(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 634 024**

(21) Número de solicitud: 201630357

(51) Int. CI.:

H04L 9/08 (2006.01)

(12) PATENTE DE INVENCIÓN B1

(22) Fecha de presentación:

23.03.2016

(43) Fecha de publicación de la solicitud:

26.09.2017

Fecha de concesión:

03.07.2018

(45) Fecha de publicación de la concesión:

10.07.2018

(73) Titular/es:

BERMÚDEZ PÉREZ, Juan José (100.0%)
C/ Emigrant 30 Bajo 2
08906 Hospitalet de Llobregat (Barcelona) ES

(72) Inventor/es:

BERMÚDEZ PÉREZ, Juan José

(54) Título: **MÉTODO SEGURO PARA COMPARTIR DATOS Y CONTROLAR EL ACCESO A LOS MISMOS EN LA NUBE**

(57) Resumen:

La presente invención tiene por objeto un método de almacenamiento de datos en la nube que permite garantizar la privacidad de dichos datos incluso frente a los administradores de los servidores que conforman la nube, sin que ello impida gestionar de forma práctica y cómoda los permisos de acceso a dichos datos. Dicha garantía se obtiene mediante la encriptación de los datos almacenados y el almacenamiento distribuido y particionado (por ejemplo mediante el método de Shamir) de las claves que permiten desencriptar dichos datos. Al ser implementado dicho método, un atacante que quisiese acceder a los datos de forma no autorizada debería obtener acceso no autorizado a al menos dos servidores distintos, ubicados en lugares físicos distintos y administrados por autoridades distintas.

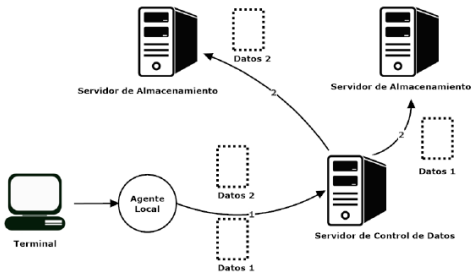

Figura 1a

ES 2 634 024 B1

Descripción

Método seguro para compartir datos y controlar el acceso a los mismos en la nube.

ANTECEDENTES

El almacenamiento de datos en la nube [1] es un servicio ampliamente extendido en la actualidad. Individuos y empresas ven en esta opción una manera de abaratar costes y mejorar la movilidad, ya que no han de preocuparse de establecer una infraestructura informática y pueden acceder a los datos desde cualquier dispositivo en cualquier lugar con una conexión a Internet. Adicionalmente, en especial para usos profesionales y de empresa, resulta útil poder compartir dichos archivos con otros usuarios, por lo que ofrecer un sistema de permisos para gestionar el acceso a ellos resulta de gran utilidad (WO 2015069234 A1).

Más recientemente, a los requisitos de disminución de coste y comodidad se ha añadido el de la seguridad. Noticias sobre espionaje informático a grandes compañías, e incluso desde gobiernos, han sensibilizado el mercado en este sentido. Para satisfacer estas nuevas inquietudes, diferentes servicios ofrecen la posibilidad de encriptar la información almacenada en la nube (US 9027108 B2). Generalmente dicha encriptación se hace por medio de una clave simétrica que solo conoce el usuario que trasmite el fichero a almacenar en la nube. Si el usuario quiere que otro usuario tenga acceso a dicho fichero, ha de transmitirle la clave. A parte de los evidentes inconvenientes prácticos de este sistema, existe el problema de la no revocabilidad de los permisos: una vez se ha enviado una clave, el usuario tiene acceso para siempre al fichero. Igualmente, si el dueño del fichero modificase la clave, debería transmitir la nueva clave a todos los usuarios a los que quisiese mantener el permiso. Otro inconveniente de esta opción de seguridad es que la clave está almacenada en un solo punto, y si alguien tuviese acceso ilegítimo al sistema informático que guarda la o las claves, tendría acceso a todos los ficheros.

El almacenamiento de ficheros en la nube es en realidad un problema idéntico al de muchos otros servicios en Internet que consisten en almacenar datos en la nube, y proporcionar permisos de acceso a dichos datos. Son, por ejemplo, servicios equivalentes: la mensajería instantánea, la publicación de mensajes en redes sociales o los foros de debate. En todos estos casos hay un usuario que sube una información y otorga permisos sobre ella. Recientemente ha aumentado también la inquietud de los usuarios de este tipo de servicios por la seguridad y privacidad.

El requisito de seguridad y privacidad es a menudo especialmente importante para corporaciones y entidades asociativas organizadas.

Definiciones:

1. La nube. La computación en la nube, conocida también como servicios en la nube, informática en la nube, nube de cómputo o nube de conceptos (del inglés cloud computing), es un paradigma que permite ofrecer servicios de computación a través de una red, que usualmente es Internet.

BREVE DESCRIPCIÓN DE LA INVENCIÓN

La presente invención tiene por objeto un sistema de protección y control de acceso de datos almacenados en una infraestructura informática remota independiente (lo que habitualmente se denomina "*la nube*").

El sistema consta de un Terminal, entendiendo en la presente invención bajo el concepto de terminal cualquier dispositivo capaz de mostrar en unos medios de visualización el contenido de una página web o contenido digital, incluyendo en consecuencia ordenadores, móviles, ordenadores de mano, portátiles, relojes inteligentes, gafas inteligentes, televisiones digitales, etc.

(a) Un Agente Local (descargable o preinstalado en el terminal) que incorpora las operativas necesarias para interactuar con los servidores en la nube y administrar localmente los datos. Dicho módulo incluye (de forma no exclusiva) operativas de comunicación, operativas de encriptación y certificación de información y operativas de detección de errores. En caso de que el usuario de la herramienta sea un circuito electrónico o computador, dicho Agente de Control Local puede estar integrado en el mismo circuito, formar parte del software del computador, o formar parte de un dispositivo independiente conectado al circuito o computador.

Habrá (b) un (o más) Servidor de Control de Datos que (entre otras funciones) recopila la información suministrada por los terminales, vigila el cumplimiento de las políticas de control de los datos, almacena particiones de las claves de acceso e implementa políticas de seguridad para minimizar los riesgos de pérdida de datos.

Habrá (c) un (o más) Servidor de Verificación de Acceso que supervisará las políticas de acceso implementadas por el Servidor de Control de Datos y guardará una o más particiones de las clave de acceso a los datos.

Optativamente puede haber (d) una (o más) red independiente de Servidores de Almacenamiento interconectados, ofreciendo un sistema de almacenamiento virtual en la nube.

Las características de la invención hacen que las claves para acceder a cualquier conjunto de datos no estén almacenadas en un único punto o bajo la supervisión de una misma autoridad. La clave para descifrar los datos almacenados se parte mediante un algoritmo de compartición de secretos en varias particiones. Algunas de dichas particiones se almacenan en el Servidor de Control de Datos, otras en el Servidor de Verificación de Acceso, y otras las guarda el usuario que incorpora los datos al sistema. Para recomponer la clave y descifrar los datos serán necesarias un número mínimo determinado de particiones. De esta manera si hay un robo de particiones a alguna de las autoridades, dichas particiones serán inútiles sin tener acceso al número mínimo de particiones necesario para descifrar los datos y que estarán custodiadas por autoridades distintas. Los permisos de acceso a los datos, por lo tanto, serán custodiados de forma criptográficamente segura por varias autoridades (idealmente independientes).

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La figura 1a representa un posible flujo de datos desarrollado durante los pasos iii y iv del procedimiento para guardar datos en la descripción detallada de la presente invención.

La figura 1b representa un posible flujo de datos desarrollado entre los pasos viii y xiii del procedimiento para guardar datos en la descripción detallada de la presente invención.

La figura 1c representa un posible flujo de datos desarrollado entre los pasos ii y vii del procedimiento para descargar datos en la descripción detallada de la presente invención.

La figura 1d representa un posible flujo de datos desarrollado en el paso ix del procedimiento para descargar datos en la descripción detallada de la presente invención.

EXPLICACIÓN DETALLADA DE LA INVENCIÓN

Notación:

TLS. Transport Layer Security (TLS; en español «seguridad de la capa de transporte») y su antecesor Secure Sockets Layer (SSL; en español «capa de conexión segura») son protocolos criptográficos que proporcionan comunicaciones seguras por una red, comúnmente Internet.

Certificado digital. Un certificado digital o certificado electrónico es un fichero informático generado por una entidad de servicios de certificación que asocia unos datos de identidad a una persona física, organismo o empresa confirmando de esta manera su identidad digital en Internet. El certificado digital es válido principalmente para autenticar a un usuario o sitio web en internet por lo que es necesaria la colaboración de un tercero que sea de confianza para cualquiera de las partes que participe en la

comunicación. El nombre asociado a esta entidad de confianza es Autoridad Certificadora pudiendo ser un organismo público o empresa reconocida en Internet.

Token. Cadena de caracteres aleatoria que obtiene un agente de software una vez se ha autentificado con un servidor y que le permite mantener credenciales con dicho servidor sin tener que autentificarse en cada operación. Normalmente el token tiene una validez limitada en el tiempo.

Supuestos previos:

- Cada Agente Local dispone de un par de claves asimétricas (una clave pública y una privada).
- Opcionalmente, cada Servidor de Verificación de Acceso puede disponer de un par de claves asimétricas (una pública y una privada).
- Opcionalmente, el servidor de Control de Datos puede disponer de un par de claves asimétricas.
- Las claves públicas de todo par de claves asimétricas son conocidas por todos los elementos que intervienen en esta invención, mientras que las claves privadas solo son conocidas por sus propietarios (salvo indicado lo contrario)
- Existe un protocolo, no especificado en esta invención, para asignar distintos permisos a distintos grupos de datos. Por ejemplo, el Agente Local podría usar HTTP para comunicar tanto a Servidor de Control de Datos como a los Servidores de Verificación de Acceso los permisos de cada unidad de datos, los permisos de cada usuario, los permisos de distintos grupos de usuarios, y los grupos a que pertenece cada usuario.

Procedimiento para guardar datos en la nube

Los siguientes pasos no necesariamente han de darse en el orden descrito.

(i) El Agente Local genera una clave aleatoria. Dicha clave usualmente corresponderá a la clave para un algoritmo de encriptación simétrico. Habitualmente será una clave para el algoritmo AES o Triple DES, si bien puede ser cualquier clave que se pueda emplear en cualquier algoritmo de encriptación de características similares a estos.

(ii) El Agente Local encripta con la clave anterior los datos que el usuario del Terminal quiere enviar a la nube. Dichos datos pueden ser por ejemplo, sin exclusión:

- Un fichero informático
- Un mensaje dentro de una conversación instantánea
- Una publicación en una red social
- Un mensaje en un foro

Opcionalmente, en lugar de encriptar directamente los datos, el Agente Local puede generar particiones de los datos, por medio de cualquier algoritmo de compartición de secretos (por ejemplo el de Shamir), para que cada partición sea guardada en un servidor distinto. Por ejemplo podría generar una partición destinada a ser almacenada en el (o los) Servidor de Verificación de Acceso. Dichas particiones estarían encriptadas, igualmente, por la clave anteriormente mencionada.

(iii) El Agente Local envía los datos encriptados al Servidor de Control de Datos. Dicha transmisión puede realizarse por cualquier medio, no siendo el método empleado parte de esta invención. Por ejemplo se puede utilizar el protocolo HTTP.

El Servidor de Control de Datos guardará la totalidad o parte de dichos datos en sus propios recursos de almacenamiento o los transferirá a otros Servidores de Almacenamiento para que realicen dicha función.

Opcionalmente, el Servidor de Control de Datos puede enviar parte de dichos datos, o particiones de los mismos, a uno o más servidores de Verificación de Acceso para que los almacenen.

Opcionalmente, el Agente Local puede enviar directamente parte de dichos datos, o particiones de los mismos, a uno o más Servidores de Verificación de Acceso para que los almacenen.

Opcionalmente, el Agente Local puede enviar directamente parte de dichos datos, o particiones de los mismos, a uno o más Servidores de Almacenamiento para ser almacenados.

(iv) El Servidor de Control de Datos confirma la recepción al Agente Local. No constituye parte de esta invención el protocolo empleado para dar dicha confirmación ni el formato de dicha confirmación. Típicamente será la respuesta a un comando GET o POST del protocolo HTTP. Típicamente se usará el protocolo TLS para que el Agente Local tenga certeza de que los datos están siendo dirigidos al Servidor de Control de Datos, el cuál usará un certificado digital de dominio.

(v) El Agente Local genera un número determinado de particiones de la clave por medio de un algoritmo de compartición de secretos (por ejemplo el de Shamir), siendo necesarias un determinado número de dichas particiones (a determinar en cada caso) para recomponer la clave. Un caso típico sería aquél en que se generan tres particiones de la clave y son necesarias dos particiones para recomponer la clave.

(vi) El Agente Local encripta por medio de una clave pública perteneciente al Servidor de Verificación de Acceso un número determinado de particiones de la clave con que se encriptaron los datos (Particiones para el Servidor de Verificación de Acceso). En caso de haber más de un Servidor de Verificación de Acceso se repetirá la operación, pudiendo seleccionar distintas particiones para cada servidor y empleando la clave pública de cada servidor. Típicamente habrá un solo Servidor de Verificación de Acceso, para el cuál se seleccionará una de las tres particiones generadas.

(vii) El Agente Local firma mediante un algoritmo de firma digital un certificado (Certificado A) que identifica o contiene los datos enviados al Servidor de Control de Datos y la encriptación de las Particiones para el Servidor de Verificación de Acceso. Por ejemplo, el certificado podría contener una

huella digital de los datos, el identificador de la operación solicitada (en este caso guardar un fichero), y la encriptación de la partición correspondiente.

En caso de haber más de un Servidor de Verificación de Acceso y haber distintas particiones de la clave para cada uno, se generará y firmará un certificado para cada servidor.

Alternativamente, en lugar de firmar, el Agente Local podría emplear cualquier otro método disponible en el estado de la técnica para identificarse, por ejemplo incluir en el Certificado A un token temporal que habría adquirido previamente del Servidor de Verificación de Acceso y que cumpliría la misma función de garantizar la identidad del usuario. En este caso, el token sería un identificador secreto obtenido por un canal seguro y que durante un tiempo determinado permitiría al Agente Local identificarse por medio de las credenciales que previamente envió mediante dicho canal seguro. No forma parte de esta invención el método concreto a usar para identificarse.

Opcionalmente, el Agente Local podría encriptar con una clave pública del Servidor de Control de Datos las particiones enviadas a dicho servidor pasa ser almacenadas por este. Asimismo, en dicho caso, el Agente Local podría generar otro Certificado A, destinado en este caso al Servidor de Control de Datos, que incluiría dichas particiones firmadas digitalmente.

(viii) El Agente Local envía al servidor de Control de Datos el (o los) Certificado A y un número determinado de particiones de la clave con que se encriptaron los datos (Particiones para el Servidor de Control de Datos). En un caso típico, se utilizará el protocolo HTTP para dicha transmisión, haciendo uso del protocolo TLS para garantizar la privacidad del mensaje y verificar la identidad de las partes. Típicamente se enviará el Certificado A, el identificador de sesión, e información que indique el destino de los datos. Por ejemplo, si es un fichero informático incluirá (entre otras posibles opciones) el directorio de destino y el nombre del fichero.

Opcionalmente, el Agente Local puede generar un Certificado A también para el Servidor de Control de Datos, que incluirá los datos a recibir por este, y que estará encriptado con la clave pública de dicho servidor y firmado digitalmente por el agente. Dicho certificado puede reemplazar, o no, los datos anteriormente citados, enviados mediante cualquier otro método seguro.

Como se ha indicado, el orden de los pasos de esta invención no necesariamente ha de ser el indicado. Por ejemplo, los pasos v,vi,vii y viii se podrían realizar perfectamente antes que los pasos ii,iii y iv o incluso en paralelo a estos.

(ix) El Servidor de Control de Datos verifica que el usuario tiene permisos para realizar la operación y guarda en un registro las Particiones para el Servidor de Control de Datos, asociándolas a los datos en cuestión. Por ejemplo, si es una petición para publicar un mensaje en un foro, verificará que tenga permiso para publicar en dicho foro, o si es una petición para guardar un fichero en un directorio verificará que tenga permiso de escritura en dicho escritorio.

(x) El Servidor de Control de Datos envía al Servidor de Verificación de Acceso el Certificado A que incluye encriptadas las Particiones para el Servidor de Verificación de Acceso. En caso de haber más de un Servidor de Verificación de Acceso, se enviará a cada servidor el certificado correspondiente. No forma parte de esta invención el protocolo de comunicación entre servidores, aunque típicamente será el protocolo HTTP junto a TLS para garantizar un canal seguro.

En alguna posible implementación de esta invención, El Agente Local enviaría directamente el Certificado A al (o los) Servidor de Verificación de Acceso.

(xi) El Servidor de Verificación de Acceso comprueba que la firma del certificado es correcta y que el usuario que firma tiene permisos para realizar la operación. Alternativamente, si por ejemplo el usuario no ha firmado pero envía un token temporal, el servidor comprobará que dicho token fuese asignado a dicho usuario.

Si todo es correcto, desencripta las particiones de la clave y las guarda con un vínculo a los datos del certificado.

(xii) El Servidor de Verificación de Acceso opcionalmente genera un certificado (Certificado B) que contiene información que identifica la petición hecha por el usuario (incluida en Certificado A), encripta dicho certificado con la clave pública del usuario que firma el Certificado A, y firma el Certificado B con su propia clave privada. Por ejemplo, si la petición consiste en almacenar un fichero en un directorio el certificado podría contener el identificador del fichero, el identificador del directorio, el id de usuario, una huella digital de las particiones y la fecha (no siendo imprescindible ninguno de estos elementos). El fin de dicho Certificado B es confirmar al Agente Local que se ha realizado la operación que este solicitó.

Opcionalmente dicho certificado se puede enviar al Agente Local que envió la solicitud o se puede guardar en una base de datos para su posterior consulta.

Opcionalmente se puede enviar al Agente Local que envió la solicitud una confirmación de la misma por cualquier otro medio, sin necesidad de generar un certificado, por ejemplo mediante un canal seguro TLS sobre protocolo HTTP.

(xiii) El Servidor de Verificación de Acceso envía al Servidor de Control de Datos el Certificado B encriptado y firmado u opcionalmente una simple confirmación.

Opcionalmente el Servidor de Verificación de Acceso podría haber enviado en el paso anterior dicha confirmación directamente al Agente Local por cualquier otro medio.

(xiv) El Servidor de Control de Datos envía al Agente Local una confirmación de que la operación se ha procesado y opcionalmente el Certificado B obtenido del Servidor de Verificación de Acceso.

(xv) El Agente Local :

a) comprueba que el Servidor de Control de Datos reporte que la operación se haya realizado correctamente, y opcionalmente

b) comprueba que la firma del Certificado B corresponda al Servidor de Verificación de Acceso, desencripta el certificado con su clave privada, y comprueba que el Certificado B indique que el Servidor de Verificación de Acceso apruebe la operación y la confirme. De esta manera el Agente Local tiene certeza de que el Servidor de Verificación de Acceso ha recibido las particiones de la clave y están efectivamente en dicho servidor. Opcionalmente el Agente Local podría haber obtenido dicha verificación por cualquier otro método, por ejemplo mediante un canal seguro TLS con el Servidor de Verificación de Acceso.

Procedimiento para descargar datos de la nube

(i) El Agente Local, opcionalmente, genera un certificado (Certificado C) con los datos de petición de acceso, encripta el certificado con la clave pública del Servidor de Verificación de Acceso, y lo firma con su clave privada. Si por ejemplo el usuario quiere leer un mensaje del muro de una red social, el certificado incluirá el identificador del mensaje.

Opcionalmente, el Agente Local puede generar también un Certificado C para el Servidor de Control de Datos, encriptado con la clave pública de este.

(ii) El Agente Local envía al Servidor de Control de Datos los datos de petición de acceso contenidos en el Certificado C, así como dicho certificado encriptado y firmado.

Opcionalmente, el Agente Local puede enviar el Certificado C directamente al Servidor de Verificación de Acceso por medio de cualquier canal seguro.

(iii) El Servidor de Control de Datos verifica que la operación cumple con los protocolos de acceso y si es así, envía el Certificado C tal como lo ha recibido del Agente Local al Servidor de Verificación de Acceso. Si por ejemplo el usuario está requiriendo el acceso de lectura a una publicación en el muro de una red social, el Servidor de Control de Datos comprobará que el usuario tenga permiso para ver dicha publicación.

Opcionalmente, el Certificado C podría haber sido enviado al Servidor de Verificación de Acceso por cualquier otro medio.

Opcionalmente, los datos contenidos en el Certificado C podrían haber sido enviados al Servidor de Verificación de Acceso por cualquier otro medio que garantice la seguridad y privacidad de la información. Por ejemplo mediante una conexión HTTP y un canal seguro mediante TLS.

(iv) El Servidor de Verificación de Acceso desencripta el Certificado C (si es el caso de haberlo recibido encriptado) con su clave privada, comprueba la firma y comprueba que el firmante tenga los permisos necesarios para ejecutar la operación especificada en dicho certificado siguiendo un procedimiento similar al del Servidor de Control de Datos.

(v) Si los datos del certificado son correctos y el usuario tiene los permisos necesarios, obtiene las particiones de la clave necesarias para desencriptar los datos, incluye dichas particiones en un nuevo

certificado (Certificado D), lo encripta con la clave pública del Agente Local, y lo firma con su propia clave privada.

Opcionalmente, los datos del Certificado D pueden ser enviados al Agente Local por medio de cualquier otro tipo de canal seguro. Por ejemplo, si el Agente Local conectó mediante HTTP y TLS directamente con el Servidor de Verificación de Acceso, este puede usar el mismo canal para devolver de forma segura y privada los datos del Certificado D.

(vi) El Servidor de Verificación de Acceso, opcionalmente, envía al Servidor de Control de Datos el Certificado D.

(vii) El Servidor de Control de Datos devuelve al Agente Local las particiones que tiene guardadas para acceder a los datos solicitados, así como, opcionalmente, el Certificado D. Si por ejemplo en el momento de partir la clave se hizo en tres particiones, requiriendo dos particiones para recomponer la clave, el Servidor de Control de Datos aportará una clave y el Servidor de Verificación de Acceso envía otra partición encriptada en el certificado D (o mediante otro canal seguro) para que solo el Agente Local pueda leerla. Esas dos particiones podrán ser suficientes para desencriptar los datos, pero en caso de pérdida de datos de un servidor, el Agente Local del usuario que subió los datos a la nube puede haber almacenado una tercera partición por cualquier otro medio, y dicha partición, junto a la de uno de los dos servidores, permitiría recuperar los datos.

(viii) El Agente Local desencripta el certificado D (si es el caso de haberlo recibido encriptado) con su clave privada y comprueba la firma del Servidor de Verificación de Acceso.

(ix) Si tanto el Servidor de Control de Datos como el Servidor de Verificación de Acceso han dado el visto bueno a la operación y le han proporcionado las particiones necesarias para recomponer la clave y desencriptar los datos, el Agente Local descarga los datos solicitados de la dirección indicada por el Servidor de Control de Datos. Dicha descarga puede ser contra el mismo Servidor de Control de Datos, contra cualquier Servidor de Almacenamiento, o contra el Servidor de Verificación de Acceso. No forma parte de esta invención la manera de almacenar internamente los datos en la nube, pudiéndose emplear cualquier método disponible en el estado de la técnica. Se puede por ejemplo usar el servicio de almacenamiento en la nube de una tercera parte (otra empresa) sin conocer qué arquitectura interna utilizan.

Opcionalmente, los datos almacenados pueden haber sido divididos en particiones por medio de cualquier método de compartición de secretos, y por lo tanto el Agente Local deberá recomponer dichos datos una vez descargados.

(x) El Agente Local recompone la clave con que fueron encriptados los datos a partir de las particiones de la clave enviadas por el Servidor de Control de Datos y el (o los) Servidor de Verificación de Acceso. Como se dijo anteriormente, el orden de estos pasos no necesariamente ha de ser el aquí expuesto. Por

ejemplo, la recomposición de la clave se puede hacer en cualquier momento desde que se tiene acceso a las particiones de la clave. Podría recomponerse antes de descargar los datos o en paralelo.

(xi) El Agente Local desencripta los datos con la clave obtenida. Si por ejemplo, los datos corresponden a un mensaje en una conversación instantánea, el Agente Local puede mostrar el mensaje al usuario en pantalla o por cualquier otro medio.

Reivindicaciones

1- Un método para compartir de forma segura datos electrónicos en la nube haciendo uso de al menos un Terminal, un (o más) Agente Local, un Servidor de Control de Datos, un (o más) Terminal de Verificación de Acceso, y uno o más Servidores de Almacenamiento de Datos, componiendo dicho método:

(i) El Agente Local genera una clave aleatoria

(ii) El Agente Local encripta con la clave anterior los datos que el usuario del Terminal quiere enviar a la nube.

(iii) El Agente Local envía los datos encriptados al Servidor de Control de Datos.

(iv) El Servidor de Control de Datos confirma la recepción al Agente Local.

(v) El Agente Local genera un número determinado de particiones de la clave por medio de un algoritmo de compartición de secretos (por ejemplo el de Shamir), siendo necesarias un determinado número de dichas particiones para recomponer la clave.

(vi) El Agente Local encripta por medio de una clave pública perteneciente al Servidor de Verificación de Acceso un número determinado de particiones de la clave con que se encriptaron los datos (Particiones para el Servidor de Verificación). En caso de haber más de un Servidor de Verificación de Acceso se repetirá la operación, pudiendo seleccionar distintas particiones para cada servidor y empleando la clave pública de cada servidor.

(vii) El Agente Local firma mediante un algoritmo de firma digital un certificado (Certificado A) que identifica o contiene los datos enviados al Servidor de Control de Datos y la encriptación de las Particiones para el Servidor de Verificación de Acceso. En caso de haber más de un Servidor de Verificación de Acceso y haber seleccionado distintas particiones para cada uno, se generará un certificado para cada servidor. Alternativamente, en lugar de firmar, el Agente Local podría enviar un token temporal que habría adquirido previamente del Servidor de Verificación de Acceso y que cumpliría la misma función de garantizar la identidad del usuario.

(viii) El Agente Local envía al servidor de Control de Datos el Certificado A y un número determinado de particiones de la clave con que se encriptaron los datos (Particiones para el Servidor de Control de Datos).

(ix) El Servidor de Control de Datos verifica que el usuario tiene permisos para realizar la operación y guarda en un registro las Particiones para el Servidor de Control de Datos, asociándolas a los datos en cuestión.

(x) El Servidor de Control de Datos envía al Servidor de Verificación de Acceso el Certificado A y las Particiones para el Servidor de Verificación de Acceso. En caso de haber más de un Servidor de Verificación de Acceso, se enviará a cada servidor el Certificado correspondiente y las particiones correspondientes.

(xi) El Servidor de Verificación de Acceso comprueba que la firma del certificado es correcta y que el usuario que firma tiene permisos para realizar la operación. Alternativamente, si el usuario no ha firmado pero envía un token temporal, el servidor comprobará que dicho token fuese asignado a dicho usuario. Si todo es correcto, desencripta las particiones y las guarda con un vínculo a los datos del certificado.

(xii) El Servidor de Verificación de Acceso opcionalmente genera un certificado (Certificado B) que contiene información que identifica la petición hecha por el usuario (incluida en Certificado A), encripta dicho certificado con la clave pública del usuario que firma el Certificado A, y firma el Certificado B con su clave privada.

(xiii) El Servidor de Verificación de Acceso envía al Servidor de Control de Datos el Certificado B encriptado y firmado u opcionalmente una simple confirmación.

(xiv) El Servidor de Control de Datos envía al Agente Local una confirmación de que la operación se ha procesado y opcionalmente el Certificado B obtenido del Servidor de Verificación de Acceso.

(xv) El Agente Local :

a) comprueba que el Servidor de Control de Datos reporte que la operación se haya realizado correctamente, y opcionalmente

b) comprueba que la firma del Certificado B corresponda al Servidor de Verificación de Acceso, desencripta el certificado con su clave privada, y comprueba que el Certificado B indique que el Servidor de Verificación de Acceso apruebe la operación y la confirme.

Los pasos anteriores pueden darse no estrictamente en dicho orden siempre y cuando se satisfaga que:

- i precede a ii
- ii precede a iiii
- iii precede a iv
- i precede a v
- v precede a vi
- vi precede a vii
- vii precede a viii
- viii precede a ix
- viii precede a x
- x precede a xi
- x precede a xii
- xi y xii preceden a xiii
- xiii precede a xiv

- xiv precede a xv.

Cuando el mismo u otro Agente Local quiere acceder a los datos:

(i) Genera un certificado (Certificado C) con los datos de petición de acceso, encripta el certificado con la clave pública del Servidor de Verificación de Acceso, y lo firma con su clave privada.

(ii) Envía al Servidor de Control de Datos los datos de petición de acceso contenidos en el certificado C, así como dicho certificado encriptado y firmado.

(iii) El Servidor de Control de Datos verifica que la operación cumple con los protocolos de acceso y si es así, envía el Certificado C tal como lo ha recibido del Agente Local al Servidor de Verificación de Acceso.

(iv) El Servidor de Verificación de Acceso desencripta el Certificado C con su clave privada, comprueba la firma y comprueba que el firmante tenga los permisos necesarios para ejecutar la operación especificada en dicho certificado.

(v) Si los datos del certificado son correctos y el usuario tiene los permisos necesarios obtiene las particiones de la clave necesarias para desencriptar los datos, incluye dichas particiones en un nuevo certificado (Certificado D), lo encripta con la clave pública del Agente Local, y lo firma con su clave privada.

(vi) El Servidor de Verificación de Acceso envía al Servidor de Control de Datos el Certificado D.

(vii) El Servidor de Control de Datos devuelve al Agente Local las particiones que tiene guardadas para acceder a los datos solicitados, así como el Certificado D.

(viii) El Agente Local desencripta el certificado D con su clave privada y comprueba la firma del Servidor de Verificación de Acceso.

(ix) Si tanto el Servidor de Control de Datos como el Servidor de Verificación de Acceso han dado el visto bueno a la operación y le han proporcionado las particiones necesarias para recomponer la clave y desencriptar los datos, el Agente Local descarga los datos solicitados de la dirección indicada por el Servidor de Control de Datos.

(x) El Agente Local recompone la clave con que fueron encriptados los datos a partir de las particiones enviadas por el Servidor de Control de Datos y el (o los) Servidor de Verificación de Acceso.

(xi) El Agente Local desencripta los datos con la clave obtenida.

Los pasos anteriores pueden darse no estrictamente en dicho orden siempre y cuando se satisfaga que:

- i precede a ii
- ii precede a iii
- iii precede a iv

- iv precede a v
- v precede a vi
- vi precede a vii
- vii precede a viii
- viii precede a ix
- viii precede a x
- ix y x preceden a xi

2- Un método para compartir de forma segura datos electrónicos en la nube haciendo uso de al menos un Terminal, un (o más) Agente Local, un Servidor de Control de Datos, un (o más) Terminal de Verificación de Acceso, y uno o más Servidores de Almacenamiento de Datos, componiendo dicho método:

(i) El Agente Local genera una clave aleatoria

(ii) El Agente Local encripta con la clave anterior los datos que el usuario del Terminal quiere enviar a la nube.

(iii) El Agente Local envía los datos encriptados al Servidor de Control de Datos, el cual a su vez puede, o no, enviarlos a uno o más Servidores de Almacenamiento.

(iv) El Servidor de Control de Datos confirma la recepción al Agente Local.

(v) El Agente Local genera un número determinado de particiones de la clave por medio de un algoritmo de compartición de secretos (por ejemplo el de Shamir), siendo necesarias un determinado número de dichas particiones para recomponer la clave.

(vi) El Agente Local envía al Servidor de Verificación de Acceso un número determinado de particiones de la clave con que se encriptaron los datos (Particiones para el Servidor de Verificación de Acceso).

(vii) El Servidor de Verificación de Acceso verifica que el usuario tiene permisos para realizar la operación y guarda en un registro las Particiones para el Servidor de Verificación de Acceso, asociándolas a los datos en cuestión.

(viii) El Servidor de Verificación de Acceso envía al Agente Local una confirmación de que la operación se ha procesado.

(ix) El Agente Local envía al servidor de Control de Datos un número determinado de particiones de la clave con que se encriptaron los datos (Particiones para el Servidor de Control de Datos).

(x) El Servidor de Control de Datos verifica que el usuario tiene permisos para realizar la operación y guarda en un registro las Particiones para el Servidor de Control de Datos, asociándolas a los datos en cuestión.

(xi) El Servidor de Control de Datos envía al Agente Local una confirmación de que la operación se ha procesado.

(xii) El Agente Local :

a) comprueba que el Servidor de Control de Datos reporte que la operación se haya realizado correctamente, y

b) comprueba que el Servidor de Verificación de Acceso reporte que la operación se haya realizado correctamente

Los pasos anteriores pueden darse no estrictamente en dicho orden siempre y cuando se satisfaga que:

- i precede a ii
- ii precede a iii
- iii precede a iv
- i precede a v
- v precede a vi
- vi precede a vii
- vii precede a viii
- v precede a ix
- ix precede a x
- x precede a xi
- xi precede a xii

Cuando el mismo u otro Agente Local quiere acceder a los datos:

(i) Envía al Servidor de Control de Datos los datos de petición de acceso a unos determinados datos almacenados.

(ii) El Servidor de Control de Datos verifica que la operación cumple con los protocolos de acceso y si es así, devuelve al Agente Local las particiones que permiten, una vez mezcladas con las particiones del Servidor de Verificación de Acceso, generar la clave que a su vez permite desencriptar los datos.

(iii) El Agente Local envía al Servidor de Verificación de Acceso los datos de petición de acceso a unos determinados datos almacenados.

(iv) El Servidor de Verificación de Acceso verifica que la operación cumple con los protocolos de acceso y si es así, devuelve al Agente Local las particiones que permiten, una vez mezcladas con las particiones del Control de Datos, generar la clave que a su vez permite desencriptar los datos.

(v) El Agente Local descarga los datos solicitados de la dirección indicada por el Servidor de Control de Datos.

(vi) El Agente Local recompone la clave con que fueron encriptados los datos a partir de las particiones enviadas por el Servidor de Control de Datos y el (o los) Servidor de Verificación de Acceso.

(vii) El Agente Local desencripta los datos con la clave obtenida.

Los pasos anteriores pueden darse no estrictamente en dicho orden siempre y cuando se satisfaga que:

- i precede a ii
- iii precede a iv
- ii y iv preceden a vi
- v y vi preceden a vii

3- Método, según la reivindicación 1, caracterizado porque el Agente Local también genera un certificado encriptado y firmado para el Servidor de Control de Datos.

4- Método, según la reivindicación 1, 2 o 3, caracterizado porque parte de los datos (o la totalidad) los guarda el Servidor de Verificación de Acceso o Servidores de Almacenamiento a los cuales proporciona los datos el Servidor de Verificación de Acceso.

5- Método, según la reivindicación 1, 2 o 3, caracterizado porque los datos son partidos mediante un algoritmo de compartición de secretos y un subconjunto de particiones de dichos datos es almacenado por el Servidor de Control de Datos y un subconjunto de las mismas es almacenado por el o los Servidores de Verificación de Acceso. Los Servidores de Verificación de Acceso pueden almacenar el mismo subconjunto de particiones cada uno de ellos o un subconjunto distinto cada uno.

6- Método, según la reivindicación 1,2,3, 4 o 5 caracterizado porque el (o los) Servidor de Verificación de Acceso es también un Agente Local que en ese momento se encuentre conectado a la red.

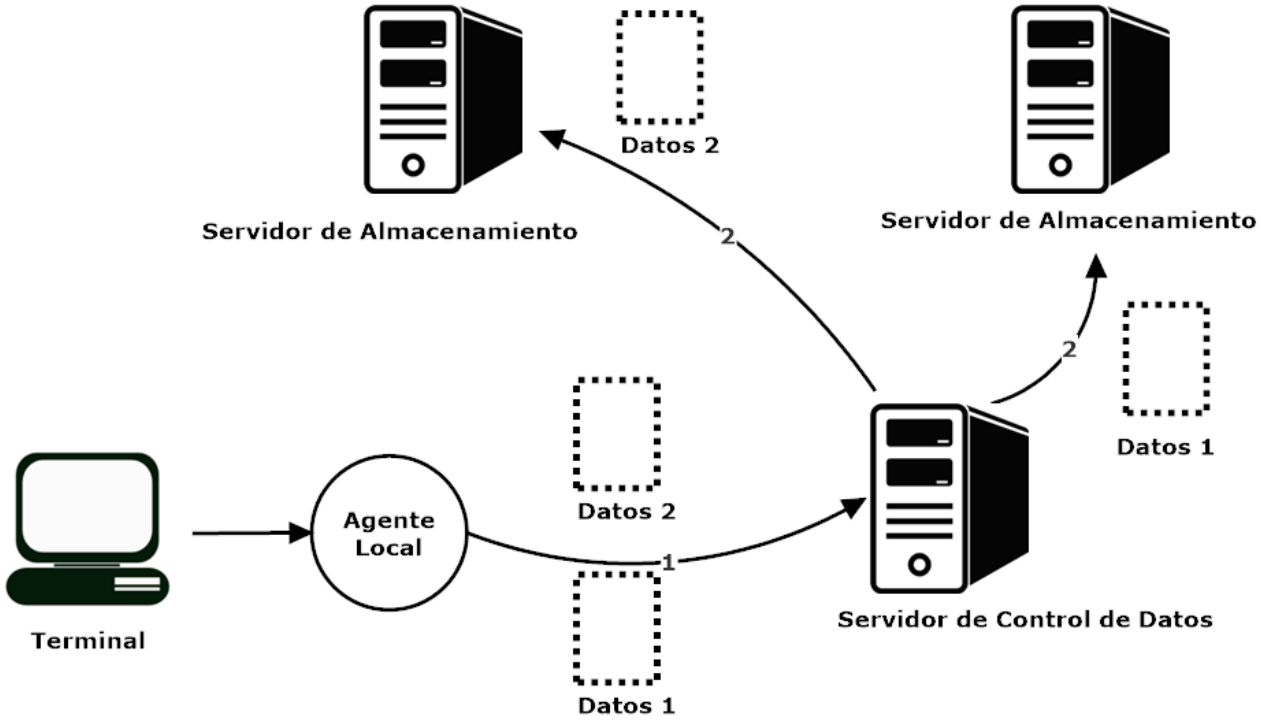
Servidor de Almacenamiento
Datos 2
Servidor de Almacenamiento
2
2
Datos 1
Datos 2
Agente Local
1
Terminal
Servidor de Control de Datos
Datos 1

Figura 1a

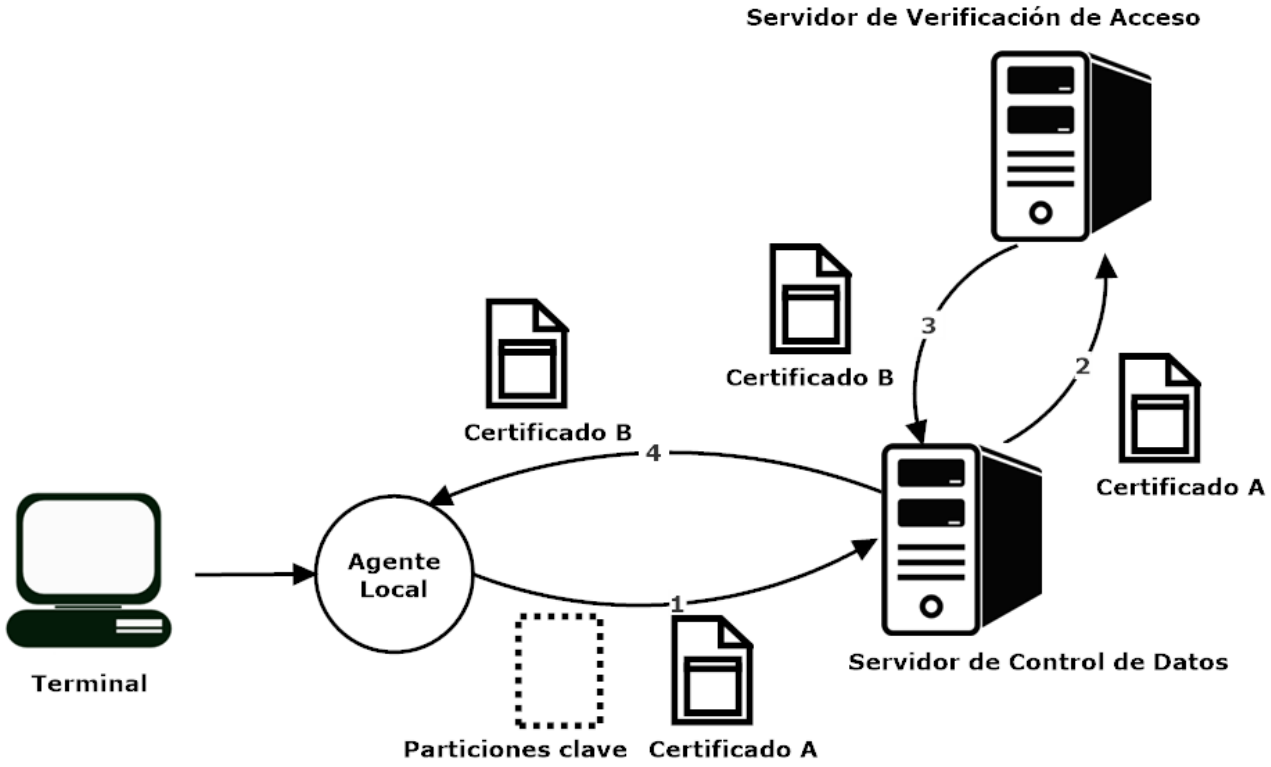
Servidor de Verificación de Acceso
Certificado B
Certificado B
3
2
Certificado A
4
Agente Local
1
Terminal
Servidor de Control de Datos
Particiones clave
Certificado A

Figura 1b

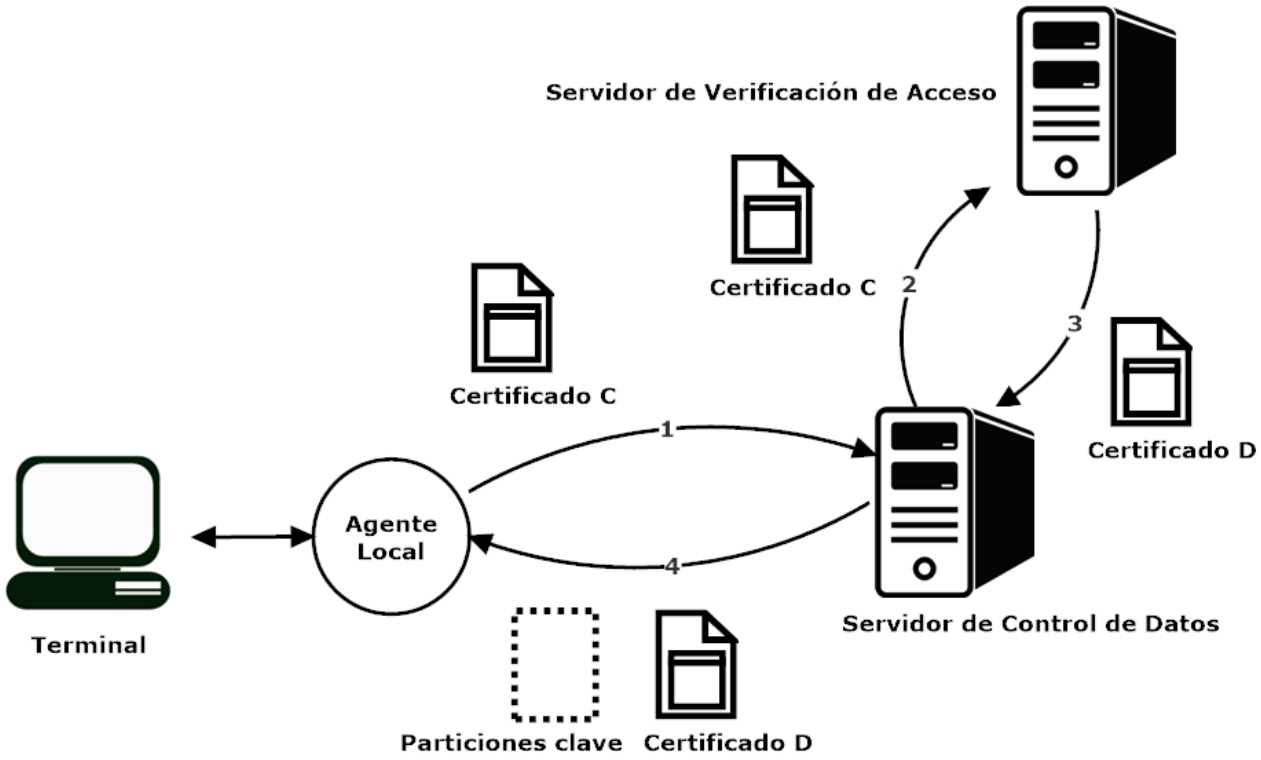

Figura 1c

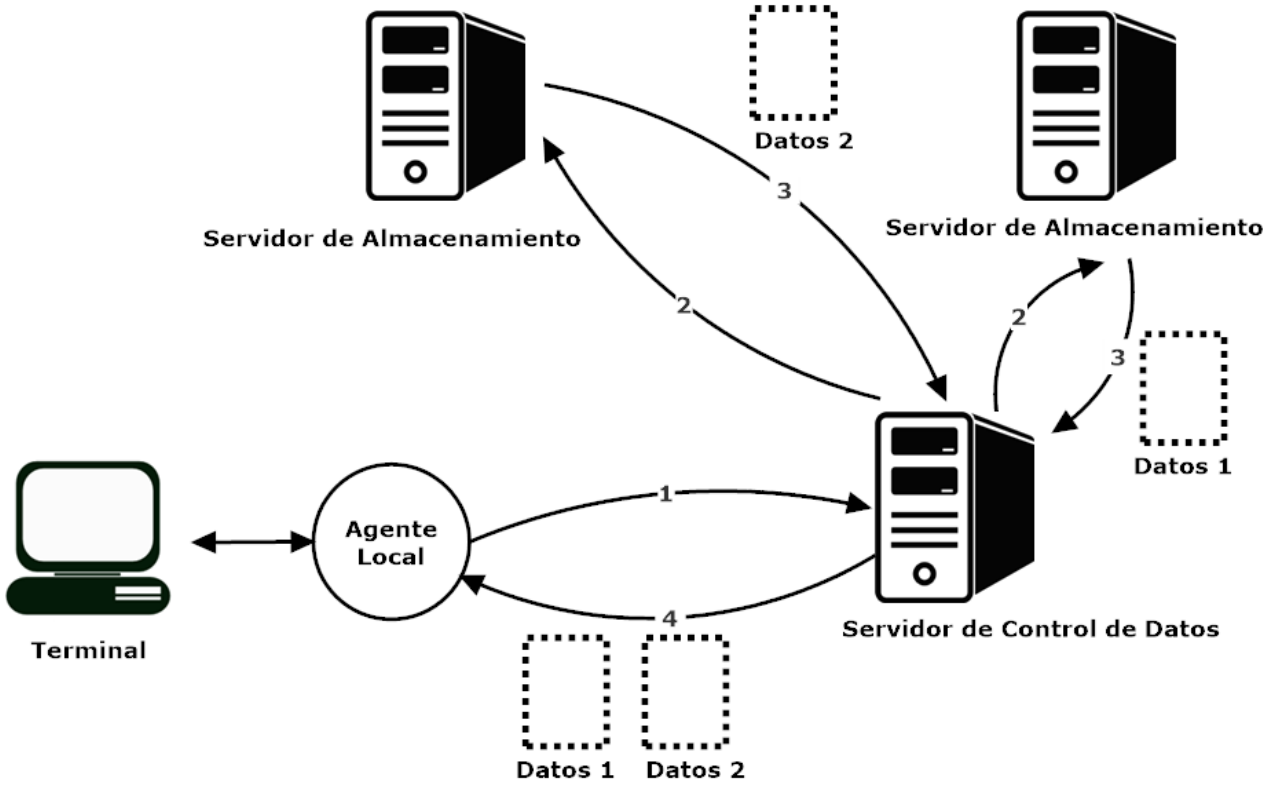

Figura 1d

OFICINA ESPAÑOLA
DE PATENTES Y MARCAS

ESPAÑA

(21) N.º solicitud: 201630357

(22) Fecha de presentación de la solicitud: 23.03.2016

(32) Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TECNICA

(51) **Int. Cl. :** ***H04L9/08*** (2006.01)

DOCUMENTOS RELEVANTES

Categoría	(56) Documentos citados	Reivindicaciones afectadas
Y	US 8520855 B1 (KOHNO TADAYOSHI et al.) 27/08/2013, Resumen.	1-6
Y	WO 2012167094 A1 (SECURITY FIRST CORP et al.) 06/12/2012, Descripción; páginas. 432-530).	1-6

Categoría de los documentos citados

X: de particular relevancia
Y: de particular relevancia combinado con otro/s de la misma categoría
A: refleja el estado de la técnica
O: referido a divulgación no escrita
P: publicado entre la fecha de prioridad y la de presentación de la solicitud
E: documento anterior, pero publicado después de la fecha de presentación de la solicitud

El presente informe ha sido realizado

☒ para todas las reivindicaciones ☐ para las reivindicaciones nº:

Fecha de realización del informe	Examinador	Página
27.07.2017	M. Muñoz Sanchez	1/4

Documentación mínima buscada (sistema de clasificación seguido de los símbolos de clasificación)

H04L

Bases de datos electrónicas consultadas durante la búsqueda (nombre de la base de datos y, si es posible, términos de búsqueda utilizados)

INVENES, EPODOC, WPI

Fecha de Realización de la Opinión Escrita: 27.07.2017

Declaración

Novedad (Art. 6.1 LP 11/1986)	Reivindicaciones	1-6	**SI**
	Reivindicaciones		**NO**
Actividad inventiva (Art. 8.1 LP11/1986)	Reivindicaciones		**SI**
	Reivindicaciones	1-6	**NO**

Se considera que la solicitud cumple con el requisito de aplicación industrial. Este requisito fue evaluado durante la fase de examen formal y técnico de la solicitud (Artículo 31.2 Ley 11/1986).

Base de la Opinión.-

La presente opinión se ha realizado sobre la base de la solicitud de patente tal y como se publica.

Consideraciones:

1. Documentos considerados.-

A continuación se relacionan los documentos pertenecientes al estado de la técnica tomados en consideración para la realización de esta opinión.

Documento	Número Publicación o Identificación	Fecha Publicación
D01	US 8520855 B1 (KOHNO TADAYOSHI et al.)	27.08.2013
D02	WO 2012167094 A1 (SECURITY FIRST CORP et al.)	06.12.2012

2. Declaración motivada según los artículos 29.6 y 29.7 del Reglamento de ejecución de la Ley 11/1986, de 20 de marzo, de Patentes sobre la novedad y la actividad inventiva; citas y explicaciones en apoyo de esta declaración

Se considera D01 el documento más próximo del estado de la técnica al objeto de la solicitud.

Reivindicaciones independientes

Reivindicación 1: el documento D01 divulga un procedimiento de encapsulación de datos utilizando una clave aleatoria para encapsularlos, con dicha clave se encriptan dichos datos. La clave se divide en particiones siendo necesarias un número mínimo de ellas para reconstruir la clave. Las partes de la clave están almacenadas en distintas ubicaciones remotas; desde ellas se recuperan dichas partes de clave, se combinan y finalmente se desencriptan los datos. El documento D01 no incluye la autenticación y control de permisos del usuario para realizar las operaciones de encriptar y desencriptar los datos (Resumen). Tampoco incluye la encriptación de las particiones de la clave.
El uso de esta encriptación adicional de las particiones y el uso de autenticación de usuarios que quieren hacer operaciones con los datos dotaría de mayor seguridad al procedimiento, resultado así el problema técnico objetivo a resolver con respecto al estado de la técnica: aumentar el nivel de seguridad de uso y conservación de datos.
Por su parte en el documento D02 se describe un procedimiento de almacenamiento distribuido seguro en el que se menciona el uso de claves públicas para autenticación y emisión de certificados y la encriptación de particiones de datos (descripción; párs. 432-530).
A la luz de ambos documentos, y por pertenecer ambos a un mismo campo técnico, el experto en la materia se vería orientado a combinarlos para obtener la solución al problema técnico objetivo.
Por tanto, la combinación de los documentos D01 y D02 afecta a la actividad inventiva de la reivindicación 1 según el art. 8.1 de la Ley 11/86 de Patentes.

Reivindicación 2: en cuanto a las variantes introducidas en este procedimiento, con la inclusión de servidores de almacenamiento, cabe repetir el análisis hecho para la reivindicación 1.
Por tanto, la combinación de los documentos D01 y D02 afecta a la actividad inventiva de la reivindicación 2 según el art. 8.1 de la Ley 11/86 de Patentes.

Reivindicaciones dependientes

Reivindicaciones 3-6: el contenido de estas reivindicaciones relativo a las distintas opciones que afectan a las particiones, teniendo en cuenta la redundancia de almacenamiento o la ubicación de dichas particiones, además de autenticaciones adicionales son alternativas sin un efecto técnico adicional con respecto al objeto de las reivindicaciones 1 o 2.
Por tanto, la combinación de los documentos D01 y D02 también afecta a la actividad inventiva de las reivindicaciones 3-6 según el art. 8.1 de la Ley 11/86 de Patentes.