructura de clave pública (PKI). Por ejemplo, el SDS puede ser una autoridad de certificación (CA) autorizada (por ejemplo, una CA raíz controlada por el gobierno) para validar la identidad de los suscriptores y emitir certificados digitales de suscriptor para asociar la identidad del suscriptor (por ejemplo, una persona, una organización, una entidad legal, un servidor, etc.) a una clave pública en el certificado digital. El certificado digital puede comprender además una clave privada (secreta) asociada a la clave pública. Al emitir un certificado de suscriptor, el certificado no se envía al cliente suscriptor. En cambio, los certificados de suscriptor son almacenados centralmente y gestionados por el SDS. Este proceso se explicará adicionalmente con referencia a la **figura 2**, que representa un esquema de un proceso ejemplar para registrar un nuevo suscriptor con el sistema **100** de almacenamiento de datos seguro, como se describe con referencia a la **figura 1.**

El proceso de registro en la **figura 2** se puede ejecutar a través de una aplicación web, que genera un formulario web que comprende al menos un número de campos de datos de registro (por ejemplo, nombre de usuario, contraseña, dirección, dirección de correo electrónico, número de teléfono, etc.). Típicamente, el tipo de datos de registro se puede determinar por la información requerida por el servidor de datos seguro para generar un certificado de suscriptor que puede tener un formato X.509. Posteriormente, el cliente puede enviar los datos de registro enviados a través de una conexión SSL encriptada al servidor de datos seguro.

Al recibir los datos de registro, el SDS genera una ID de suscriptor (interna) (por ejemplo, un número entero asociado con el nombre de usuario o un hash del nombre de usuario) para asociar el suscriptor con una PDSU **204** (es decir, una ubicación segura reservada de la memoria en la base **202** de datos). A continuación, el SDS o un servidor de claves separado puede generar un certificado de suscriptor firmado por el SDS que comprende un par de claves pública-privada, por ejemplo, un par de claves pública-privada RSA. El certificado puede ser válido durante un cierto período y/o un número de sesiones. Después de ese período o número de sesiones, un certificado puede caducar. Alternativamente, antes de la expiración, el certificado puede ser revocado por la CA por otros motivos. El SDS puede mantener una lista de revocación de certificados de suscriptor revocados y/o expirados para verificar si se utiliza un certificado de suscriptor válido para acceder a una PDSU. Para fines de verificación de contraseña, el SDS genera una firma (por ejemplo, un hash que usa una función de un solo sentido) de la clave privada. La clave **208** privada se encripta posteriormente utilizando la contraseña **206** proporcionada por el suscriptor al registrarse.

Además, el SDS puede generar una única clave **212** personal simétrica, por ejemplo, un número aleatorio de una longitud predeterminada, que se utiliza para el encriptado eficiente (aleatorización) de datos **222** sensibles almacenados por el suscriptor en su PSDU. El uso de una clave simétrica permite un encriptado rápido y eficiente de los datos y no está limitado por la longitud de la clave. La clave simétrica personal se encripta con la clave pública y posteriormente se almacena con la ID de suscriptor, la clave privada encriptada, la firma de la clave privada y la clave **210** pública como información de seguridad personal en una tabla **224** de información de seguridad personal asociada con la PDSU **204.** La información de seguridad personal solo puede desbloquearse con la contraseña del suscriptor que no está almacenada en la base de datos.

La pérdida de una contraseña da como resultado una situación en la que los datos en la PDSU se bloquean desde el desencriptado y vuelven inútiles los contenidos de la unidad de almacenamiento. Por lo tanto, el sistema puede generar un código **214** de desbloqueo personal (PUC) que se usa para encriptar la contraseña. El SDS puede almacenar la contraseña **220** encriptada como información de seguridad personal en la PDSU. El suscriptor puede usar el código PUC para recuperar la contraseña y puede almacenarse de forma segura con un tercero de confianza, por ejemplo, un notario.

El registro de un suscriptor provoca, por lo tanto, la asignación de una PDSU al suscriptor. Una ID de suscriptor asocia información de seguridad personal que puede comprender una clave **216** privada codificada por contraseña,

una firma de la clave privada, una clave **218** simétrica encriptada de clave pública y una contraseña **220** codificada de código PUC a la PSDU. Por lo tanto, la información de seguridad personal para fines de autentificación e intercambio de datos se almacena de forma centralizada y segura en la base de datos usando, por ejemplo, una base de datos relacional para un acceso y recuperación eficiente, y solo puede desbloquearse mediante la contraseña del usuario.

En otras variantes, las claves encriptadas pueden almacenarse de manera distribuida en el sistema de almacenamiento de datos seguro, por ejemplo, en una base de datos de claves que está separada físicamente de la base de datos que comprende los datos sensibles encriptados almacenados en una unidad de almacenamiento personal. Después del registro, el servidor de datos seguro puede informar al suscriptor de la creación de la cuenta del suscriptor, por ejemplo, en forma de un código de activación.

Las **figuras 3** y **4** representan esquemas de un procedimiento **300** de inicio de sesión y un procedimiento de configuración posterior que usa un sistema de almacenamiento de datos seguro como se describe con referencia a las **figuras 1** y **2.** Típicamente, un procedimiento **300** de inicio de sesión como se representa en la **figura 3** puede ser iniciado por un suscriptor que accede al SDS usando una sesión web segura, por ejemplo, una sesión HTTP segura con SSL utilizando un navegador web. Alternativamente, el acceso se puede lograr usando otras técnicas seguras, por ejemplo, usando una red privada virtual (VPN).

Después de la iniciación de la sesión web, se genera un identificador de sesión, que proporciona una referencia a la información de sesión que se almacena como un objeto de sesión en una ubicación de memoria segura del SDS. La información de sesión puede comprender la ID del suscriptor y la información del estado de la sesión que se intercambia entre el cliente (el navegador web) y el servidor mediante el envío de cookies entre el cliente y el servidor.

El SDS puede requerir que el suscriptor introduzca un nombre de usuario (por ejemplo, en la forma de una ID digital) y una contraseña en una ventana de inicio de sesión. Al asociar el nombre de inicio de sesión del suscriptor a una ID de suscriptor, el servidor de datos seguro puede recuperar la clave **302** privada encriptada por contraseña desde la PDSU asociada con la ID de suscriptor. A continuación, el SDS usa la contraseña **304** proporcionada por el suscriptor para desencriptar la clave **306** privada encriptada. La verificación de la contraseña desencriptada de este modo se puede realizar comparando el hash de la contraseña y el hash de la contraseña almacenada en la base de datos durante el proceso de registro. Si los valores hash difieren, el procedimiento de inicio de sesión finaliza.

Si la verificación tiene éxito (es decir, los valores hash son idénticos) el procedimiento de inicio de sesión puede continuar mediante la generación de una clave **308** de sesión. La clave de sesión es una clave de encriptado que puede ser válida durante un período predeterminado durante la sesión y que puede usarse para encriptar la clave privada, que se desencriptó durante la sesión de inicio de sesión. A continuación, el procedimiento de inicio de sesión puede completarse almacenando la clave **310** privada encriptada como información de sesión en el objeto de sesión y enviando la clave de sesión en una cookie al cliente **312.** Después del inicio de sesión del suscriptor, el objeto de la sesión solo contiene una clave privada encriptada, que solo puede desencriptar el cliente asociado a la sesión. Como medida de seguridad, la clave de sesión puede cambiarse regularmente. En una realización, la clave de sesión se actualiza generando una nueva clave de sesión. La generación de una nueva clave de sesión puede requerir la repetición de las etapas **306-312** del procedimiento de inicio de sesión.

Si el suscriptor decide acceder a los datos en la PDSU o autorizar la divulgación de una parte predeterminada de los datos a un tercero, un procedimiento **400** de configuración como se describe en la **figura 4** se puede iniciar mediante el envío de una solicitud HTTP que comprende una cookie con la ID de sesión y la clave **402** de sesión al SDS. Usando la ID de sesión, el SDS recupera la clave **404** privada encriptada desde la información de sesión almacenada en el objeto de sesión y desencripta la clave **406** privada. En una realización, antes de desencriptar la clave simétrica personal, el SDS puede verificar la validez del certificado de usuario comprobando si el certificado de usuario figura en la lista de revocación.

Después de ello, utilizando el ID de suscriptor en el objeto de sesión, el clave **408** simétrica personal encriptada se recupera desde la PDSU y se desencripta utilizando la clave privada. El SDS puede usar la clave **410** simétrica para encriptar datos sensibles que se almacenan en la PDSU y para desencriptar datos sensibles para su divulgación al suscriptor y/o a terceros autorizados por el suscriptor. Después de la finalización de la sesión, la PDSU comprende datos sensibles encriptados e información clave de seguridad asociada con información clave encriptada que se requiere para desencriptar los datos y a la que el suscriptor solo puede acceder utilizando su contraseña.

Por lo tanto, el SDS de acuerdo con la invención permite el almacenamiento de datos en una PDSU que se pueda acceder solo por el suscriptor o un tercero autorizado por el suscriptor. El acceso es gestionado por el SDS utilizando un certificado de suscriptor que se almacena de forma segura en la PDSU. Al almacenar y gestionar centralmente los certificados de suscriptor, no se requiere un esquema complejo de distribución de certificados. Después de la autentificación del suscriptor, el servidor de datos seguro desbloquea el certificado para el acceso a datos y/o con fines de transacción. Este esquema es particularmente ventajoso para terminales con capacidades limitadas, por ejemplo, terminales de teléfonos móviles o de tipo de cliente ligero.

Además, cada PDSU solo puede acceder usando el certificado de suscriptor asociado que puede ser desbloqueado mediante la contraseña del suscriptor. Por lo tanto, a diferencia de un sistema de almacenamiento de datos central convencional, el administrador del SDS no tiene acceso a los datos en las unidades de almacenamiento de datos personales. Por lo tanto, no se requieren reglas de privacidad de datos complejas para garantizar la privacidad de los datos. Cualquier solicitud de acceso (es decir, divulgación de datos) se enruta al suscriptor que puede o no haber autorizado el acceso de la parte solicitante (solo lectura) a los datos solicitados. Además, el riesgo de divulgación no autorizada de partes grandes de las PDSU se reducirá enormemente a medida que los datos de cada PDSU se encripten usando una clave de encriptado personal única (simétrica) y el desencriptado de todas las PDSU requiere el conocimiento de las contraseñas de todos los suscriptores. Si un intruso logra comprometer una unidad de almacenamiento de datos personales mediante el acceso no autorizado a una contraseña, la seguridad de las otras unidades de almacenamiento de datos personales aún se conserva.

Las ventajas de la presente invención más evidentes se harán más evidentes con referencia a la **figura 5**, que ilustra un diagrama **500** de flujo de un procedimiento de transacción utilizando la invención como se describe con referencia a las **figuras 1 a 4** de acuerdo con una realización de la invención. El procedimiento **500** de transacción representado puede ser parte de un procedimiento de transacción más grande (por ejemplo, una transacción comercial o legal) entre una primera y una segunda parte en el que al menos una de las partes requiere el intercambio de información personal y/u otra información sensible antes de que la transacción pueda cerrarse. El procedimiento de transacción puede comprender una fase de autentificación, una fase de autorización y, si una parte se autentifica y autoriza satisfactoriamente, una fase de divulgación en la que se puede acceder (divulgar) a los datos solicitados (por ejemplo, una copia de un pasaporte y una copia de un título universitario) y/o transmitir a la otra parte en un procedimiento de transacción.

El procedimiento de transacción representado en la **figura 5** se puede ejecutar entre una primera parte, un consumidor, y una segunda parte, un proveedor de servicios. El consumidor puede acceder electrónicamente a los servicios a través de un sitio web del proveedor de servicios que utiliza software de cliente (CL), por ejemplo, un navegador web, ejecutado en un terminal. Para completar una transacción, el proveedor del servicio, la parte fiable (RL), puede requerir la autentificación del consumidor, incluida, por ejemplo, la prueba de que el consumidor es holandés y tiene al menos 18 años de edad, utilizando un sólido esquema de autentificación.

A tal fin, la parte fiable utiliza un servicio de autentificación de terceros, preferiblemente un servicio de autentificación de terceros autorizados por el gobierno, utilizando un sistema de almacenamiento seguro de datos como se describe con referencia a las **figuras 1 a 4.** A los efectos de la siguiente descripción, se supone que el consumidor ya está registrado en el sistema de almacenamiento de datos seguro, por lo que tiene una PDSU que puede utilizarse para el proceso de autentificación con el proveedor de servicios.

El consumidor puede enviar una solicitud para una transacción **502** al proveedor de servicios, accediendo a una página web del proveedor de servicios. El acceso al sitio web puede requerir un procedimiento de inicio de sesión que requiere la entrada de datos de la transacción, incluyendo un nombre de usuario y una contraseña, en un formulario web. La identidad digital puede ser un ENUM o un identificador de tipo OpenID, por ejemplo, URL my.trust-id.com/name, que puede ser proporcionada por el sistema de almacenamiento de datos seguro al suscriptor en el momento del registro. Después de transmitir los datos ingresados en una solicitud al proveedor de servicios, el proveedor de servicios puede transmitir una solicitud **504** de autentificación, que comprende al menos el nombre de usuario, la contraseña del consumidor y la información de la transacción, a través de una sesión segura SSL al SDS del servicio de autentificación de terceros. La información de transacción puede comprender una referencia a los datos personales a los que el proveedor de servicios quiere acceder con fines de autentificación (por ejemplo, una referencia a una copia electrónica de las partes relevantes del pasaporte del consumidor almacenadas en la PDSU que indica que el consumidor es holandés y al menos tiene 18 años de edad).

Tras recibir la solicitud de autentificación, el SDS puede entonces proceder con el procedimiento **506** de conexión como se ha descrito en relación con la **figura 3**. Este procedimiento de inicio de sesión puede incluir las etapas de asociar el nombre de usuario a través de una ID de suscriptor (interna) en la PDSU del cliente y verificar la contraseña desencriptando la clave privada encriptada almacenada en la PDSU usando la contraseña. En el ejemplo de la **figura 5**, el SDS puede iniciar una etapa de autentificación de desafío-respuesta adicional usando un canal de comunicación fuera de banda. El SDS puede, por ejemplo, transmitir un desafío **508a**, por ejemplo, desafíos textuales y/o visuales tales como Captcha, a través de una plataforma de SMS/MMS al teléfono móvil del suscriptor **508b.** En otras realizaciones, se pueden emplear otros esquemas de autentificación, por ejemplo, el uso de un token de hardware libre de alteraciones o una tarjeta inteligente se puede usar para proporcionar una autentificación fuerte y segura.

Después de una respuesta **510a, 510b** exitosa al desafío, el SDS puede enviar una solicitud **512** de datos al cliente. Dicha solicitud puede implementarse como un formulario web solicitando al cliente que apruebe el acceso de solo lectura a las partes relevantes de sus datos personales, es decir, una copia de su pasaporte, almacenada en su PDSU. Después de la aprobación **514,** el SDS puede establecer un enlace SSL seguro con la parte fiable RL usando el procedimiento de incremento similar al esquema descrito con referencia a la **figura 4.** Durante el procedimiento **516** de configuración, la clave privada almacenada en la PDSU se desencripta utilizando la clave de sesión en el objeto de sesión de la sesión web entre el cliente y el SDS. Usando la clave privada, se obtiene la clave simétrica

personal para desencriptar los datos solicitados. Estos datos se envían posteriormente a la parte **518** fiable con fines de autentificación. En una realización, los datos solicitados están firmados por el SDS usando la clave privada. En ese caso, la clave pública para verificar la firma puede proporcionarse por el SDS enviando un certificado digital al proveedor de servicios. La invención permite así la firma de datos utilizando el certificado de suscriptor que se almacena centralmente con la unidad de almacenamiento de datos personales y la transmisión de los datos firmados a una parte fiable que requiere de dichos datos para una transacción electrónica. Este esquema es particularmente ventajoso, ya que no requiere la instalación de certificados de suscriptor en el terminal del suscriptor, por ejemplo, un teléfono móvil. La firma de los datos en la transacción es manejada centralmente por el servidor seguro.

La **figura 6** representa el diagrama **600** de flujo de un procedimiento de transacción que usa la invención como se describe con referencia a las **figuras 1 a 4** de acuerdo con otra realización de la invención. En particular, en esta realización, se usa un módulo de seguridad de hardware (HSM) separado durante el procedimiento de autentificación. El HSM se refiere a un dispositivo de hardware inviolable, que no se puede abrir sin la destrucción completa de los datos almacenados en el mismo. El HSM puede comprender una o más claves secretas almacenadas en una memoria segura del HSM. Usando las claves secretas, puede recibir datos encriptados, desencriptar los datos usando una de las claves secretas y ejecutar un procedimiento sobre la base del contenido de los datos desencriptados.

En particular, el HSM está configurado para recibir un mensaje de un dispositivo de creación de firma segura (SSCD) desde el SDS que comprende información de autentificación, por ejemplo, al menos el MSISDN (el número de móvil de un usuario) y la clave de autentificación privada asociada con el usuario en forma encriptada. El encriptado del contenido del mensaje del SSCD se puede realizar utilizando la clave simétrica personal asociada con el usuario.

Por lo tanto, la PDSU asociada con el usuario puede comprender un mensaje del SSCD en el que el MSISDN y la clave de autentificación privada son encriptados usando una clave secreta que solo está disponible en el hardware de seguridad del HSM. En particular, durante el registro de un usuario en el SDS como se describe con referencia a la **figura 2**, se puede asignar un mensaje del SSCD que comprende al menos el MSISDN (el número de móvil de un usuario) y la clave de autentificación privada asociada con el usuario al usuario y encriptarse usando la clave simétrica personal.

Como será evidente a continuación, durante el procedimiento de transacción, en particular, después del procedimiento de inicio de sesión y del procedimiento de configuración posterior en el que la clave simétrica personal se recupera de manera segura, el HSM puede proporcionar un procedimiento de autentificación segura en el que al usuario se le puede proporcionar una clave de autentificación privada para firmar los datos manejados durante la transacción.

El procedimiento de transacción puede comenzar de una manera similar a la del proceso descrito con referencia a la **figura 5.** El consumidor puede enviar una solicitud de una transacción **602** al proveedor de servicios accediendo a un sitio web del proveedor de servicios, donde después el proveedor de servicios puede transmitir una solicitud **604** de autentificación, que comprende al menos el nombre de usuario, la contraseña del consumidor y la información de transacción, a través de una sesión web SSL segura al SDS del servicio de autentificación de terceros.

A continuación, el SDS puede ejecutar el procedimiento **606** de inicio de sesión y un procedimiento **608** de configuración posterior, como se describe en detalle con referencia a las **figuras 3** y **4**, respectivamente. Después de la ejecución del procedimiento de configuración, el SDS inicia primero un procedimiento de autentificación sobre la base de la clave simétrica personal desencriptada recuperada a través del procedimiento de configuración. El SDS puede recuperar el mensaje del SSCD encriptado, desencriptarlo utilizando la clave simétrica personal y enviar el mensaje del SSCD en una solicitud de autentificación al HSM. En una realización, el mensaje de autentificación puede comprender otros datos asociados con el proceso de transacción al HSM, por ejemplo, un hash de un pfd de un documento utilizado durante la transacción (etapa **610**).

El SHM desencripta el contenido del mensaje del SSCD e inicia un proceso de desafío-respuesta sobre la base del MSISDN en el SSCD (etapa **612**). El desafío se puede enviar a través de la plataforma móvil MMS al cliente (etapa **614**). El usuario puede responder al desafío y enviar la respuesta nuevamente al HSM (etapa **616**). Si el HSM ha establecido que el procedimiento de desafío-respuesta se ejecuta con éxito, el HSM puede firmar un valor hash asociado con los documentos de transacción utilizando la clave de autentificación privada. A continuación, el HSM puede instruir al SDS (etapa **618**) para que establezca una línea de datos segura entre el SDS y se envía a la parte fiable (etapa **620**). Por lo tanto, de esta manera, al menos parte del procedimiento de autentificación y el proceso de firma digital de documentos de transacción se pueden ejecutar en el entorno seguro del HSM.

Debe entenderse que cualquier característica descrita en relación con cualquier realización puede utilizarse en solitario, o en combinación con otras características descritas, y también puede usarse en combinación con uno o más características de cualquier otra de las realizaciones, o cualquier combinación de cualquier otra de las realizaciones. Además, también se pueden emplear equivalentes y modificaciones no descritos anteriormente. El alcance de la invención se define mediante las reivindicaciones adjuntas.

REIVINDICACIONES

1. Procedimiento de gestión de una o más unidades de almacenamiento de datos personales para almacenar de forma segura y central datos confidenciales, estando conectadas dichas unidades de datos personales a un servidor de datos seguro y asociadas con una clave privada, la clave pública correspondiente, y una clave de aleatorización personal utilizada para encriptar y desencriptar datos en dicha unidad de datos personales, en el que dicha clave de aleatorización personal se encripta con dicha clave pública y dicha clave privada se encripta con un código de identidad del suscriptor, comprendiendo el procedimiento las etapas de:

al establecer una sesión entre un cliente y dicho servidor de datos seguro, generar una ID de sesión que identifica dicha sesión, proporcionando dicha ID de sesión una referencia a información de sesión almacenada como un objeto de sesión en una ubicación de memoria segura de dicho servidor de datos seguro;
recibir una solicitud de acceso desde un cliente, comprendiendo dicha solicitud un código de identidad de suscriptor asociado con una unidad de almacenamiento de datos personales;
autentificar dicho cliente utilizando el código de identidad del suscriptor contenido en dicha solicitud de acceso para desencriptar la clave privada encriptada almacenada en dicha unidad de almacenamiento de datos personales; generar una clave de sesión para encriptar dicha clave privada, siendo dicha clave de sesión válida para una parte predeterminada de dicha sesión;
almacenar la clave privada encriptada con dicha clave de sesión como información de sesión en dicho objeto de sesión; y,
transmitir la clave de sesión y dicha ID de sesión a dicho cliente.

2. Procedimiento según la reivindicación 1, en el que dicha autentificación comprende adicionalmente las etapas de:

comparar un hash de la clave privada asociada con dicha unidad de datos personal con la comprobación de la clave privada desencriptada con el código de identificación de suscriptor contenido en dicha solicitud de acceso.

3. Procedimiento según las reivindicaciones 1 o 2, en el que dicha autentificación comprende además las etapas de:

enviar un desafío, preferiblemente en un canal fuera de banda, al suscriptor de la unidad de almacenamiento de datos personales;
recibir una respuesta del suscriptor;
comparar dicha respuesta con una respuesta esperada almacenada en el servidor de datos seguro.

4. Procedimiento según cualquiera de las reivindicaciones 1 a 3, en el que la clave privada y la clave pública están asociadas con un certificado de suscriptor, teniendo preferiblemente dicho certificado una vida útil limitada, determinándose dicha vida útil mediante un período de tiempo predeterminado o un número predeterminado de sesiones.

5. Procedimiento según la reivindicación 4, en el que el servidor seguro comprende una lista de revocación de certificados de suscriptor revocados, comprendiendo dicha autentificación además la etapa de:

verificar si el certificado de suscriptor asociado con el código de identidad del suscriptor está listado en la lista de revocación.

6. Procedimiento según cualquiera de las reivindicaciones 1 a 5, comprendiendo el procedimiento además la etapa de:

recibir una solicitud de transacción desde el cliente, comprendiendo dicha solicitud de transacción una clave de sesión;
desencriptar la clave privada almacenada en la memoria usando la clave de sesión;
desencriptar la clave de aleatorización almacenada en la unidad de almacenamiento de datos personales utilizando la clave privada.

7. Procedimiento según la reivindicación 6, en el que dicha unidad de almacenamiento de datos personales comprende datos codificados por dicha clave de aleatorización personal y en el que dicha solicitud de transacción comprende información de acceso a datos para identificar los datos a acceder, comprendiendo el procedimiento además la etapa de:

desaleatorizar al menos parte de los datos identificados en la información de acceso a datos y almacenados en dicha unidad de almacenamiento de datos personales utilizando la clave de aleatorización personal.

8. Procedimiento según la reivindicación 7, comprendiendo el procedimiento además la etapa de transmitir los datos desaleatorizados al cliente.

9. Procedimiento según la reivindicación 8, comprendiendo el procedimiento además la etapa de firmar el transmisor de datos al cliente usando la clave privada.

10. Procedimiento según la reivindicación 6, comprendiendo el procedimiento además la etapa de:

recuperar un mensaje de SSCD encriptado desde dicha unidad de almacenamiento de datos personales, comprendiendo preferiblemente dicho mensaje de SSCD un MSISDN y/o una clave de autentificación privada;
desencriptar dicho mensaje de SSCD encriptado usando la clave de aleatorización;
enviar dicho mensaje de SSCD en una solicitud de autentificación a un módulo de hardware seguro;
ejecutando el módulo de hardware seguro un procedimiento de autentificación sobre la base de la información en dicha solicitud de autentificación.

11. Procedimiento según la reivindicación 10, comprendiendo el procedimiento además la etapa de:

el módulo de hardware seguro firma datos de transacción utilizando la clave de autentificación privada en dicho mensaje de SSCD.

12. Un servidor de datos seguro para gestionar una o más unidades de almacenamiento de datos personales conectadas a dicho servidor seguro, estando asociada cada unidad de almacenamiento de datos con una clave privada, la clave pública correspondiente y una clave de aleatorización personal utilizada para encriptar y desencriptar datos en dicha unidad de datos personales, en la que dicha clave de aleatorización personal se encripta con dicha clave pública y dicha clave privada se encripta con un código de identidad de suscriptor, configurándose el servidor de datos para realizar las etapas del procedimiento según la reivindicación 1.

13. Un sistema de almacenamiento de datos seguro, que comprende un servidor de datos seguro según la reivindicación 12, estando conectado dicho servidor de datos seguro con una o más bases de datos, comprendiendo dichas bases de datos una o más unidades de almacenamiento de datos personales, comprendiendo además el sistema uno o más clientes para acceder a dichas unidades de almacenamiento de datos personales.

14. Un producto de programa informático que comprende porciones de código de software configuradas para, cuando se ejecutan en la memoria de un ordenador, preferiblemente un servidor de datos seguro de acuerdo con la reivindicación 12, ejecutar las etapas del procedimiento de acuerdo con cualquiera de las reivindicaciones 1 a 11.

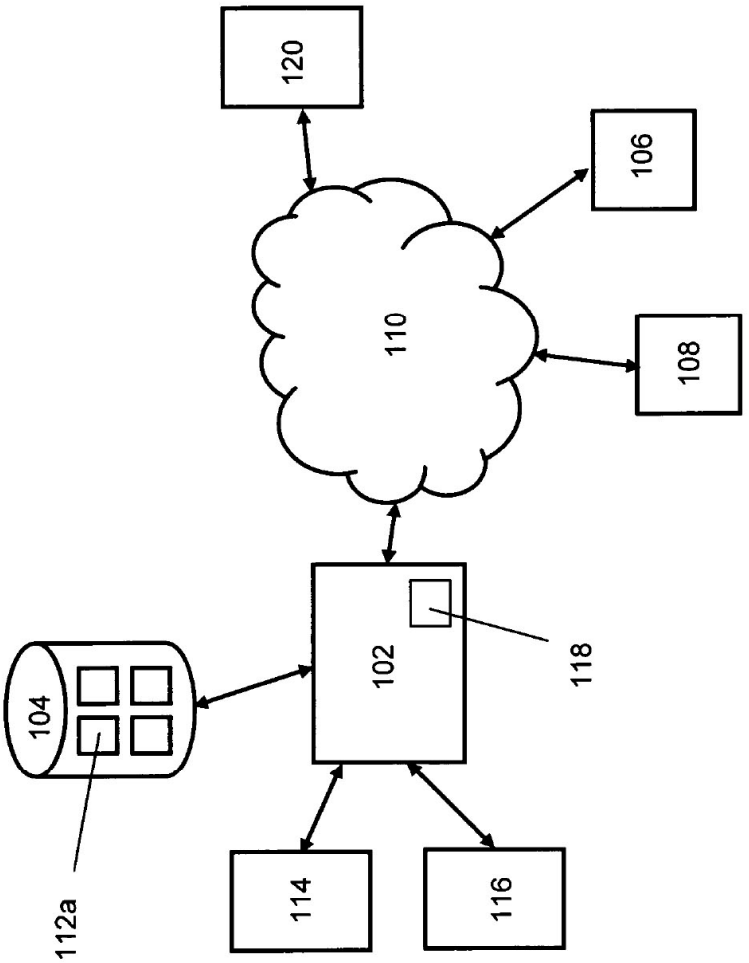

Figura 1

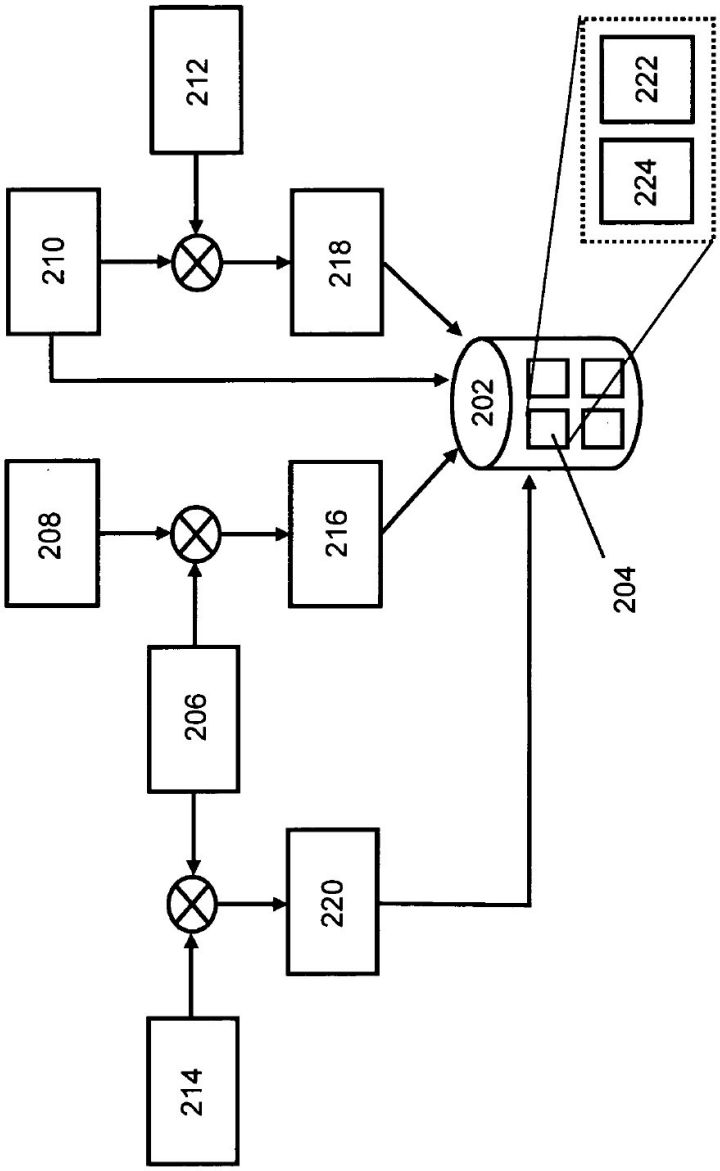

Figura 2

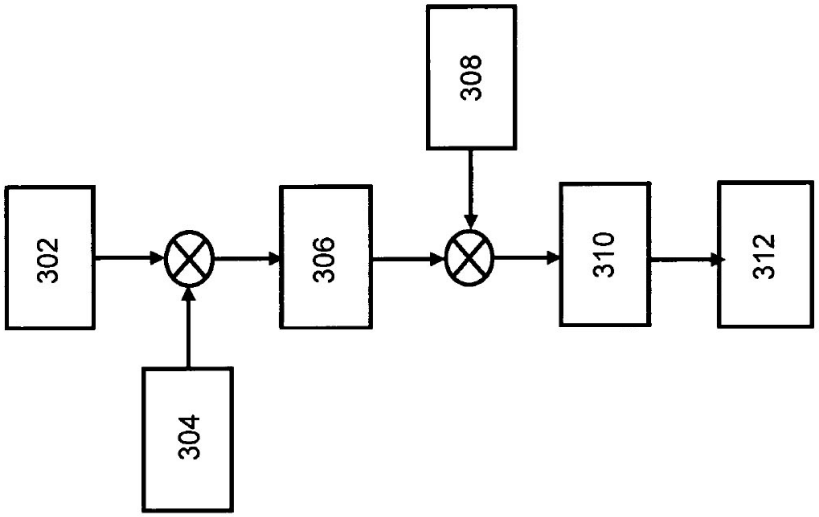

Figura 3

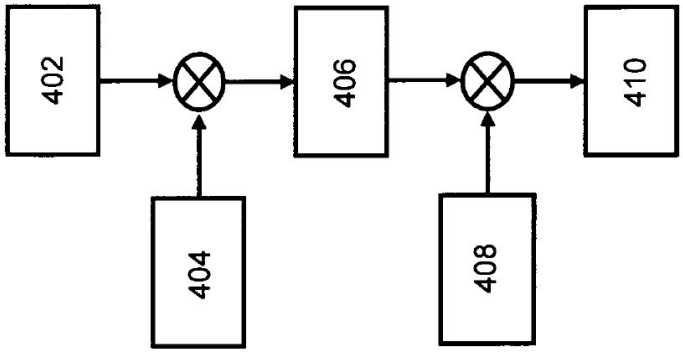

Figura 4

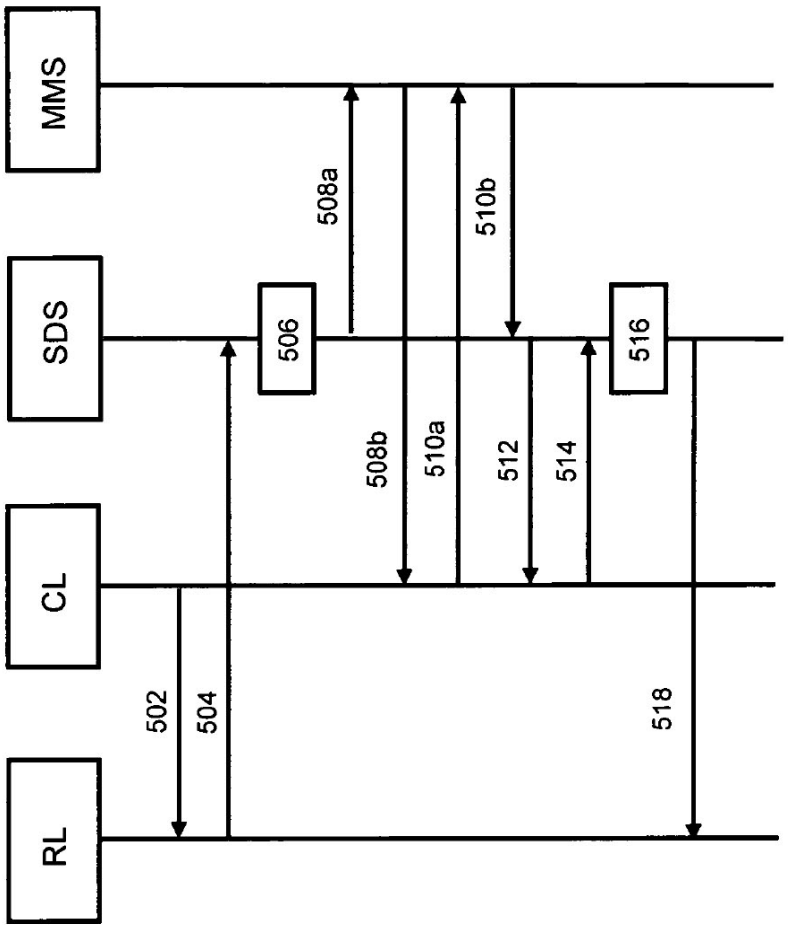
MMS
SDS
CL
RL
502
504
506
508a
508b
510a
510b
512
514
516
518
500

Figura 5

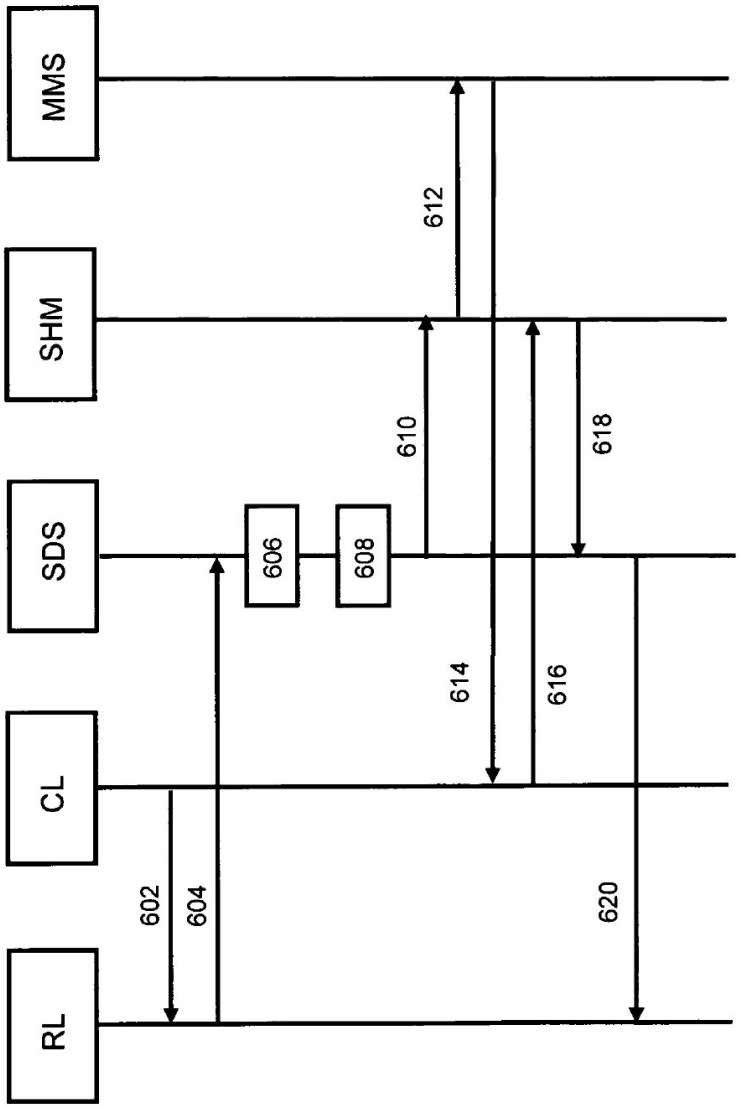

Figura 6